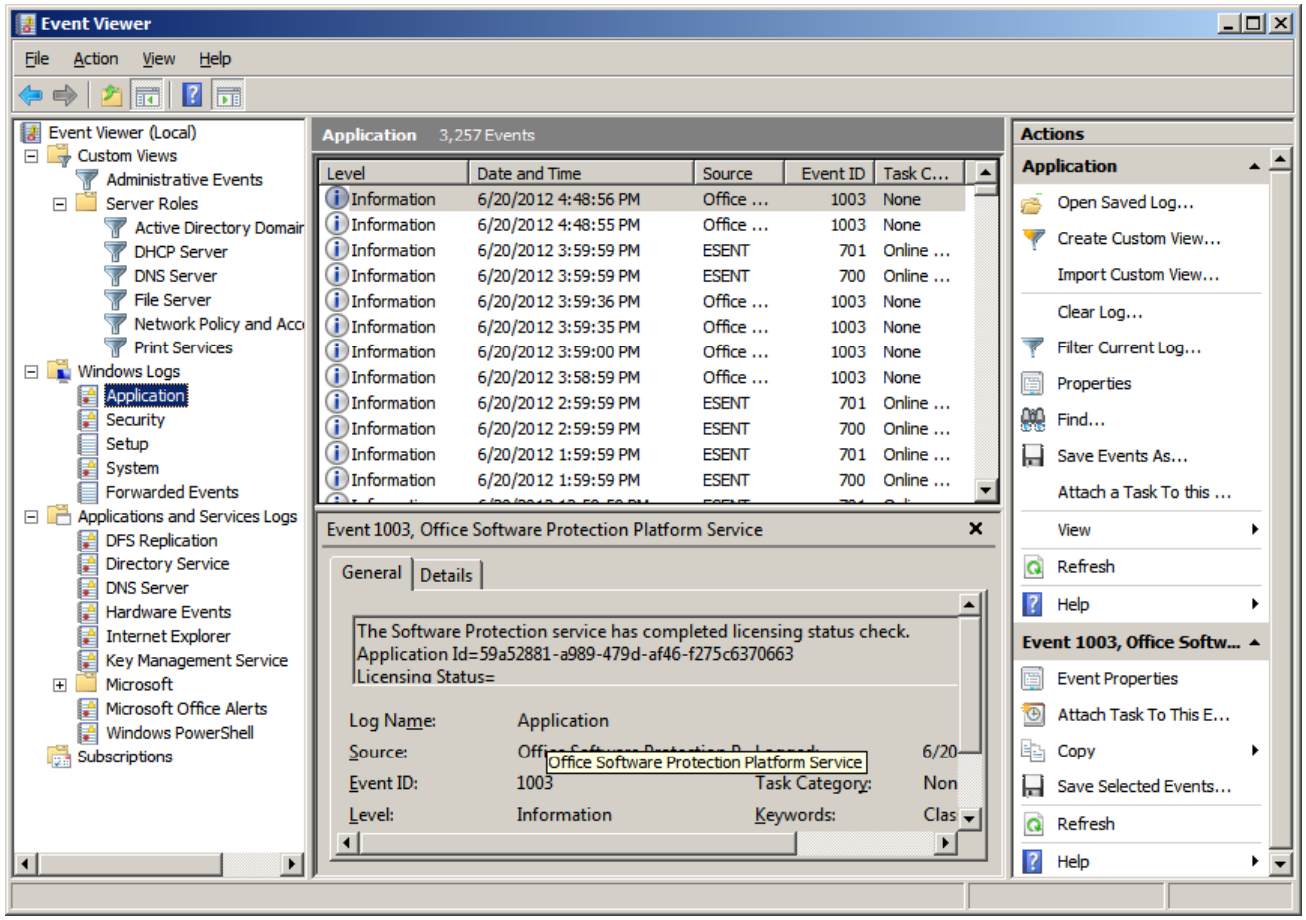
Windows 2008 Server Event Logs

June 20, 2012

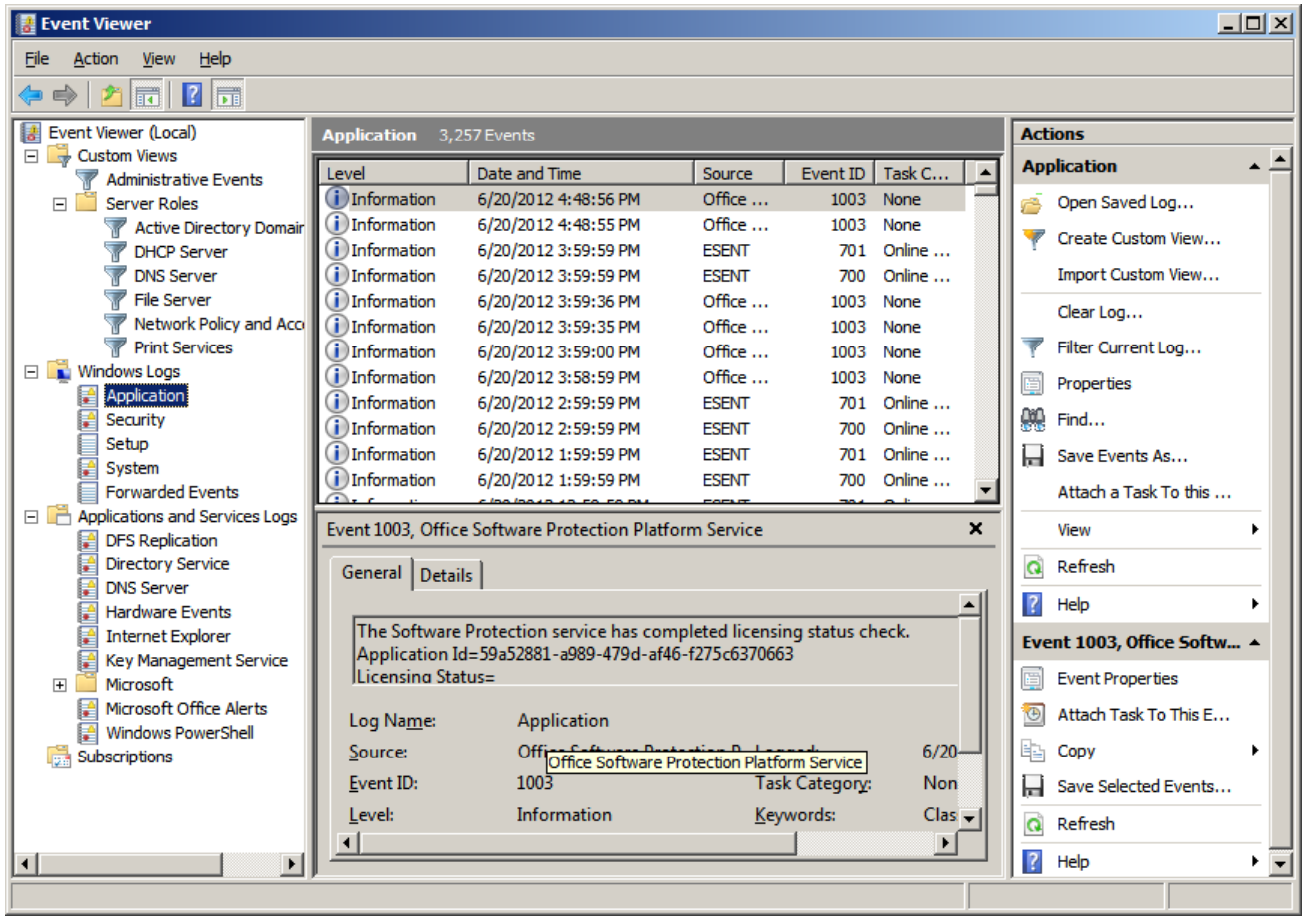
Event Viewer Window

Nearly everything that happens to the server or the Domain can be read in a report if we are tracking the occurrence. We can see many samples of these snapshots in the Event Viewer. We can reach the window by clicking on Event Viewer on the Administrative Tools menu.



