

People. Your most valuable asset.
Your greatest risk.

Creating Alerts based upon User Actions or Accessed Applications

System and software downtime frequently mean lost revenues, lowered employee productivity and reduced customer satisfaction. Despite the fact that companies are investing in high-availability systems and performance monitoring solutions for data centers, many are failing to follow best practice procedures to avoid human errors.

While some very limited capabilities exist within the built-in Windows Auditing mechanism, they are limited to a very basic set of actions, such as shutting down a system or deleting a file. Even if configured properly, these resulting events are cryptic and hard to understand, quickly filling the Windows Event Viewer and giving only a limited understanding of what the user has done during that period.

Imagine being able to receive alerts whenever a user performs an action such as deleting a file, opening a specific network share, using the Registry Editor to change a key or value, opening an RDP connection to a specific server, using Internet Explorer to navigate to a specific page in the company's intranet website, or even using Microsoft Word to read through a document. Existing Windows Auditing cannot even begin to deliver. Imagine being able to distinguish between various users, all logging on as "Administrator" to your servers, and knowing the exact name of the person logging on.

Furthermore, imagine being able to visually replay the entire user session whenever such an alert is received, thus visually seeing what the user did, where else they performed the same action, and what the context of their action was.

Enter ObserveIT.

ObserveIT for Servers is a client/server software application that monitors, audits and records all activities performed by people on an enterprises servers. The indexed, searchable, visual database allows those activities to be replayed to see exactly what is happening on the monitored servers.

When using ObserveIT, all user sessions are captured and recorded. Whenever a user logs on to the server, either locally or by using RDP/VNC/Damware/NetOp or other means, a user session is created, and any application opened by the user in that session is fully recorded. ObserveIT captures the screen seen by the user, and by combining multiple screenshots into one stream, a video is created.

In addition to capturing the screen image for each user action, ObserveIT for Servers extracts information about the state of the operating system and the application being used, which allows ObserveIT for Servers to precisely identify what the user is doing in any given moment. This metadata is analyzed and encoded in a standardized format

People. Your most valuable asset. Your greatest risk.

that is stored in the Database Server. Because this information is stored along with the metadata describing what is seen on the screen, you can perform very powerful searches across your entire enterprise.

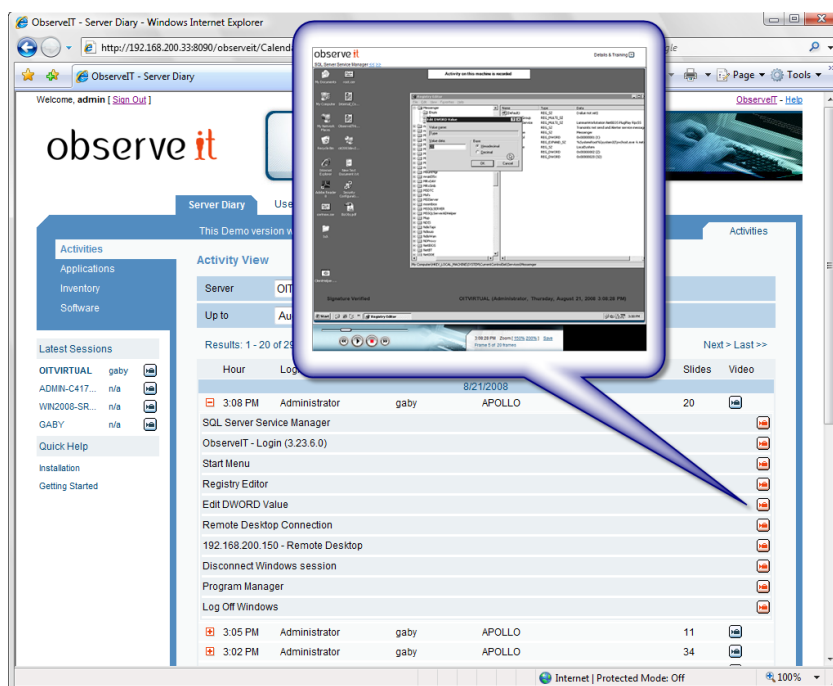


Figure 1: Using ObserveIT's Server Diary and stored metadata

Another feature of ObserveIT is its capability to also create textual log files for monitoring purposes. These files are stored on the server's hard disk, and can be parsed by 3rd-party tools, generating events or alerts based upon information written in them.

