



Seamlessly Integrating eG Manager with Microsoft SCOM

eG Innovations Product Documentation

www.eginnovations.com



Table of Contents

CHAPTER 1: INTRODUCTION	1
CHAPTER 2: HOW DOES THE EG UNIVERSAL MANAGEMENT PACK FOR SCOM WORK?	4
CHAPTER 3: HOW TO DEPLOY THE EG UNIVERSAL MANAGEMENT PACK (MP) FOR SCOM ...	6
3.1 Pre-requisites for Deploying the eG Universal Management Pack for SCOM	6
3.2 Steps for Deploying the eG Universal Management Pack for SCOM	6
3.2.1 Installing the eG SCOM Connector	7
3.2.2 Configuring the eG SCOM Connector	13
3.2.3 Tuning the Monitoring Thresholds of the SCOM Agent on the Connector Machine	21
3.2.4 Installing the eG Console Tasks Application	29
3.3 High Availability Support	31
3.4 Scaling the eG Universal MP for SCOM	33
3.4.1 Configuring Multiple eG SCOM Connectors for a Single eG Manager	33
3.4.2 Integrating Multiple eG Managers with SCOM	34
CHAPTER 4: USING THE EG UNIVERSAL MANAGEMENT PACK (MP) FOR SCOM	36
4.1 Viewing the Active Alerts	37
4.2 Viewing All Alerts	42
4.3 Closing Alerts in the SCOM Console	44
4.4 Viewing Component Health	44
4.5 Viewing Infrastructure Health	46
4.6 Viewing Component Type Health	50
4.7 Working with the Health Explorer	57
4.8 Monitoring Business Services	60
4.9 Publishing Dashboards	78
4.9.1 Pre-requisites for Publishing Custom MyDashboards in the SCOM Console	78
4.9.2 Automated Dashboard Views	79
4.10 Alert Filter	80
4.11 Performance Tuning of the eG SCOM Connector	81
4.12 Updating SCOM with Measure-level Changes Made After Deploying the eG Universal MP	82
CHAPTER 4: UNINSTALLING THE EG SCOM CONNECTOR	83
4.13 Deleting the Connector Service, the eG SCOM Connector Configuration, and the eG Management Pack	83
4.14 Removing the Installation Files of the eG SCOM Connector from the Target Host	85
4.15 Uninstalling the eG SCOM Console Tasks Application	88
CHAPTER 5: FREQUENTLY ASKED QUESTIONS	91
ABOUT EG INNOVATIONS	95

Table of Figures

Figure 1.1: Challenges in using multiple MPs	1
Figure 2.1: How the eG Universal Management Pack for SCOM works	4
Figure 3.1: Checking whether the .NET Framework 3.5 Features is installed	7
Figure 3.2: The Welcome screen	10
Figure 3.3: The License agreement	10
Figure 3.4: Specifying the install directory of the connector	11
Figure 3.5: Clicking 'Install' to begin the installation	12
Figure 3.6: Progress of the installation	12
Figure 3.7: Finishing the installation	13
Figure 3.8: The SCOM Server tab page	14
Figure 3.9: Connection to the SCOM server is successful	15
Figure 3.10: Connect to the SCOM server failed	15
Figure 3.11: Configuring the eG Manager	17
Figure 3.12: The Connector tab page	18
Figure 3.13: The Setup tab	21
Figure 3.14: Clicking on the Authoring tab	22
Figure 3.15: Looking for 'private bytes' in the list of monitors	23
Figure 3.16: Overriding the 'Health Service Private Bytes Threshold' monitor	24
Figure 3.17: Selecting the server that hosts the eG SCOM Connector service	25
Figure 3.18: Modifying the 'Override value' of the 'Agent Performance Monitor Type - Threshold' parameter of the 'Health Service Private Bytes Threshold' monitor	26
Figure 3.19: Choosing the server on which the eG SCOM Connector is running	27
Figure 3.20: Modifying the 'Override value' of the 'Agent Performance Monitor Type - Threshold' parameter of the 'Health Service Handles Count Threshold' monitor	28
Figure 3.21: Welcome screen of the Console Tasks Application wizard	29
Figure 3.22: Click 'Install' to install the eG Console Tasks application	30
Figure 3.23: Completing the installation	30
Figure 3.24: Login credentials for accessing the eG management console	31
Figure 3.25: The eG SCOM Connector can discover and work with an eG Manager Redundant Cluster	31
Figure 3.26: The eG SCOM Connector can be installed on a Windows failover cluster	32
Figure 3.27: A single connector communicating with clustered SCOM management servers	33
Figure 3.28: A single eG manager communicating with multiple eG SCOM connectors	34
Figure 3.29: Integrating multiple managers with SCOM	35
Figure 4.1: The tree-structure displaying a new 'eG Enterprise' node	37
Figure 4.2: Personalizing the Active Alerts view	39
Figure 4.3: Scrolling down the Alert Details section to View additional knowledge	40
Figure 4.4: The description of a measure reported by a test	40
Figure 4.5: Launching the eG monitoring console from the SCOM console	41

Figure 4.6: The eG monitoring console indicating the problem layer, test, and measurement related to the alert chosen from the SCOM console	42
Figure 4.7: The All Alerts view	43
Figure 4.8: The All Components sub-node	45
Figure 4.9: Launching the eG monitoring console from the SCOM console	46
Figure 4.10: The Management Topology of the eG-managed infrastructure	47
Figure 4.11: Drilling down from the high-level topology view to know which VMware vSphere server is in a Critical state	48
Figure 4.12: Isolating the layer and test that reported the Critical issue	49
Figure 4.13: Health Explorer revealing the accurate reason for the Network problem with the VMware vSphere ESX server	50
Figure 4.14: The Components Overview Dashboard	51
Figure 4.15: Expanding the sub-node representing a component type	52
Figure 4.16: Viewing the active alerts of VMware vSphere ESX servers	53
Figure 4.17: Viewing the managed components of type VMware vSphere ESX and their current state	54
Figure 4.18: Viewing the layers as sub-nodes of the 'Layers' node	55
Figure 4.19: The topology representation revealing the exact component of a type, layer of component, and test mapped to the layer that is a Critical state	56
Figure 4.20: Health Explorer revealing the accurate reason for the Network problem with the VMware vSphere ESX server	57
Figure 4.21: Clicking on the Health Explorer option of a test mapped to a particular layer	58
Figure 4.22: Health explorer for the VM Snapshots test mapped to the OutsideView of VMs layer of a VMware vSphere ESX server	59
Figure 4.23: State Change Events tab	60
Figure 4.24: The topology of the Infomart service as viewed in the eG web interface	61
Figure 4.25: Starting Distributed Application Configuration	62
Figure 4.26: Creating a Distributed Application	63
Figure 4.27: The Distributed Application Designer	64
Figure 4.28: A message indicating that new component groups have to be added	65
Figure 4.29: Naming the component group	66
Figure 4.30: Selecting the Network Node Component group	66
Figure 4.31: The newly added Network Node Component group appearing in the Designer window	67
Figure 4.32: Adding the infoway_network component to the NET component group you created	68
Figure 4.33: Creating an IIS Web Component group	69
Figure 4.34: The IIS Web Component group appearing in the Designer window	70
Figure 4.35: Adding the infoway_nfuse2:80 component to the IIS component group	71
Figure 4.36: Creating a relationship between the IIS and NET components	72
Figure 4.37: The fully-configured topology of the Infomart distributed application	73
Figure 4.38: Viewing the state of the Infomart distributed application in the Monitoring mode	74
Figure 4.39: Accessing the topology map of the Infomart application in the Monitoring mode	75

Figure 4.40: The abridged distributed application topology indicating the component in the Critical state	76
Figure 4.41: Drilling down from the ESXi component to know which eG test reported the Critical problem	77
Figure 4.42: End-to-end correlation using SCOM	78
Figure 4.43: Viewing a custom MyDashboard in the SCOM console	80
Figure 4.44: Clicking on the Setup tab page for uninstalling the connector configuration	84
Figure 4.45: The tasks performed by the uninstallation	84
Figure 4.46: Completion of all uninstallation tasks	85
Figure 4.47: The Welcome screen of the uninstallation	86
Figure 4.48: Select the Remove option	86
Figure 4.49: Confirming the connector uninstallation	87
Figure 4.50: End of uninstallation	87
Figure 4.51: Uninstalling the eG SCOM Console Tasks application	89
Figure 4.52: Selecting the Remove option	89
Figure 4.53: Clicking the Remove button	90
Figure 4.54: The completion of the uninstallation of the eG SCOM Console Tasks application	90
Figure 5.1: Clicking on the Setup tab page for uninstalling the connector configuration	92
Figure 5.2: Configuring a new eG user	92
Figure 5.3: Installing the configuration for the new eG user	93

Chapter 1: Introduction

System Center Operations Manager (SCOM), formerly Microsoft Operations Manager (MOM or OpsMgr), is a performance and event monitoring product for Microsoft Windows operating systems. Typically, SCOM agents installed on target Windows systems monitor several sources for specific events or alerts generated by the applications executing on the systems, and forwards the alerts (if any) to a central SCOM server; the SCOM server then triggers some pre-defined action to correct the cause of the alert. Many Microsoft server products, such as Active Directory, Microsoft SQL Server, Microsoft Exchange Server and SCOM itself can be monitored with SCOM. In addition, SCOM also provides limited out-of-the-box support to Unix hosts and network devices.

However, in the present times, when IT infrastructures are characterized by a multitude of components executing on heterogeneous platforms, a tool such as SCOM that is an expert in monitoring Windows-based applications alone might not suffice. Where SCOM is used, administrators are often seen using Management Packs (MP) from third-party monitoring tools to extend SCOM's monitoring functionality to non-Microsoft servers / applications.

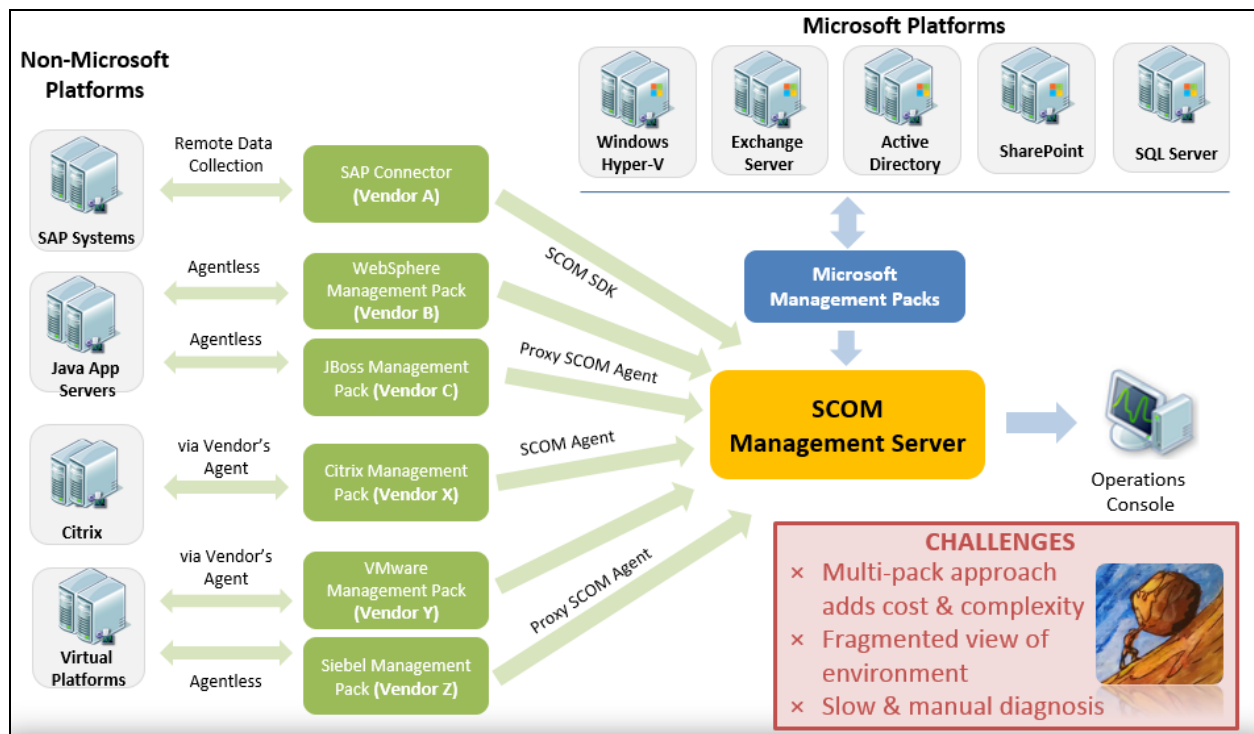


Figure 1.1: Challenges in using multiple MPs

The key challenge in using multiple MPs is that these MPs are primarily from different vendors, and are hence not integrated. Licensing policies binding each MP may be different. Also, no visual or operational consistency may exist between the various MPs used. This adds to the cost and complexity of monitoring. Moreover, the lack of integration makes correlation and root-cause diagnosis near-impossible! This in turn extends diagnosis cycles, resulting in poor user experience and increased IT operations cost.

What is needed therefore is a single, integrated solution that can update administrators on component health and alert them to anomalies across the target environment, regardless of the operating system or type of application/device in use.

eG Enterprise provides a **Universal Management Pack (MP) for SCOM** that can be used to monitor any application in an IT infrastructure – be it packaged enterprise applications and custom applications, Microsoft and non-Microsoft servers / applications, Virtualized and SaaS applications, or server hardware, network devices, or storage systems. Using the eG Universal MP for SCOM, administrators can check the status of eG-managed Windows and non-Windows operating systems, and Microsoft and non-Microsoft applications and network devices directly in the SCOM operation console itself. This MP enables every target monitored in eG Enterprise to be represented in SCOM as a monitoring object, and its operational state updated in SCOM from time to time. Whenever the state of any eG-managed component changes in SCOM, "SCOM alerts" are automatically generated. These alerts are automatically closed when the state of the object becomes healthy. In addition, administrators can quickly launch the eG monitoring console from specific eG-managed objects in SCOM and thus initiate instant diagnosis. Moreover, the eG Universal MP for SCOM also enables the following tasks to be directly performed in the SCOM console for the eG-managed objects:

- Use the features and interfaces built into the SCOM console to instantly determine the health of eG-managed components and easily troubleshoot issues;
- Define custom views in the SCOM console for effectively analyzing the performance data reported by the eG manager;
- Quickly turn on/off specific monitors in the SCOM console;
- Instantly launch the eG monitoring console from the SCOM console to deep dive into performance issues;

The key benefits of eG Universal MP for SCOM are as follows:

- **Single pane-of-glass view of performance of an IT infrastructure, from a single console:**
With the help of a single eG Universal MP for SCOM, you can successfully combine the Windows

monitoring capabilities of the SCOM agents with the multi-platform, multi-application expertise of the eG agents, in a single, central console. This provides you with an end-to-end, single pane of glass view of the performance of an entire IT infrastructure.

- **Shorter learning curve for administrators:** Besides fusing the strengths of two monitoring solutions, this MP also saves administrators the trouble of shuttling between and operating multiple consoles to receive status and problem updates related to the monitored environment.
- **Low monitoring investment:** The eG Universal MP for SCOM enables you to leverage existing investments in SCOM and easily extend monitoring capabilities for any application. Every time a new server / application / device is to be monitored, you no longer need to invest in another MP from a different vendor.
- **Cost-effective and simple:** The eG Universal MP for SCOM eliminates the cost and complexity involved in deployment and management of multiple MPs.
- **Shorter troubleshooting cycles:** The eG Universal MP for SCOM streamlines IT operations and provides auto-correlated, accurate performance results available to SCOM users. This shortens troubleshooting cycles and makes problem diagnosis and resolution faster.

Chapter 2: How Does the eG Universal Management Pack for SCOM Work?

Figure 2.1 depicts how the integration works.

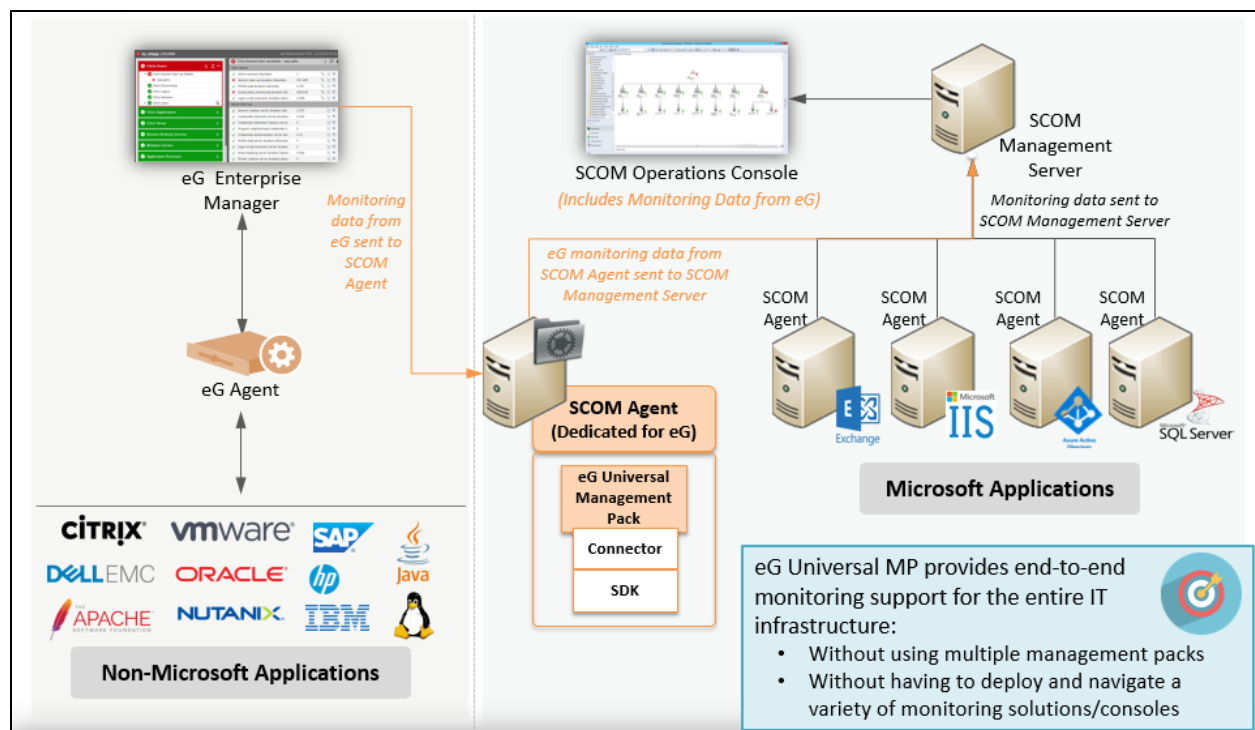


Figure 2.1: How the eG Universal Management Pack for SCOM works

The eG Universal MP for SCOM includes the following components:

- The **eG SCOM Connector**: The eG SCOM Connector is a software component, which needs to be installed and started on a system hosting a SCOM agent. The connector polls the eG manager at pre-configured intervals to retrieve the complete list of components/layers/tests/descriptors managed by the eG Enterprise system, import the required eG management packs, and inserts corresponding monitoring objects in the SCOM server via the SCOM SDK. In addition, from time to time, the connector pulls out the state of the managed components/layers/test/descriptors/measures from the eG manager, and publishes the state information to an eventlog called eG Enterprise on the local machine.
- The **SCOM Agent**: The SCOM agent, which runs on the same system as the connector, uses its **Health Service** to manage the state of all the eG monitoring objects in the SCOM server. The SCOM agent executes the unit monitors created in the eG management pack for every

measurement reported by the eG Enterprise system. Upon execution, the unit monitors listen for any new eventlog entries in the eG Enterprise log. If a new entry is created in the eventlog, the unit monitors execute and update the SCOM server with the state information. The SCOM server then processes the state information so received, and accordingly changes the state of the monitoring objects.

Every time the state of a monitoring object changes, the SCOM server automatically generates alerts. Likewise, once the object is restored to normalcy, the SCOM server automatically closes the alert.

This document provides the detailed procedure for enabling the eG Manager-SCOM integration, and uses an example to discuss how this integration works.

Chapter 3: How to Deploy the eG Universal Management Pack (MP) for SCOM

This chapter discusses the pre-requisites and the procedure for integrating the eG manager with SCOM, using the eG Universal MP for SCOM.

3.1 Pre-requisites for Deploying the eG Universal Management Pack for SCOM

The eG manager-SCOM integration can be implemented only if the following broad pre-requisites are fulfilled:

- eG Manager v6 (or above) should be available
- The 'External Super Manager' capability should be enabled in the eG manager license
- Set the **quick_launch** flag available under the **[QUICK_LAUNCH]** section of the **eg_services.ini** file in the **<eG_INSTALL_DIR>/manager/config** folder to **true**. By default, this flag is set to **false**.
- Microsoft System Center Operations Manager 2012 / 2012 SP1 / 2012 R2 / 2016 / 2019 should be available

3.2 Steps for Deploying the eG Universal Management Pack for SCOM

The broad steps to be followed are:

- Installing the eG SCOM Connector
- Configuring the eG SCOM Connector
- Installing the eG Console Tasks Application
- Tuning the Monitoring Thresholds of the SCOM Agent on the Connector Machine

The sections that follow will discuss the procedure involved in accomplishing the tasks enumerated above.

3.2.1 Installing the eG SCOM Connector

3.2.1.1 Pre-requisites for Installing the eG SCOM Connector

The first step towards integrating the eG manager with SCOM is to install the eG SCOM Connector. Before installing this software, ensure that the following requirements are met:

Software Requirements

Operating Systems

- Windows 2008 R2 / 2012 / 2016 / 2019
- Windows 7 / 8 / 10
- All operating systems must be installed with latest service pack
- Server operating system is recommended for production deployments

Other Software Requirements

- SCOM Agent 2012 / 2012 SP1 / 2012 R2 / 2016 / 2019
- For SCOM 2012 / SP1 / R2, Microsoft .NET version 4.0 and above is required. Also, make sure that .NET Framework 3.5 Features (indicated by Figure 3.1 below) is installed on the host on which the eG SCOM Connector is to be installed.

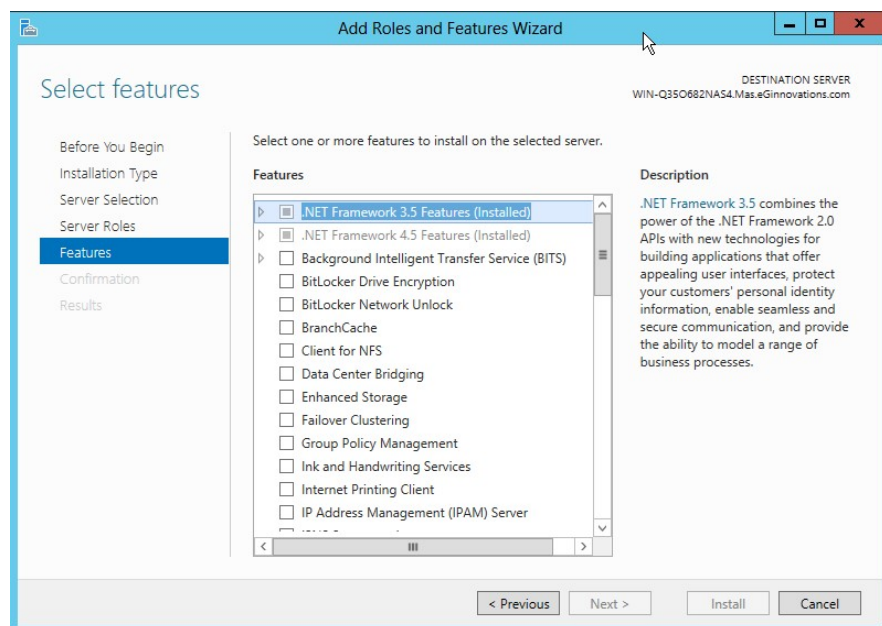


Figure 3.1: Checking whether the .NET Framework 3.5 Features is installed

-
- For SCOM 2016 and above, Microsoft .NET version 4.5.2 (or above) is required.
-

Hardware Requirements:

CPU	2GHz or faster x86 or x64 processor. This can support integration of up to 100 monitored components in eG manager. Thereafter, for every additional 100 components to be integrated, add 1 additional processor with 2GHz processing speed.
Memory	Minimum 2 GB (recommended: 4 GB); this can support integration of up to 100 monitored components in eG manager. Thereafter, for every additional 100 components to be integrated, add another 2 GB.
Disk Space	Minimum 2 GB (recommended: 4 GB)

Other Requirements:

- The connector software should be installed on a system that is installed with a SCOM agent and is managed by a SCOM server;

Note:

Do not uninstall or upgrade the SCOM agent after deploying the connector software.

- The Windows Installer Service should pre-exist on the system chosen for installing the eG connector;
- The system hosting the connector should be able to communicate with the eG manager and the SCOM SDK service via TCP ports; the specific ports that need to be opened and the direction of communication has been provided below:

Source	Destination	Access Required
eG SCOM Connector	eG Manager Server	TCP 7077
eG SCOM Connector	SCOM Management Server / SDK Service	TCP 5723

- It is recommended that the connector software be deployed on a dedicated system; this is because, the connector machine hosts the SCOM agent as well, and the load on the SCOM agent is normally high. You also have the option of installing the eG SCOM connector on a VM. While

running on a VM, make sure that the VM is allocated with 2 or more virtual processors. For large environments where hundreds of eG components need to be integrated with SCOM, you can also uniformly distribute the load amongst multiple SCOM agents and eG SCOM connectors.

- To enable the connector to communicate with the eG manager, configure the connector with the credentials of a user who is registered with the eG Enterprise system. **We recommend that a user who is assigned the Monitor role be used for this purpose.**
- To enable the connector to communicate with the SCOM server, configure the connector with the credentials of a user who has the right to access the SDK service.

3.2.1.2 How to Install the eG SCOM Connector?

The eG SCOM Connector installable is provided as an MSI package named, **eG SCOM Connector.exe**. To install the connector using this package, do the following:

1. From the URL that is provided to you, download the **eG SCOM Connector.exe** that corresponds to the SCOM version that is in use in your environment (i.e., SCOM 2012/2016/2019) and the processor configuration (i.e., 32-bit or 64-bit).
2. Once the executable is downloaded to a directory on the local host, run the executable by double-clicking on it.
3. If the target server does not meet the software pre-requisites described in Section 2.1 above, the installer will not proceed.
4. If all the documented pre-requisites are fulfilled, then Figure 3.2 will appear.



Figure 3.2: The Welcome screen

5. Click the **Next** button in Figure 3.2 to proceed with the installation. Figure 3.3 will then appear.



Figure 3.3: The License agreement

6. Accept the license agreement and click the **Next** button in Figure 3.3.
7. When Figure 3.4 appears, the directory in which the eG SCOM Connector will be installed by default, will be displayed. **This default directory cannot be changed.** Click the **Next** button to

proceed.

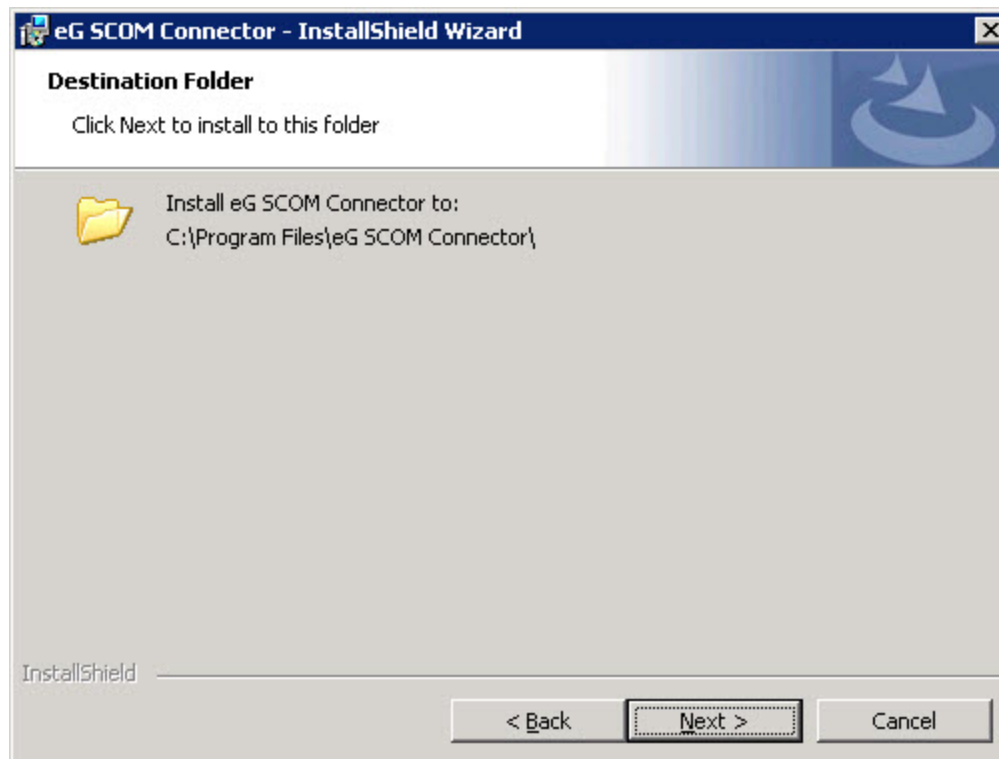


Figure 3.4: Specifying the install directory of the connector

8. When Figure 3.5 appears, click **Install** to begin the installation.

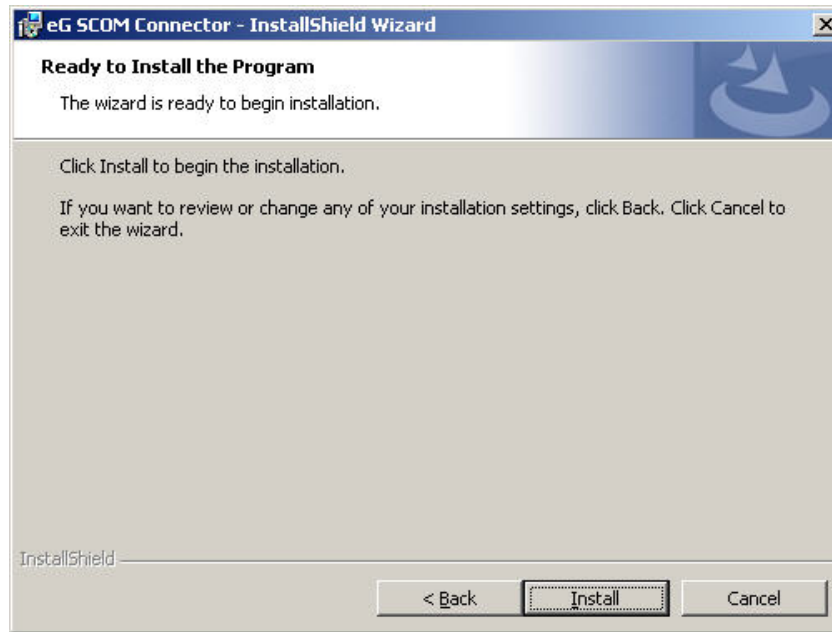


Figure 3.5: Clicking 'Install' to begin the installation

9. Figure 3.6 will indicate the progress of the installation to you.

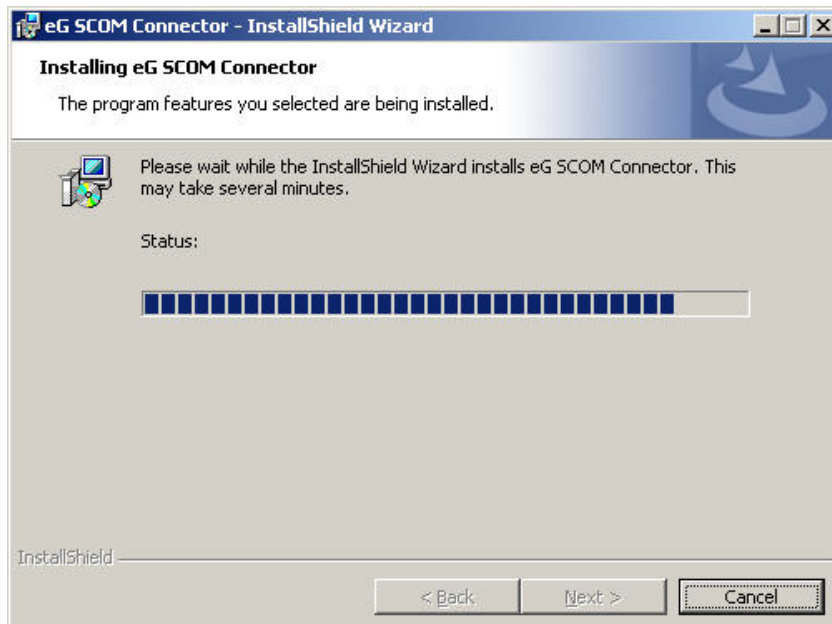


Figure 3.6: Progress of the installation

10. When installation ends, Figure 3.7 will appear. Click **Finish** to exit the wizard.

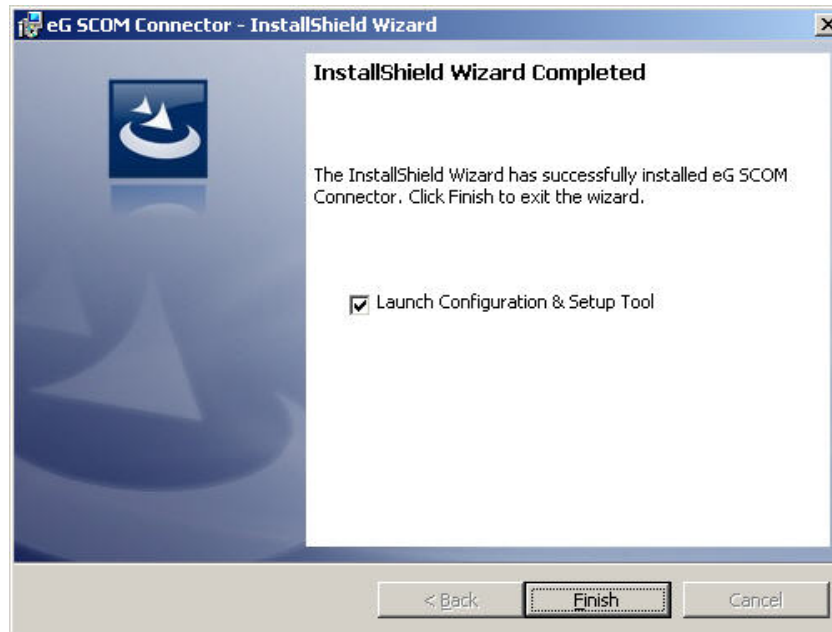


Figure 3.7: Finishing the installation

3.2.2 Configuring the eG SCOM Connector

If the **Launch Configuration & Setup Tool** check box is selected in Figure 3.7, then finishing the installation will automatically launch the eG SCOM Connector configuration tool. If this check box is deselected, then, you will have to manually launch the configuration tool by following the menu sequence: *Start -> Programs -> eG SCOM Connector*. Either way, once the tool is launched, proceed to configure the connector using the steps discussed below:

1. Upon launching the tool, Figure 3.8 will appear with the **SCOM Server** tab page open.

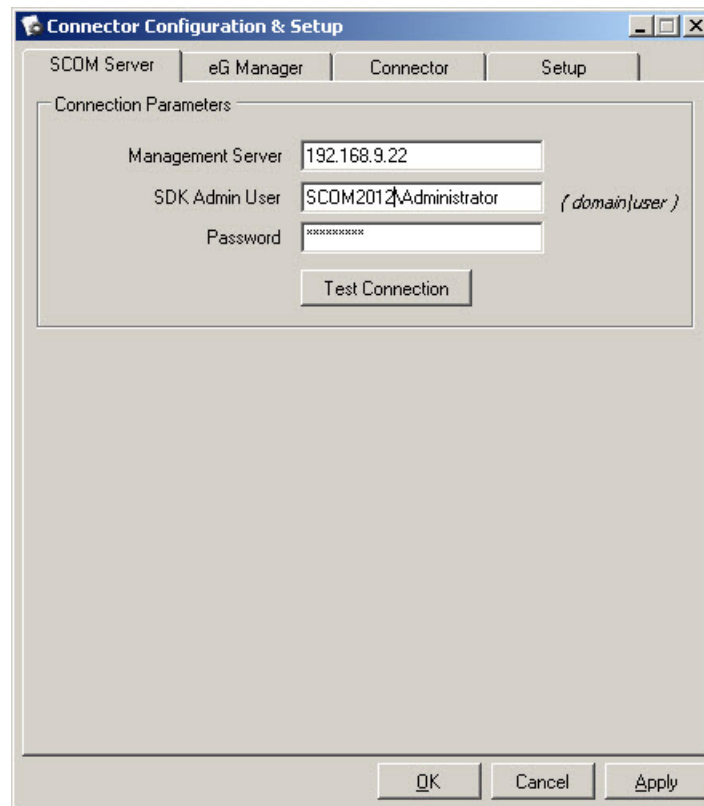


Figure 3.8: The SCOM Server tab page

2. If the eG manager is integrating with SCOM 2012/2016/2019, you can specify the IP address/host name of any management server in the environment in the **Management Server** text box of Figure 3.8.
3. The eG SCOM Connector needs to connect to the SCOM SDK Service (on the SCOM server) to update the SCOM server with monitoring objects that have been newly added/removed from the eG Enterprise system, and to import and author eG management packs. To enable this connection, you need to configure the connector with the credentials of a user who is authorized to connect to the SDK service and perform administration functions. Specify the credentials of such a user in the **SDK Admin User** and **Password** text boxes. **Note that the SDK Admin User has to be specified in the following format: <domainname>\<username>**
4. Then, to check whether your specifications are correct, click the **Test Connection** button. If the eG SCOM Connector is able to connect to the SCOM server with the given specifications, then a message to that effect will appear.