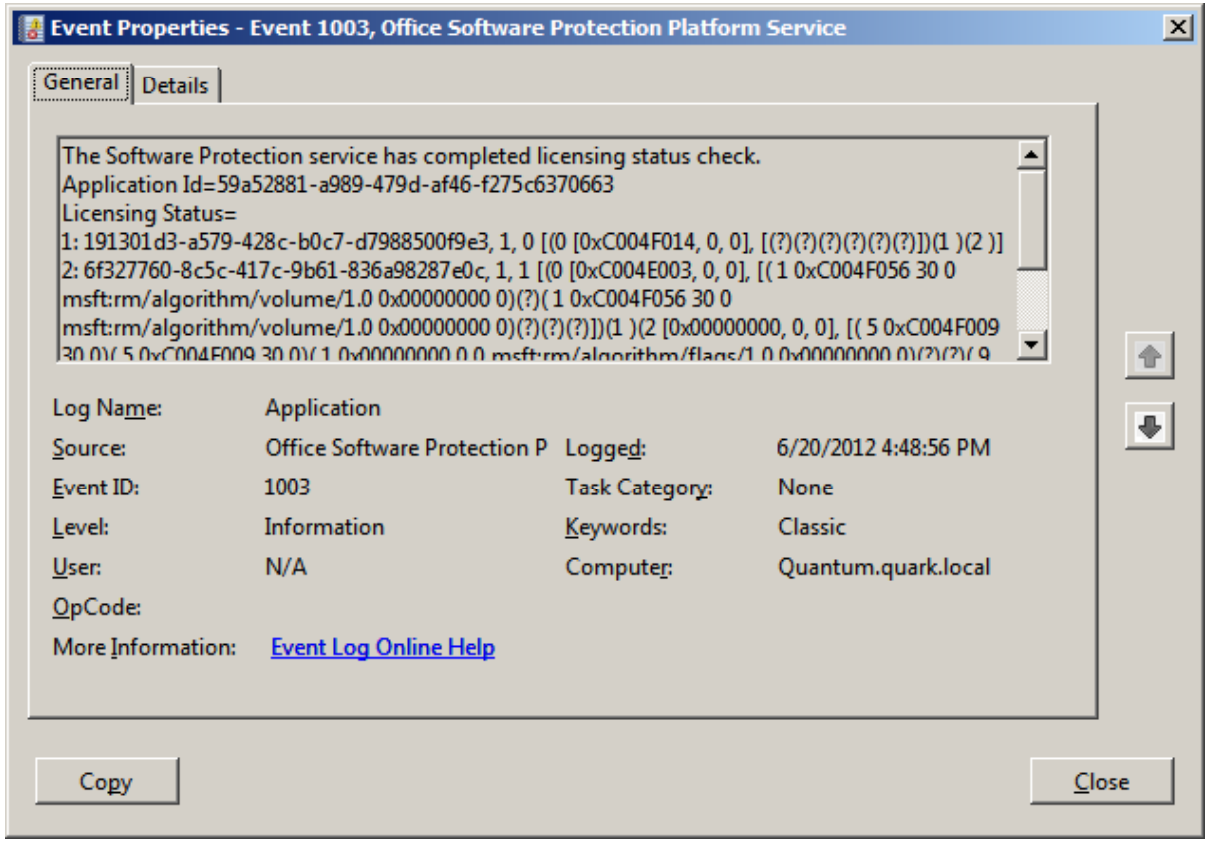
Windows Logs - Application

Open the Windows Log folder and highlight Applications. These events shown in the middle pane are logged by applications on the Windows Server. Double click on the top report.