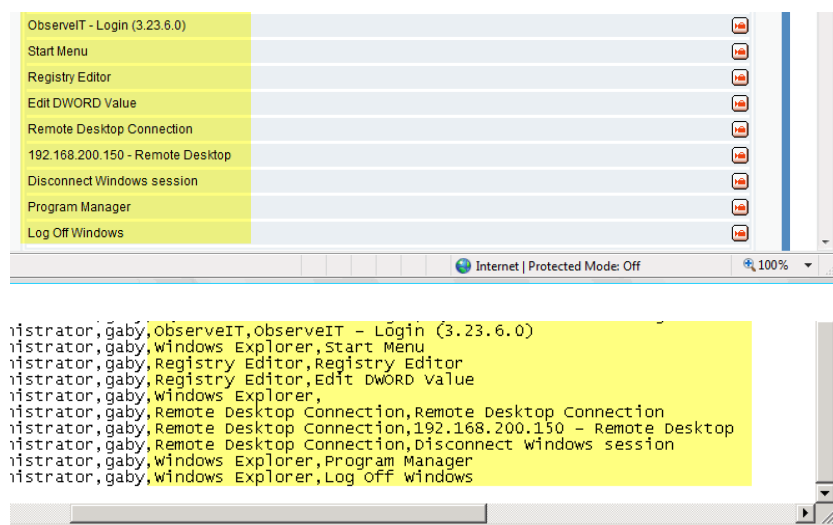


Figure 2: ObserveIT's metadata and textual log files

People. Your most valuable asset. Your greatest risk.

Read more about ObserveIT in the following link: <http://www.observeit-sys.com>

Such a tool is Microsoft System Center Operation Manager (SCOM) 2007 - a unified IT management tool scaled to the needs of mid to enterprise-sized businesses. Microsoft System Center Operations manager 2007 contains some great tools that allow you to monitor conditions that can occur on monitored servers or workstations. By using SCOM 2007 to parse the textual log files created by ObserveIT, we can easily create a Unit Monitor that will query these log file for specific string of text, and will set the health state based on the match. By carefully selecting the correct string, the monitor can be triggered by a pre-defined textual string, which will set the health state of the monitored server to either warning or critical state. We can then further extend these capabilities by generating E-mail, SMS or Instant Messenger alerts, immediately notifying us about a specific server's change of state.

In this guide, we will demonstrate the process of creating a new monitor in SCOM 2007, and use the log files generated by ObserveIT to identify actions performed by users, or applications that were used on any server monitored by ObserveIT.

Creating a new monitor

Please follow these steps in order to create a Unit Monitor, based on ObserveIT's monitoring log files:

On a server that is installed with System Center Operation Manager, log on with an account that is a member of either Operations Manager Administrators or Operations Manager Authors.

Open the Operations Console from the Start > Programs > System Center Operations Manager 2007 menu.

In the management console, click and expand the Authoring button, expand Management Pack Objects, and then click Monitors.

People. Your most valuable asset. Your greatest risk.