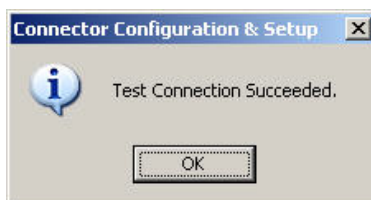


Figure 3.9: Connection to the SCOM server is successful

5. On the other hand, if the connector is not able to connect to the SCOM server, then a message indicating the connection failure and reasons for the same will appear.

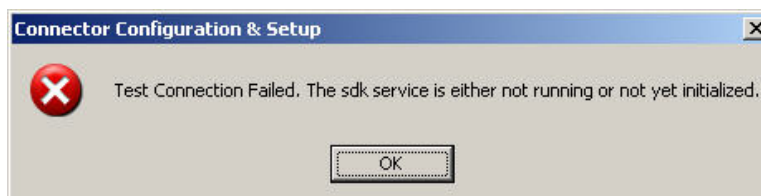


Figure 3.10: Connect to the SCOM server failed

6. In case of a failure, first click the **OK** button in Figure 3.10 to close the message box. Then, take another look at your specifications, make changes wherever necessary, test the connectivity yet again, and if successful, proceed with your configuration. To proceed, click the **eG Manager** tab page in Figure 3.11. Typically, the eG connector polls the eG manager for discovering the managed components/layers/tests/descriptors/measures from the eG Enterprise system and inserting corresponding monitoring objects and unit monitors in the SCOM server. Using the **eG Manager** tab page of Figure 3.11, you can indicate which eG manager is integrating with the SCOM server and how to connect to it. As part of this exercise, specify the following:

- In the **Manager Unique ID** text box, provide a unique ID for the eG manager with which the SCOM server will be integrating.

Note:

- Before providing the manager ID, make sure that you have not used the same ID for any other eG SCOM Connector that may be communicating with the target SCOM server.
- Ensure that the **Manager Unique ID** you provide does not contain any special character, other than the underscore (_).
- In the **Manager URL** text box, specify the URL using which the connector should connect to the eG manager. The URL should be of one of the following formats, depending upon whether the eG manager is SSL-enabled or not: *http://<eGManagerIP>:<Portno>* or *https://<eGManagerIP>:<Portno>*.

Note:

The integration will work in a redundant eG manager setup as well. In other words, if the primary manager fails, then the SCOM connector is capable of automatically polling the secondary manager in the environment for state information.

- Next, in **User** and **Password** text boxes specify the credentials of a user who is registered with the eG Enterprise system, and who has the right to monitor one/more components in the target environment. The components assigned to this user will only be managed by the SCOM server.
- Currently, the eG SCOM Connector does not support Active Directory group users registered with the eG Enterprise system.
- If VMs are mapped to a user registered with the eG SCOM Connector, such VMs will not be visible in the SCOM console after the integration.
- For an Enterprise deployment of eG Enterprise, ensure that the eG user account configured in the SCOM connector does not contain special characters other than Underscore (_) and Dot (.). For a SaaS deployment of eG Enterprise, ensure that the eG user account configured in the SCOM connector does not contain special characters other than At (@), Underscore (_) and Dot (.).
- If you have built custom help pages in eG Enterprise for IC-based tests and for new aggregate tests, then the **Knowledge Base** feature of SCOM will not support these help pages.
- If an IC/aggregate test, measure, layer or component type in eG consists of double-byte characters (i.e., Chinese, Korean, or Japanese characters), then such tests, measures, layers, and component types will not be displayed in the SCOM console.
- Finally, test whether the given specifications are correct by clicking the **Test Connection** button.

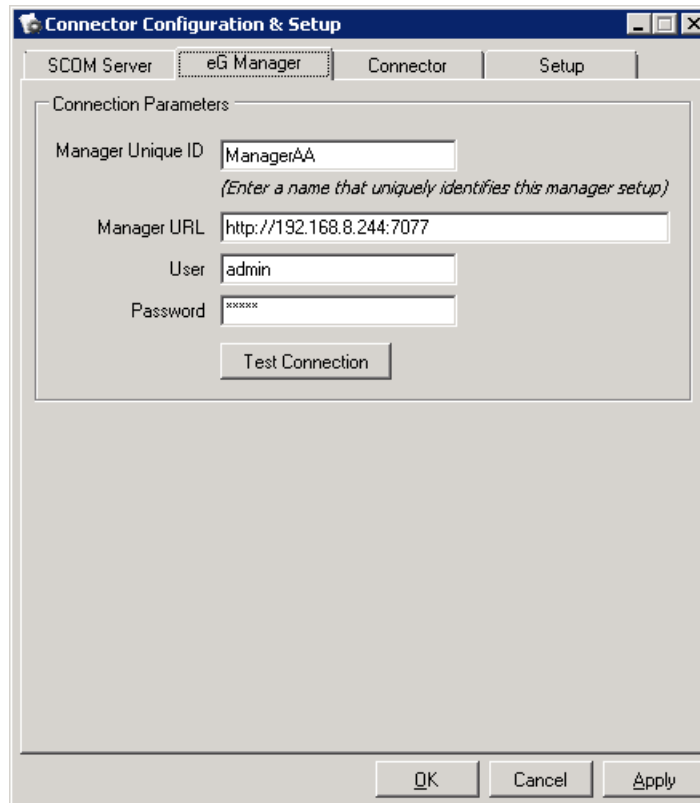


Figure 3.11: Configuring the eG Manager

7. Then, click on the **Apply** button in Figure 3.11 to apply the changes.
8. Click on the **Connector Service** tab page. If the connector service is yet to be installed, then the **Start** and **Stop** buttons in Figure 3.12 will be disabled. Also, the **Connector Service Status** will be *Not installed* (as shown by Figure 3.12). If the connector has been installed but is yet to be started, then the **Start** button alone will be enabled. You can click on the **Start** button to start the service and the **Stop** button to stop the service.

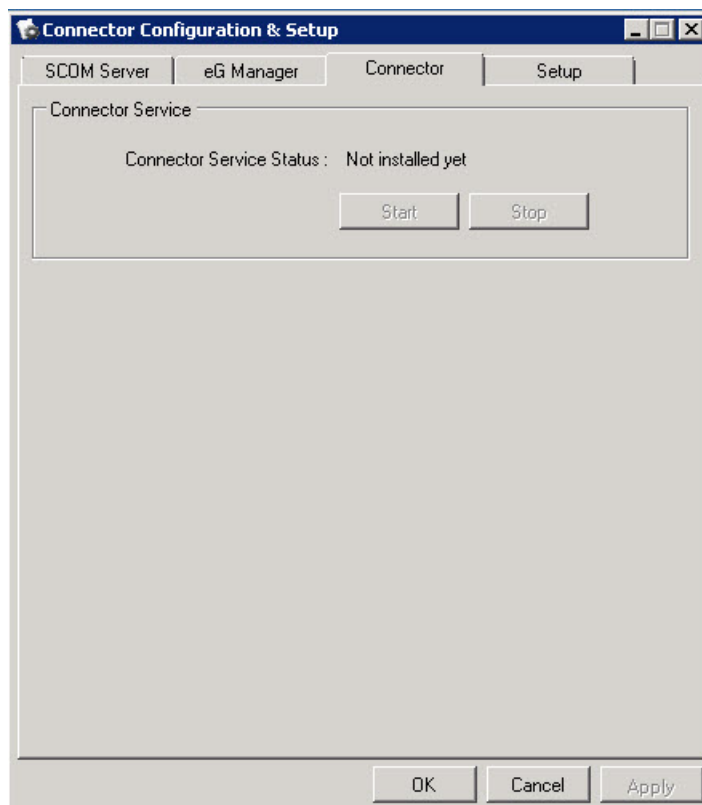


Figure 3.12: The Connector tab page

9. Now, click on the **Setup** tab in Figure 3.12 to execute the setup tasks. The **Setup** tab provides 2 options. Automatic setup will execute all the required tasks in a single action. To perform this auto setup, click on the **Install** button in the **Automatic** section of Figure 3.13. You can uninstall the connector at any point in time, by simply clicking the **Uninstall** button in the **Automatic** section.

On the other hand, if you wish to execute specific setup tasks, click on the **Custom** option and proceed as follows:

- **Connector Windows Service:** Click the **Install** button here to install the Windows service for the eG SCOM Connector, and use the **Uninstall** button to uninstall the service.
- **Connector Configuration:** The **Create** button here, when clicked, will create a new connector configuration for eG integration in the SCOM server. The **Delete** option can be used to remove the connector configuration from the server. When the delete operation is performed, all the monitoring objects discovered by the eG connector will also be deleted from the SCOM server. You can also use the **Create/Delete** options to cleanup and recreate monitoring objects in SCOM server.

- **Management Pack:** Using the **Import** option here, you can import the eG management pack which is stored in the connector's installation directory into the SCOM server. The management pack includes abstract classes, relationships, monitor types, default views etc. Once the management pack is imported into the SCOM sever, the connector service will start to update it as and when new component types are discovered. The **Delete** option can be used to remove the eG management pack from the SCOM server.
- **SCOM Agent:** In large environments where hundreds of components are managed by the eG Enterprise manager, the load on the connector would increase as it attempts to discover all the components from the eG manager. This in turn may increase the load on the SCOM agent on the connector system as well, as this agent would now be handling the hundreds of discovered components and their corresponding state changes. Under conditions of such high load, the default performance settings for the SCOM agent may not be conducive to healthy agent-connector traction. By clicking the **Optimize** button here, you can change the values of default parameters to the values shown in the table below:

Registry Parameter	Location in Registry	Value
Persistence Version Store Maximum	HKLM\System\CurrentControlSet\Services\HealthService\Parameters\	65536 decimal
Persistence Cache Maximum	HKLM\SYSTEM\CurrentControlSet\Services\HealthService\Parameters\	1048576 decimal
State Queue Items	HKLM\SYSTEM\CurrentControlSet\Services\HealthService\Parameters	250000 decimal
MaximumQueue SizeKb	HKLM\SYSTEM\CurrentControlSet\Services\HealthService\Parameters\ ManagementGroups\<Management_Group_Name>	262144 decimal
Persistence Checkpoint Depth Maximum	HKLM\SYSTEM\CurrentControlSet\Services\HealthService\Parameters	52428800 decimal

These default settings are ideal for small/medium-sized environments, where only a few components are monitored - say, less than 50 components. Where the connector needs to handle a large number of components, the value of these registry entries have to be tuned further. This is because, with an increase in monitored targets, the load on the SCOM agent also increases. The agent will hence require more memory for its processing to be faster and also to avoid the following error in “Operations Manager” event log on the connector machine.

```
Event ID: 4506
Event Source: HealthService
Event Description: Operations Manager

Data was dropped due to too much outstanding data in rule <rule name> running for
instance <instance name> with id:<instance id> in management group <management group
name>.
```

To allow the SCOM agent to utilize more memory available in the system, you can use **regedit** to manually set a higher value for the **Persistence Cache Maximum** registry entries in *HKLM\System\CurrentControlSet\Services\HealthService\Parameters*.

First, double the current value of this parameter and check if performance improves. Also, confirm that no errors are captured by the event log post this change. If no performance improvements are visible, double the value of this parameter again. Repeat this procedure until the value of this parameter is set as high as “2048000”.

With the above setting, the typical memory usage of SCOM agent processes would be around 3GB.

Also, with this value increased, the startup and stopping of the “Health Service” will take longer than normal.

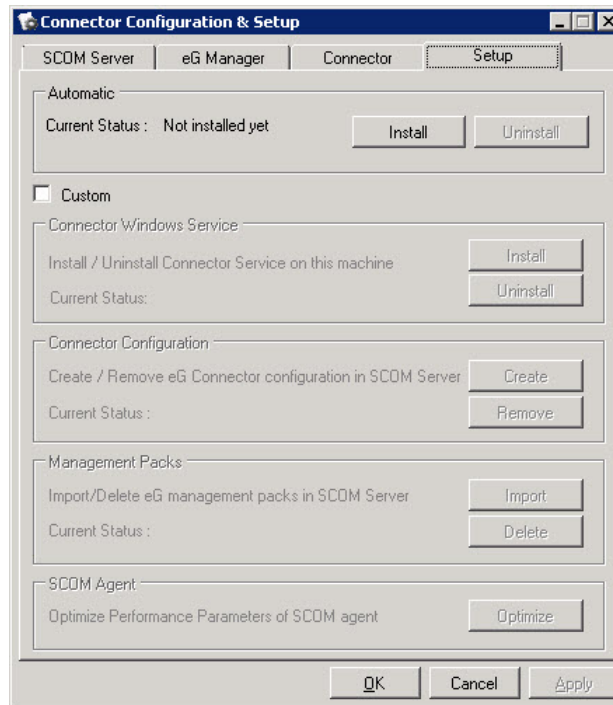


Figure 3.13: The Setup tab

Note:

The **Optimize** button will be disabled if the registry entries mentioned in the table above have already been set to the values prescribed above.

10. Finally, click the **OK** button to exit the connector configuration window.

3.2.3 Tuning the Monitoring Thresholds of the SCOM Agent on the Connector Machine

If the SCOM agent on the connector machine is not configured with adequate memory and handles, then, in the event of excessive activity, the SCOM server may experience delays while receiving status or problem updates related to the monitoring objects from the agent. To avoid such delays, you have to tune the monitoring thresholds of the SCOM agent on the connector machine. This can be achieved by following the steps below:

1. Login to the SCOM console and click the **Authoring** tab indicated by Figure 3.14 below:

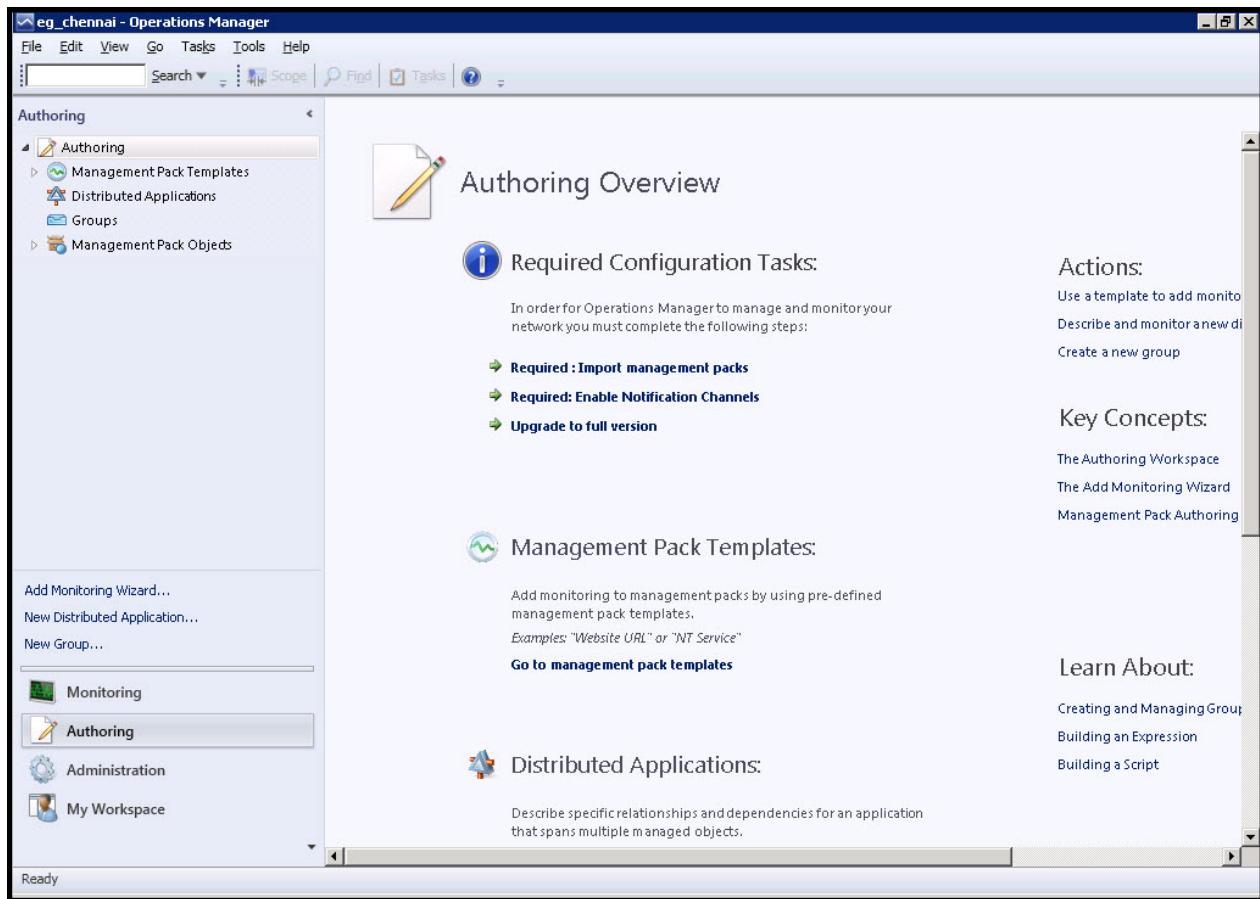


Figure 3.14: Clicking on the Authoring tab

2. When Figure 3.15 appears, expand the **Management Pack Objects** node in the tree-structure in the left panel of Figure 3.15, and select the **Monitors** sub-node within. The right panel will then change to display a variety of monitors. Next, using the **Look for** text box just above the list of monitors in Figure 3.15, type **private bytes**, and click **Find Now**.

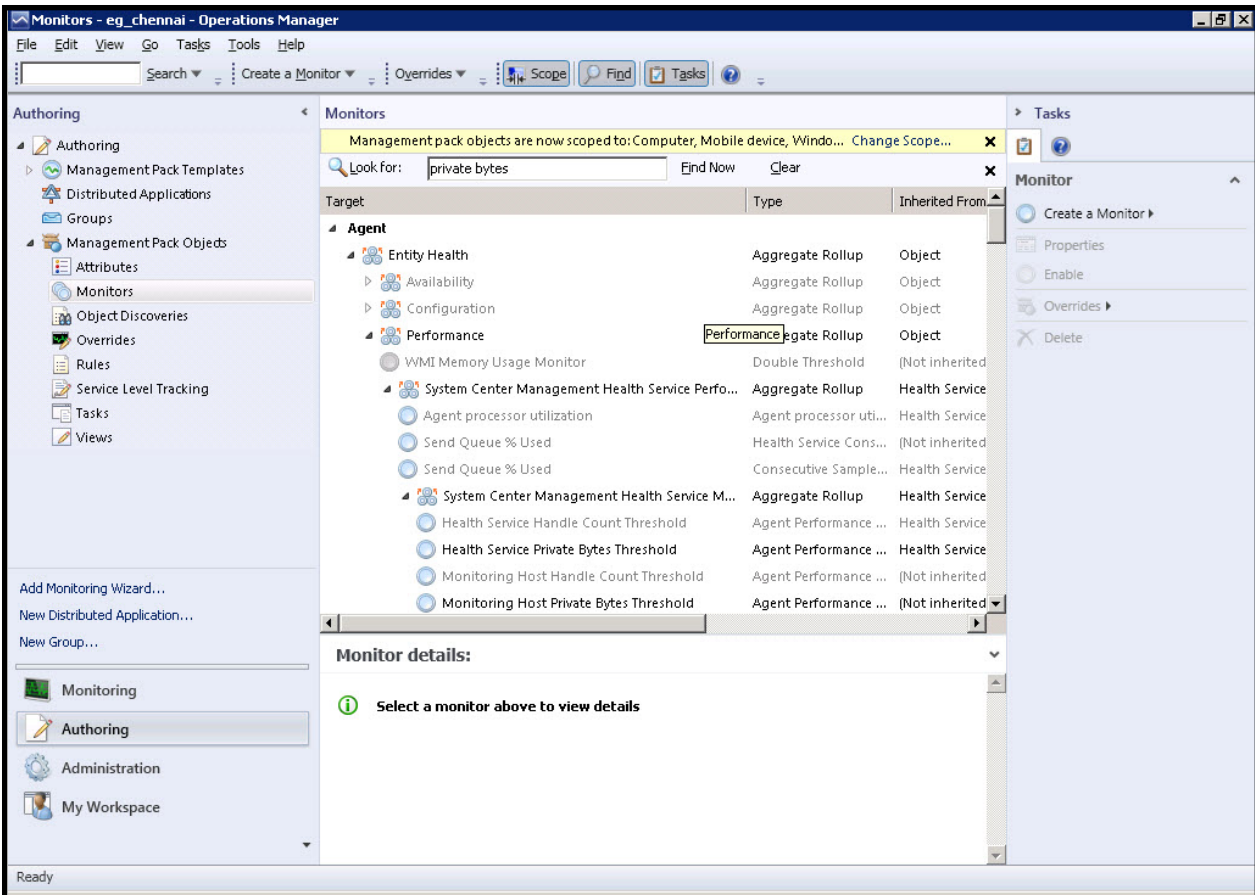


Figure 3.15: Looking for 'private bytes' in the list of monitors

- First, scroll down the list of monitors to look for the target, **Health Service**. Under the **Performance** category of that target, look for the monitor named, **Health Service Private Bytes Threshold**. Then, right-click on that monitor and follow the menu sequence, *Overrides -> Override the Monitor -> For a specific object of class: Health Service* (see Figure 3.16).

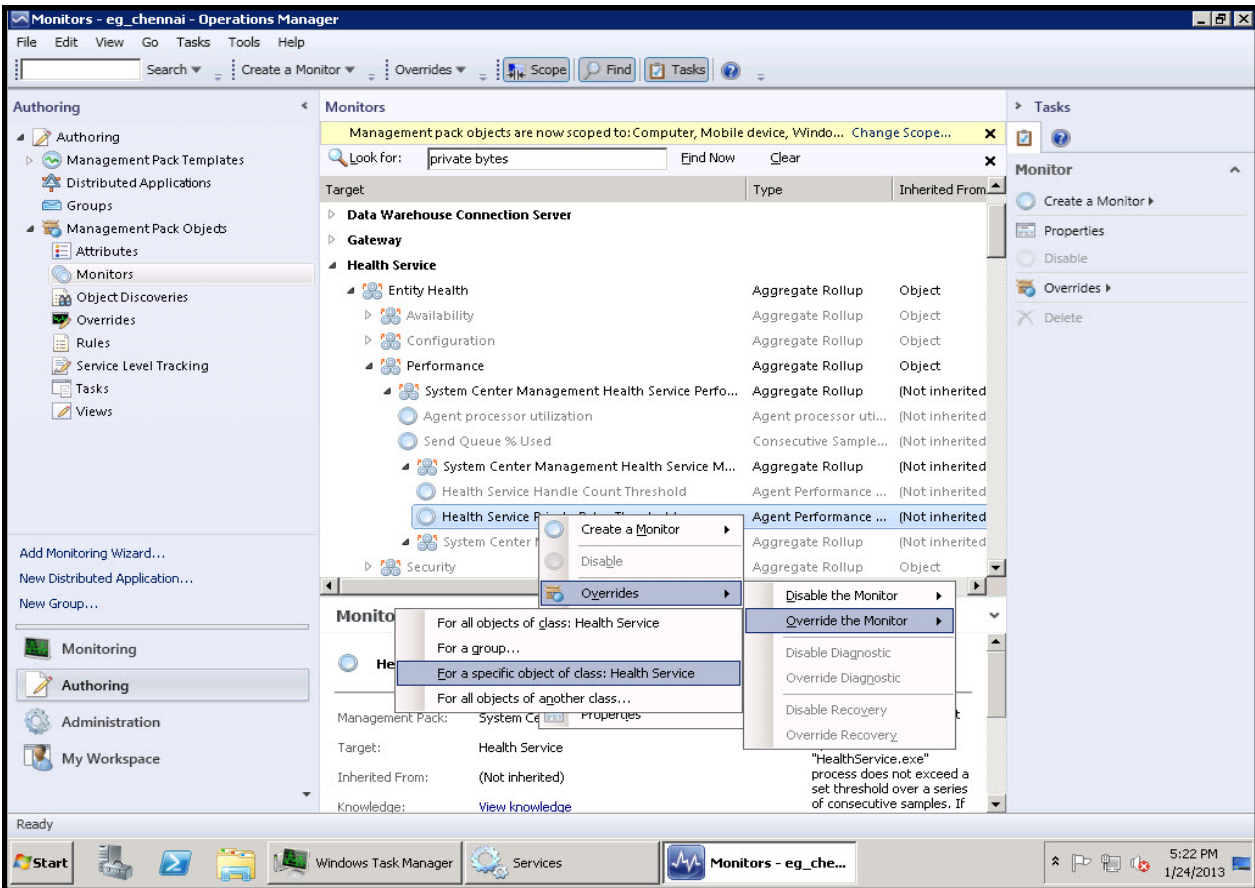


Figure 3.16: Overriding the 'Health Service Private Bytes Threshold' monitor

4. Figure 3.17 will then appear. From the list of **Matching objects** displayed here, pick the server that hosts the eG SCOM Connector. Then, click the **OK** button in Figure 3.17.

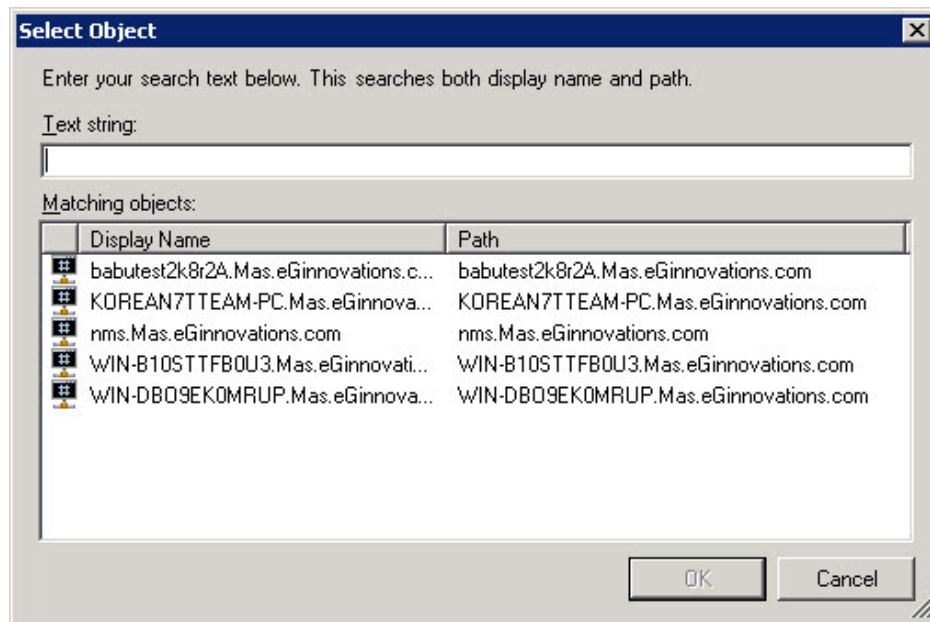


Figure 3.17: Selecting the server that hosts the eG SCOM Connector service

- From the **Override-controlled parameters** listed in Figure 3.18, select **Agent Performance Monitor Type - Threshold** by clicking on the corresponding check box. Then, set the **Override value** of this parameter to 3221225472 (equal to 3 GB). Pick the **Default Management Pack** option from the **Management Pack** section, and click the **Apply** and **OK** buttons in Figure 3.18.

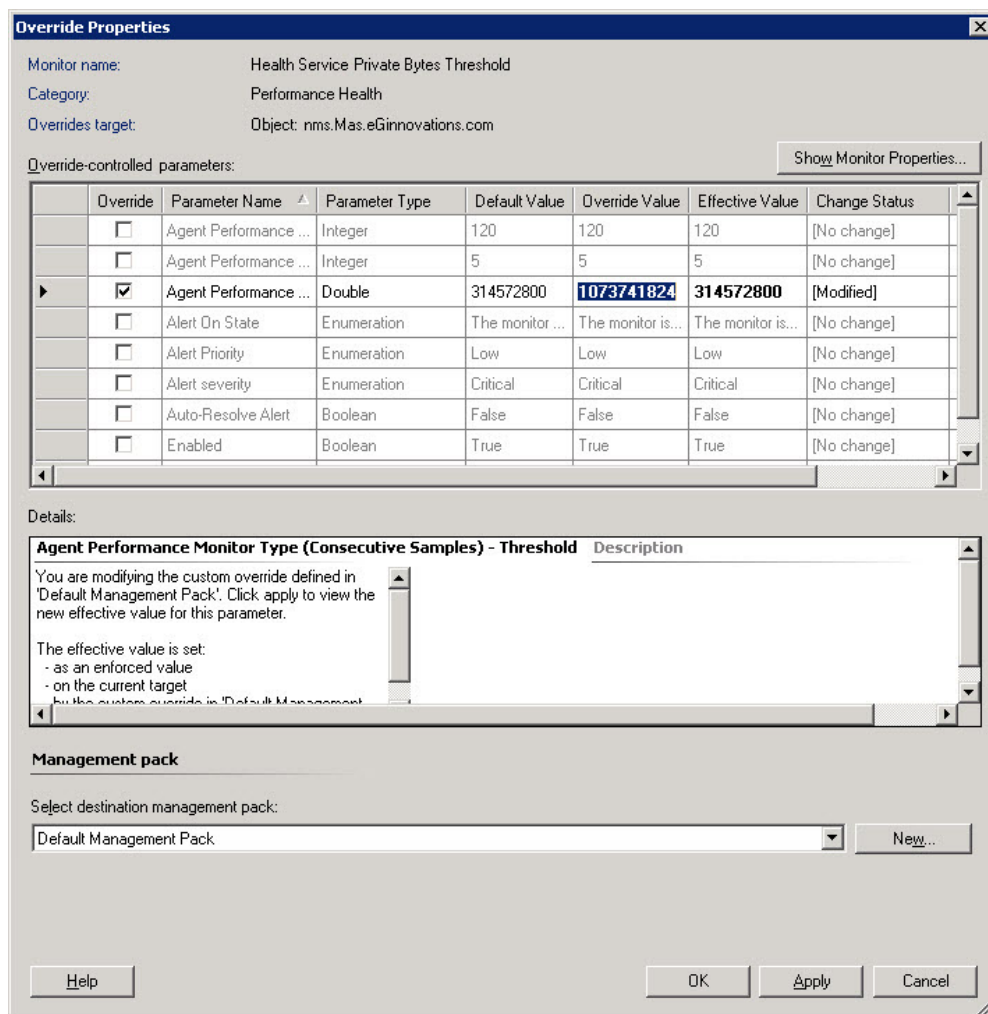


Figure 3.18: Modifying the 'Override value' of the 'Agent Performance Monitor Type - Threshold' parameter of the 'Health Service Private Bytes Threshold' monitor

- You will then return to the **Monitors** view of Figure 3.16. Now, from the **Performance** category of the **Health Service** target, right-click on the monitor named **Health Service Handle Count Threshold**, and follow the menu sequence: *Overrides -> Override the Monitor -> For a specific object of class: Health Service*
- Figure 3.19 then appears. Like before, from Figure 3.19, select the server on which the eG SCOM Connector service is running, and click the **OK** button therein.