Event Properties – Event 1003

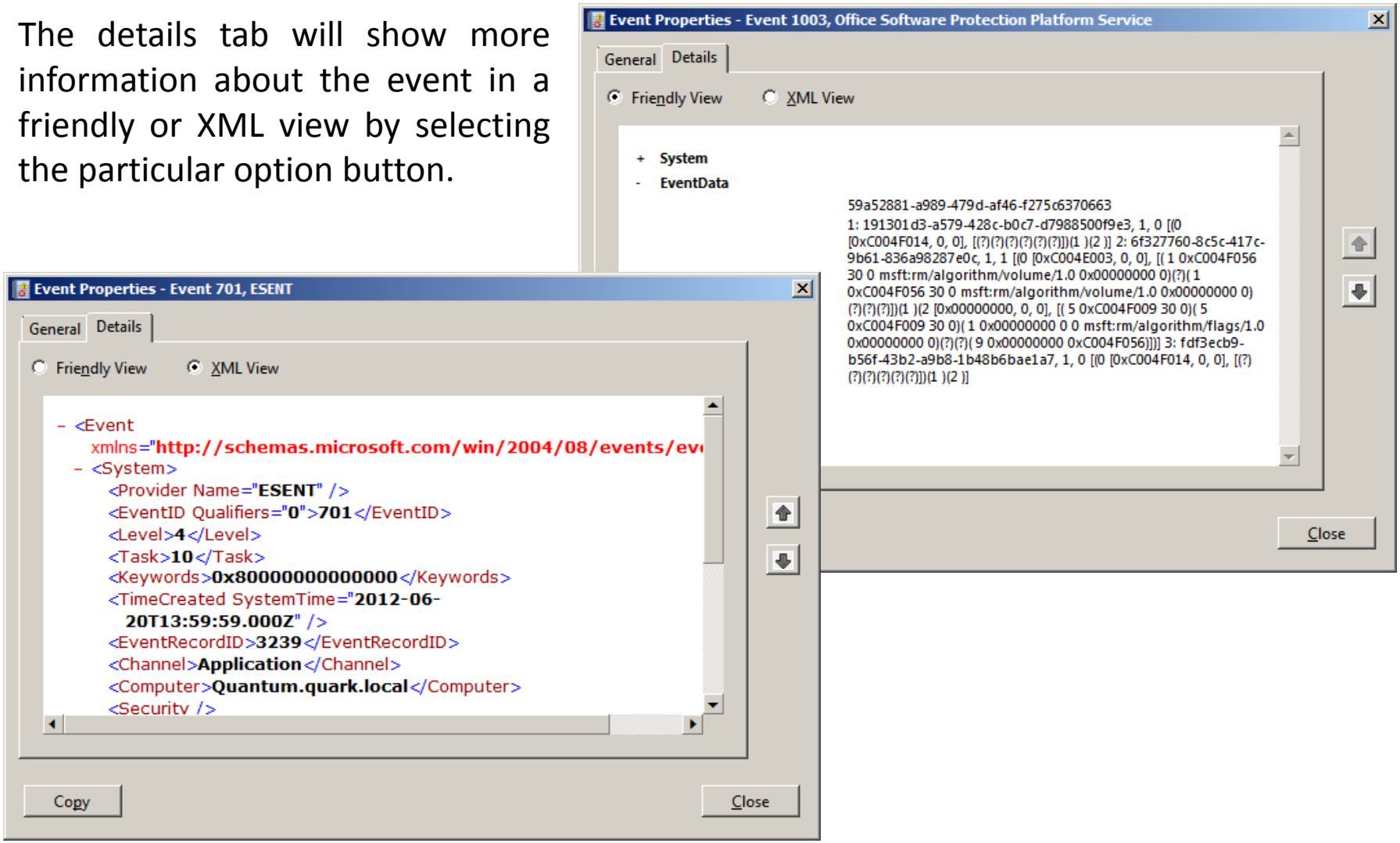
The properties window for the first event will open. We will see two tabs, general and details. The general tab has an event ID and other important data about the event such as level which are information, warning, error, success audit and failure audit. All error need to be researched followed by warnings.



Network Administrators check the servers regularly and solve server errors as they arise.