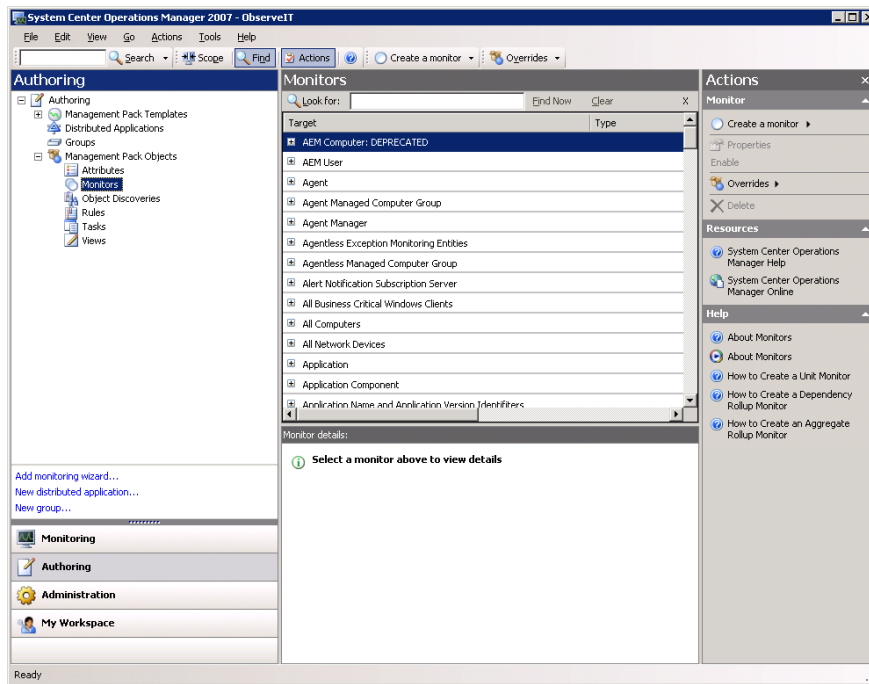


Figure 3: Operations Console Monitors node

Click the Scope button. In the Scope Management Pack Objects by target(s) dialog box, in the Look for text box, type “*Windows Computer*”. Select the Windows Computer target check box, and then click OK.

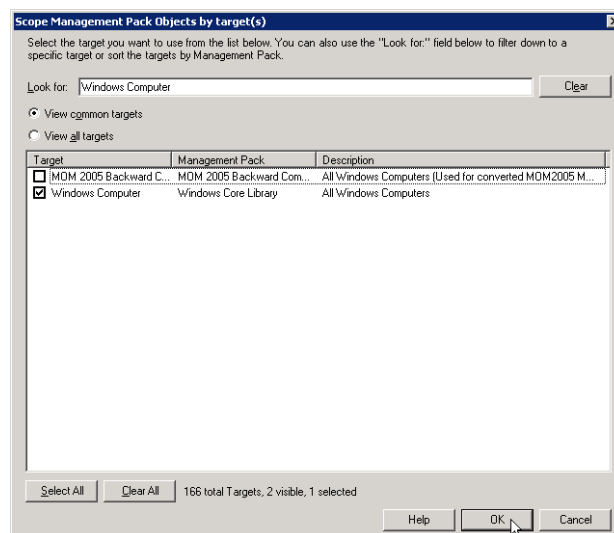


Figure 4: Scope Management Pack Objects by target(s) dialog box

In the Monitors pane, expand Windows Computer > Entity Health. Right-click Security, and select Create a Monitor > Unit Monitor.

People. Your most valuable asset. Your greatest risk.

Note: You can select a different target for the new monitor, based upon your requirements. You can also make changes to the target during the monitor's creation process, and afterwards.

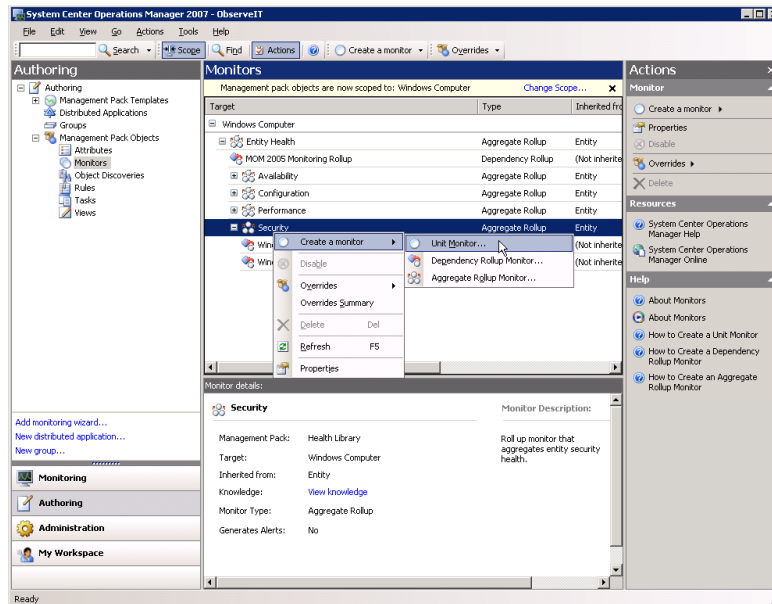


Figure 5: Scope Creating a Unit Monitor

In the Create Monitor Wizard, on the Select a Monitor Type page, expand Log Files > Text Log > Simple Event Detection. Click Manual Reset, and then click on the Next button.