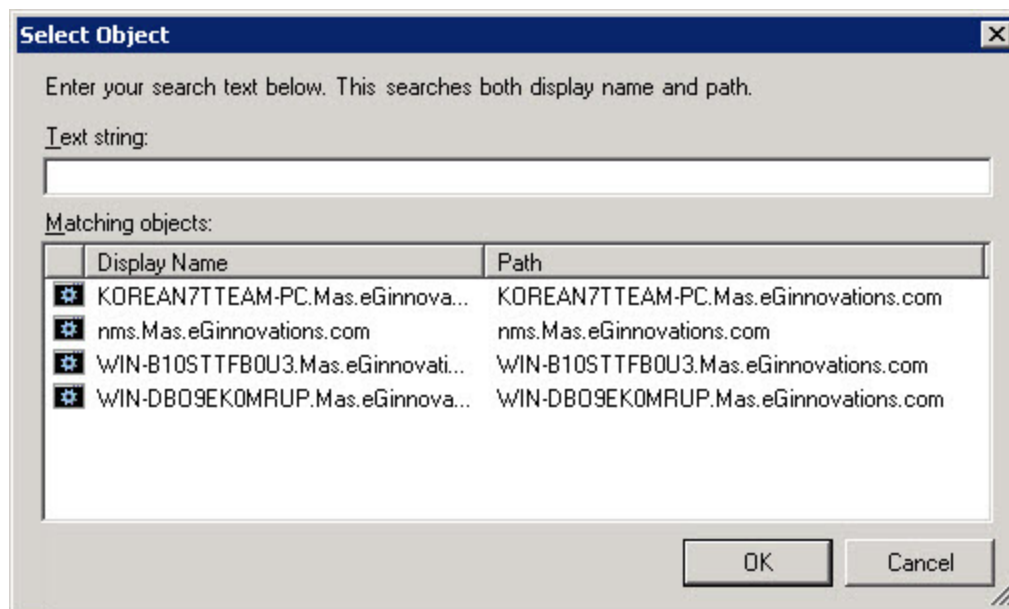


Figure 3.19: Choosing the server on which the eG SCOM Connector is running

8. From the **Override-controlled parameters** listed in Figure 3.20, select **Agent Performance Monitor Type - Threshold** by clicking on the corresponding check box. Then, set the **Override value** of this parameter to **30000**. Finally, pick the **Default Management Pack** option from the **Management Pack** section, and click the **Apply** and **OK** buttons in Figure 3.20.

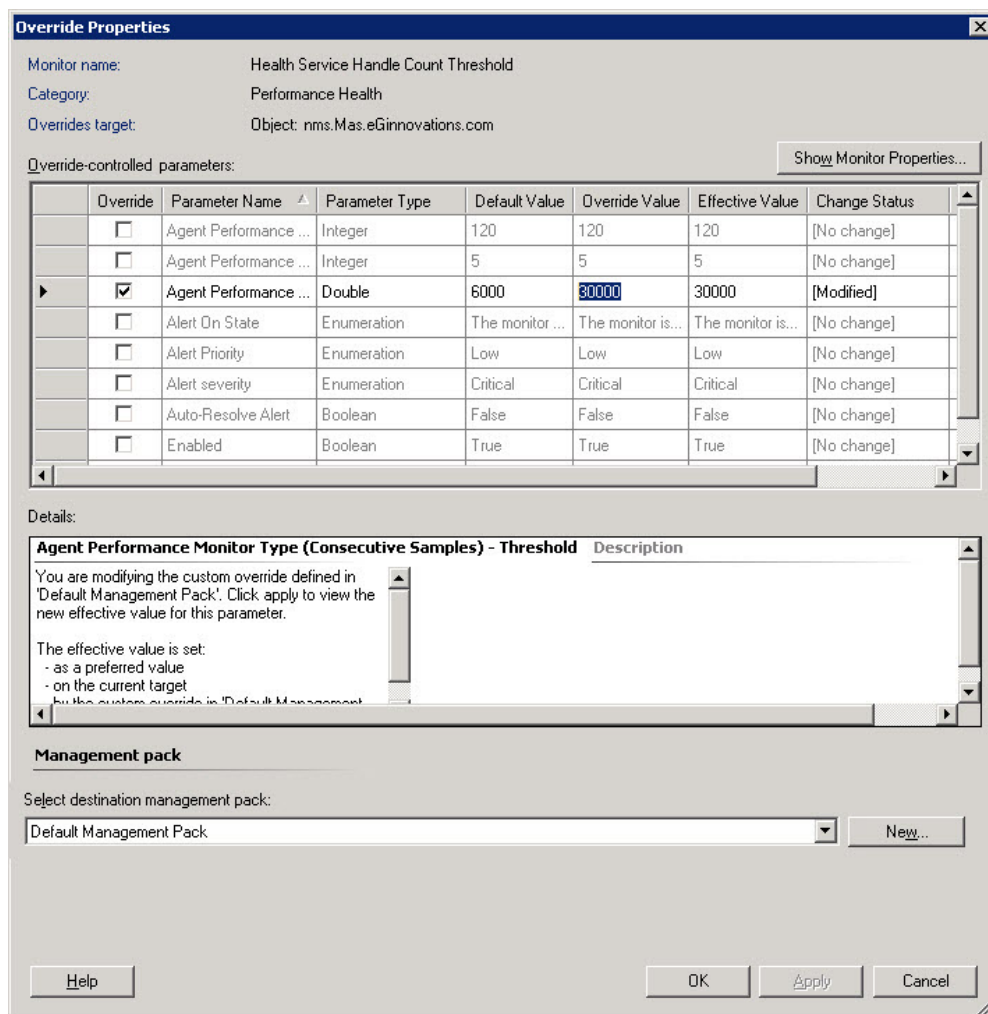


Figure 3.20: Modifying the 'Override value' of the 'Agent Performance Monitor Type - Threshold' parameter of the 'Health Service Handles Count Threshold' monitor

9. Once back in the **Monitors** view of Figure 3.20, locate the target **Agent** and expand its **Performance** category. Then, using the procedure discussed in steps 3-5 or 6-9 above, set the **Override value** of the **Agent Performance Monitor Type - Threshold** parameter of the following monitors to the value prescribed in the table below:

Monitor Name	Override Value
Monitoring Host Private Bytes Threshold	3221225472
Monitoring Host Handle Count Threshold	30000

3.2.4 Installing the eG Console Tasks Application

The **eG Console Tasks** application enables users to the SCOM console to instantly launch the eG monitoring console from the SCOM console itself. This way, users can take the help of analytical and daignostic tools provided by the eG monitoring console to investigate performance setbacks experienced by eG-managed components. To install this application, do the following:

1. Login to the SCOM console's host.
2. Download the **eG SCOM Console Tasks.zip** file from the URL that is provided to you, to any location on the SCOM host.
3. Extract the contents of the zip file and then run the **eG SCOM Console Tasks.msi** file within.
4. Then, switch to the directory that holds the downloaded executable, and double-click on it.
5. Figure 3.21 will then appear.

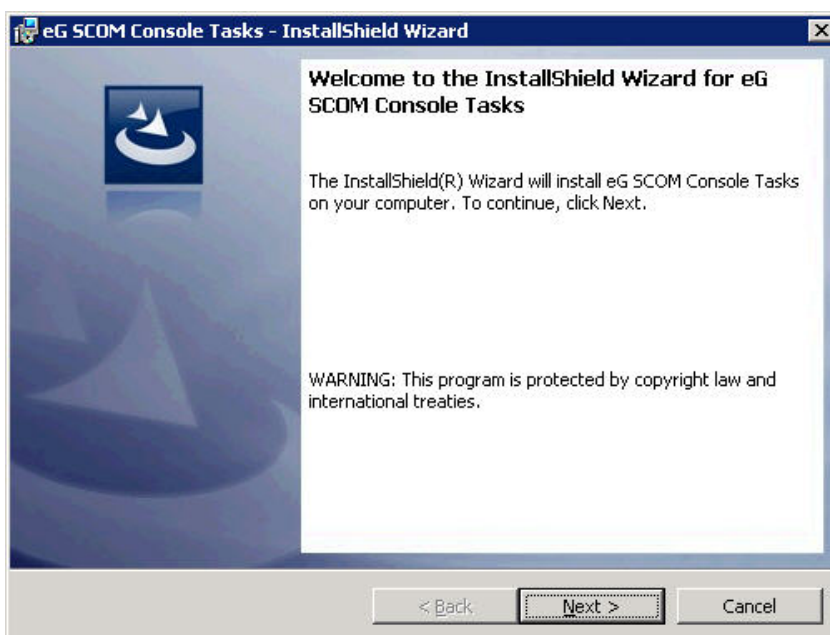


Figure 3.21: Welcome screen of the Console Tasks Application wizard

6. Click **Next** on Figure 3.21 to proceed. When Figure 3.22 appears, click **Install** to begin installing the eG Console Tasks application.

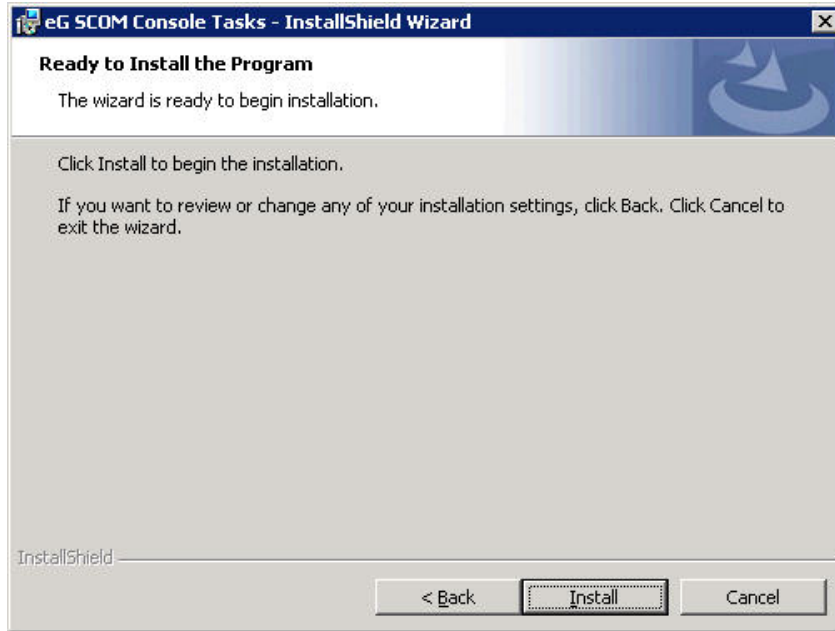


Figure 3.22: Click 'Install' to install the eG Console Tasks application

7. Upon completion of installation, click the **Finish** button in Figure 3.23.

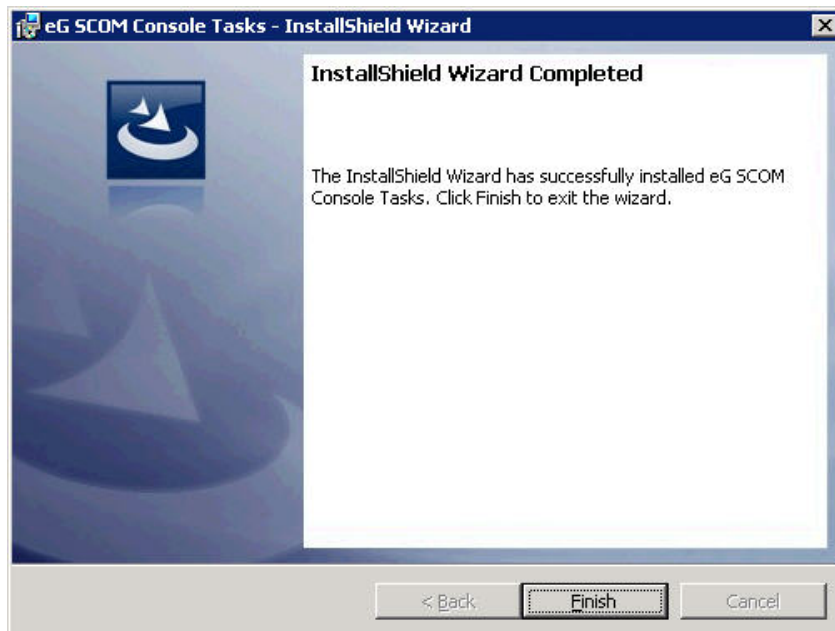


Figure 3.23: Completing the installation

8. If you now click on the **Diagnose using eG** option in the **Actions** pane of your SCOM console, you will be prompted for the login credentials (see Figure 3.24) for accessing the eG monitoring console. This prompt will appear only when you click the **Diagnose using eG** option for the very

first time. Provide valid login credentials and click the **OK** button in Figure 3.24. This will automatically invoke the eG monitoring console. The same credentials will be used to launch the eG monitoring console during all your subsequent attempts to **Diagnose using eG**.

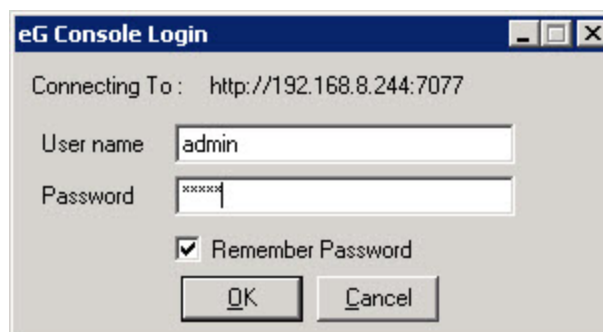


Figure 3.24: Login credentials for accessing the eG management console

3.3 High Availability Support

To ensure that SCOM users are able to perform end-to-end monitoring of their IT infrastructure at all times, the eG Universal MP for SCOM supports three levels of high availability.

1. Failover clustering of eG managers

You can have two eG managers operate within a redundant cluster, with one primary manager and one secondary manager. The eG SCOM connector embeds the intelligence to detect a cluster setup, identify which manager in the cluster is currently active, and communicate with it for performance and problem updates on eG-managed components.

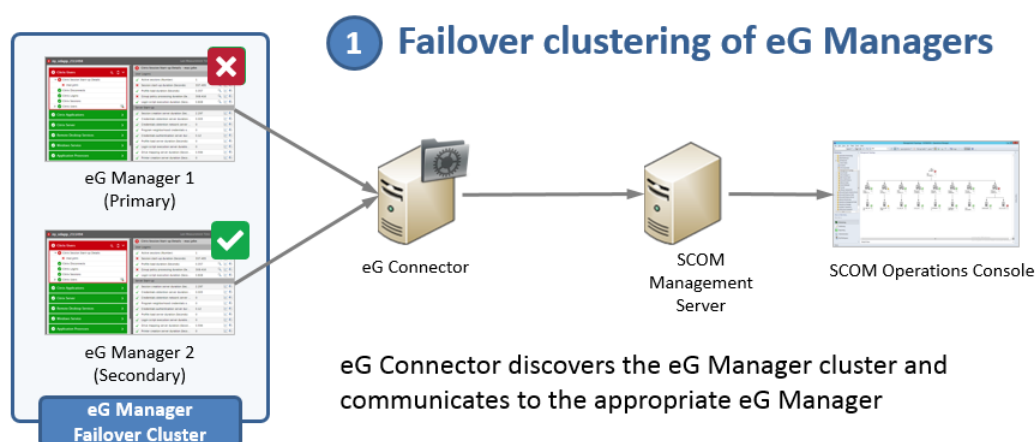


Figure 3.25: The eG SCOM Connector can discover and work with an eG Manager Redundant Cluster

If you want to configure a SCOM connector for a redundant manager setup that pre-exists in an environment – i.e., a redundant manager setup that was operational before connector was installed – then, post the installation, you just have to point the connector to use the primary manager's URL. The connector automatically discovers secondary managers and if there is a failure in the redundancy, it will automatically switch to the available manager.

On the other hand, if you configure a redundant manager setup post connector deployment, then, you will first have to point the connector to use the primary manager's URL, and then, **restart the eG SCOM Connector** – i.e., stop and then start the eG SCOM Connector. Only after the restart will the eG SCOM connector automatically discover the secondary managers

2. Failover clustering of eG SCOM Connectors

You can also deploy multiple eG SCOM connectors on a Windows failover cluster. You can then register the same eG manager with each of these connectors. Even if one connector is rendered unavailable, the eG manager will continue to communicate with any of the other available connectors in the cluster to transmit problem and performance information to the SCOM console.

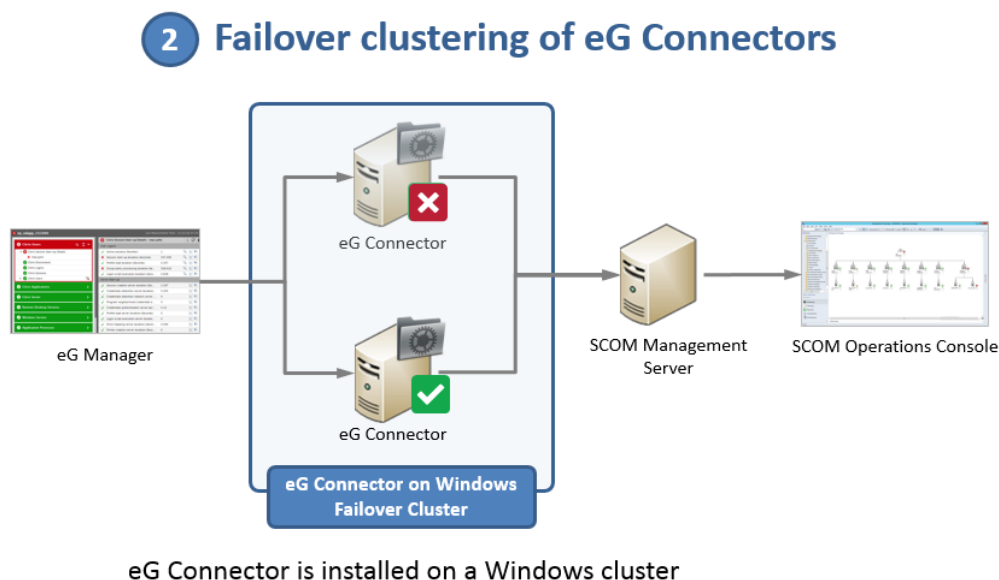


Figure 3.26: The eG SCOM Connector can be installed on a Windows failover cluster

3. Failover clustering of SCOM management servers

High availability can also be ensured by configuring two SCOM management servers to operate in a cluster. The eG SCOM connector should be configured to communicate with both the management servers in the cluster. If this is done, then, if the primary SCOM management server is unavailable, the eG SCOM connector will be able to intelligently detect unavailability of

the primary, identify which is the secondary management server, and automatically connect to that server to transmit performance updates.

3 Failover clustering of SCOM Management Servers

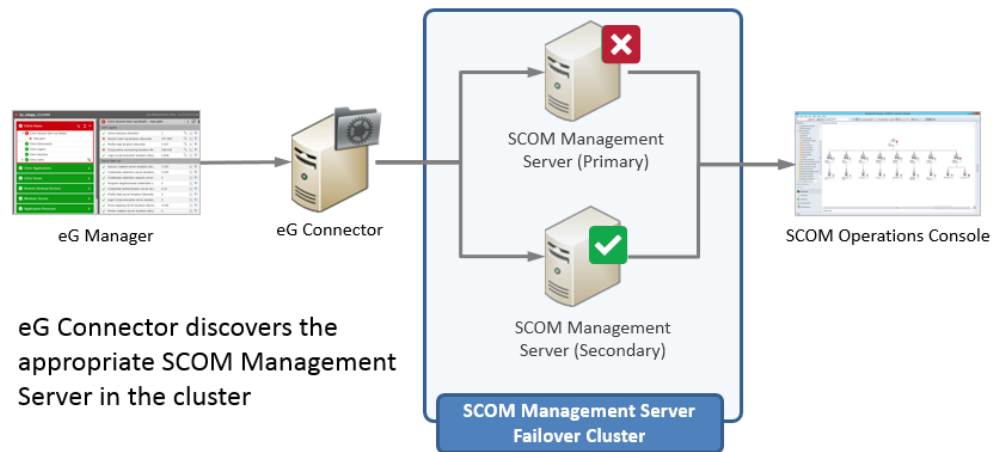


Figure 3.27: A single connector communicating with clustered SCOM management servers

3.4 Scaling the eG Universal MP for SCOM

The eG Universal MP for SCOM lets you easily scale up to meet the growing monitoring needs of an IT infrastructure that uses SCOM. The ways to achieve it are explained in the below sections.

3.4.1 Configuring Multiple eG SCOM Connectors for a Single eG Manager

The number of eG-managed components a single SCOM connector can support depends upon the processing capability of the SCOM agent. Where hundreds of components are to be monitored, to ensure scalability, one may wish to setup multiple connectors on different machines, each of which integrates with the same eG manager.

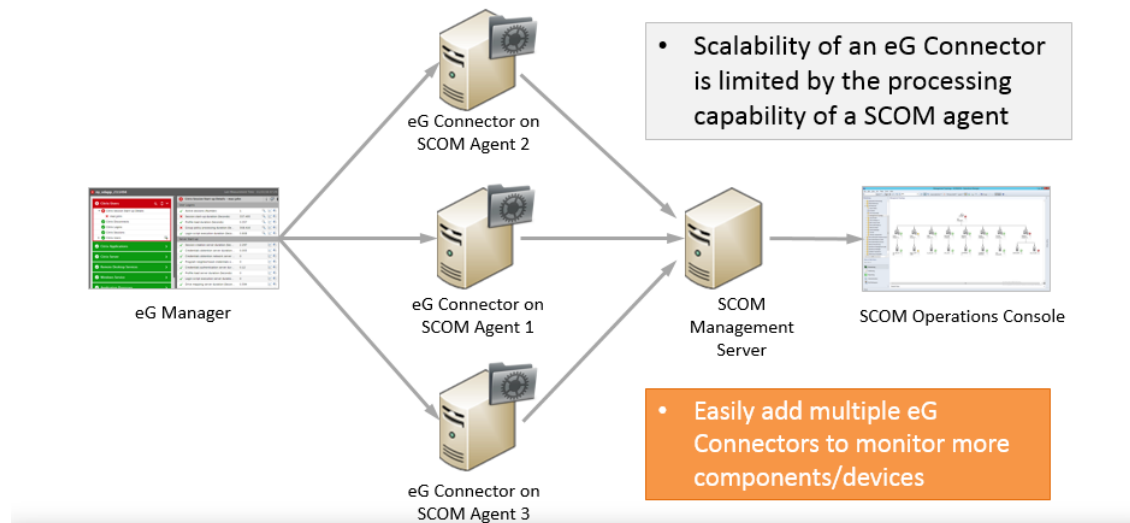


Figure 3.28: A single eG manager communicating with multiple eG SCOM connectors

The process of installing and configuring each of these connectors is the same as what has been discussed in the previous sections. However, while doing so, consider the following points:

- Configure the same SDK user account in all connectors.
- Configure different manager IDs (for the same eG manager) – one for each eG SCOM connector.
- Every connector is configured with a unique eG user. Only the list of components assigned to that user get integrated with SCOM.
- Each eG user has to be associated with a unique list of components. If say, two users are assigned the same component, component discovery will fail for the second user.

3.4.2 Integrating Multiple eG Managers with SCOM

Typically, a single eG manager can monitor upto 3000 components/devices. In large IT infrastructures, where tens of thousands of components are to be monitored, multiple eG managers are common-place. To ensure the scalability of the eG Universal MP in such environments, a dedicated eG SCOM connector setup is required for every eG manager.

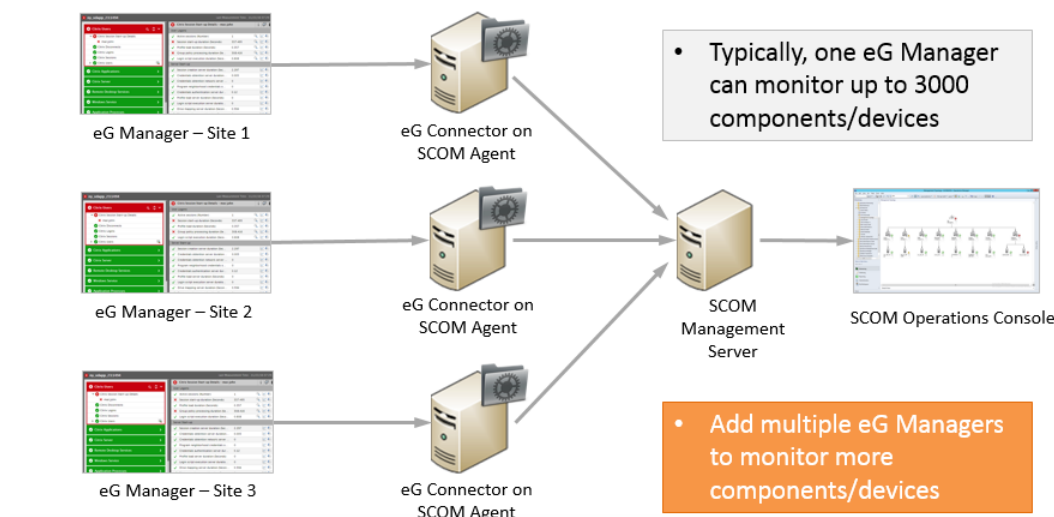


Figure 3.29: Integrating multiple managers with SCOM

The following configuration guidelines need to be followed for this specific case.

- Configure the same SDK user account in all connectors.
- Configure a different manager ID for every connector.
- The eG management pack which gets installed on the SCOM server will be common for all connectors. The configuration tool automatically determines whether/not multiple connectors are configured on the SCOM server. If some other connector is already using the eG management pack, the tool will skip the import/delete operation for the eG management pack.

Note:

If two/more managers that are to be integrated with SCOM have IC/aggregate tests with the same names, then before integrating these managers with SCOM, make sure that these common tests report the same measures – i.e., the names, functionality, and the count of measures should be the same.

Chapter 4: Using the eG Universal Management Pack (MP) for SCOM

Once the eG Universal MP is successfully deployed, you will find eG-managed components appear as monitoring objects in the SCOM console. Using the SCOM console, you can then:

- View the current state of the eG-managed components;
- Be alerted to problems experienced by eG-managed components;
- Isolate problem layers, tests, and measurements;
- Analyze state transitions experienced by eG-managed components;
- Monitor business service performance using SCOM and identify the root-cause of service slowdowns/outages
- Launch the eG monitoring console from the SCOM console to perform further diagnosis of problems;
- Enable/disable specific monitors using the SCOM console

This chapter takes the help of an example to explain how the eG-SCOM integration works.

This example takes the case of a target environment comprising of an eG manager that is monitoring a VMware vSphere/ESX server, a Cisco router, and a Microsoft Terminal server. Soon after the eG manager is integrated with the SCOM server, login to the SCOM console. Figure 4.1 will then appear. Post the integration, the tree-structure in the left pane of Figure 4.1 will display a new **eG Enterprise** node.

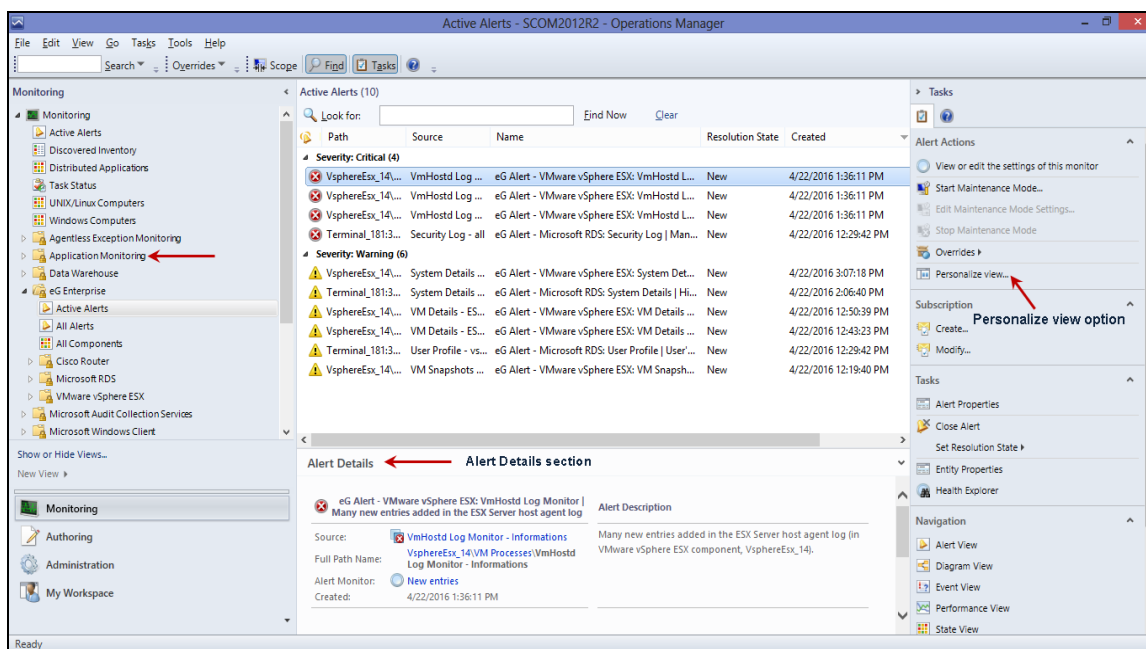


Figure 4.1: The tree-structure displaying a new 'eG Enterprise' node

If you expand the **eG Enterprise** node, you will find a series of sub-nodes. Clicking on each sub-node will enable you to do the following:

- View the currently active alerts pertaining to eG-managed components;
- View all the alerts that were generated by the eG manager during the last 3 days;
- View the components managed by eG Enterprise and their current state;
- Focus on the overall performance and problems related to each eG-managed component;

The sections that follow will take a closer look at each sub-node of the **eG Enterprise** node.

4.1 Viewing the Active Alerts

Let us begin by clicking the **Active Alerts** node under **eG Enterprise**.

1. When the **Active Alerts** node is clicked, the contents of the right panel will change to display all the currently open alarms for the eG-managed components, grouped by the alarm severity/priority. Each alert displayed in the right panel will indicate the following by default:

- **Severity:** This refers to the alarm priority. The severity that corresponds to each of the alarm priorities supported by eG Enterprise are as follows:

eG Alert Priority	SCOM Alert Severity
Critical	Critical
Major	Warning
Minor	Warning

Note:

Though the SCOM console categorizes both the **Major** and **Minor** eGalerts as **Warnings**, you can differentiate between the two by instantly launching the eG monitoring console from the SCOM console. To do so, just click on the **Diagnose using eG** option indicated by Figure 3.1.

- **Path:** The **Path** specification indicates the problem component, the problem component type, and the problem layer, and is expressed in the following format:
<ComponentName>\<ComponentType>\<Layer>
- **Source:** This indicates the problem test and problem descriptor (in case of a descriptor-based test).
- **Name:** For all alerts related to eG-managed components, this will be **<Component_Type>:<Test_Name>|<Measure_Name>**.
- **Resolution State:** This typically indicates whether the problem is currently active or has been closed. For all **Active Alerts** however, the **Resolution State** will be **New**.
- **Created:** This indicates when the problem was detected by the eG manager.
- **Age:** This indicates how long the problem has remained unresolved.

2. You can, if you so need, customize your default **Active Alerts** view to include more columns or exclude one/more default columns. To achieve this, click on the **Personalize view** option in the **Actions** pane to the far right of Figure 4.1. Figure 4.2 will then appear. Select one/more check boxes from the **Columns to display** section to add more information to the **Active Alerts** view, or deselect one/more check boxes to remove the alarm details that pre-exist. Click the **OK** button in Figure 4.2 to save your customizations.

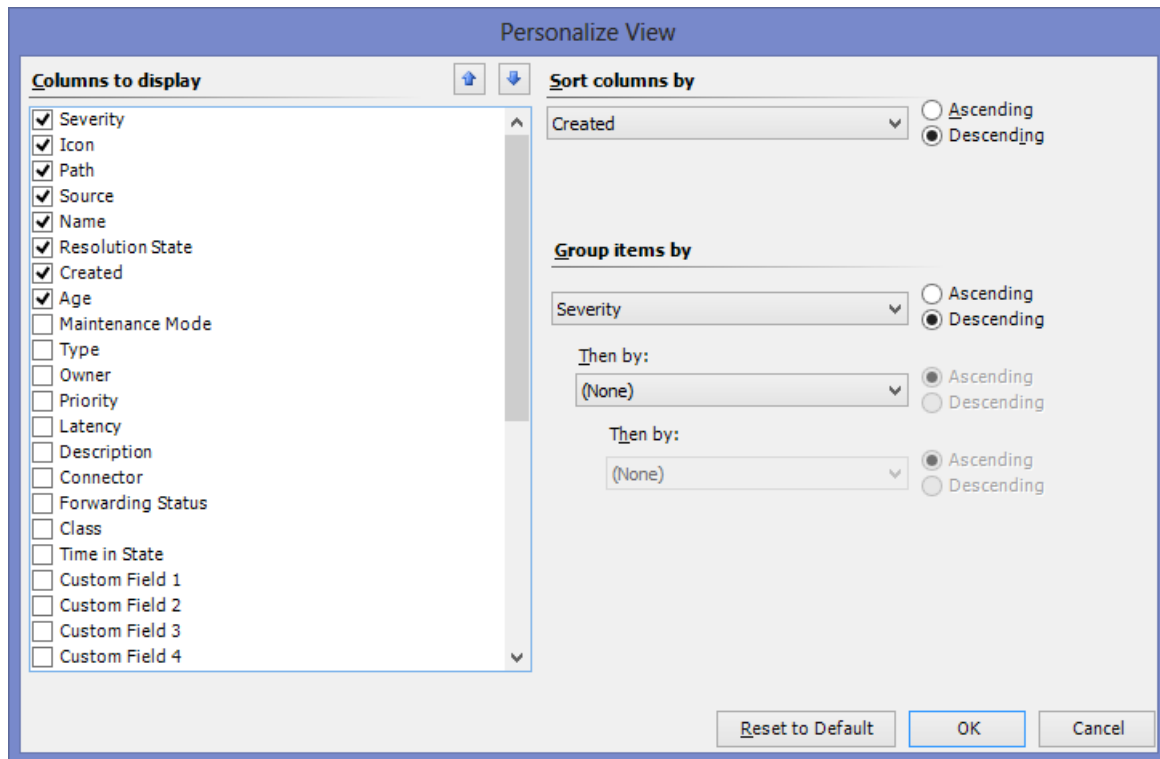


Figure 4.2: Personalizing the Active Alerts view

3. Once back in the **Active Alerts** view, you can click on a specific critical alert/warning to view the alert details more clearly in the **Alert Details** section indicated by Figure 4.1. Scrolling down the contents of the **Alert Details** section will reveal a **View additional knowledge** link (see Figure 4.3).