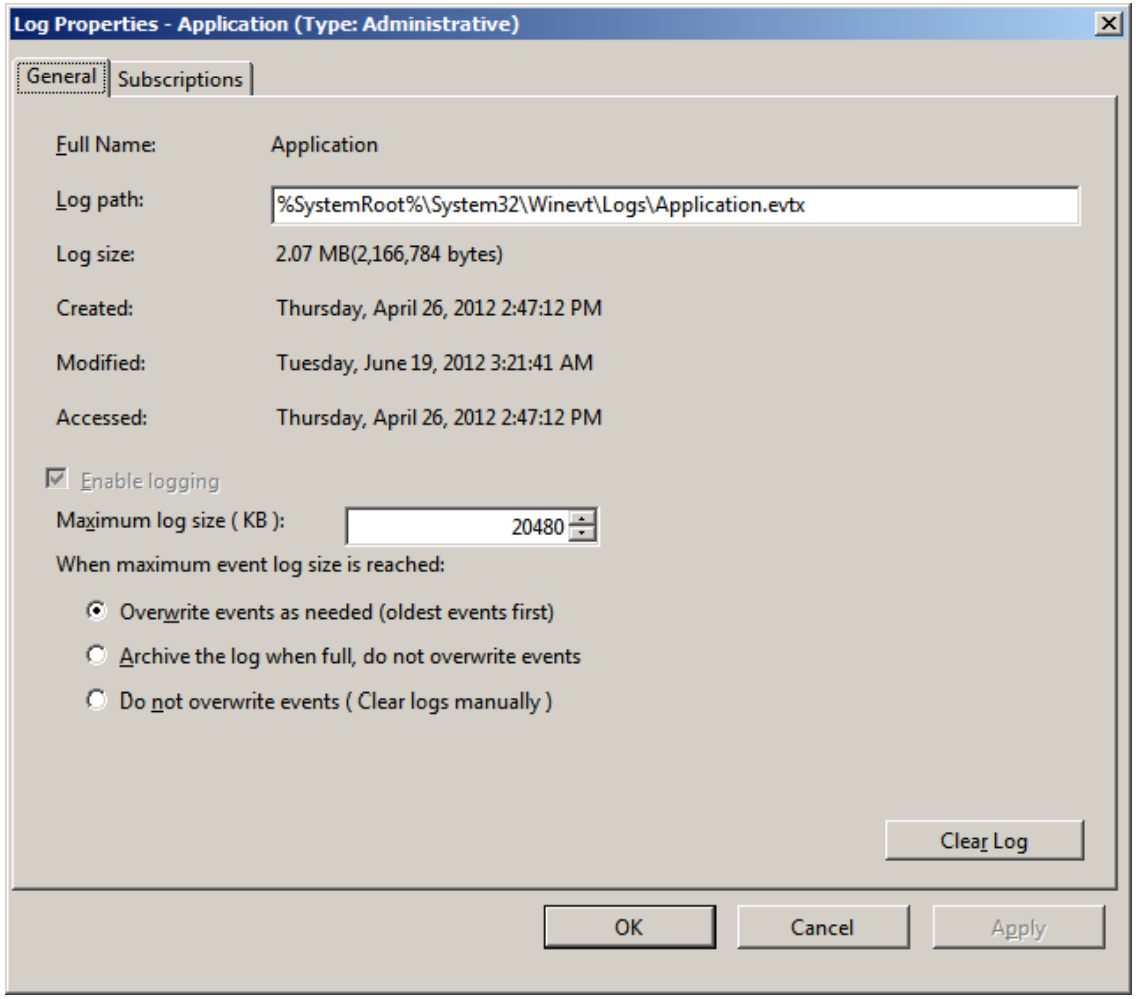
Event Properties – Details Tab

The details tab will show more information about the event in a friendly or XML view by selecting the particular option button.