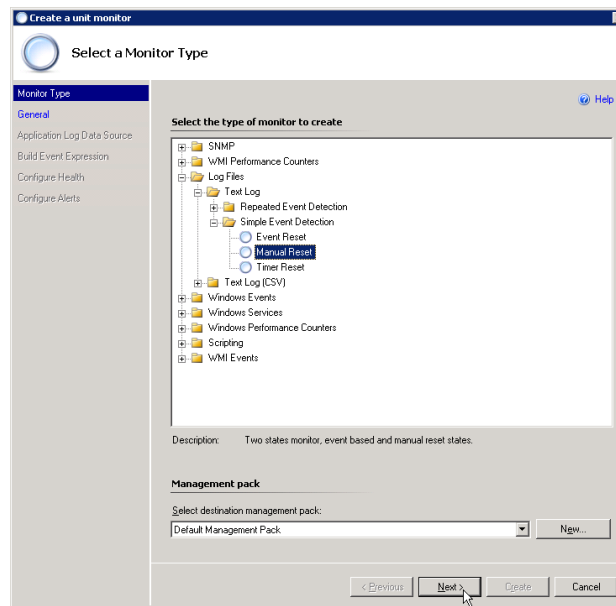


Figure 6: Monitor creation wizard

People. Your most valuable asset. Your greatest risk.

Note: You can select a different type of event, such as an Event Reset type, or Timer Reset. The Manual Reset type is triggered when an event happens, but the reset is performed manually.

Note: In the above step, you can either select a Management Pack from the Select destination management pack list or create a new unsealed Management Pack by clicking New. If you select to create a new Management Pack, give it an appropriate name such as “*ObserveITApplicationServer Management Pack*” or similar.

On the General Properties page, in the Name box, type a name for the unit monitor, such as “*Remote Access to 192.168.200.33*”. You can also type a description. In the Parent monitor list, click the appropriate parent monitor. Make sure that “Monitor is enabled” is selected, and then click on the Next button.

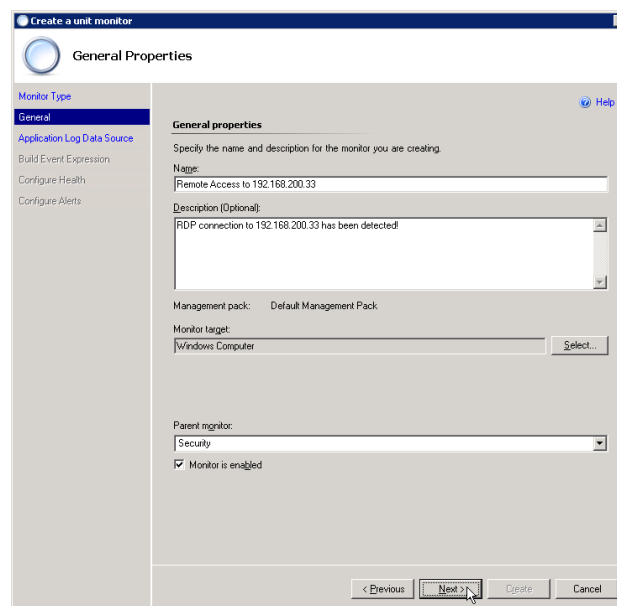


Figure 7: Monitor name and description

On the Application Log Data Source page (for the First Generic Log), under Define the application log data source, in the Description text box, type a path to where the log files are located. When using ObserveIT, you need to type the following path:

C:\Program Files\ObserveIT\NotificationService\LogFiles\1

In the Pattern text box, type a pattern string to select log files. In this case use “**.log*” (without the quotes). If applicable, select UTF8.

Note: In order to learn how to configure ObserveIT to record textual log files please consult with the product documentation.

Click on the Next button.

People. Your most valuable asset. Your greatest risk.