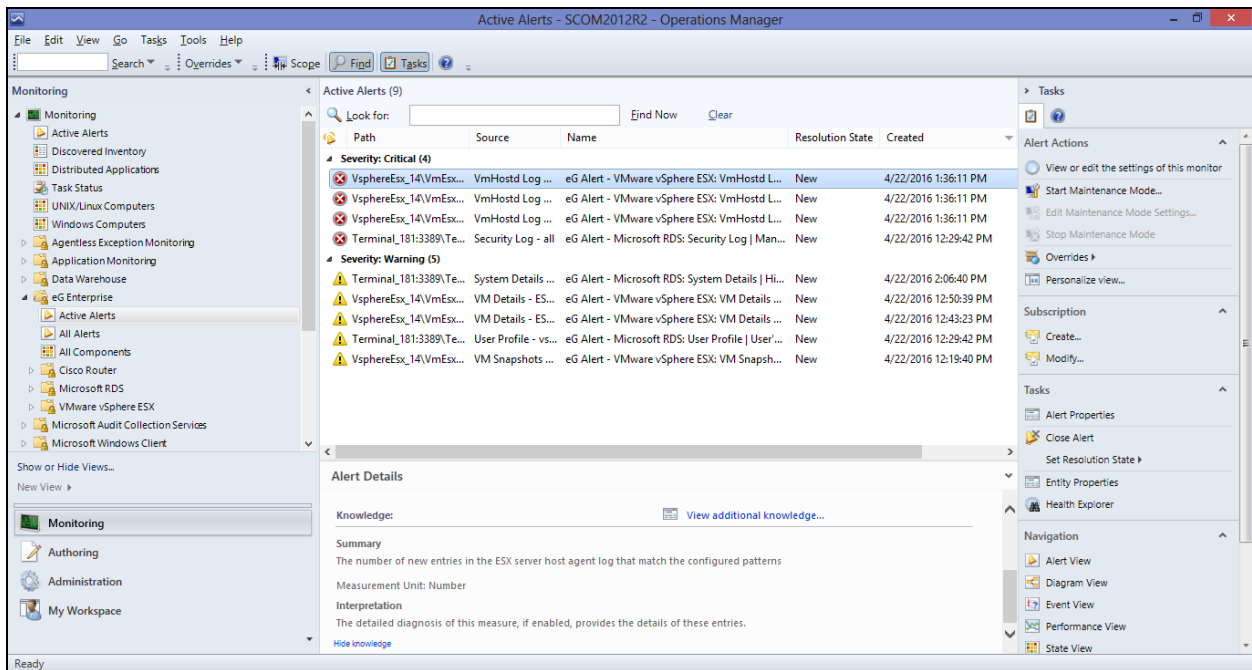


Figure 4.3: Scrolling down the Alert Details section to View additional knowledge

- To understand a problem better, click on the **View additional knowledge** link and tap the knowledge base of the eG Enterprise system. The **Product Knowledge** tab page of the **Alert Properties** window will automatically open displaying the details related to the measure on which the selected alert was raised. Figure 4.4 depicts a sample **Alert Properties** window displaying the details of the **Number of system errors** measure.

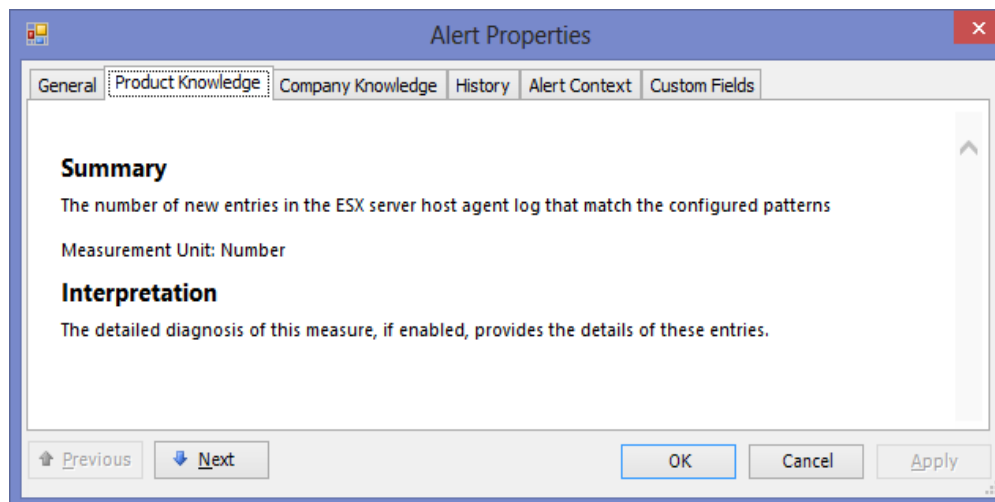


Figure 4.4: The description of a measure reported by a test

- To investigate the problem at hand further, you can even instantly launch the eG monitoring

console from the **Active Alerts** view. For this, just select an alert from the view and click on the **Diagnose using eG** link in the **Actions** pane of Figure 4.5.

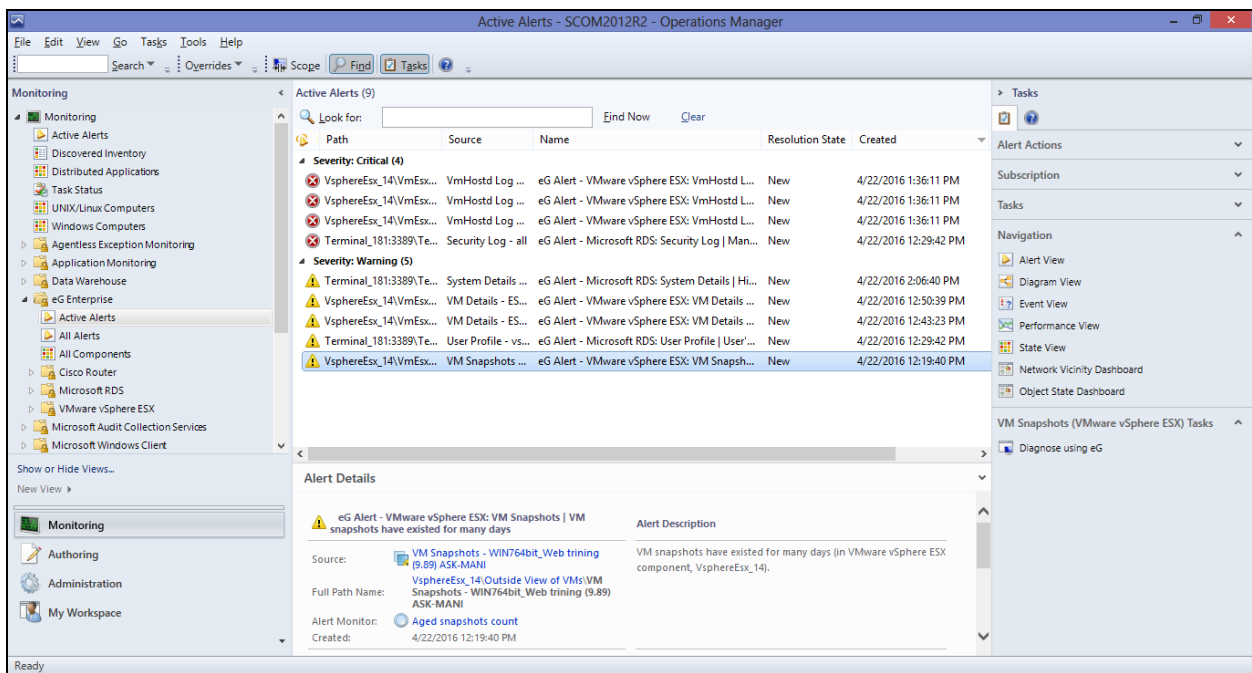


Figure 4.5: Launching the eG monitoring console from the SCOM console

6. Doing so will lead you to that page in the eG monitoring console that indicates the problem layer, test, and measurement that corresponds to the alert chosen from the SCOM console.

Note:

Clicking on the **Diagnose using eG** option will launch the eG monitoring console only if the **eG Console Tasks** application is installed on the system on which the SCOM console is operating. To know how to install this application, refer to Section 3.2.4. Also, when the eG console is launched for the very first time from the SCOM console, a login screen will appear, where you will have to manually key in the user credentials for logging into the eG monitoring console. The same credentials will be used to launch the eG monitoring console during your subsequent attempts to **Diagnose using eG**.

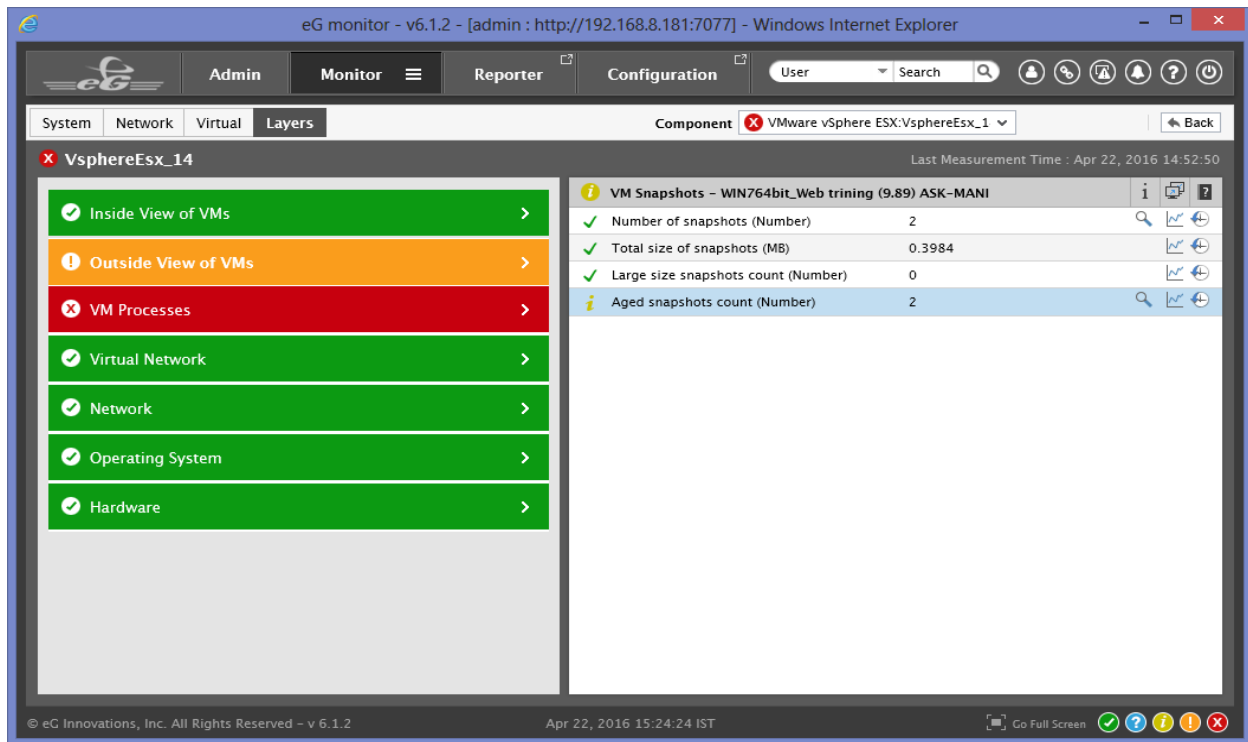


Figure 4.6: The eG monitoring console indicating the problem layer, test, and measurement related to the alert chosen from the SCOM console

4.2 Viewing All Alerts

To view the alert history of eG-managed components from the SCOM console, do the following:

If the documentation phase of the Project Life Cycle likely depends on your role in the IT organization. If you are a manager or project lead, documentation is critical to the success of the project. If you are in a non-managerial position, documentation is an annoying nuisance that gets in the way of your *real* work. While the 10 tips below are mainly targeted toward the latter category, managers and supervisors can also benefit from them.

1. Click on the **All Alerts** sub-node of the **eG Enterprise** node in the tree-structure in the left panel of the SCOM console.

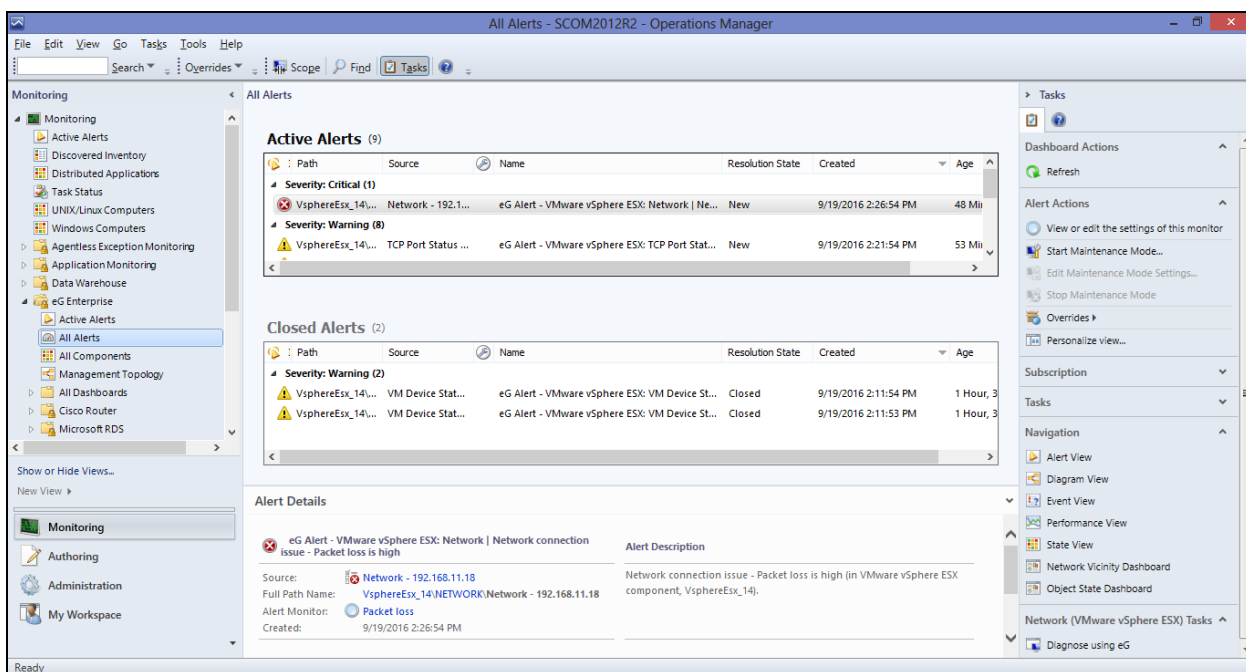


Figure 4.7: The All Alerts view

- The right dashboard panel will then display all alerts that were raised on the eG-managed components (see Figure 4.7). Here again, the alerts will be grouped by severity. Also, like in the **Active Alerts** view, each alert in the **All Alerts** view will display the alert **Path**, **Source**, **Name**, **Resolution State**, **Created** date/time, and **Age**, by default. If one/more problems were resolved, then the **Resolution State** of such alerts will be **Closed**. **Closed Alerts** will be displayed in a separate section in the alerts view. The **Closed Alerts** section will display alerts on the basis of the following criteria: “View all alerts with Closed(255) resolution state”. New alerts will be displayed on the basis of the following criteria: “View all alerts with New(0) resolution state”.

You can access the eG knowledge base (i.e., the eG online help system) from the **All Alerts** view, and also launch the eG monitoring console to perform deeper diagnosis of a particular problem.

Note:

Clicking on the **Diagnose using eG** option will launch the eG monitoring console only if the **eG Console Tasks** application is installed on the system on which the SCOM console is operating. To know how to install this application, refer to Section 3.2.4. Also, when the eG console is launched for the very first time from the SCOM console, a login screen will appear, where you will have to manually key in the user credentials for logging into the eG monitoring console. The same

credentials will be used to launch the eG monitoring console during your subsequent attempts to **Diagnose using eG**.

4.3 Closing Alerts in the SCOM Console

The eG-SCOM integration is by default **uni-directional**. In other words, it is the eG manager that communicates state changes and alarm transitions to the SCOM server, and not the other way round. By default therefore, an alarm deleted in the eG manager gets automatically closed in the SCOM server, but an alarm that is closed using the SCOM console, does not get automatically deleted in the eG manager. This default behavior however, can be overridden starting from v6.0 of the eG Enterprise Suite. From v6.0, the eG SCOM Connector can be configured to automatically delete alarms in the eG manager, as soon as the same alarms are closed in the SCOM console. To enable this capability, follow the steps below:

- Stop the eG SCOM Connector service.
- Edit the **ConnectorService.exe.config** file located in the <EG_SCOM_CONNECTOR_INSTALL_DIR> directory.
- Look for the following entry in the file:

```
<add key="BidirectionalAlertClosing" value="false" />
```
- Change the text *"false"* in the above entry to *"true"*.
- Finally, save the file.
- Start the eG SCOM Connector service.

4.4 Viewing Component Health

To view the current state of the eG-managed components, do the following:

1. Click on the **All Components** sub-node under the **eG Enterprise** node in the tree-structure in the left panel of the SCOM console. The right panel will then display all the eG-managed components and their current state (see Figure 4.8).

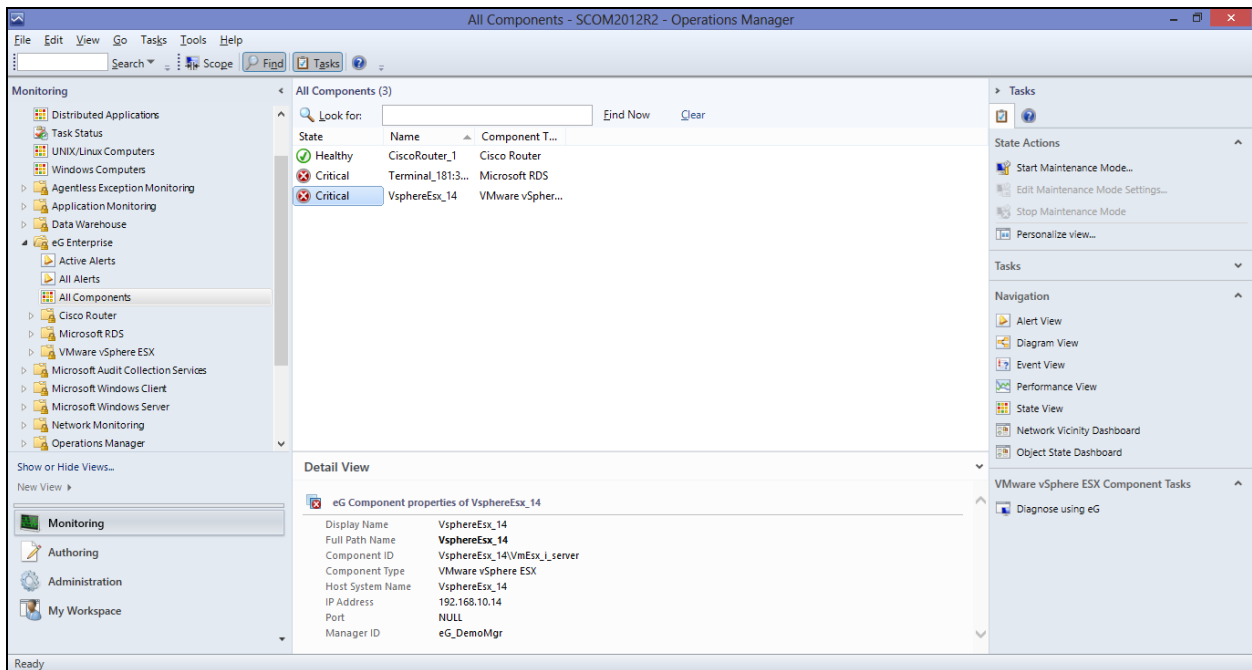


Figure 4.8: The All Components sub-node

2. From the **All Components** view, you can determine the current **State** of the eG-managed components, the **Name** of the components, and the **Component Type**. The SCOM states that correspond to the states prescribed by eG Enterprise are discussed in the table below:

eG State	SCOM State
Normal	Healthy
Critical	Critical
Major	Warning
Minor	Warning
Unknown	Not Monitored / Uninitialized

3. From Figure 4.8, it is evident that while the Terminal and vSphere servers in our example are in a **Critical** state currently, the Cisco router is in a healthy state.
4. Clicking on a row in the **All Components** view will reveal additional details of the chosen component in the **Detail View** section below. You can use the **Personalize view** option in the **Actions** pane to customize the **All Components** view - this way, you can include more columns to the default view or exclude existing columns.
5. If you select a component from the **All Components** view and click the **Diagnose using eG** option in the **Actions** pane, Figure 4.9 will appear.

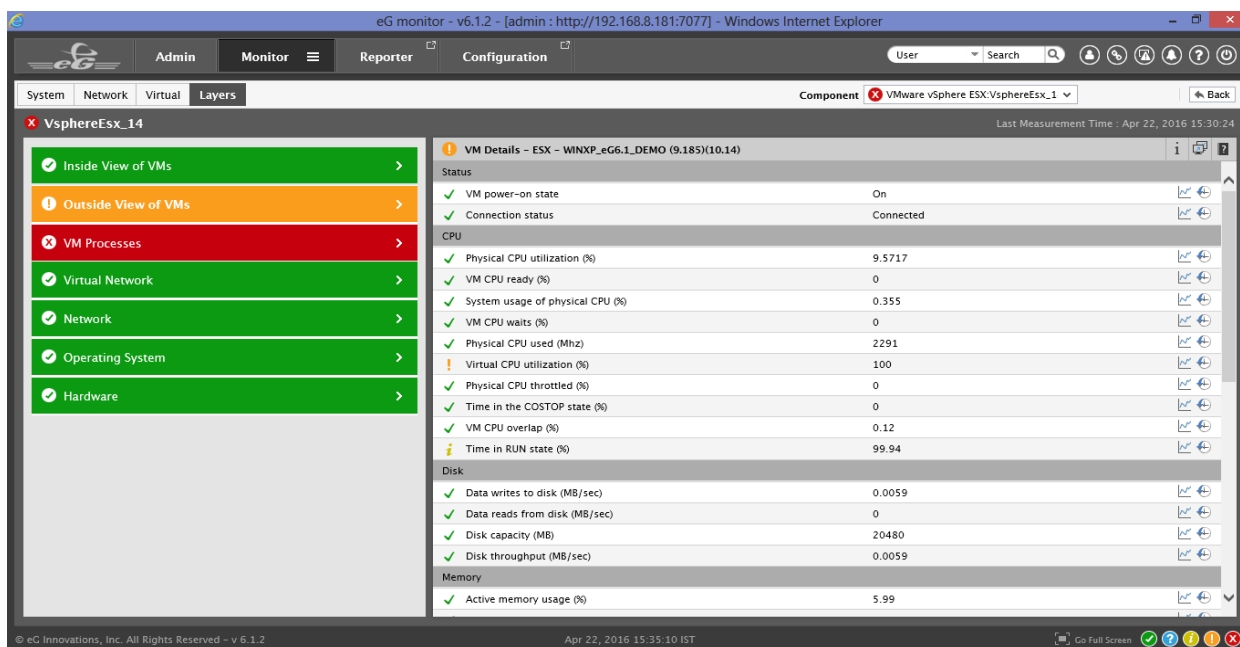


Figure 4.9: Launching the eG monitoring console from the SCOM console

6. Figure 4.9 reveals the layer model of the component chosen from the **All Components** view, and also displays the problem layer, problem test and problem measures related to that component. This way, you can quickly isolate why the component is in an abnormal state currently.

Note:

Clicking on the **Diagnose using eG** option will launch the eG monitoring console only if the **eG Console Tasks** application is installed on the system on which the SCOM console is operating. To know how to install this application, refer to Section 3.2.4. Also, when the eG console is launched for the very first time from the SCOM console, a login screen will appear, where you will have to manually key in the user credentials for logging into the eG monitoring console. The same credentials will be used to launch the eG monitoring console during your subsequent attempts to **Diagnose using eG**.

4.5 Viewing Infrastructure Health

The SCOM console also provides a more graphical, end-to-end view of the eG-managed infrastructure via its topology representation. To obtain this view, do the following:

1. Click the **Management Topology** node below the **All Components** node (see Figure 4.10). The right panel will then display the topology representation depicted by Figure 4.10. From the

topology, it is clear that the eG-managed infrastructure is currently in a Critical state, because one of the servers in the infrastructure – namely, the VMware vSphere server – is experiencing Critical issues.

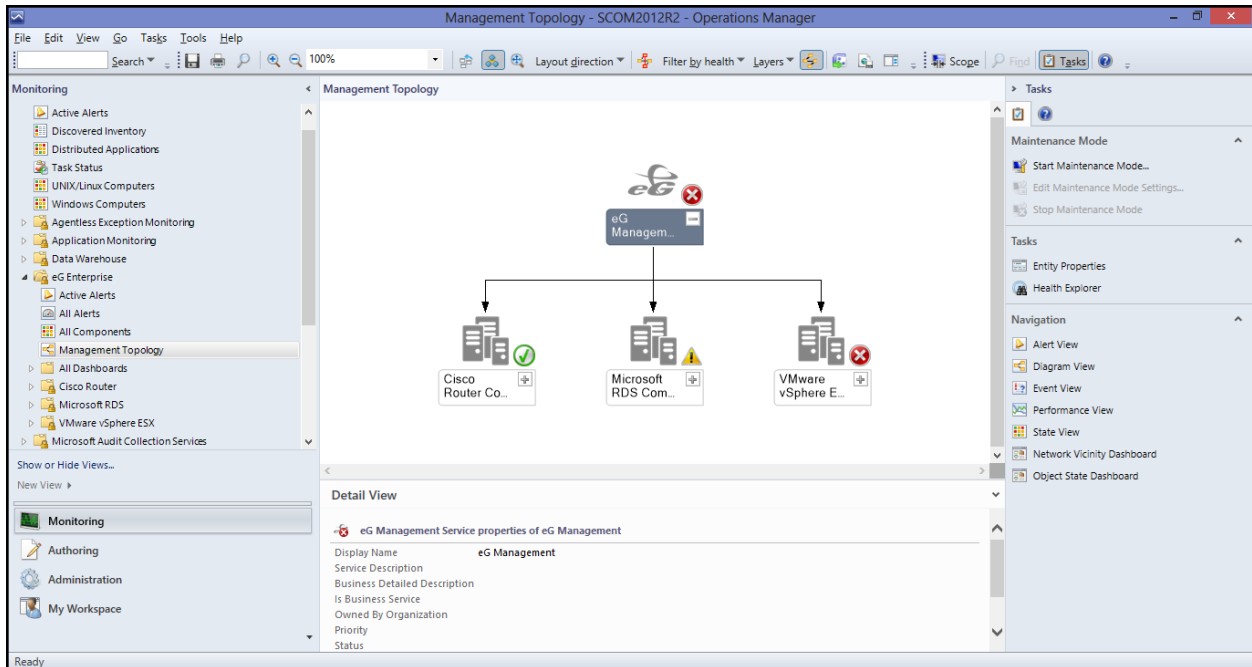


Figure 4.10: The Management Topology of the eG-managed infrastructure

2. You can also drill-down from the high-level topology view of Figure 4.10 to identify the vSphere server that is experiencing the Critical issues and to zero-in on the precise problems that are impacting this server's performance. For this click on the '+' icon alongside *VMware vSphere ESX* in Figure 4.10. Figure 4.11 will then appear.

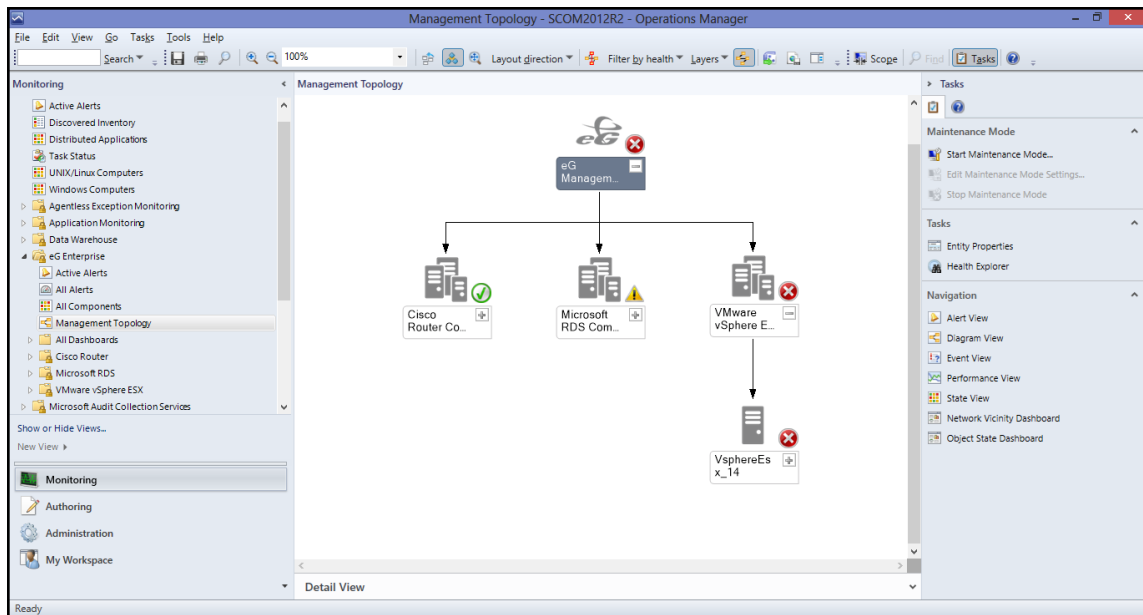


Figure 4.11: Drilling down from the high-level topology view to know which VMware vSphere server is in a Critical state

- Figure 4.11 reveals that the vSphere server, *VsphereEsx_14*, is the only vSphere server that is managed in the environment, and is currently in a Critical state. To identify the exact layer where the Critical issue occurred, drill down from the component view by clicking on the '+' icon alongside *VsphereEsx_14*. Figure 4.12 will then appear displaying the layers of eG's specialized layer model for VMware vSphere ESX. From the state of the layers, it is clear that Critical issues have occurred in **NETWORK** layer. If you now drill down from the **NETWORK** layer by clicking on the '+' icon alongside, you can identify the exact test that reported the Critical problem. In the case of our example, the **Network** test seems to have captured a Critical issue; this implies that a critical network-related issue is what caused the performance of the VMware vSphere server to suffer.

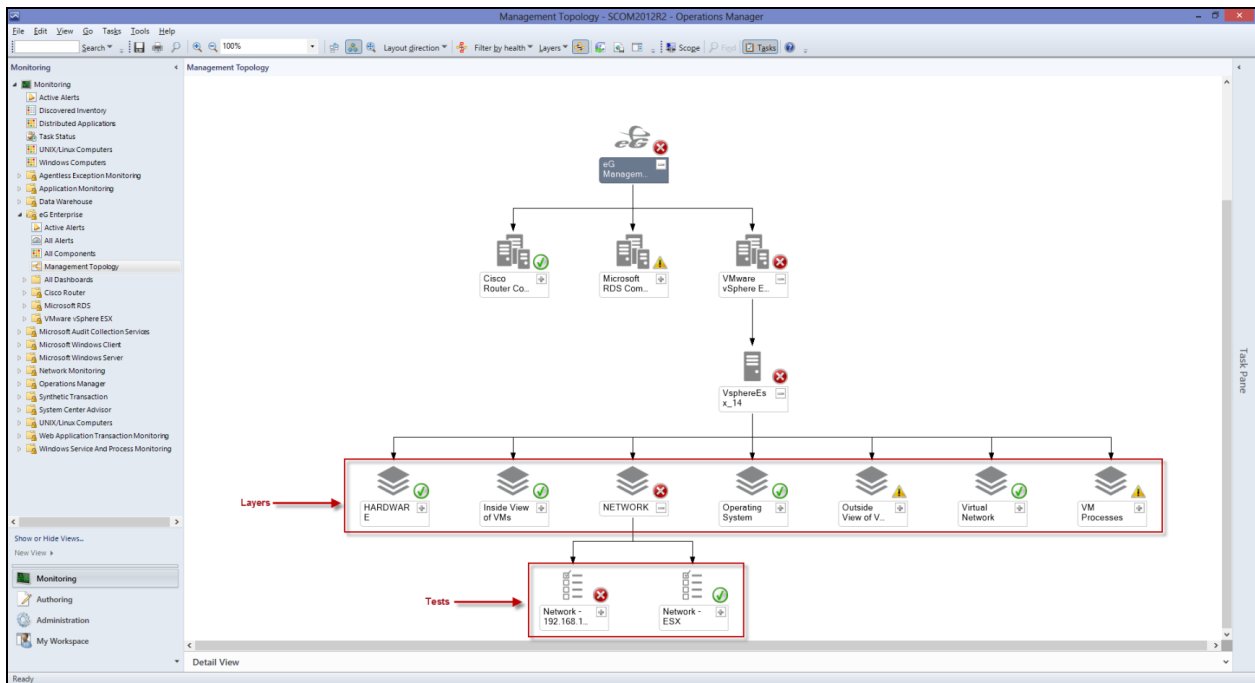


Figure 4.12: Isolating the layer and test that reported the Critical issue

4. To zero-in on the precise issue, right-click on the **Network** test representation in the topology and pick the **Health Explorer** option. Figure 4.13 will then appear pointing you to the exact measure that deviated from the threshold and caused the Critical problem. As can be inferred from Figure 4.13, a high packet loss on the network link to the VMware vSphere ESX server is what led to the Critical state of the vSphere server.

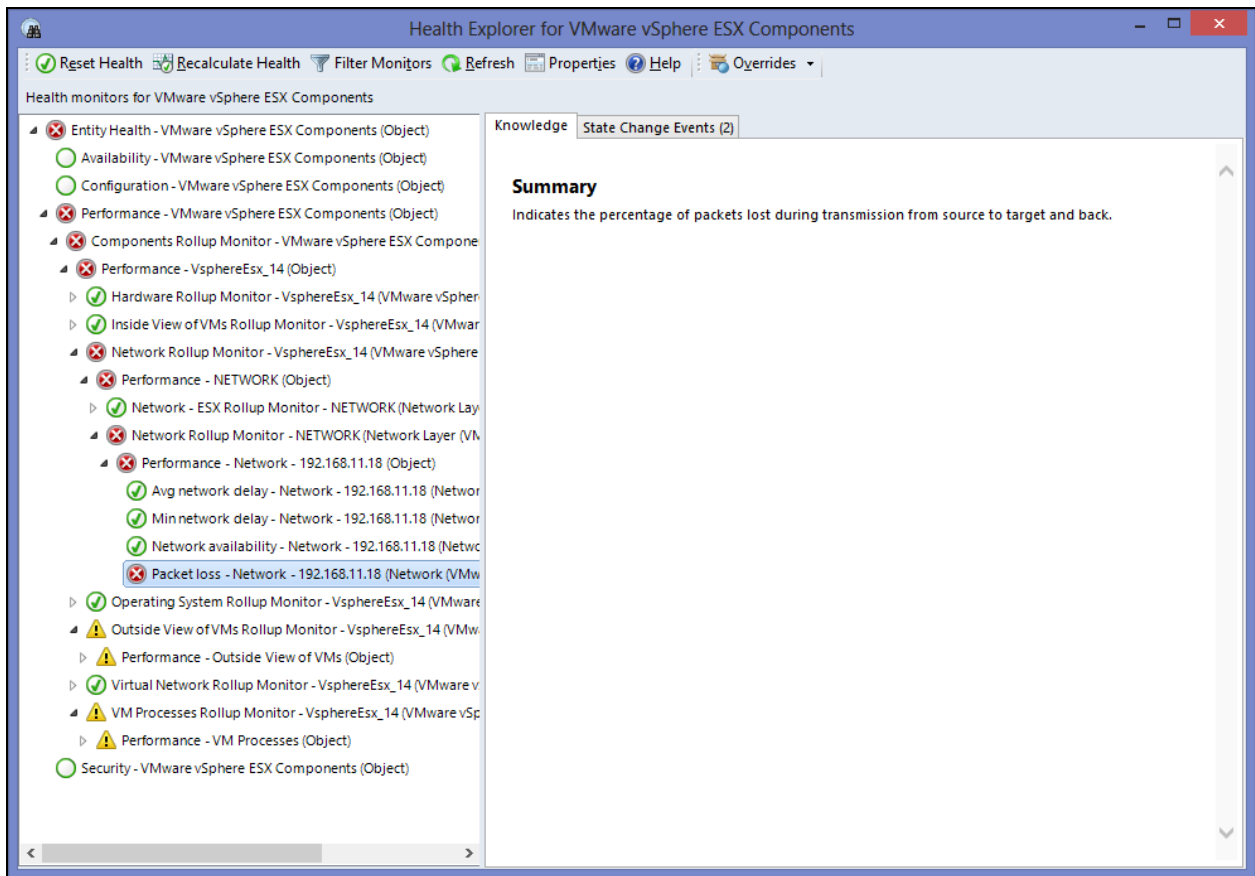


Figure 4.13: Health Explorer revealing the accurate reason for the Network problem with the VMware vSphere ESX server

4.6 Viewing Component Type Health

To view the health of eG-managed component types, do the following:

1. In the tree-structure in the left panel of the SCOM console, expand the *_All Dashboards* sub-node under the **eG Enterprise** node. Then, click the **Component Overview** node within. This will present to you a **Components Overview** dashboard, as depicted by Figure 4.14.