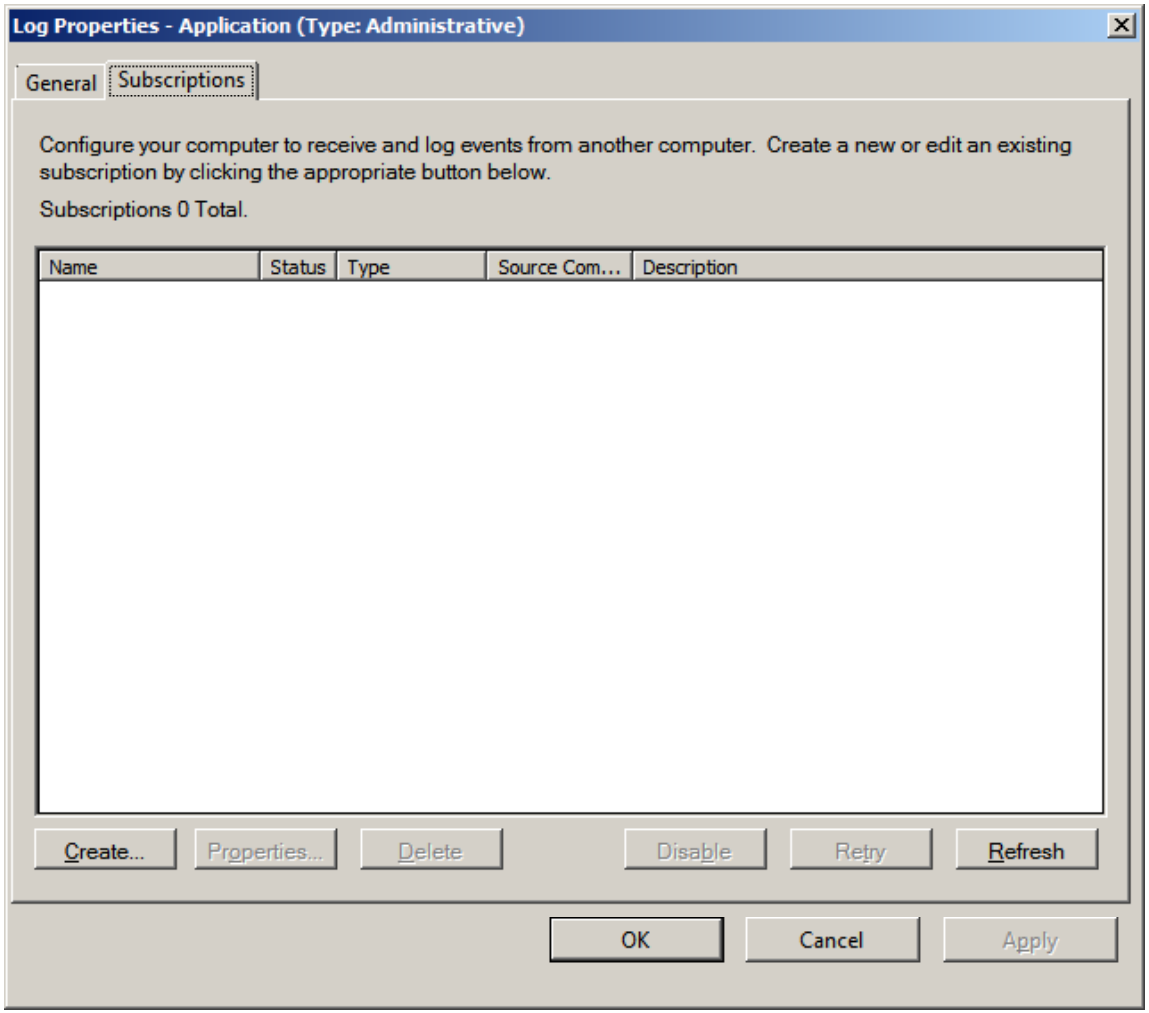
Application Log Properties

Server Administrators can receive directives from senior managers to change the Windows Server log size. We right click on Application in the left pane and we pick properties from the menu and the Application log properties window will appear. To change the maximum log size, we would enter the number of kilobytes in the textbox. There is a Clear Log button to erase the log.