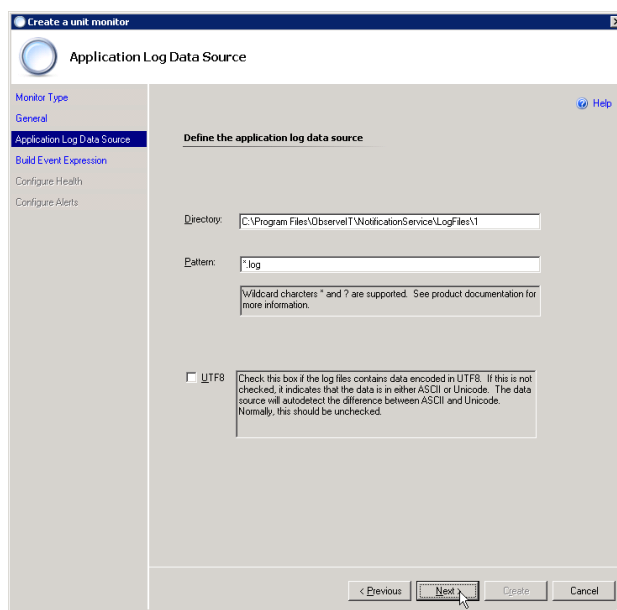


Figure 8: Log file directory and file name pattern for the first log

On the Build Event Expression page click Insert and then enter the following:

- Parameter Name = *"Params/Param[1]"* (without the quotes)
- Operator = *"Matches Wildcards"*
- Value = an expression to be searched for, for example, *"*Remote Desktop Connection,192.168.200.33*"*

Click on the Next button.

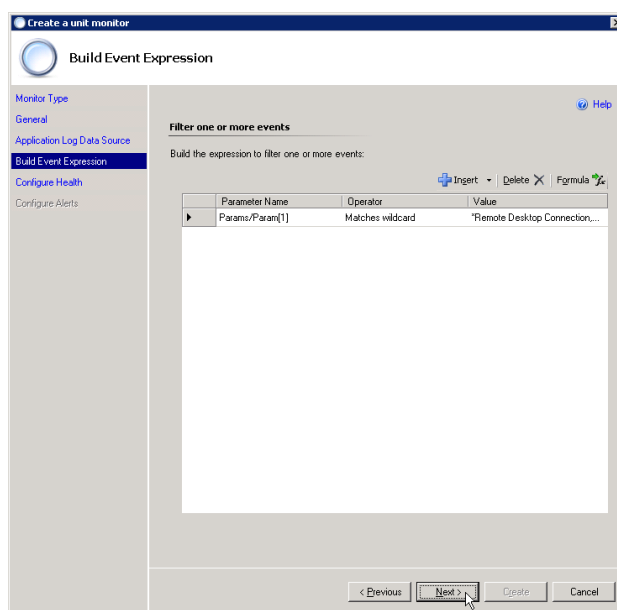


Figure 9: Event expression

People. Your most valuable asset. Your greatest risk.

Note: You can obtain the required textual value by looking at one of the log files generated by ObserveIT. These files are located in the following folder path:

C:\Program Files\ObserveIT\NotificationService\LogFiles\1

When you open one of these files, you'll see that each recorded action is listed in a separate line containing the following information:

FirstScreenshotTime, SessionId, ServerName, DomainName, LoginName, UserName, ApplicationName, WindowTitle