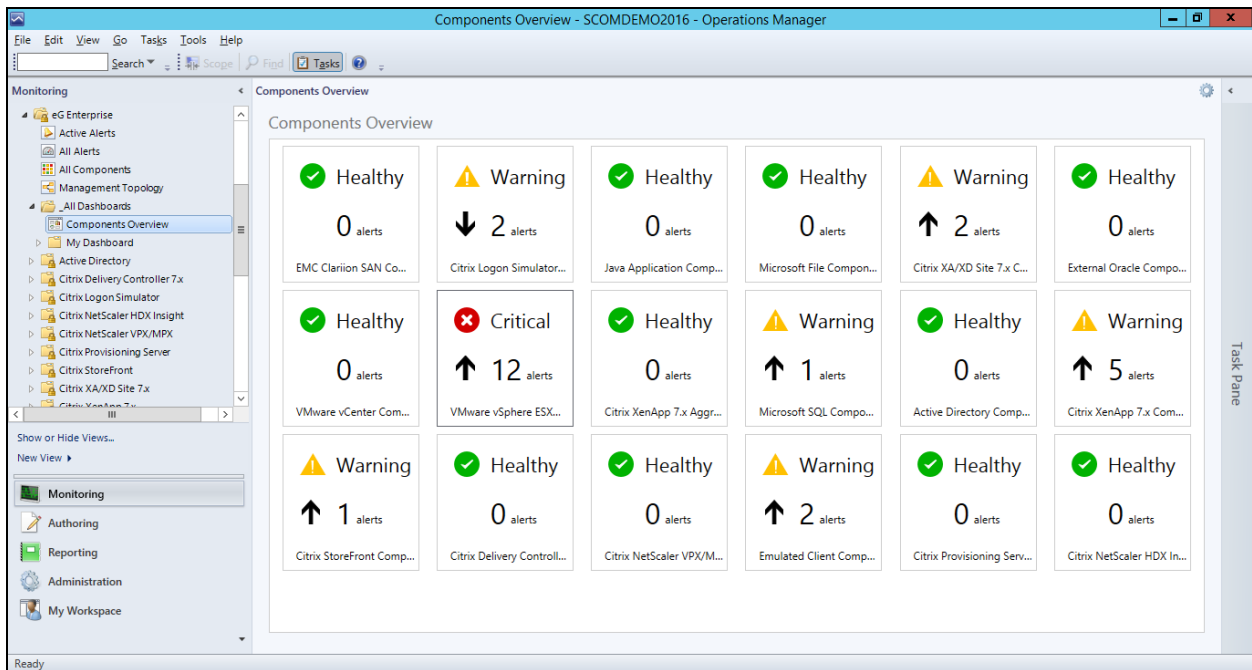


Figure 4.14: The Components Overview Dashboard

2. A quick glance at this dashboard, will reveal to you:

- The different types of components that are managed in eG Enterprise;
- The total number of problems that are currently open for each component type;
- An indicator (up or down arrow) as to whether the count of outstanding problems per component type has been increasing or decreasing with time. This is a good indicator to how problem-prone a component type is. This is also a good measure of the efficiency of help desk in resolving problems.
- The current state of every component type; typically, the state of the individual components of a type, determines the state of that component type. The type assumes the highest abnormal state of the underlying components. For instance, if 5 VMware vSphere servers are monitored, out of which one server is in a Critical state, 2 in the Major state, and 2 in the Normal state, the state of the component type will be Critical. This is because, Critical is the highest abnormal state.

3. Problematic component types can be quickly identified using this dashboard.

4. To zoom into the health of a particular component type, expand the sub-node representing that component-type under the **eG Enterprise** node in the left panel. For instance, to view the health of all components of type *VMware vSphere ESX* in the case of our example, expand the **VMware**

vSphere ESX sub-node of the **eG Enterprise** node.

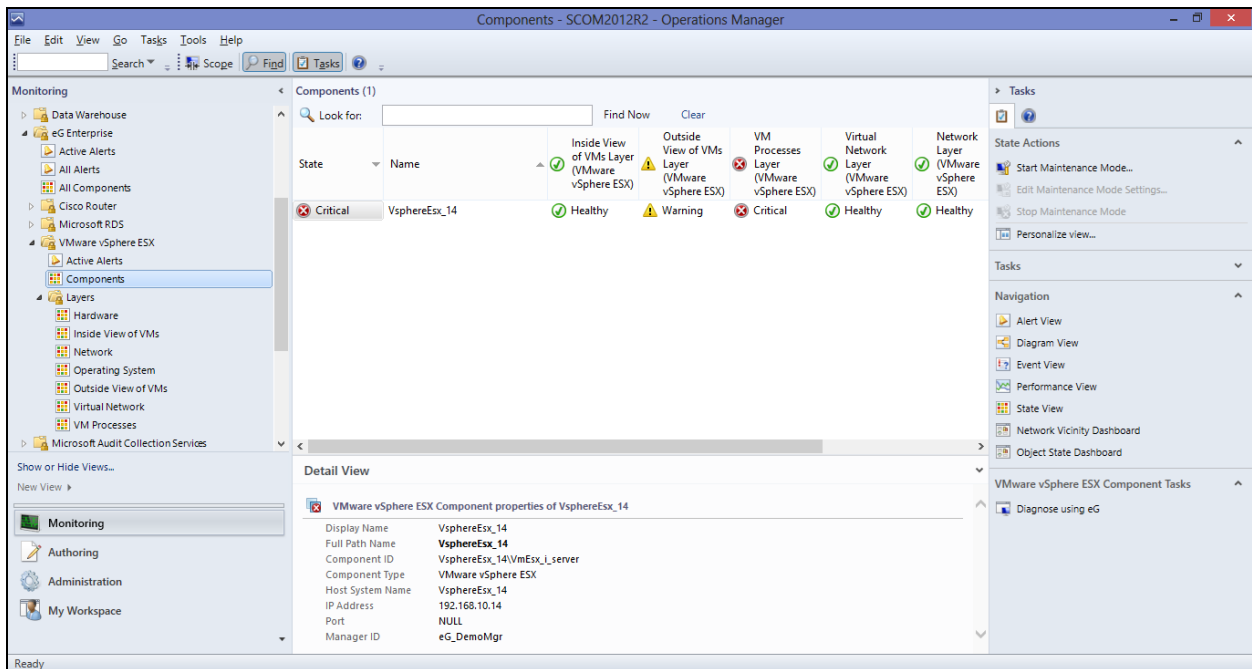


Figure 4.15: Expanding the sub-node representing a component type

5. Expanding the **VMware vSphere ESX** sub-node will provide you with the following options:

- Viewing only the **Active Alerts** pertaining to the managed *VMware vSphere ESX* servers;
- Determining the overall health of each managed component of type **VMware vSphere ESX**;
- Viewing a **Components Topology** of the **VMware vSphere ESX** component type, and graphically isolating the vSphere server that is performing poorly and the reason for its performance degradation;
- Exploring the health of every layer of every component of type **VMware vSphere ESX**, and isolating the problem layers

To view the open alarms related to VMware vSphere ESX servers, click on the **Active Alerts** sub-node. Figure 4.16 will then appear.

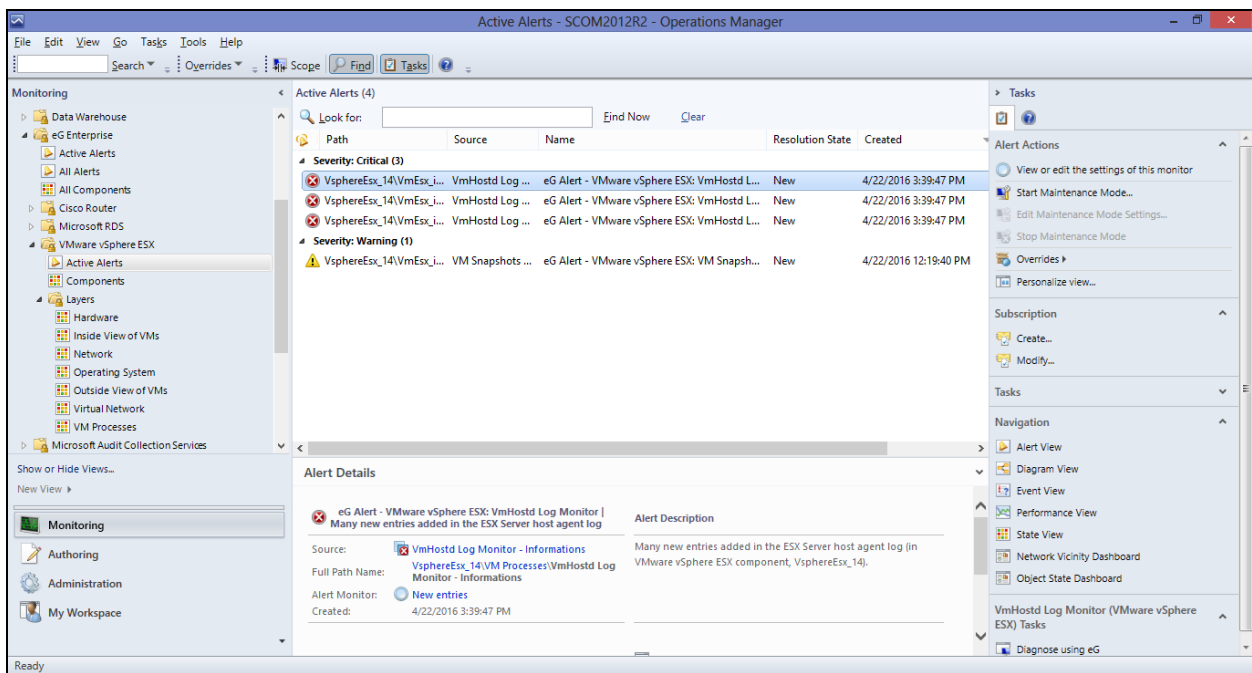


Figure 4.16: Viewing the active alerts of VMware vSphere ESX servers

6. In the right panel of Figure 4.16, you can view all the currently unresolved issues pertaining to VMware vSphere ESX servers, grouped by severity.
7. Next, if you want to know which components of type **VMware vSphere ESX** are currently managed and what their current states are, click on the **Components** sub-node under the **VMware vSphere ESX** node. You will then view the complete list of managed **VMware vSphere ESX** components and their current states in the right panel (see Figure 4.17).

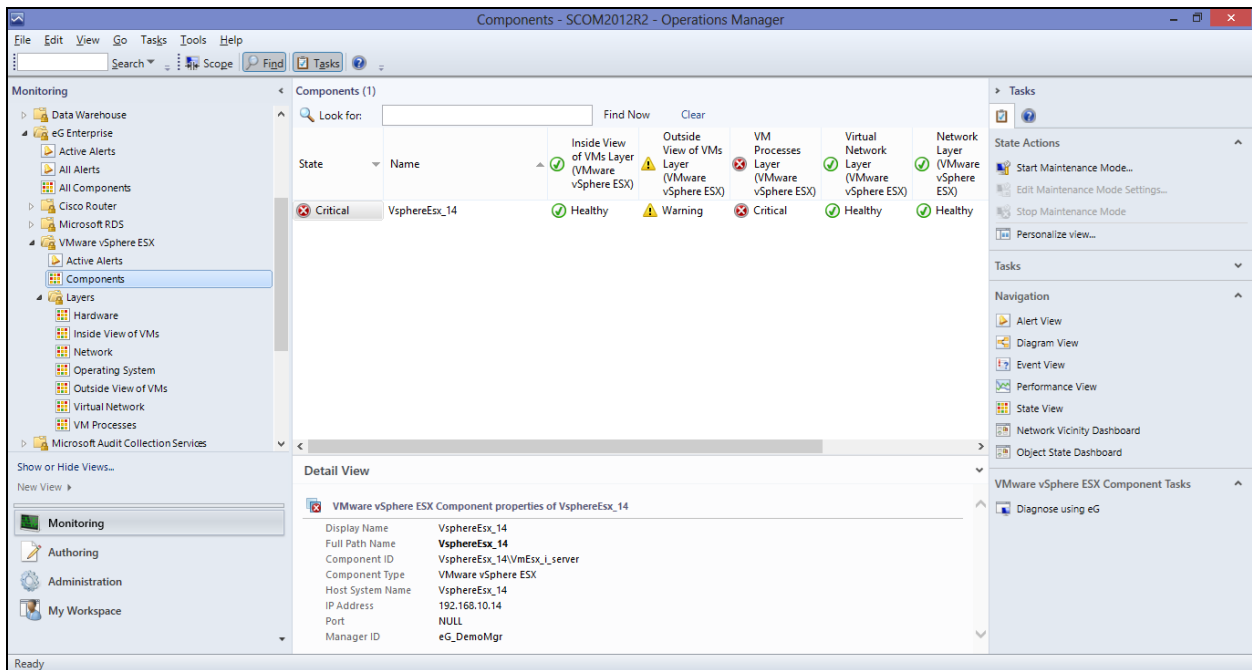


Figure 4.17: Viewing the managed components of type VMware vSphere ESX and their current state

8. In addition to the component **Name** and **State**, the right panel will also display all the layers that form the layer model of the *VMware vSphere ESX* server, and the state of each layer for every managed **VMware vSphere ESX** component. This way, you can not only identify problem components, but also accurately isolate the layers that contributed to the problem.
9. To focus on the health of the individual layers, expand the **Layers** sub-node of the **VMware vSphere ESX** node. This will reveal all the layers that are part of the built-in monitoring model that eG Enterprise offers for the *VMware vSphere ESX* server.

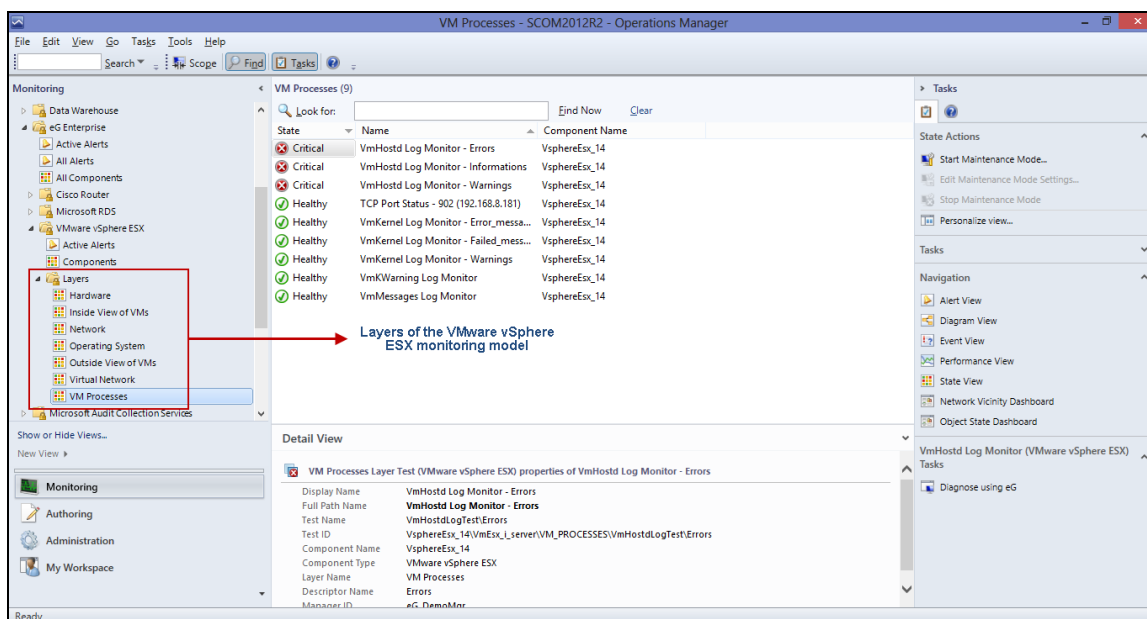


Figure 4.18: Viewing the layers as sub-nodes of the 'Layers' node

10. Then, click on a layer in the tree-structure. Upon clicking, all the tests mapped to that layer, the descriptors they support (if any), and the current state of each test will be available in the right panel (see Figure 4.18). Clicking on a row of information here will provide complete details of the test and descriptor in the **Detail View** below.
11. If a test is in a **Critical** or **Warning** state, you may want to know which measure of that test reported the abnormal measures and why. To zoom into the root-cause, you may want to launch the eG monitoring console from the SCOM console itself. For that, click on the **Diagnose using eG** option in the **Actions** pane of Figure 4.18. This will launch the eG monitoring console, where the complete layer model of the VMware vSphere ESX server will be displayed, and the problem layer, test, and measurement highlighted.

Note:

Clicking on the **Diagnose using eG** option will launch the eG monitoring console only if the **eG Console Tasks** application is installed on the system on which the SCOM console is operating. To know how to install this application, refer to Section 3.2.4. Also, when the eG console is launched for the very first time from the SCOM console, a login screen will appear, where you will have to manually key in the user credentials for logging into the eG monitoring console. The same credentials will be used to launch the eG monitoring console during your subsequent attempts to **Diagnose using eG**.

12. For a more graphical, comprehensive view of the performance of a component type, click on the

Components Topology node (see Figure 4.19). An icon representing the *VMware vSphere ESX* component type will then appear. Using an intuitive icon and a conventional color code (Red), the component-type representation clearly indicates that the *VMware vSphere ESX* component-type is in a Critical state presently. To know which vSphere servers have contributed to this abnormal state, drill down by clicking the '+' icon alongside. This will reveal all managed vSphere servers and their current state. In the case of our example, only a single vSphere server has been managed. We can infer from Figure 4.19 that this vSphere server is in a Critical state presently. To understand why, click on the '+' icon alongside the vSphere server (i.e., component) representation in Figure 4.19.

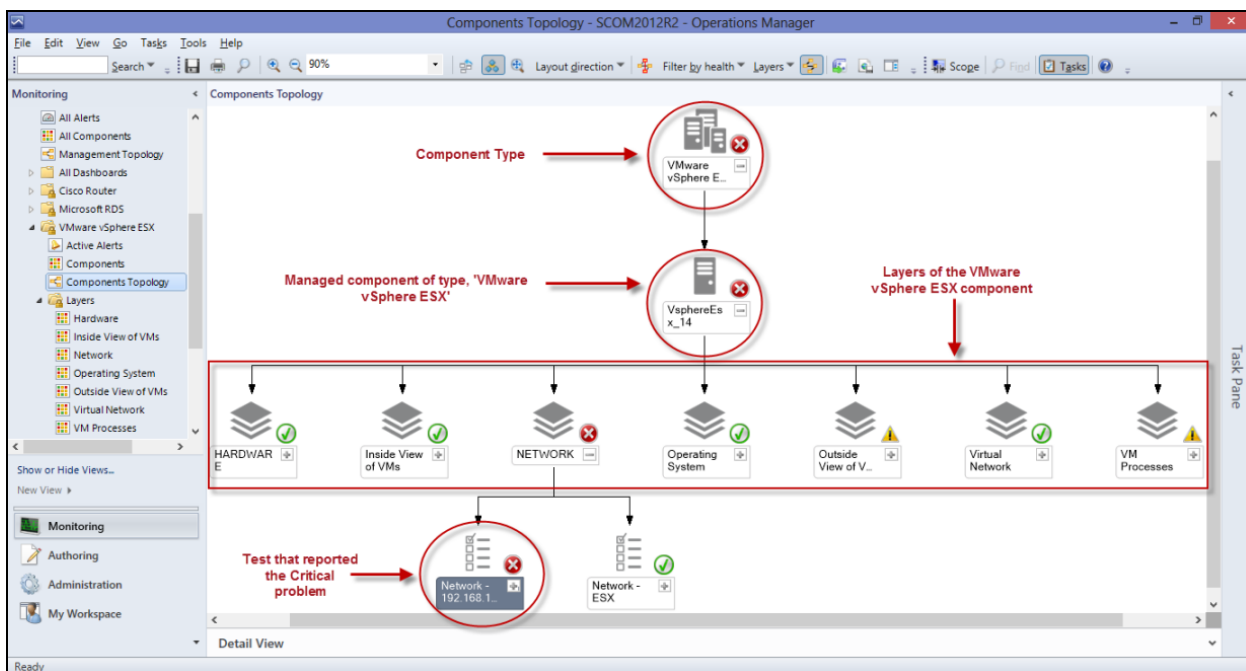


Figure 4.19: The topology representation revealing the exact component of a type, layer of component, and test mapped to the layer that is a Critical state

13. This will invoke the layer model of the VMware vSphere ESX server. Each layer will be represented as a separate object in the topology and its state will be indicated. From the layer display, it is evident that the Critical issue has been detected in the **NETWORK** layer. If you now click on the '+' icon alongside **NETWORK**, the tests mapped to that layer will appear, accurately pinpointing the test that captured the Critical issue. In the case of our example, the Critical issue has been reported by the **Network** test. To zero-in on the precise issue, right-click on the **Network** test representation in the topology and pick the **Health Explorer** option. 4.6 will then appear pointing you to the exact measure that deviated from the threshold and caused the Critical problem. As can be inferred from 4.6, a high packet loss on the network link to the VMware vSphere ESX server is what led to the Critical state of the vSphere server.

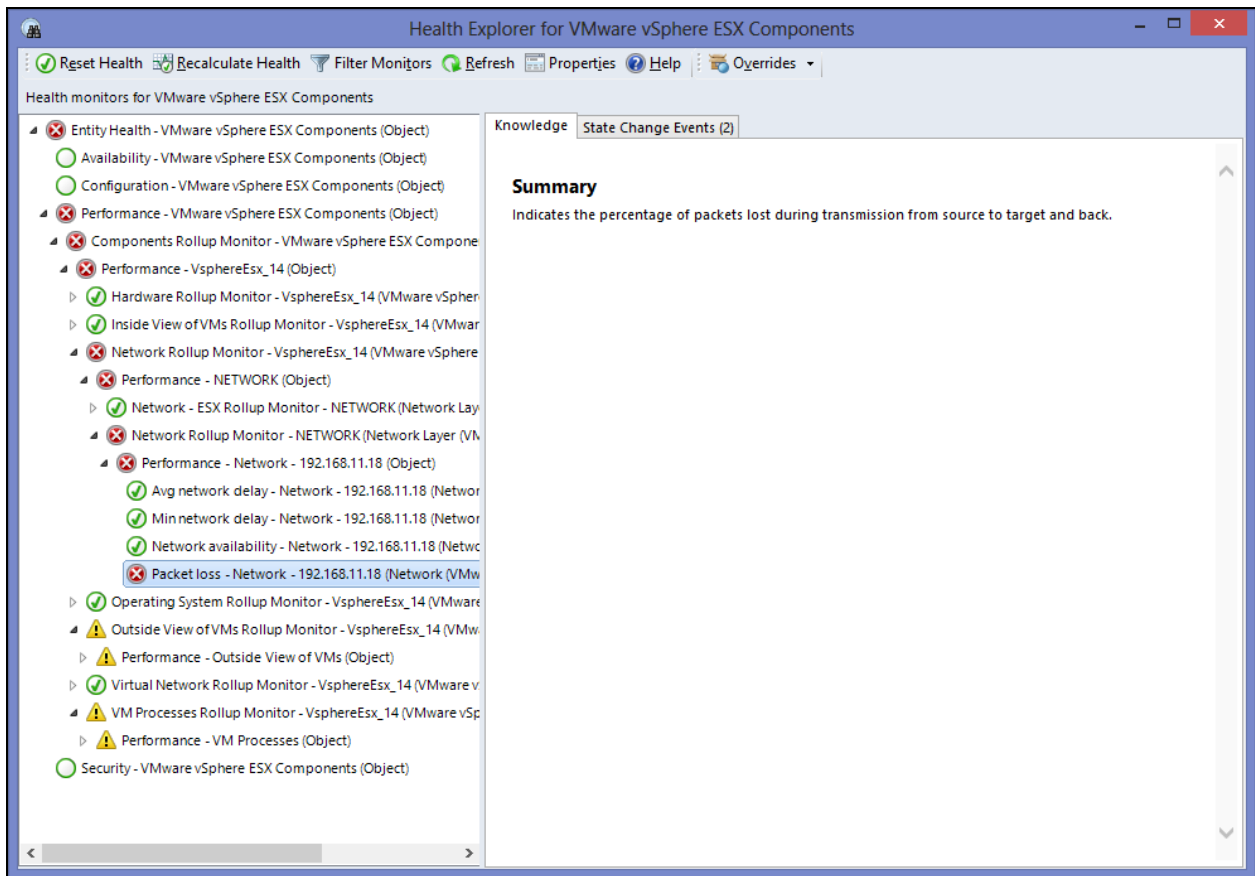


Figure 4.20: Health Explorer revealing the accurate reason for the Network problem with the VMware vSphere ESX server

4.7 Working with the Health Explorer

The health explorer provides options to troubleshoot the problems detected by health monitors. It depicts how the various health monitors inter-operate to determine the state of a monitoring object. Every measurement reported by an eG test is mapped to a corresponding health monitor in SCOM. The monitors of a test are grouped together under the **Performance** category. A rollup monitor exists for every test which automatically propagates the state of a test object into its parent layer object. Similarly, a rollup monitor exists for every layer object which automatically propagates the state of a layer object into its parent component object. This entire state hierarchy is called as **Heath Model** in SCOM.

To access the health explorer screen, do the following:

1. In the SCOM operation console, select the monitored target (component/layer/test/measure) from one of the eG views and then select the **Health Explorer** option in the **Actions** pane. In the case of our example, let us launch the **Health Explorer** for the **Warning** raised on the **VM**

Snapshots test mapped to the **OutsideView of VMs** layer of a *VMware vSphere ESX* server.

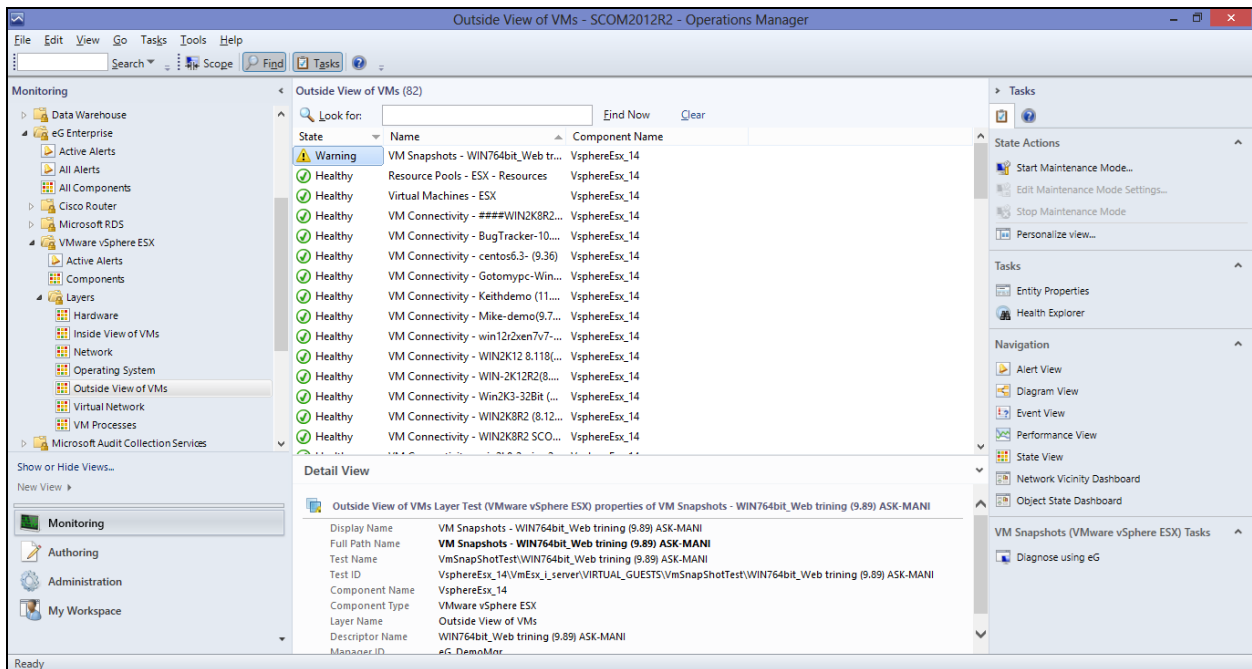


Figure 4.21: Clicking on the Health Explorer option of a test mapped to a particular layer

- Figure 4.22 will then appear. As you can see, in the left panel of Figure 4.22, all the measures of the **VM Snapshots** test (that we had earlier selected from the SCOM console of Figure 4.21) are grouped under the **Performance** node (i.e., category) as monitors. From the left panel, we can clearly infer that the **Warning** on the **VM Snapshots** test is owing to a **Warning** alert on the **Aged snapshots count** measure of the test.

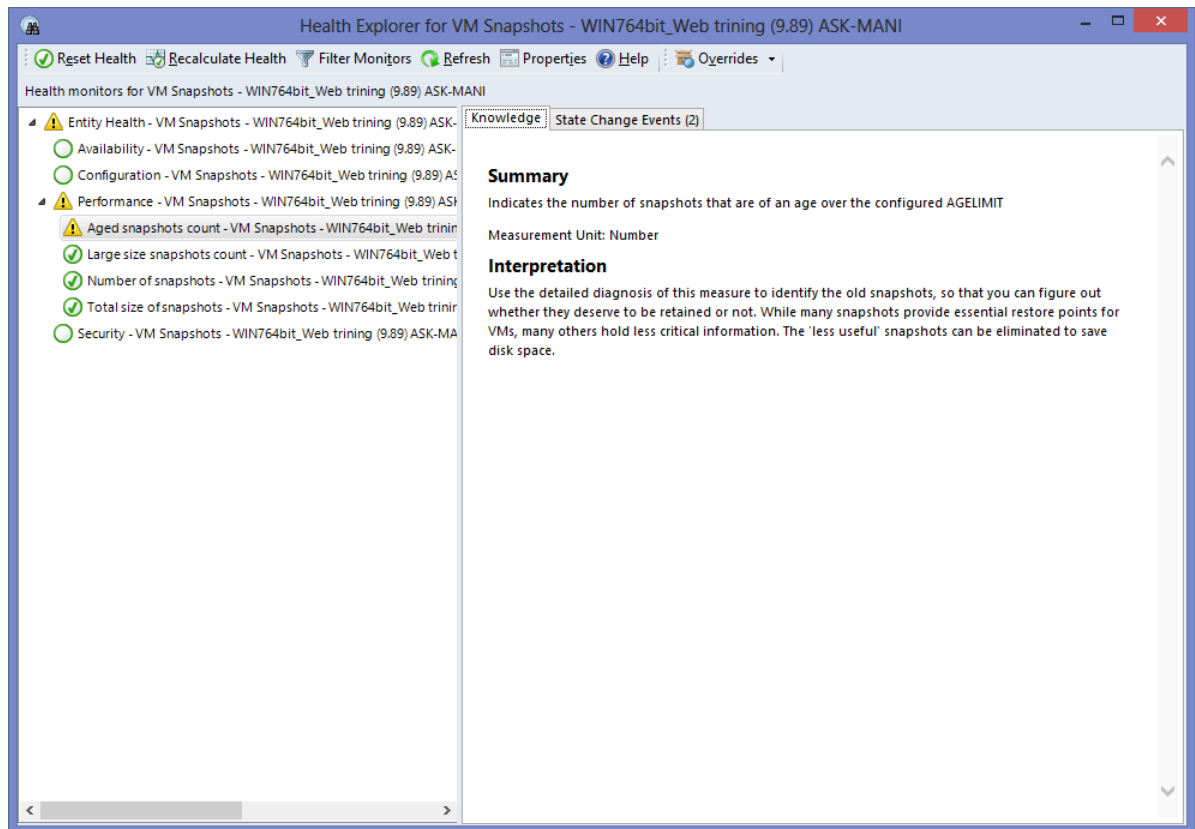


Figure 4.22: Health explorer for the VM Snapshots test mapped to the OutsideView of VMs layer of a VMware vSphere ESX server

3. The right panel comes with two tabs. In the **Knowledge** tab, you can easily and instantly view the details of the chosen measure as described in the context-sensitive help page that corresponds to the chosen test. In the **State Change Events** tab on the other hand, you can view the transitions in the state of a test/measure chosen from the left panel. For instance, in Figure 4.23 below, you can view the state transitions for the **Aged snapshot counts** measure chosen from the left panel. This way, you can easily view the state history of a test/measure and effortlessly figure out what state a test/measure has been in at what time.