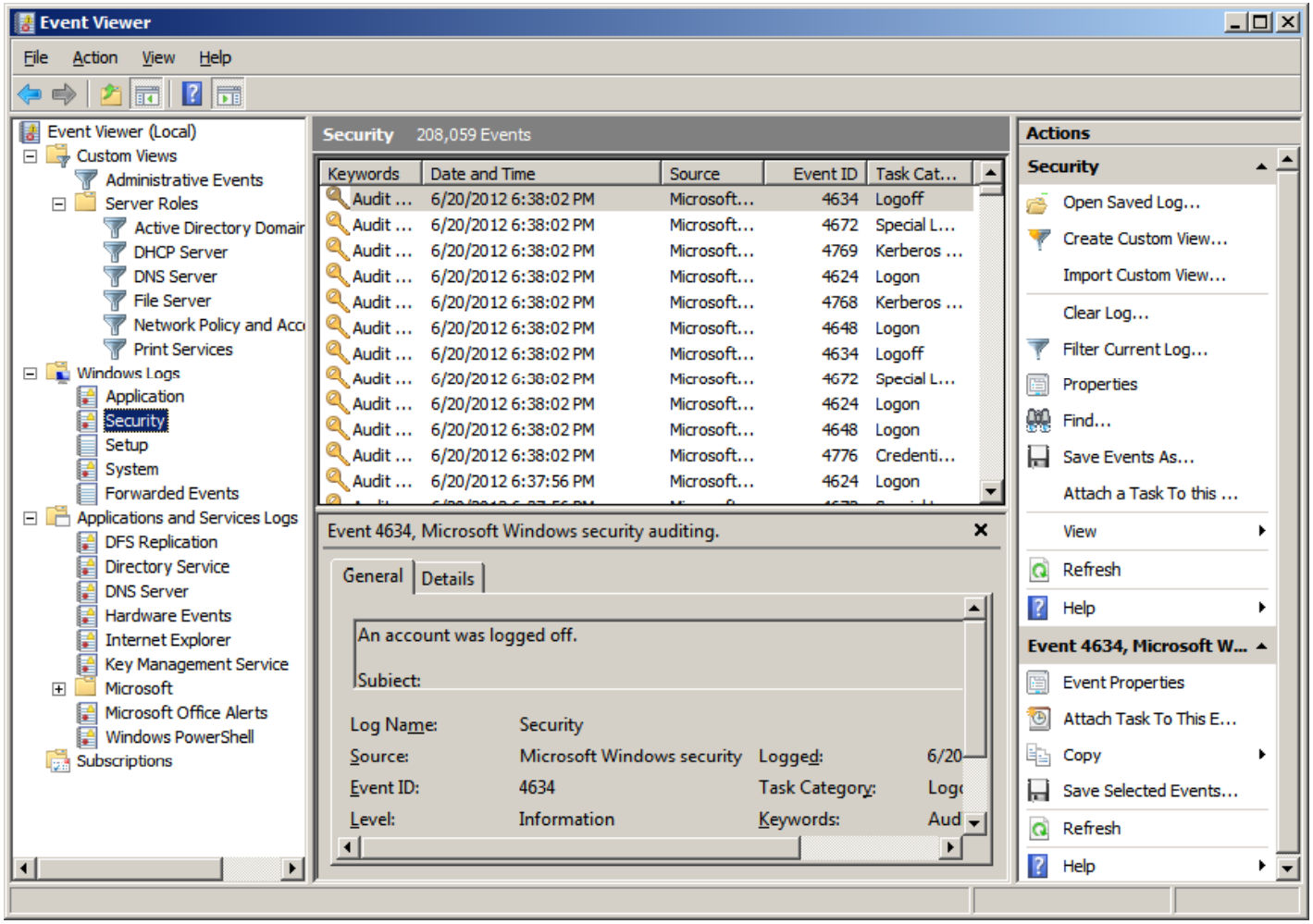
Application Log - Subscriptions Tab

This would enable us to get a log from another server.