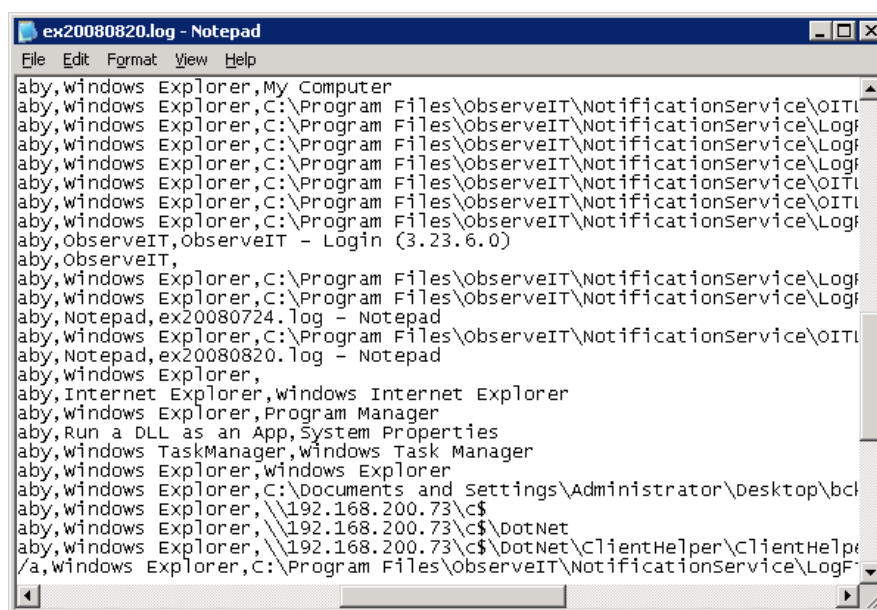


Figure 10: Log file example

By looking at that information, you can easily see information such as this (actual data will vary, depending on your recorded data):

- *Server73, Mydomain.local, Administrator, gaby, Windows Explorer, \\192.168.200.73\c\$*
- *Server33, Mydomain.local, Administrator, daniel, Remote Desktop Connection, 192.168.200.33 - Remote Desktop*
- *Server12, Mydomain.local, Administrator, avi, Registry Editor, Registry Editor*
- *Server33, Mydomain.local, Administrator, daniel, Run a DLL as an App, Date and Time Properties*
- *Server80, Mydomain.local, Administrator, james, Windows Command Processor, C:\WINDOWS\system32\cmd.exe*

And so on. Use whatever parameter you need.

People. Your most valuable asset. Your greatest risk.

Next, on the Configure Health page, for the Event Raised line, set the Health State type to “Warning” (or other, based upon your requirements). Click on the Next button.

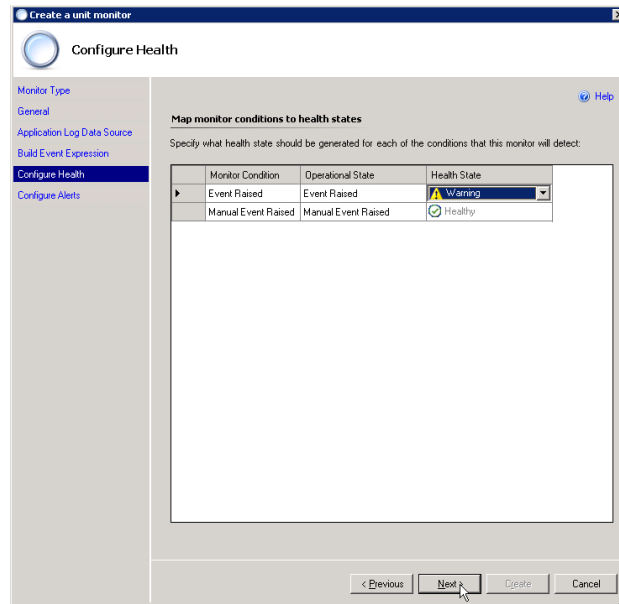


Figure 11: Map monitor conditions to health states

On the Configure Alerts page, use the default settings or select the Generate alerts for this monitor check box to set custom alert properties, and then click on the Create button.

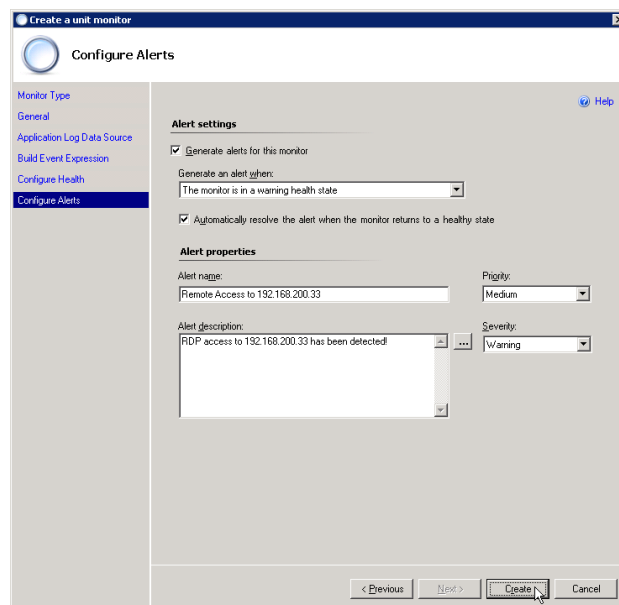


Figure 12: Alert settings

People. Your most valuable asset. Your greatest risk.