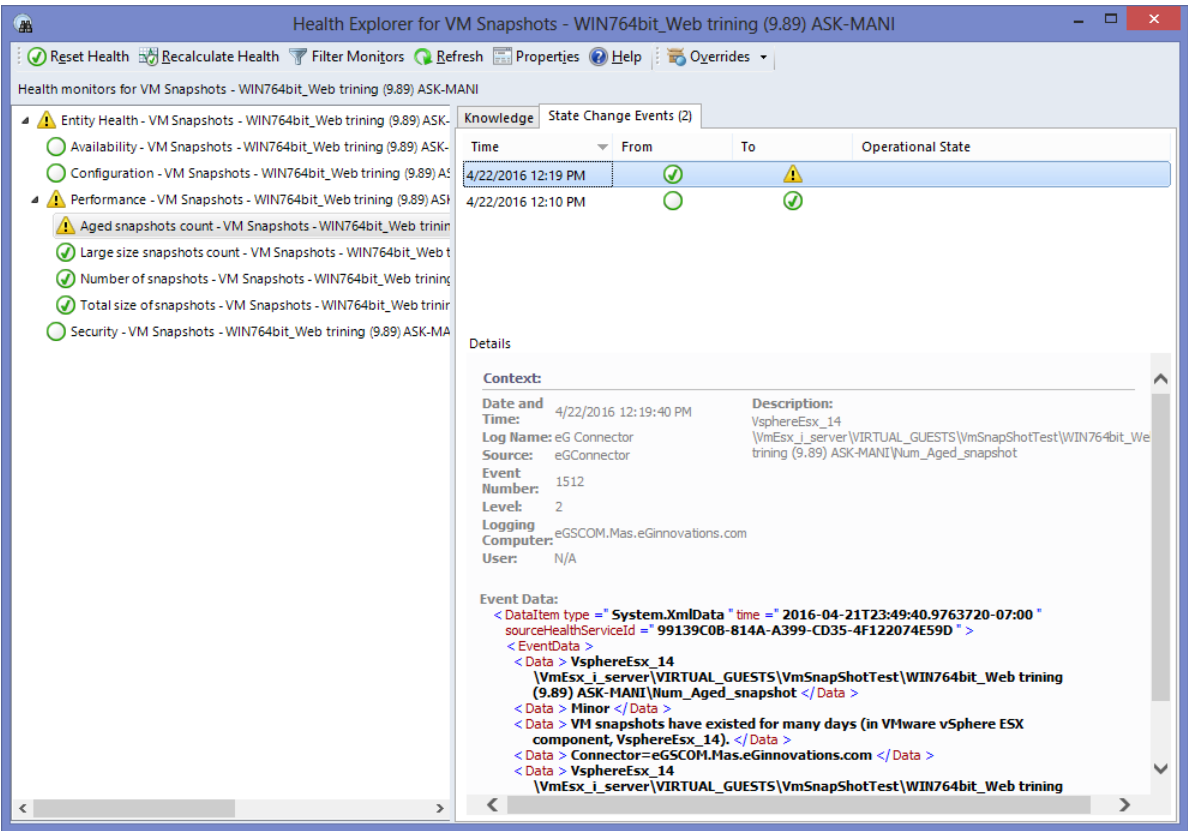


Figure 4.23: State Change Events tab

4.8 Monitoring Business Services

If you have configured one/more business services for monitoring in eG Enterprise, then post the integration with SCOM, you can use SCOM to view the current state of these business services. Moreover, in the event of a service slowdown/outage, you can even view and analyze the service topology in the SCOM console itself, and isolate the service component that could have caused the abnormality, without launching the eG monitoring console!

To achieve this, you will have to login to the SCOM console and recreate the topology of each business service that you want monitored. To help you understand this process better, let us take the example of the *infomart* service. Figure 4.24 below depicts the topology of this service.

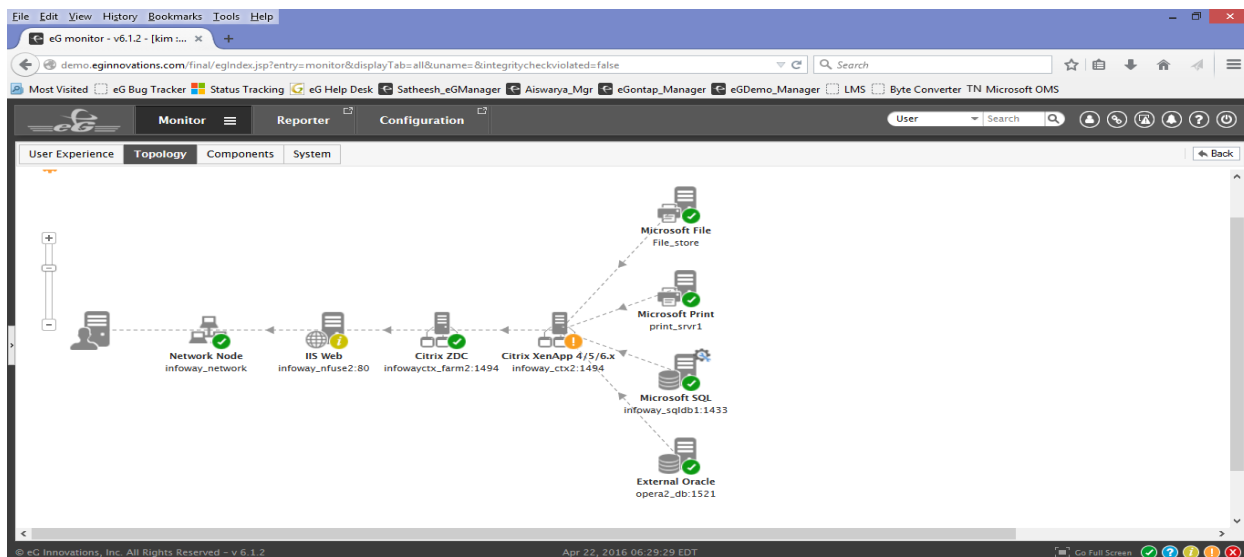


Figure 4.24: The topology of the *Infomart* service as viewed in the eG web interface

The *Infomart* service, as you can see, is a virtualized Citrix XenApp service, where the XenApp server, *Infoway_ctx2:1494*, is running on a VM configured on the ESXi server, *nyc_vm_02*. Users login to the Citrix farm via the Citrix web interface hosted on the IIS web server, *infoway_nfuse2:80*. The Citrix ZDC, *infowayctx_farm2:1494*, that balances the load on the farm, receives the user request and transmits it to the least-loaded XenApp server, *infoway_ctx2:1494*, in the farm. The XenApp server services the user request by taking help from the MSSQL database server, External Oracle server, an MS File sever, and the Print server.

To build the topology of the *Infomart* service in the SCOM console, do the following:

1. A business service in eG has to be defined as a 'Distributed Application' in SCOM. In other words, the *Infomart* service in our example, will have to be configured as the *Infomart* distributed application in SCOM. This implies that the topology that you built for the *Infomart* service in eG should be built again in SCOM for the *Infomart* distributed application. For this, first, login to the SCOM console. Then, click the **Authoring** tab page depicted by Figure 4.25 below.

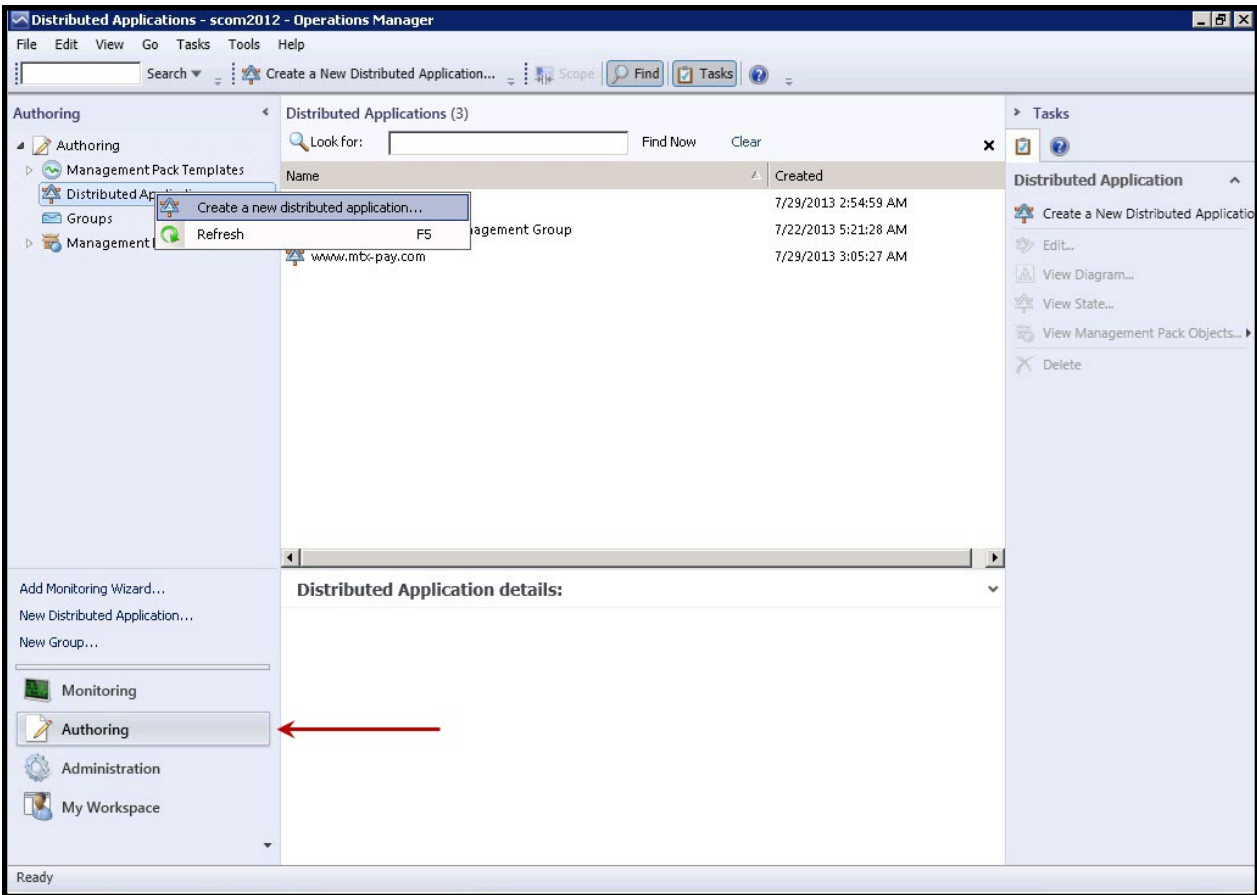


Figure 4.25: Starting Distributed Application Configuration

2. When the **Authoring** tree appears in the left panel, expand the **Authoring** node in the tree-structure, right-click on the **Distributed Application** sub-node, and pick the **Create a new distributed application** option (see Figure 4.25).
3. Figure 4.26 then appears.

Distributed Application Designer

Create a Distributed Application

1. Name Your Distributed Application
Choose a name that best matches the distributed application you want to create. You can fill a description for it if you like.

Name: **Description (optional):**

2. Choose Distributed Application Template
Select a template that most closely matches the distributed application you have deployed. A distributed application object will be created along with a set of monitors, rules, views, and reports.

Template:

- .NET 3-Tier Application
- Line of Business Web Application
- Messaging
- Blank (Advanced)

Description:
This distributed application contains presentation, business and data tiers with availability measured by synthetic transactions.

[View Details](#)

3. Save to a Management Pack
Select a management pack where your distributed application and its components will be saved.

Management Pack:

Figure 4.26: Creating a Distributed Application

- In the **Name Your Distributed Application** section of Figure 4.26, provide a unique Name to your distributed application – for easy identification, its best to name the distributed application after the business service it corresponds to. In the case of our example therefore, set *Infomart* as the **Name** of the distributed application. Next, select the **.NET 3-Tier Application** option from the **Template** list in the **Choose Distributed Application Template** section, and pick the **eG Customization Management Pack** option from the **Management Pack** drop-down in the **Save to a Management Pack** section. Finally, click the **OK** button in Figure 4.26. This will invoke the **Distributed Application Designer** window (see Figure 4.27).

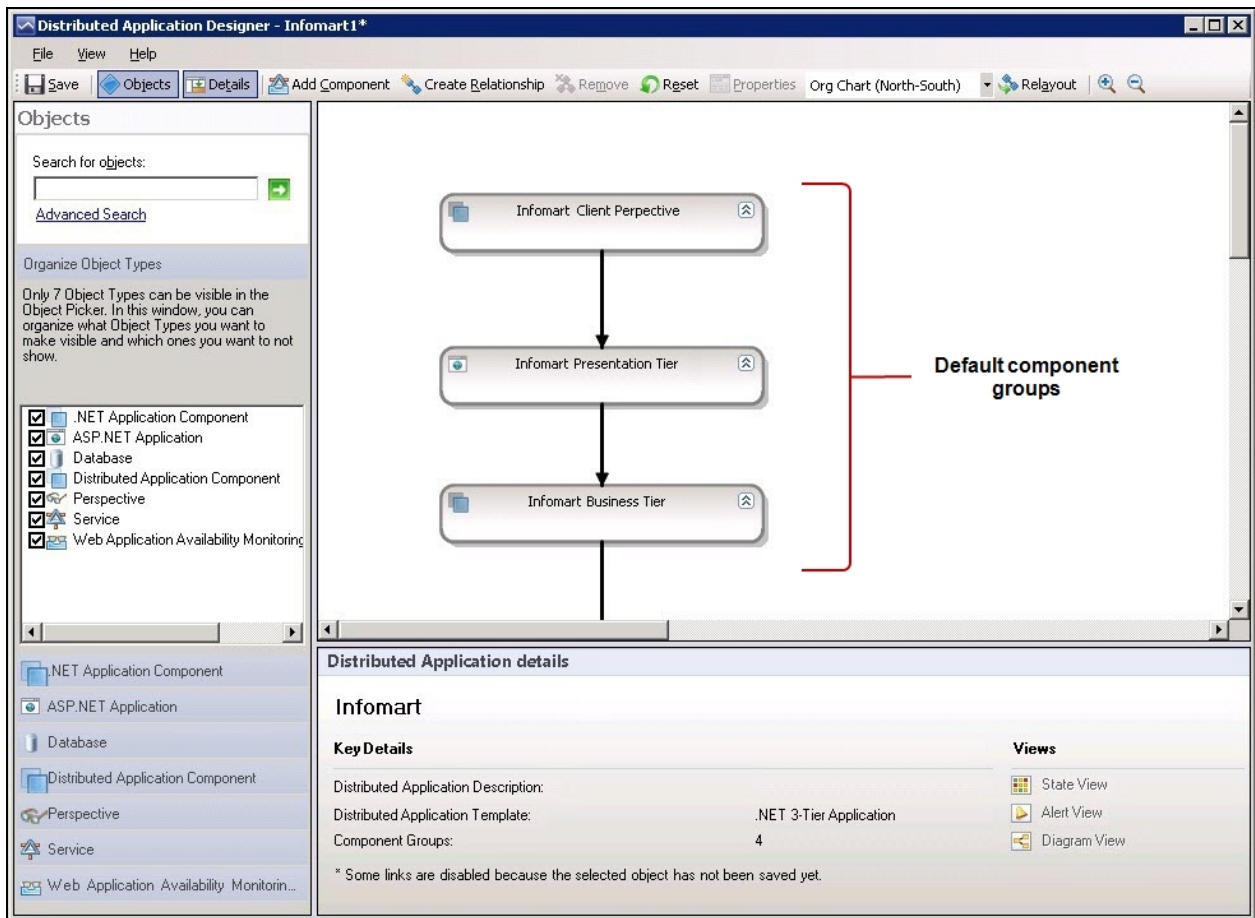


Figure 4.27: The Distributed Application Designer

5. The **Distributed Application Designer** window will display a default template for constructing the topology of the distributed application. Each 'box' in the default template represents a default component group that you can use in your service topology. As we do not intend to use this default template, delete it by selecting every 'box' in the template and pressing the **Delete** button on the keyboard. Once all the default component groups are removed, you can proceed to add new component groups (see Figure 4.28) using the **Distributed Application Designer** window.

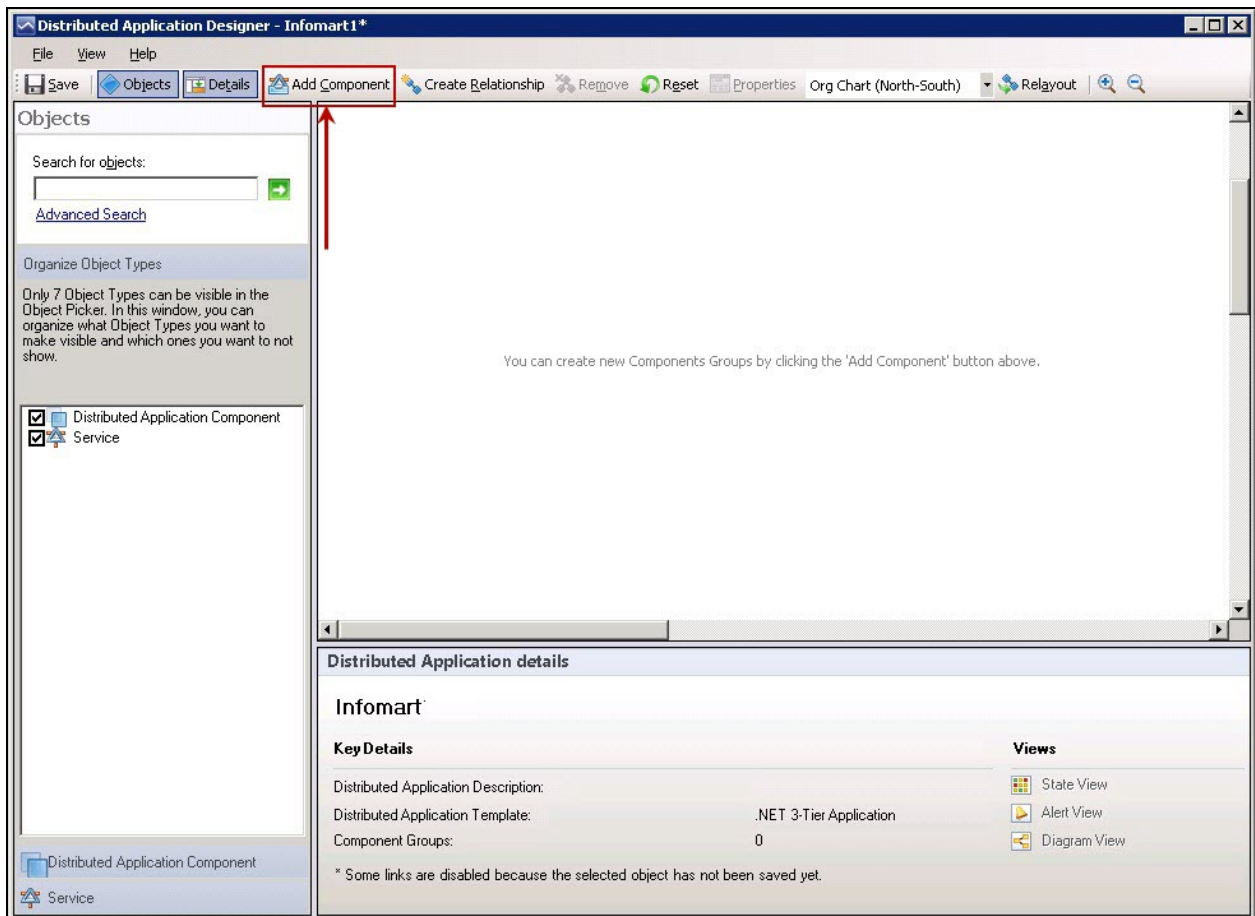


Figure 4.28: A message indicating that new component groups have to be added

6. To add a new component group, click on the **Add Component** button indicated by Figure 4.28. The **Create New Component Group** dialog box will then appear (see Figure 4.29). Let us begin topology building by adding the *Network Node* component in our example, *infoway_network*. For this, first create the *Network Node* component group using Figure 4.29 and then add the *infoway_network* component to it. To achieve this, first specify the name that you wish to assign to the *Network Node* component group in the **Name your component group** text box in Figure 4.29. For the purpose of our example, let us name this group, **NET**. Then, pick the **Objects of the following type(s)** option in Figure 4.29 and then scroll down the tree-structure below until you find the **eG Component** node (see Figure 4.30). Expand the node, and pick the **Network Node Component** group by selecting the check box alongside. Then, click the **OK** button in Figure 4.30.

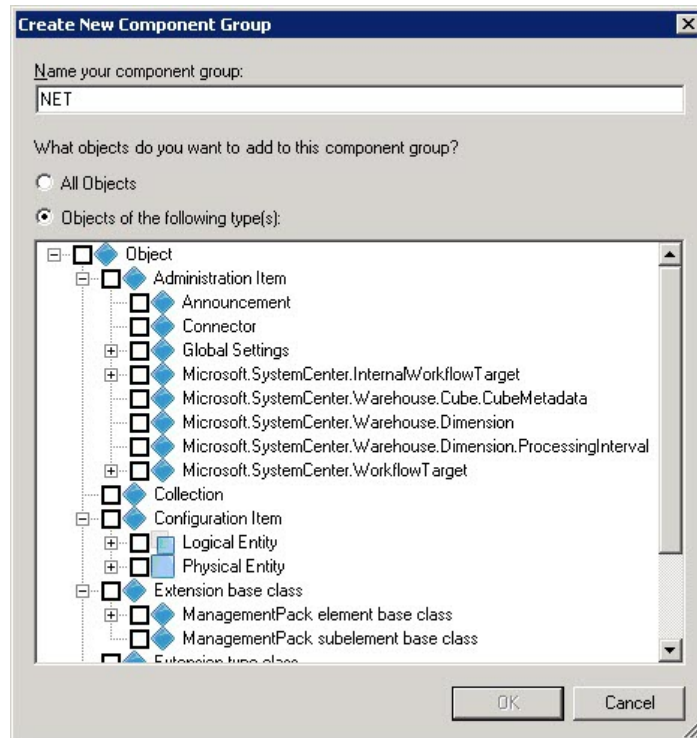


Figure 4.29: Naming the component group

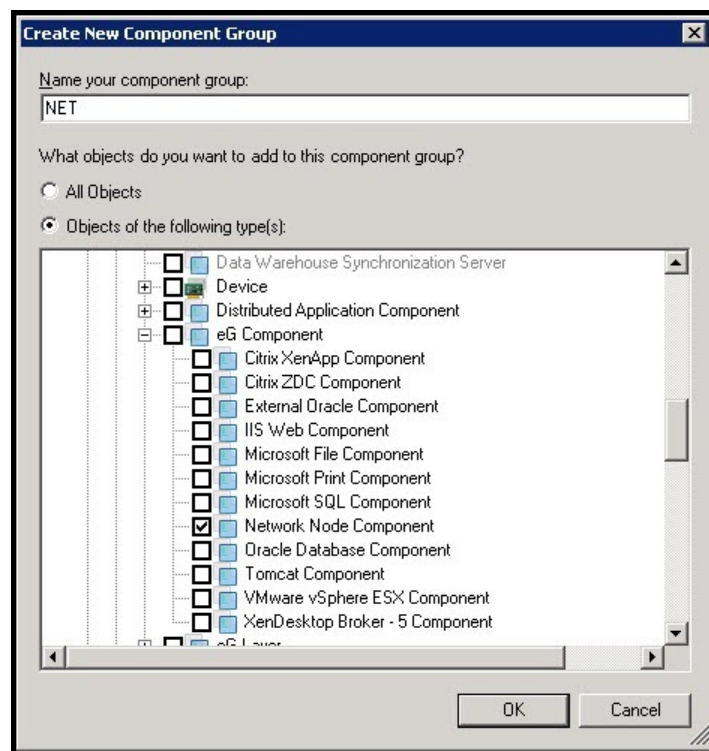


Figure 4.30: Selecting the Network Node Component group

7. This will invoke Figure 4.31. In the **Distributed Application Designer** window of Figure 4.31, you will find a 'box' representing the new **NET** component group that you just added.

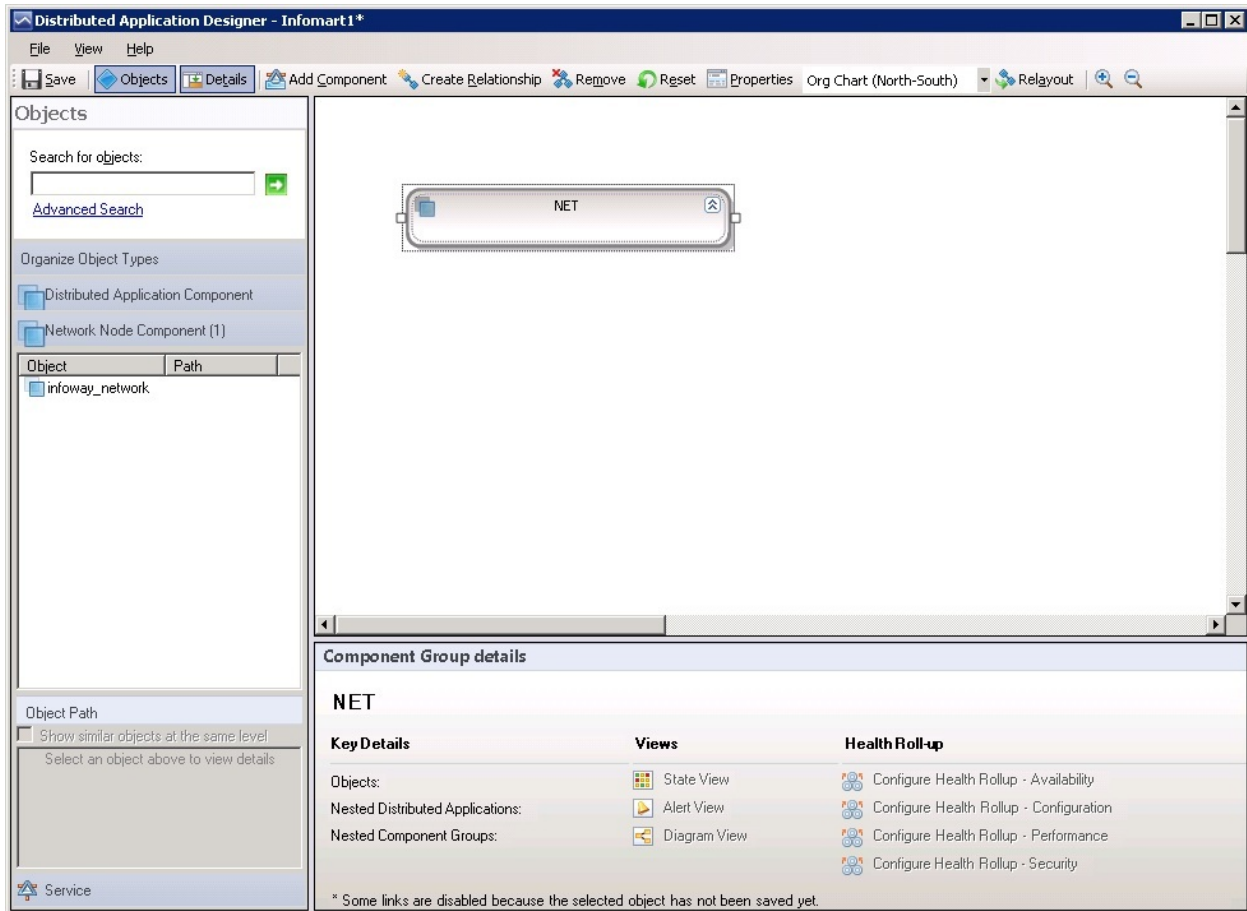


Figure 4.31: The newly added Network Node Component group appearing in the Designer window

8. Next, click on the **Network Node Component** section in the left panel of Figure 4.31 (as indicated), to view all the eG-managed network nodes. From the list that appears beneath, select the *infoway_network* component, drag it, and drop it into the **NET** box in the right panel (see Figure 4.32).

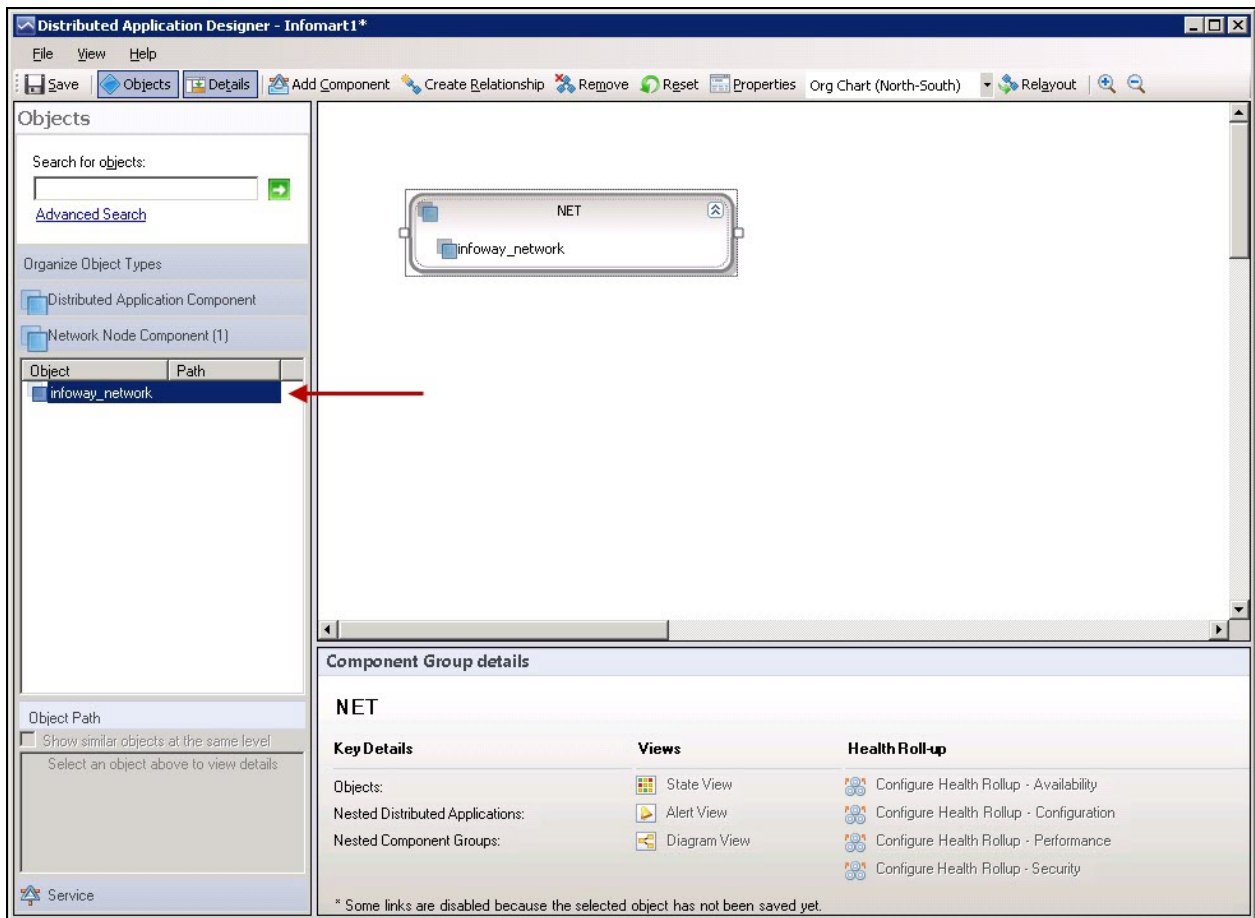


Figure 4.32: Adding the *infoway_network* component to the NET component group you created

9. With that, the **Network Node Component** group has been created, and the *infoway_network* component has been added to it. The next step is to create the IIS web server component and configure a relationship between the network node and the web server. For this, click on the **Add Component** button in Figure 4.32 again. When the **Create New Component Group** dialog box of Figure 4.33 appears, name the new component group as **IIS**, select the **Object of the following type(s)** option, scroll down the object type list, expand the **eG Component** node, and select the **IIS Web Component** group.

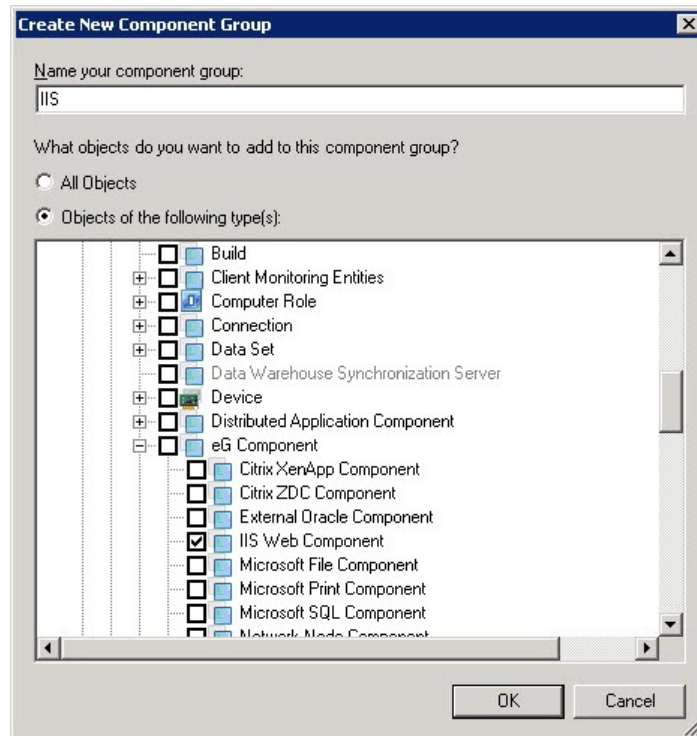


Figure 4.33: Creating an IIS Web Component group

10. The **Distributed Application Designer** window now reappears displaying a separate box for the **IIS** component group that you just created (see Figure 4.34). In the left panel of Figure 4.34, click on the **IIS Web Component** section (as indicated), select the *infoway_nfuse2:80* component from the web server list that appears, drag it, and drop it into the **IIS** box (as shown by Figure 4.35).