Note: In order to make future changes to this monitor, right-click it and select Properties.

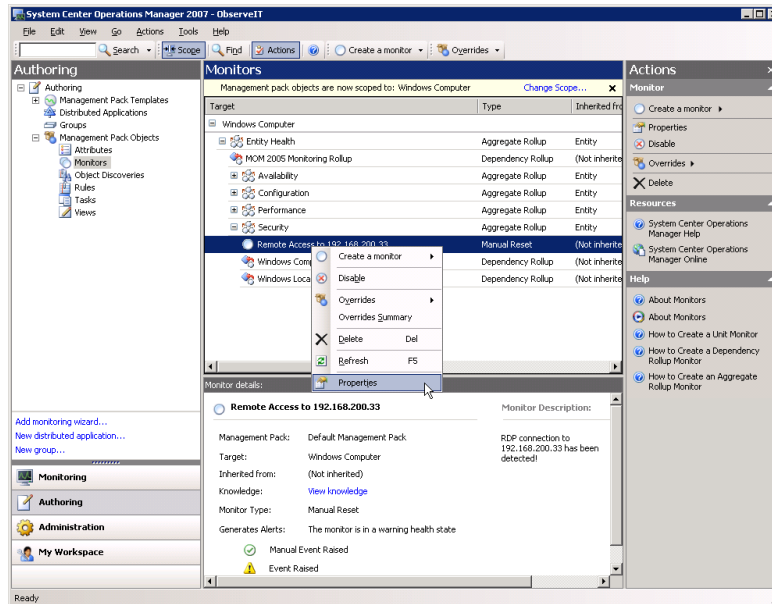


Figure 13: Change monitor properties

The Monitor properties page will be displayed, allowing you to view or make changes to the monitor settings.

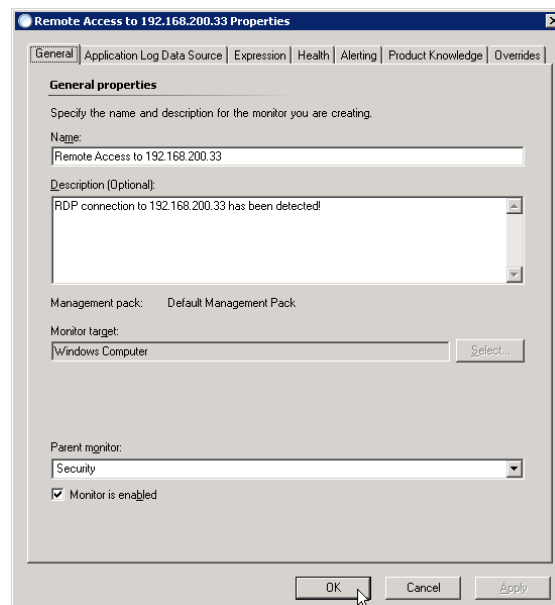


Figure 14: Monitor properties

People. Your most valuable asset. Your greatest risk.

Back in the System Center Operation Manager main console, click on the Monitoring button. You can view computer status messages by clicking on the Computers item on the left-hand pane.