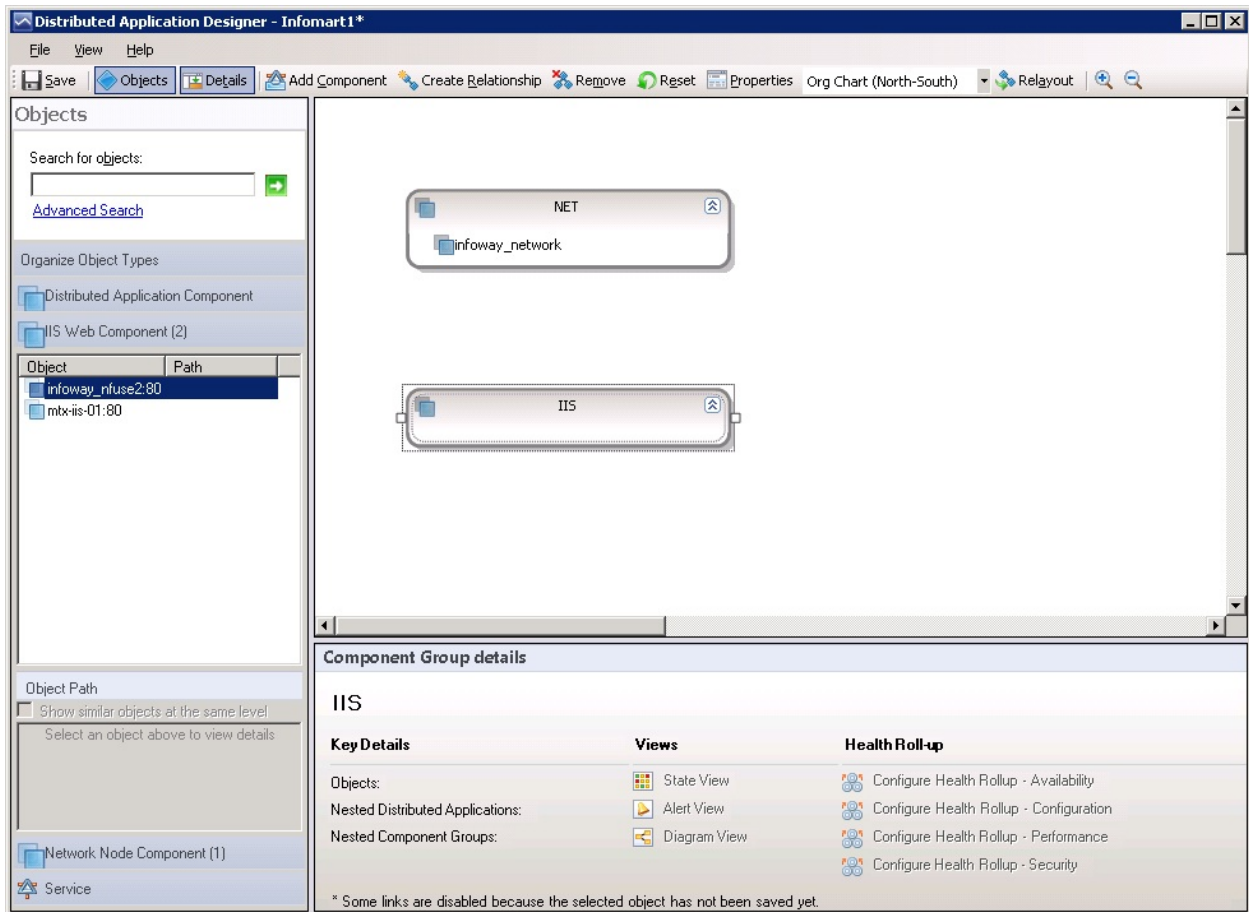
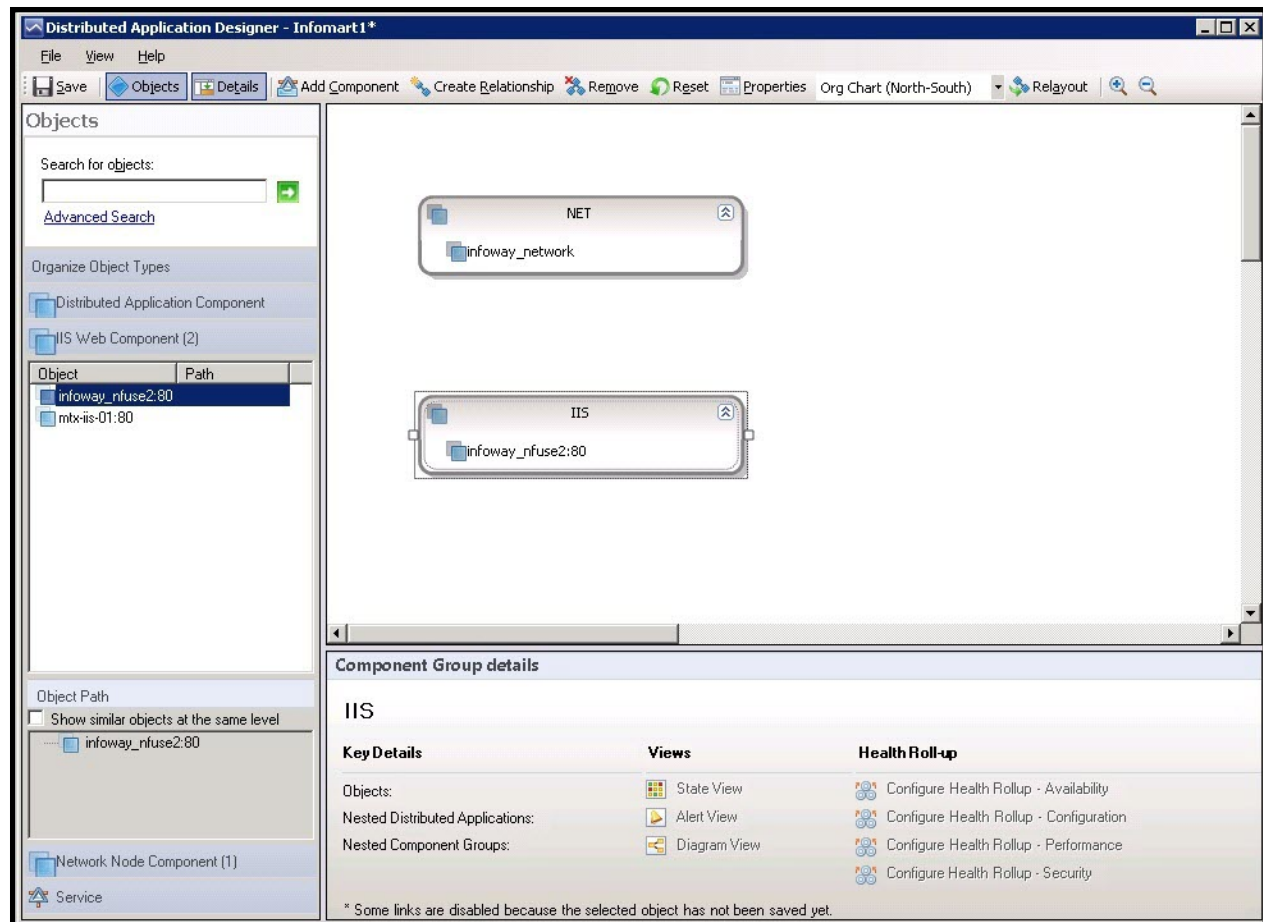


Figure 4.34: The IIS Web Component group appearing in the Designer window

Figure 4.35: Adding the *infoway_nfuse2:80* component to the IIS component group

11. Now, proceed to create a relationship between the IIS web component and the Network node component. For this, click on the **Create Relationship** button in Figure 4.35, and then draw an arrow connecting the **IIS** box in the **Designer** window with the **NET** box, as depicted by Figure 4.36. Since **IIS** is dependent on the **NET** component in our example for its functioning, the direction of the arrow should indicate the 'Uses' relationship – i.e., the arrow head should face the **NET** component. Once done, you can look up the **Reference Details** section of the **Designer** window to know whether the intended relationship has been established between the two components. For instance, in the case of our example, if this section displays the message, **IIS** uses **NET**, it is a clear indication that your 'relationship configuration' is correct.

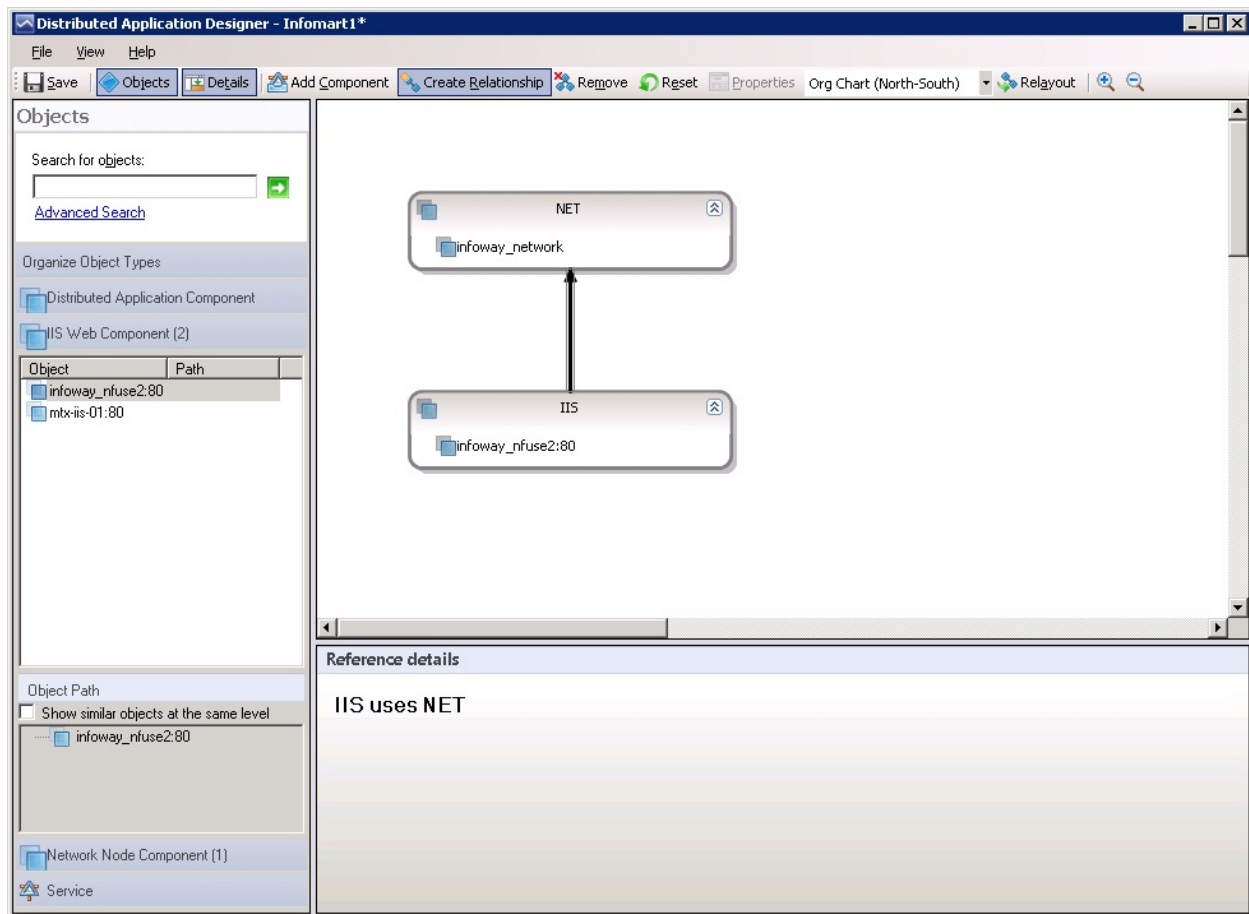


Figure 4.36: Creating a relationship between the IIS and NET components

12. Likewise, proceed to add the other component groups and components as required by the *Infomart* application, and configure the same relationship between these components as depicted by the service topology preview of Figure 4.24. Figure 4.37 below depicts the final topology of the *Infomart* application.

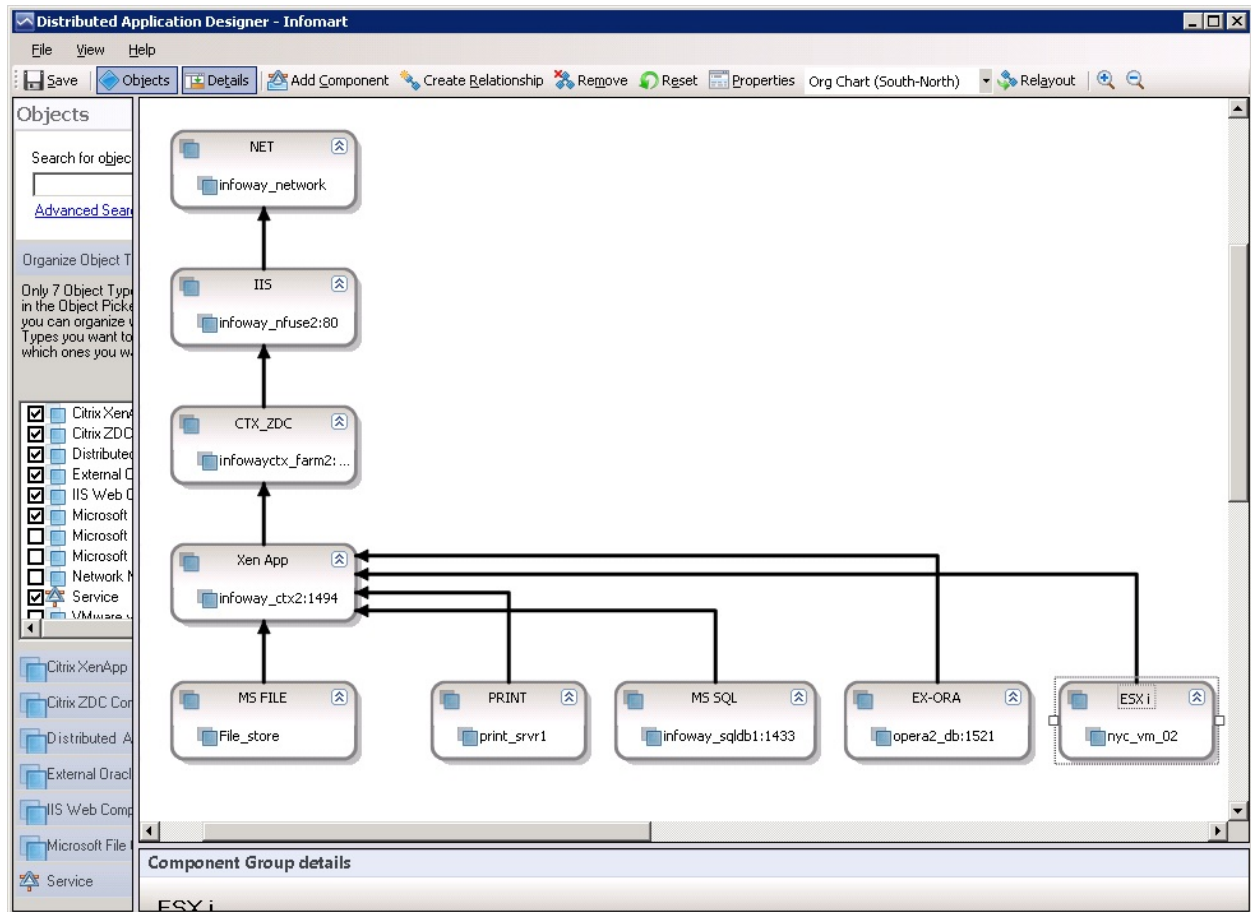


Figure 4.37: The fully-configured topology of the *Infomart* distributed application

13. With that, the topology of the distributed application has been fully configured. Once eG Enterprise is integrated with SCOM, the SCOM connector updates the state of the distributed application and its member components based on state computations performed in eG. To view the current state of the *Infomart* application, move to the **Monitoring** view, by clicking on the **Monitoring** tab page indicated by Figure 4.38. Then, click on the **Distributed Applications** sub-node in the **Monitoring** tree-structure in the left panel of Figure 4.38.

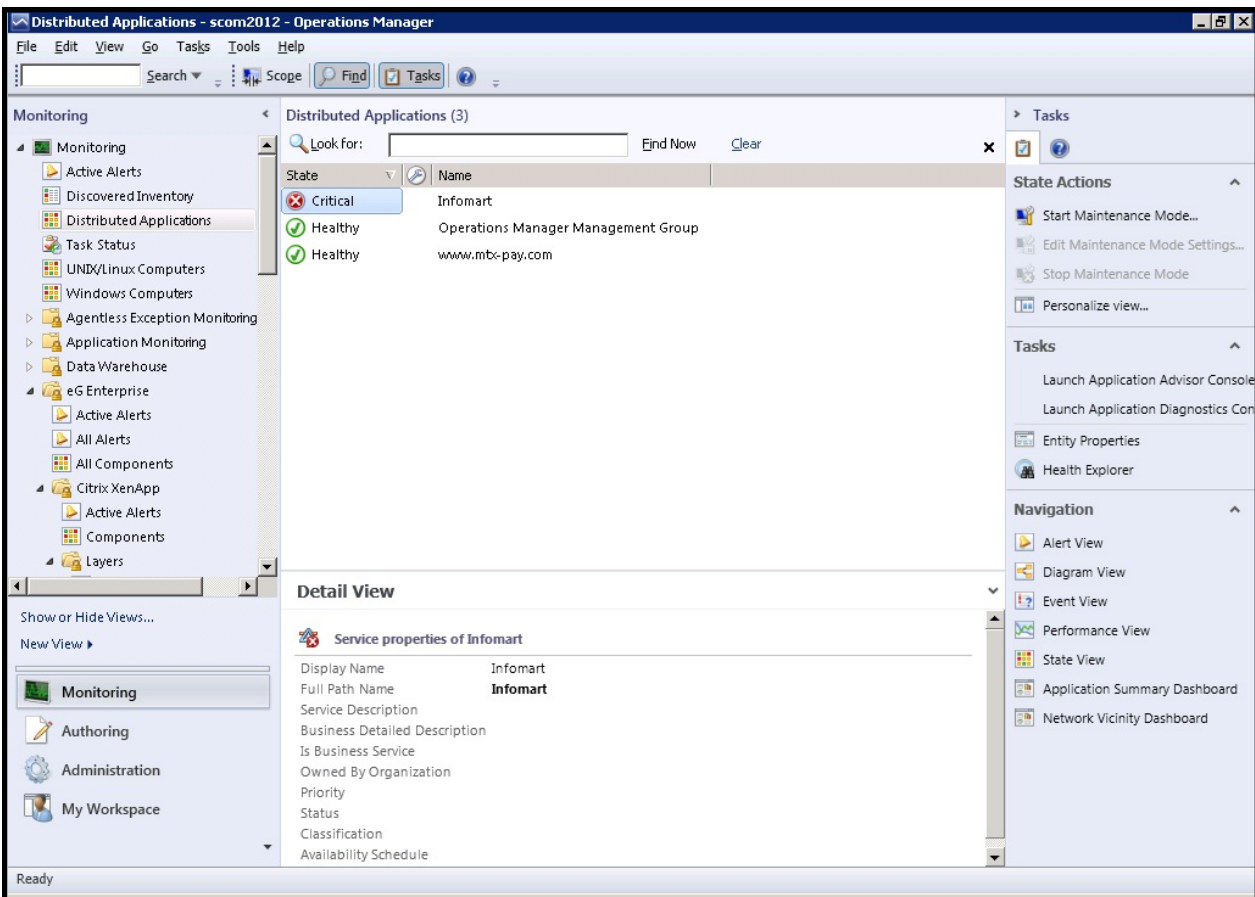


Figure 4.38: Viewing the state of the Infomart distributed application in the Monitoring mode

14. The right panel of Figure 4.38 will then display all the **Distributed Applications** that have been configured and their current state. From Figure 4.38, it is evident that the *Infomart* application is in a **Critical** state. To know which component engaged in the delivery of the *Infomart* application is responsible for this **Critical** problem, view the topology map of the *Infomart* application. For this, right-click on the **State** of that application (which is currently, **Critical**), and follow the menu sequence: Open -> Diagram View (see Figure 4.39).

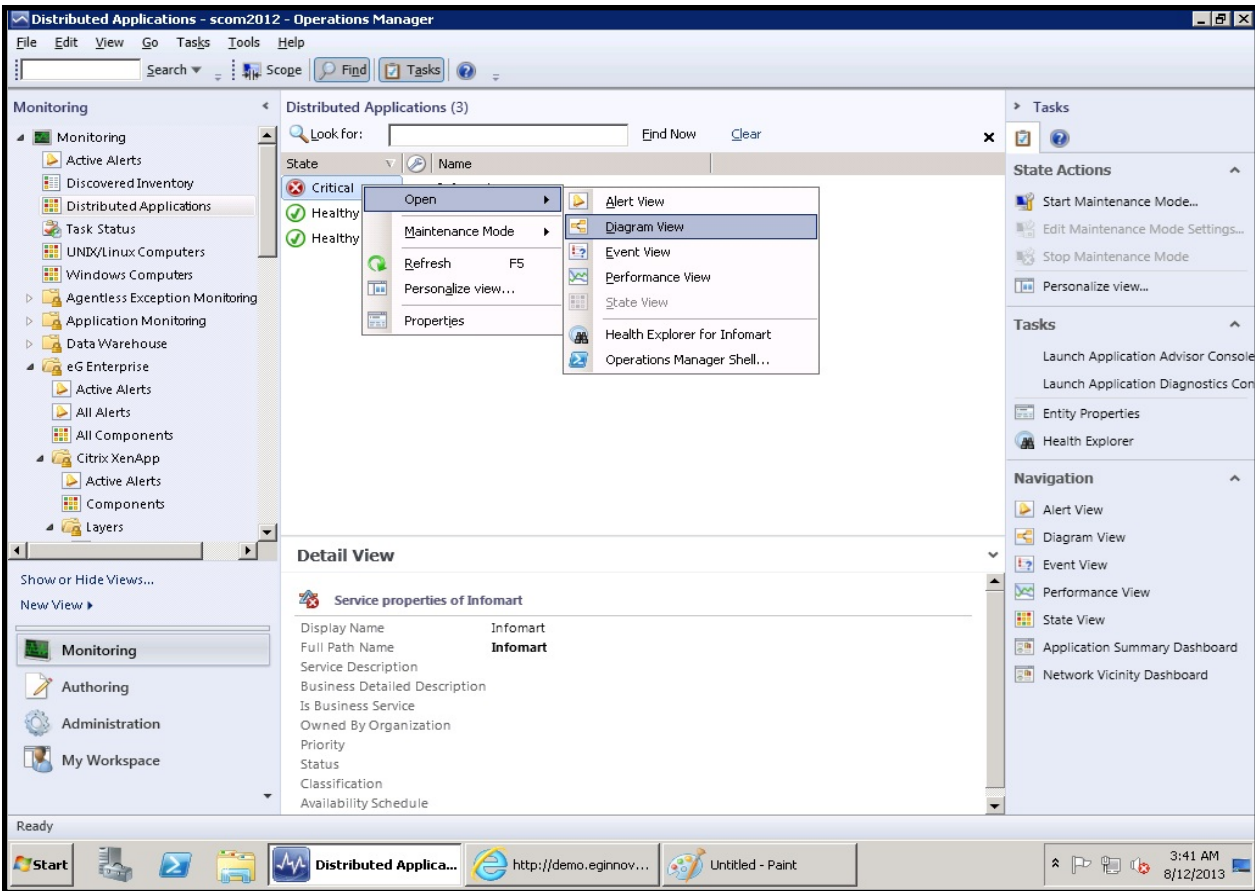


Figure 4.39: Accessing the topology map of the Infomart application in the Monitoring mode

15. Figure 4.40 will then appear, displaying an “abridged” topology of the *Infomart* application; this topology indicates that while a single component is in the **Critical** state, some components are in the **Healthy** state and some others in the **Warning** state. From Figure 4.40, we can easily infer that the **ESXi** component is in the **Critical** state and is hence responsible for the dip in the performance of the *Infomart* application. Could this **Critical** issue have caused some components to be in the **Warning** state? Only detailed investigation can confirm that. To begin with however, let us focus on the **Critical** issue with the **ESXi** component.

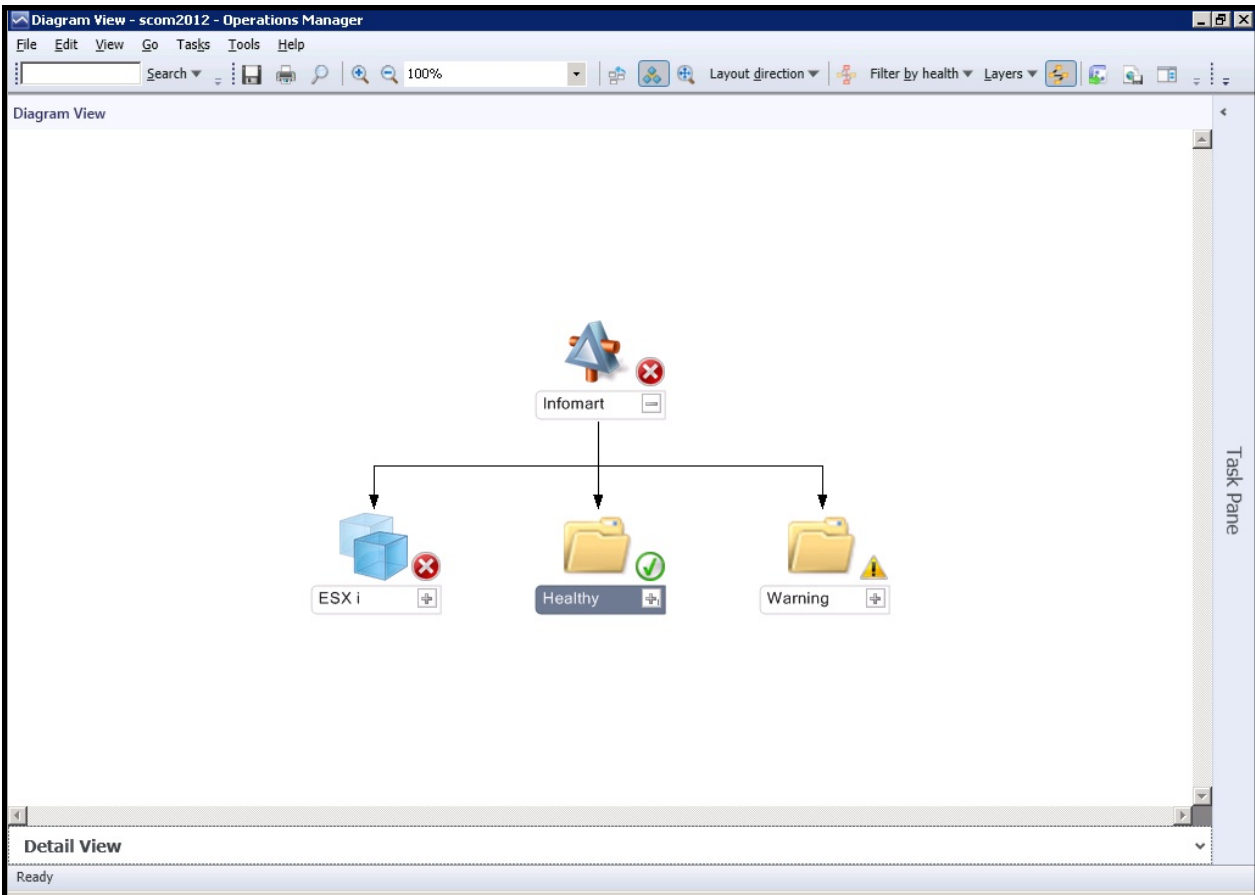


Figure 4.40: The abridged distributed application topology indicating the component in the Critical state

16. From the topology map of Figure 4.40, you can drill down further to discover where in the **ESXi** component's architecture the **Critical** issue occurred and which eG test caused it. To drill down, click on the **+** button adjacent to **ESXi** in Figure 4.40. This will reveal the name of the problematic **ESXi** component, which is *nyc_vm_02* in the case of our example (see Figure 4.41). Clicking on the **+** button next to *nyc_vm_02* will lead you to the layer in which the problem occurred – this is the **Operating System** layer in our example. By drilling one level down, you can determine the exact test that reported the problem – this is the **System – Console** test in the case of our example. It is now apparent that the **Critical** anomaly occurred in the service **console** of the *nyc_vm_02* component. From Figure 4.41, it is also clear that the **Critical** problem with the **System-Console** test has rippled and affected the performance of the **CPU-Esx** test, forcing SCOM to signal the problem with that test as a **Warning**. To know the exact measures that captured these abnormalities, you have to use SCOM's Health Explorer. Refer to Section 3.6 of this document to know how to use the Health Explorer.

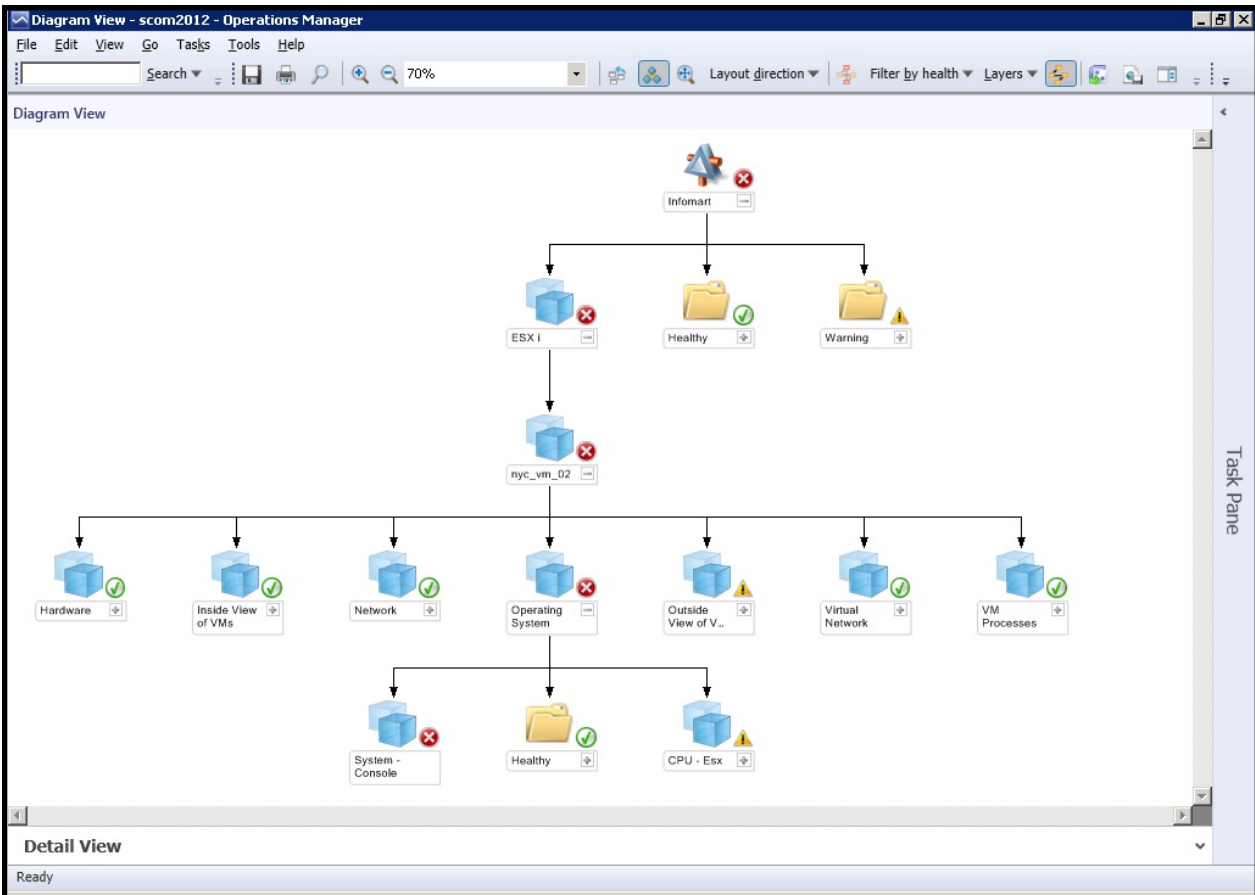


Figure 4.41: Drilling down from the ESXi component to know which eG test reported the Critical problem

17. Now, let us drill down the **Warning** node under **Infomart** in the topology map. This reveals that the **IIS** web server component and the **XenApp** server component in our example are currently in the **Warning** state, indicating that **Major** problems have been noticed in these two components. Also, the 'dotted arrow' in blue connecting the **ESXi** component and the **XenApp** component (see Figure 4.42) reveals that the XenApp server depends upon the ESXi server for its proper functioning; this implies that the **Critical** issue with the **ESXi** component impacted the performance of the XenApp server that was running on one of the VMs of the ESXi server, thus creating a **Major** problem with the XenApp server. This is how SCOM indicates cause-effect equations and helps you isolate the source of issues with your distributed applications –i.e., business services.

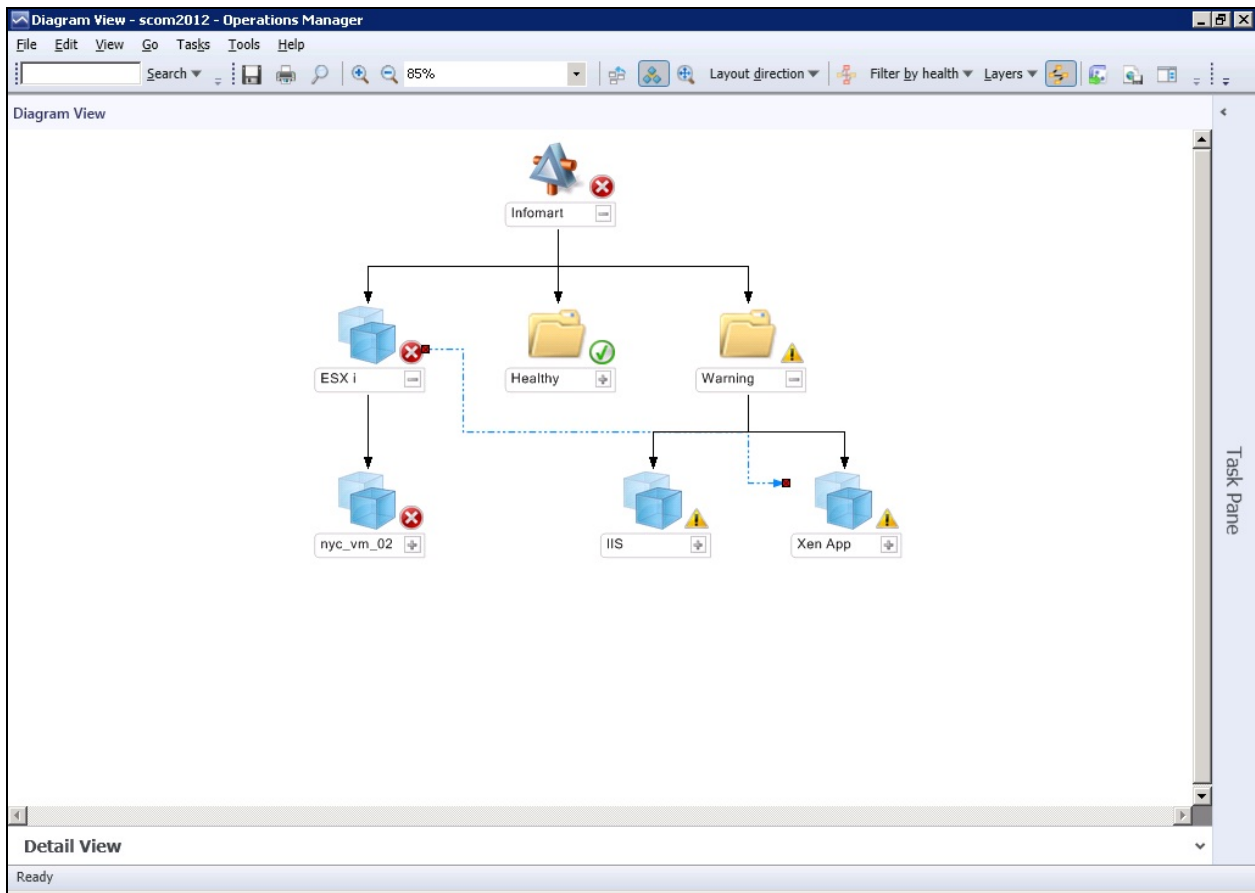


Figure 4.42: End-to-end correlation using SCOM

4.9 Publishing Dashboards

The SCOM console provides users with instant access to custom My Dashboards published from the eG monitoring console. This section explains the procedure for enabling access to these dashboards.

4.9.1 Pre-requisites for Publishing Custom MyDashboards in the SCOM Console

Before publishing the custom MyDashboards in the SCOM console, the following pre-requisites should be fulfilled:

- SCOM version should be **SCOM 2012 SP1 with Update Rollup 6 (or above)** (OR) **SCOM 2012 R2 with Update Rollup 2 or above**

- Make sure that the latest version of *Microsoft.SystemCenter.Visualization.Library.mpb* and *Microsoft.SystemCenter.Visualization.Component.Library.mpb* management packs are imported.
- MyDashboard names can include only the following characters: alphabets, integers, underscore (_), hyphen (-), and white spaces.
- Make sure that the MyDashboard is **Published** using the eG monitoring console before attempting to access it in the SCOM console.
- By default, SCOM publishes dashboards to Internet Explorer v7. However, custom dashboards published using eG can be viewed only using Internet Explorer v10 (or above). To be able to view eG dashboards in the SCOM console, you first need to make sure that the SCOM console is registered with Internet Explorer v10 (or above). To achieve this, follow the steps below:
 - On the SCOM connector host, open the command prompt as administrator and move to *eGconsoletaskHandler* setup installed directory.
 - Run the following command:
eGconsoletaskHandler.exe presetup
 - Re-open the SCOM console.