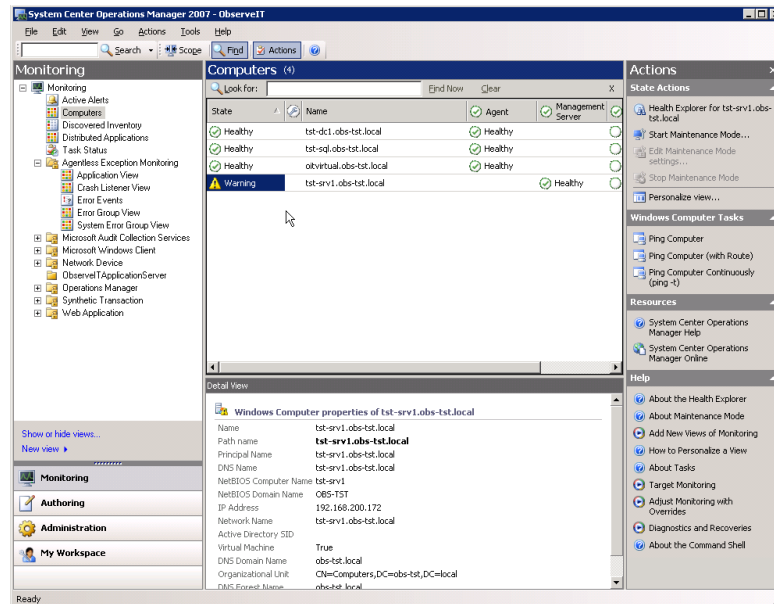


Figure 15: Computer status

You can also view any active alerts by clicking on the Active Alerts item on the left-hand pane.

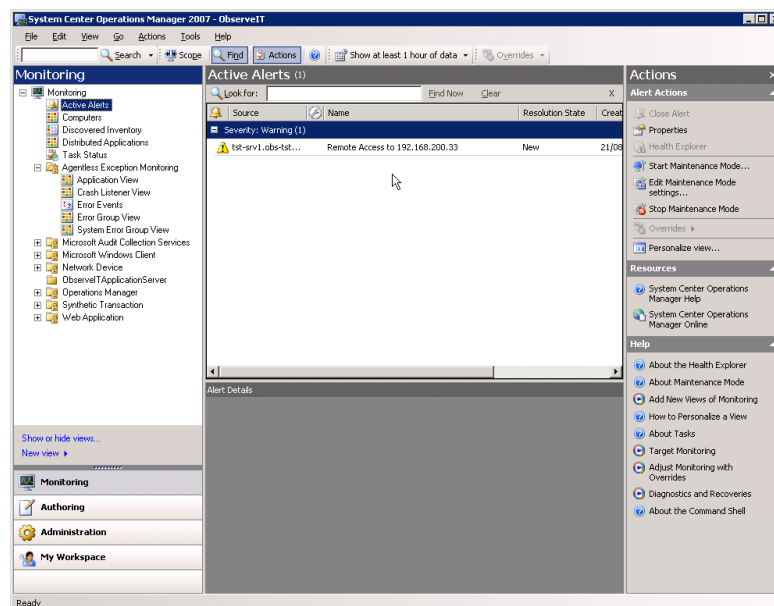


Figure 16: Active alerts

People. Your most valuable asset. Your greatest risk.

A third method to view the alert is by using the Health Explorer for the specific server.

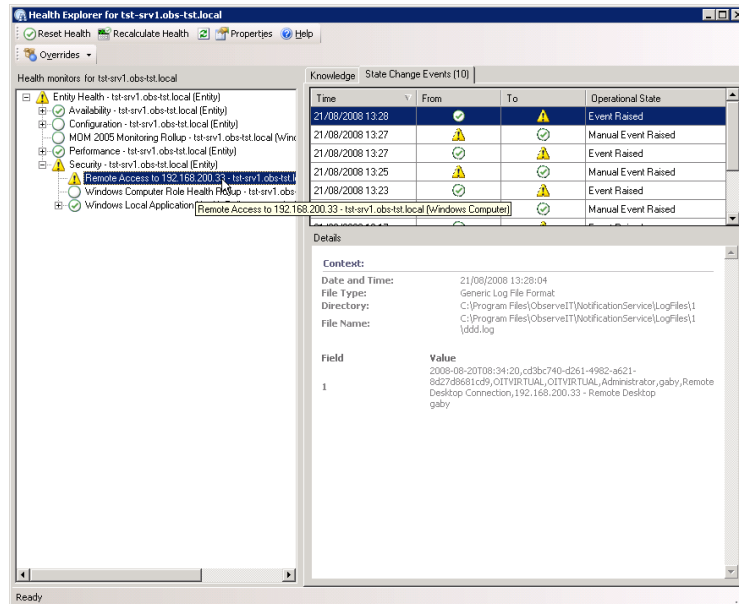


Figure 17: Health Explorer

This concludes the process of creating a new monitor based upon the log files generated by ObserveIT. By using System Center Operation Manager 2007 to monitor these log files, you can easily generate alerts and create events based upon actions performed by users, or applications that were used on any server monitored by ObserveIT.