4.9.2 Automated Dashboard Views

To view the custom MyDashboards, do the following once the aforesaid pre-requisites are fulfilled:

1. Open the SCOM console.
2. Expand the **eG Enterprise** node in the left panel of the console. Then, expand the **All Dashboards** sub-node within. This will reveal the **My Dashboard** node. Expand this node to view all the MyDashboards created by or shared with the user whose credentials were used for integrating the eG manager with SCOM. To view a dashboard, click on it. The dashboard will then be displayed in the left panel (see Figure 4.43).

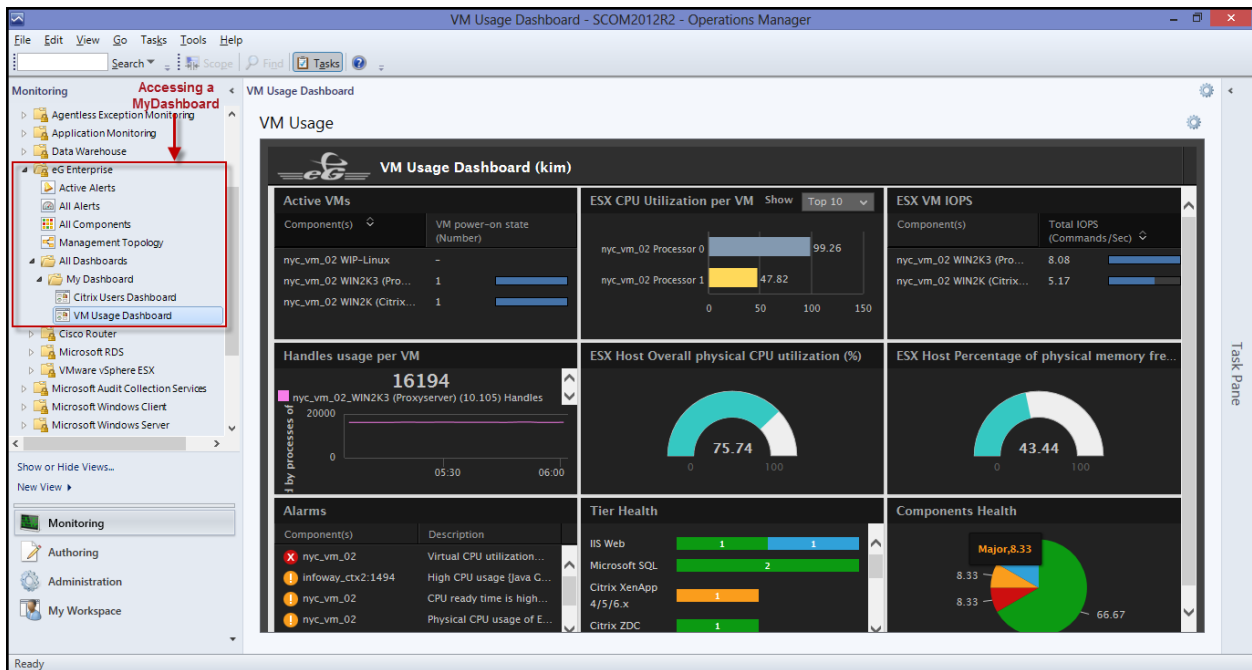


Figure 4.43: Viewing a custom MyDashboard in the SCOM console

4.10 Alert Filter

By default, all eG alarms are displayed in the SCOM console. If required, you can have eG alarms of specific priorities/severities alone to be displayed in the SCOM console. To achieve this, do the following:

1. Edit the **eg_scom.ini** file in the `<EG_MANAGER_INSTALL_DIR>\manager\config` directory.
2. By default, the **StatePriority** parameter in the **[MISC_ARGS]** section is set to *All*, indicating that all eG alarms are displayed in the SCOM console by default.
3. To ensure that alarms of a specific priority are alone displayed in the SCOM console, set the **StatePriority** parameter to a specific priority. For instance, to display only Critical alarms in the SCOM console, your specification should be:

StatePriority=Critical

4. You can even provide a comma-separated list of priorities against **StatePriority**. For instance:

StatePriority=Critical,Major

5. Finally, save the file.

4.11 Performance Tuning of the eG SCOM Connector

To minimize the load on the SCOM connector and to ensure its peak performance at all times, eG Enterprise sends the measures of only the ‘abnormal’ descriptors to the SCOM connector by default. This default setting is governed by the *DisplayDescriptors* parameter and the *DescriptorsToTransmit* parameter in the **eg_scom.ini** file (in the <EG_INSTALL_DIR>\manager\config directory). By default, the *DisplayDescriptors* flag, which is in the **[MISC_ARGS]** section of the file, is set to *concise*. This indicates that measures reported by a concise set of descriptors alone will be communicated to the SCOM connector. To know which are these descriptors, take a look at the default setting of the *DescriptorsToTransmit* parameter in the **[CONCISE_SETTINGS]** section of the file. This parameter is set to *bad* by default. This indicates that measures of ‘abnormal’ descriptors will only be transmitted to the SCOM connector at all times. For instance, take the case of the *Disk Space* test, which reports metrics for descriptor *C* and *D*. Say that the descriptor *C* is in an abnormal state and *D* is in a normal state. In this case, the default setting of the *DescriptorsToTransmit* parameter will ensure that only the descriptor *C* and its measures are sent to the connector, and not descriptor *D*.

If you want the measures of all descriptors of all tests to be transmitted to the SCOM connector, regardless of their state, then set the *DisplayDescriptors* parameter to *All*. Once this is done, then the **[CONCISE_SETTINGS]** section and the parameters within will no longer apply.

On the other hand, if you want the measures of all descriptors (i.e., both normal and abnormal descriptors) of ‘abnormal’ tests alone to be transmitted to the SCOM connector, then, do the following:

1. Set the *DisplayDescriptors* parameter in the **[MISC_ARGS]** section to *concise*.
2. Set the *DescriptorsToTransmit* parameter in the **[CONCISE_SETTINGS]** section to *all*.

In this case however, normal tests and their descriptors will be disregarded. For instance, if the descriptor *C* of *Disk Space* test is in an abnormal state and descriptor *D* is in a normal state, then the measures of both descriptor *C* and *D* will be sent to the SCOM connector. However, if a *Disk Activity* test exists, with all descriptors in a normal state, then this test and all its descriptors will be ignored.

Since the *all* setting of the *DescriptorsToTransmit* parameter ensures that even normal descriptors (of abnormal tests) are considered, the connector may sometimes experience a descriptor overload – this is commonplace where tests report metrics for hundreds of descriptors. To minimize load on the connector under such circumstances, a *DescriptorMaxLimit* parameter is available in the **[CONCISE_SETTINGS]** section. This parameter applies only if the *DisplayDescriptors* flag is set to *concise* and the *DescriptorsToTransmit* parameter is set to *all*. By default, the *DescriptorMaxLimit*

parameter is set to 10. This means that for each 'abnormal test' (that supports descriptors), eG Enterprise will send the measures of a maximum of 10 descriptors alone to the SCOM connector. These 10 descriptors will include both normal and abnormal descriptors. If the 'abnormal' test supports more than 10 descriptors, then eG Enterprise will automatically send the measures of the 'abnormal' descriptors alone to the SCOM connector.

4.12 Updating SCOM with Measure-level Changes Made After Deploying the eG Universal MP

By default, after the eG manager is integrated with SCOM, if any *measure-level* changes are made using the eG management console, then such changes will not be reflected in the SCOM console. These changes include:

- Adding/removing a new measure using the Integration Console plugin
- Changing the display name of a measure using the Integration Console plugin
- Removing an aggregate measure from an aggregate test
- Changing the display name of an aggregate measure
- Adding an aggregate measure to an aggregate test

To update SCOM with these changes, do the following:

- a. Stop the eG SCOM Connector service.
- b. Open the command prompt on the Connector host as an *administrator* and switch to the **<EG_SCOM_CONNECTOR_INSTALL_DIR>**.
- c. Run the following command:

MpconfigSyncup.exe

- d. Finally, start the eG SCOM Connector service

Note:

If you change the display name of the measure of a pre-defined Performance Rating test post the eG- SCOM integration, then this change will not be supported by the Connector, even if **MpconfigSyncup** is used.

You can enable debugging of the **MpconfigSyncup** tool using the **MPConfigSyncUp.exe.config** file. Once debugging is enabled, an **MpConfigSyncUp.log** file will be created in the **Logs** folder in the **<EG_SCOM_CONNECTOR_INSTALL_DIR>**.

Chapter 4: Uninstalling the eG SCOM Connector

Uninstalling the eG SCOM Connector involves the following broad steps:

1. Deleting the connector service from the local machine
2. Deleting the connector configuration from the SCOM server
3. Deleting the eG management pack from the SCOM server
4. Removing the installation files of the eG SCOM Connector from the connector host
5. Uninstalling the eG SCOM Console tasks

While the top 3 steps are to be performed using the **Configuration & Setup Tool** of the eG SCOM Connector, the last two steps require that you use the Windows Control Panel.

This chapter discusses these steps in detail.

4.13 Deleting the Connector Service, the eG SCOM Connector Configuration, and the eG Management Pack

To remove the eG management pack and connector configuration from the SCOM server, and to delete the connector service from the connector host, do the following:

1. Launch the **Configuration & Setup Tool** using the menu sequence *Start -> Programs -> eG SCOM Connector*.
2. When the **Connector Configuration & Setup** dialog box appears (see Figure 4.44), click on the **Setup** tab page therein.

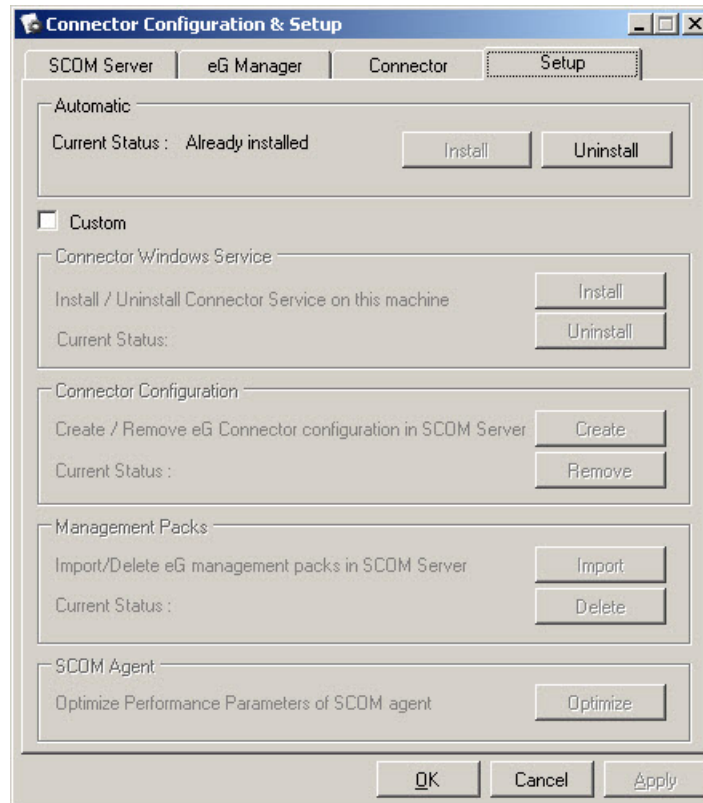


Figure 4.44: Clicking on the Setup tab page for uninstalling the connector configuration

- Click on the **Uninstall** button in the **Automatic** section of Figure 4.44. This will invoke Figure 4.45, which will list all the **Tasks** the uninstallation will perform.

Uninstall Tasks		
	Tasks	Status
	Uninstall Connector Service	
	Remove Connector Configuration	
	Delete eG Management packs	
		<input type="button" value="Execute"/> <input type="button" value="Close"/>

Figure 4.45: The tasks performed by the uninstallation

- Click on the **Execute** button in Figure 4.45 to begin performing the **Tasks** listed. The uninstallation process will perform each task automatically and update the **Status** column of Figure 4.45 accordingly. When all tasks are completed, the **Status** column will indicate the same (see Figure 4.46).

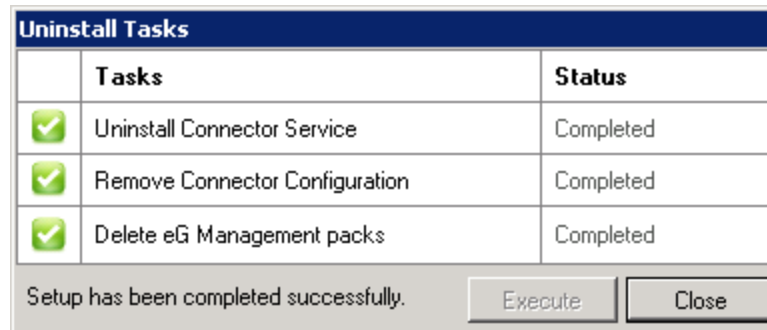


Figure 4.46: Completion of all uninstallation tasks

5. Click the **Close** button in Figure 4.46 to close the **Uninstall Tasks** window.

4.14 Removing the Installation Files of the eG SCOM Connector from the Target Host

To achieve this, do the following:

1. Login to the eG SCOM Connector host.
2. Go to Start -> Control Panel -> Add/Remove Programs
3. Select the **eG SCOM Connector** service from the list of Programs installed on that host, and click on **Remove**.
4. Figure 4.47 will then open. Click the **Next** button to proceed.



Figure 4.47: The Welcome screen of the uninstallation

5. From Figure 4.48 that then appears, pick the **Remove** option to uninstall the connector.

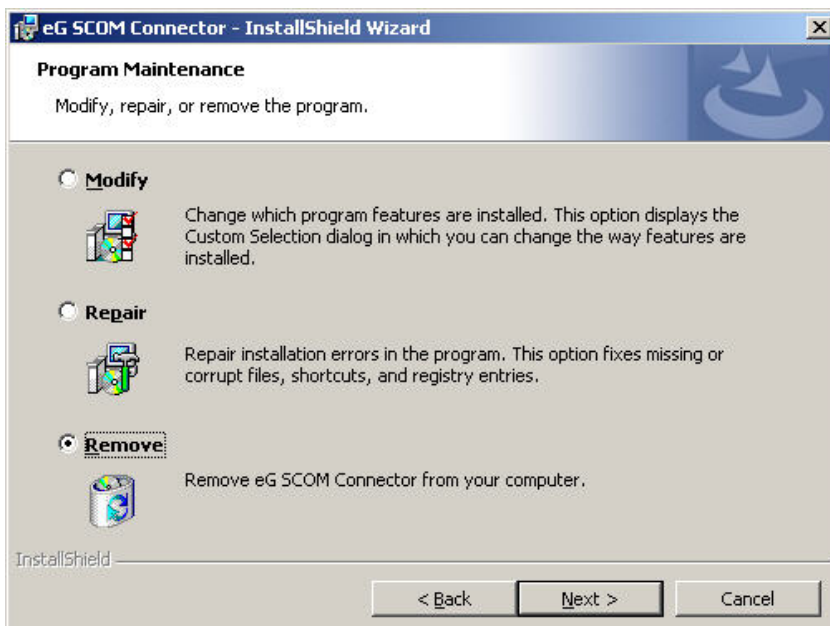


Figure 4.48: Select the Remove option

6. When Figure 4.49 appears, click the **Remove** button here to confirm the uninstallation of the connector.

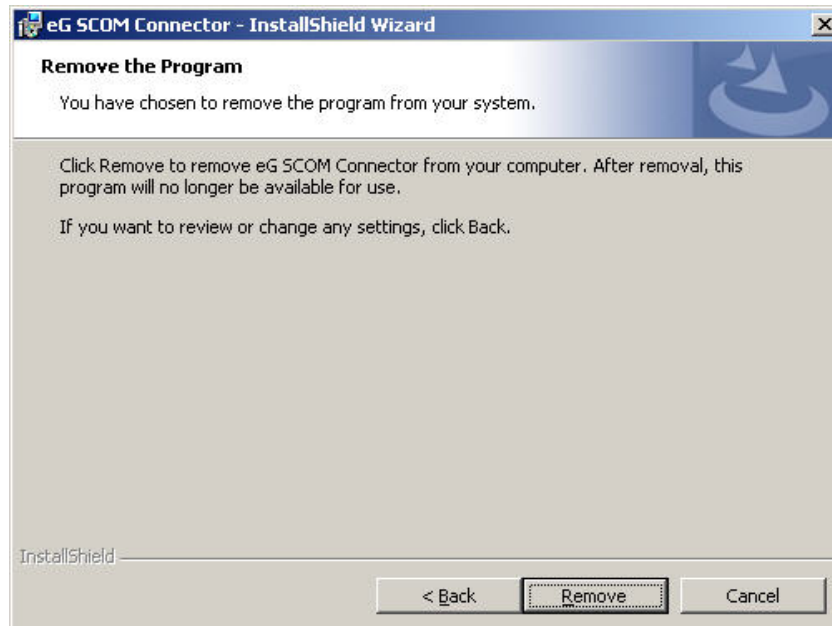


Figure 4.49: Confirming the connector uninstallation

7. Once uninstallation completes, Figure 4.50 will appear. Click **Finish** here to exit the wizard.

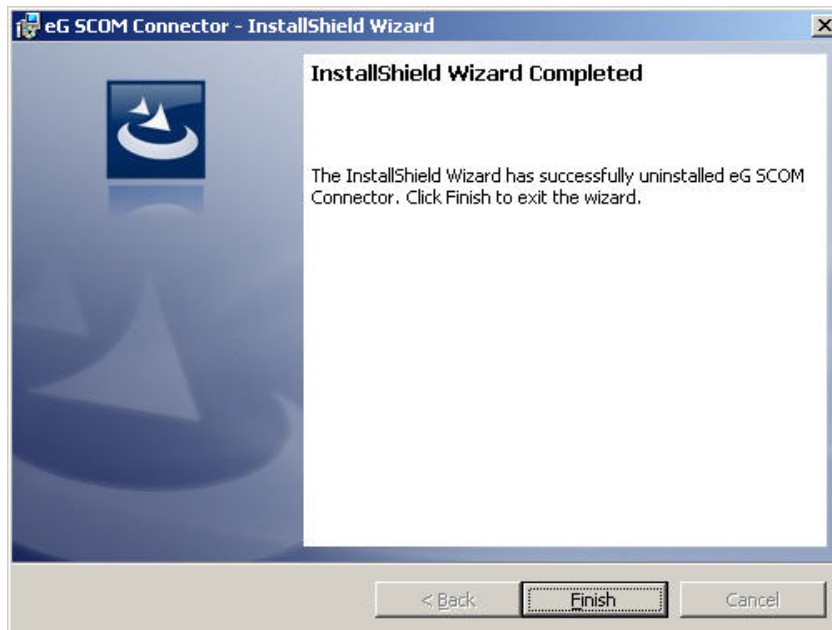


Figure 4.50: End of uninstallation

4.15 Uninstalling the eG SCOM Console Tasks Application

The **eG SCOM Console Tasks** application enables users to the SCOM console to instantly launch the eG monitoring console from the SCOM console itself. This way, users can take the help of analytical and diagnostic tools provided by the eG monitoring console to investigate performance setbacks experienced by eG-managed components.

Before uninstalling this application, you will have to stop all running instances of the application. For this, go to the command prompt in 'Run as administrator' mode, switch to the install directory of the **eG SCOM Console Tasks** application and run the following command:

```
eGConsoleTaskHandler.exe StopAllInstances
```

Then, proceed to uninstall the application. To uninstall, do the following:

1. Login to the eG SCOM Connector host.
2. Go to Start -> Control Panel -> Add/Remove Programs
3. Select the **eG Console Tasks** application from the list of Programs installed on that host, and click on **Remove**.
4. Figure 4.51 will then open. Click the **Next** button to proceed.

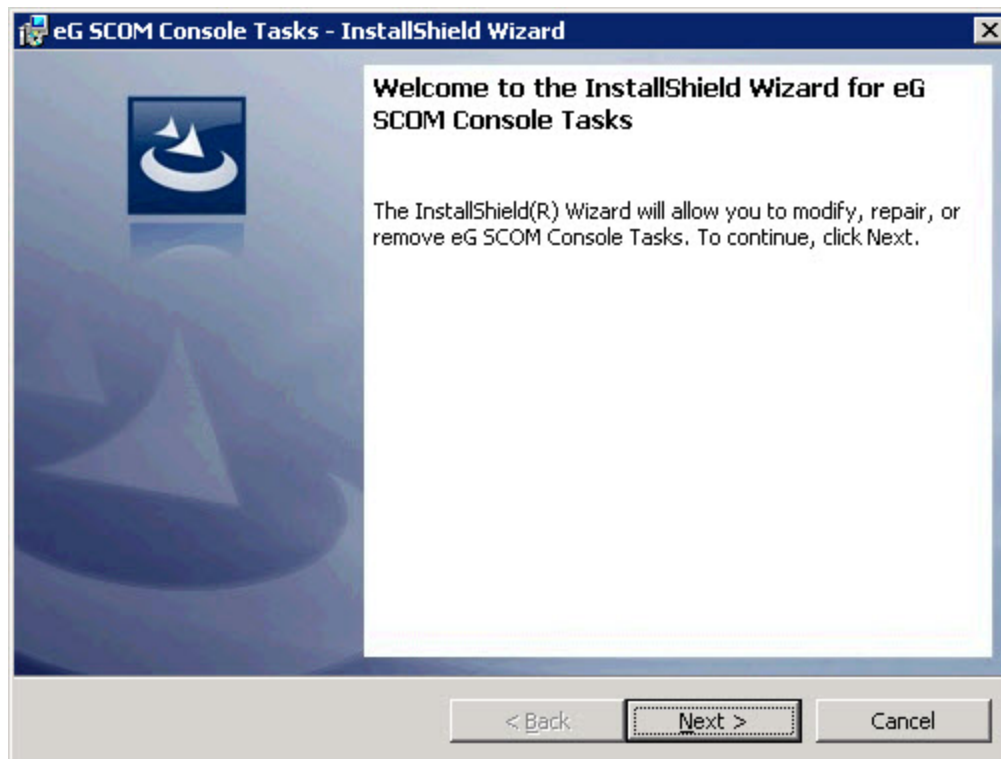


Figure 4.51: Uninstalling the eG SCOM Console Tasks application

5. When Figure 4.52 appears, select the **Remove** option to begin the uninstallation. Then, click the **Next** button therein to proceed.

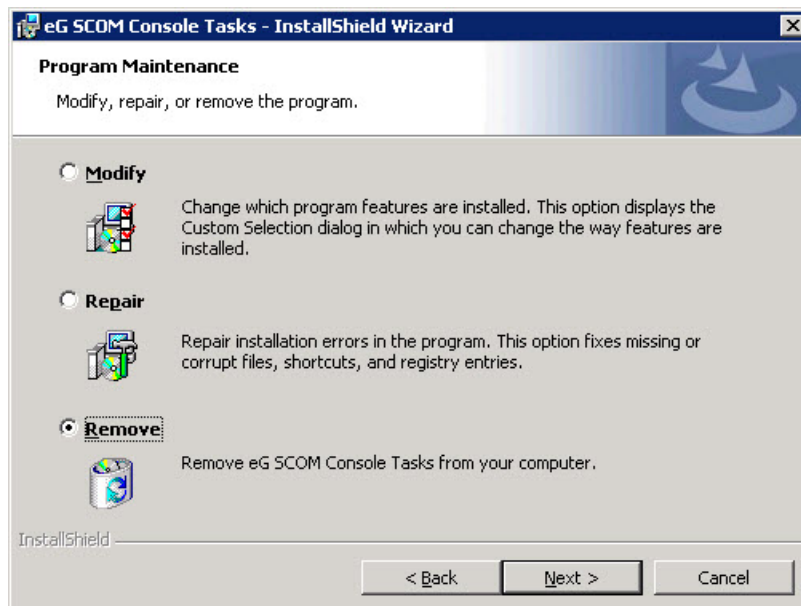


Figure 4.52: Selecting the Remove option

6. Then, click the **Remove** button in Figure 4.53 to confirm removal of the eG Console Tasks application.

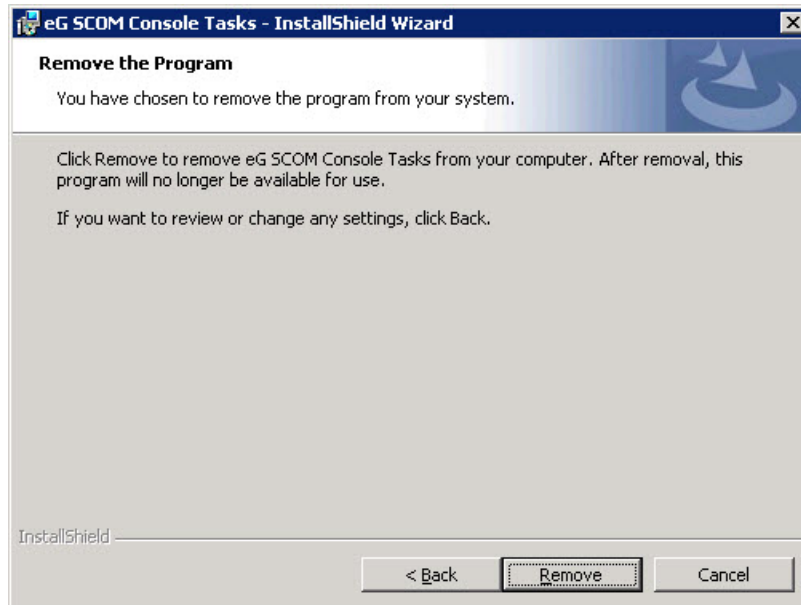


Figure 4.53: Clicking the Remove button

7. Upon successful uninstallation of the application, the message depicted by Figure 4.54 will appear. Click the **Finish** button in Figure 4.54 to exit the wizard.

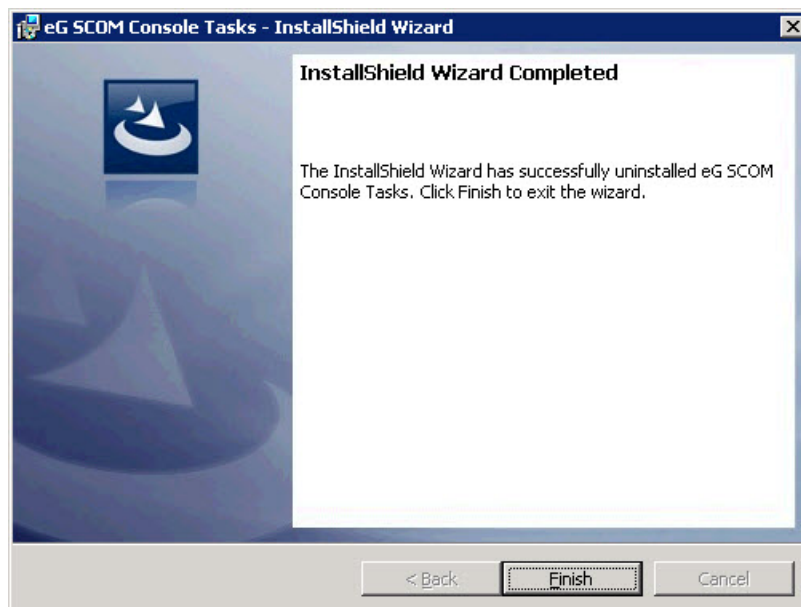


Figure 4.54: The completion of the uninstallation of the eG SCOM Console Tasks application

Chapter 5: Frequently Asked Questions

This chapter is a compilation of some of the frequently asked questions in SCOM integration and their responses.

1. **Can the SCOM connector work with a redundant eG manager setup? If so, how to configure it?**

Yes. The SCOM connector can work in a redundant eG manager setup.

If you want to configure a SCOM connector for a redundant manager setup that pre-exists in an environment – i.e., a redundant manager setup that was operational before the eG manager was integrated with SCOM – then, post the integration, you just have to point the connector to use the primary manager's URL. The plugin automatically discovers secondary managers and if there is a failure in the redundancy, it will automatically switch to the available manager.

On the other hand, if you configure a redundant manager setup post the eG-SCOM integration, then, you will first have to point the connector to use the primary manager's URL, and then, restart the **eG SCOM Connector** – i.e., stop and then start the eG SCOM Connector. Only after the restart will the eG SCOM connector automatically discover the secondary managers.

2. **I have configured an eG user account in the SCOM connector and the integration has already been done. Can I now reconfigure the setup to use a different eG user? If so, how?**

Yes, you can reconfigure the setup to use a different eG user. The steps in this regard are as follows:

- Stop the connector.
- Launch the **Configuration & Setup Tool** by following the menu sequence: *Start -> Programs -> eG SCOM Connector*
- Switch to the **Setup** tab page of the **Connector Configuration & Setup** dialog box that then appears (see Figure 5.1). Click the **Uninstall** button therein to uninstall the configuration.

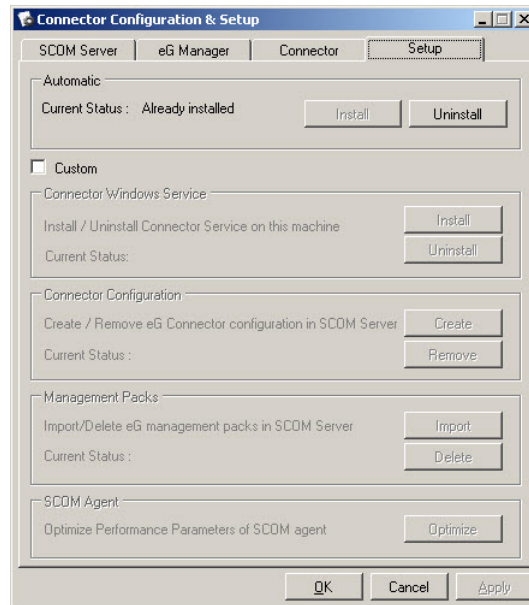


Figure 5.1: Clicking on the Setup tab page for uninstalling the connector configuration

- Then, switch to the **eG Manager** tab page. Provide a unique manager ID, specify the URL of the manager with which the connector has to integrate, and then provide the credentials of the new eG user for the integration.

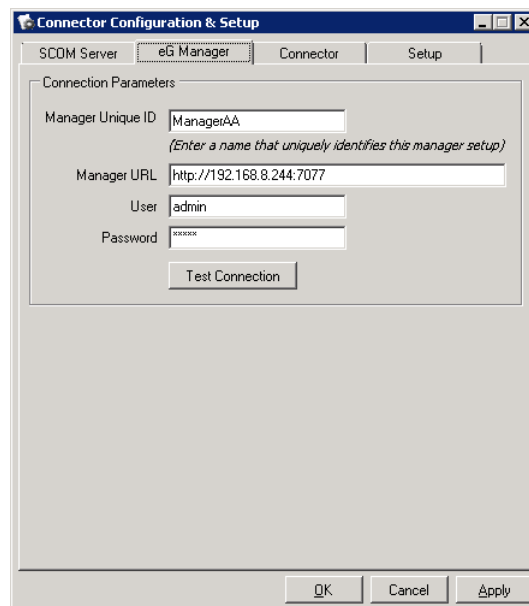


Figure 5.2: Configuring a new eG user

- Finally, return to the **Setup** tab page, and this time, click on the **Install** button (see Figure 5.3)

to install the configuration for the new eG user.

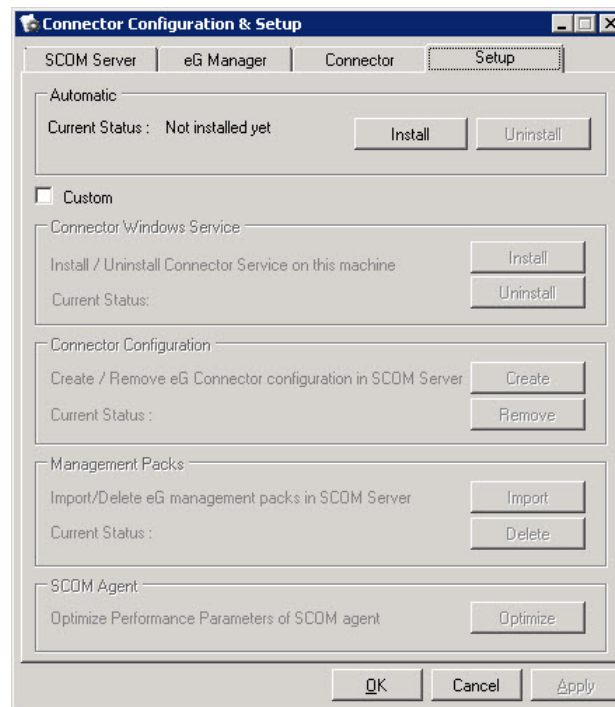


Figure 5.3: Installing the configuration for the new eG user

- Finally, click the **Apply** and **OK** buttons in Figure 5.3.

3. I have two eG user accounts in a manager that needs to be integrated with SCOM? How do I achieve integration for two users?

As per design, a single eG SCOM Connector can only integrate with a single eG user. If you want the SCOM Connector to integrate with all components managed by two different eG users, and each of these users require separate access rights to the SCOM console, then it is recommended that you install two different SCOM Connectors on two separate machines and configure each of them to integrate with a different user.

4. How do I enable the eG SCOM Connector to integrate with multiple eG managers?

Please refer to Integrating Multiple eG Managers with SCOM for the relevant details.

5. In my SCOM 2012 environment, the SCOM connector is configured to report to a specific SCOM management server in a management group. If the configured management server is down, will the SCOM connector automatically report to the next

available management server in the management group ?

Yes. The SCOM connector keeps track of the available management servers in the management group that it is currently reporting to. If the configured management server is down, the plugin automatically starts reporting to the next available management server. For this scenario to work, the connector should be able to connect to all management servers in the management group.

6. **In my SCOM environment, I have deployed SCOM agents in an untrusted domain. These SCOM agents are being managed by a SCOM server in a different domain via a gateway server. Can the eG SCOM Connector that is deployed along with the SCOM agents be able to communicate with the SCOM server via this gateway server?**

Yes. The eG SCOM Connector is capable of integrating with the SCOM server in a different domain via a gateway server. No configuration changes need to be made to enable this communication.

7. **Am I required to install the eG SCOM Connector on all SCOM agent hosts?**

No. It would suffice to install the connector in any one of the SCOM agent hosts.

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.

Copyright © 2020 eG Innovations Inc. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of eG Innovations. eG Innovations makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information contained in this document is subject to change without notice.

All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of eG Innovations. All trademarks, marked and not marked, are the property of their respective owners. Specifications subject to change without notice.