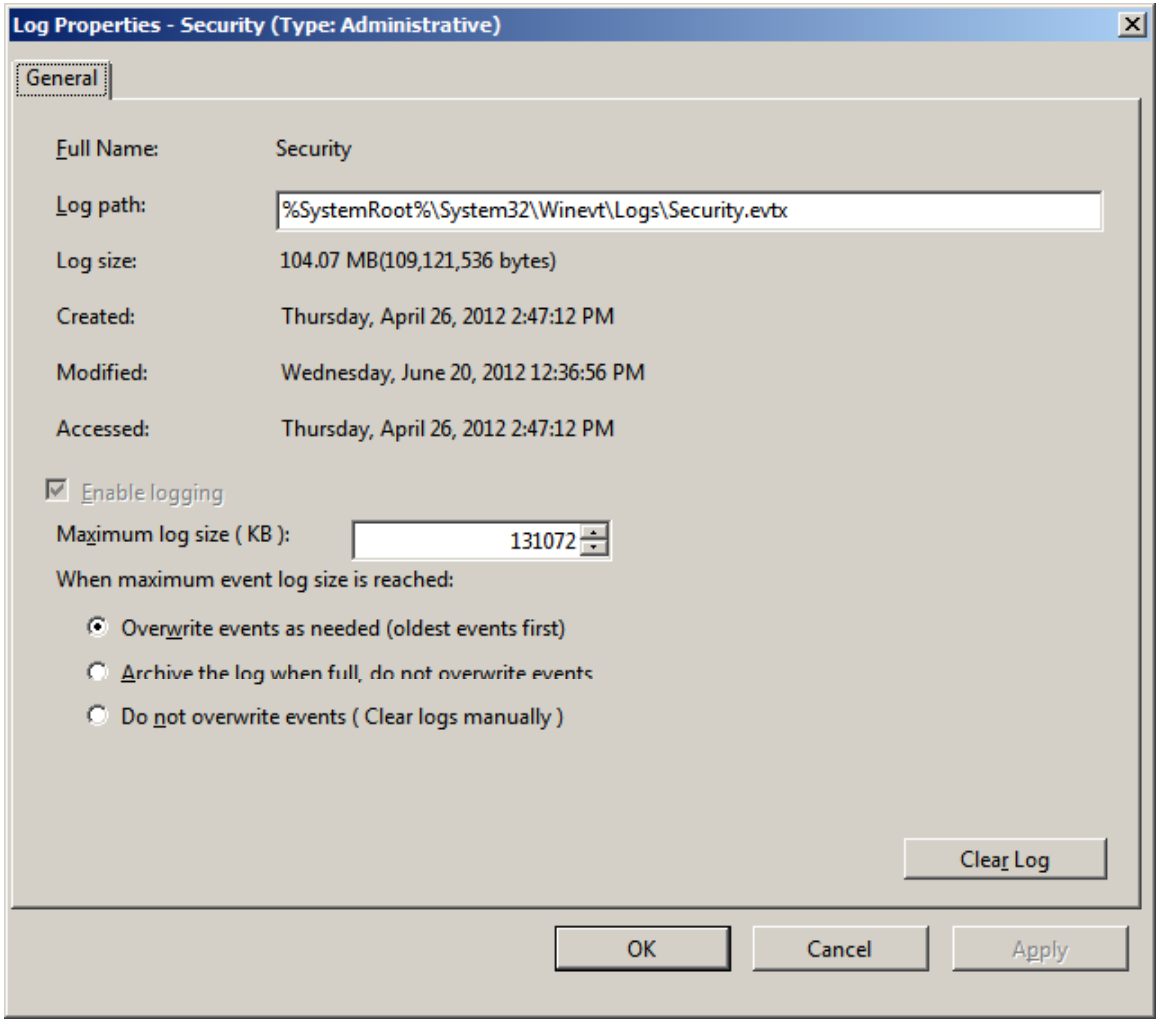
Windows Logs - Security

Open the Windows Log folder and highlight Security. These events shown in the middle pane are logged from security polices on the Windows Server.



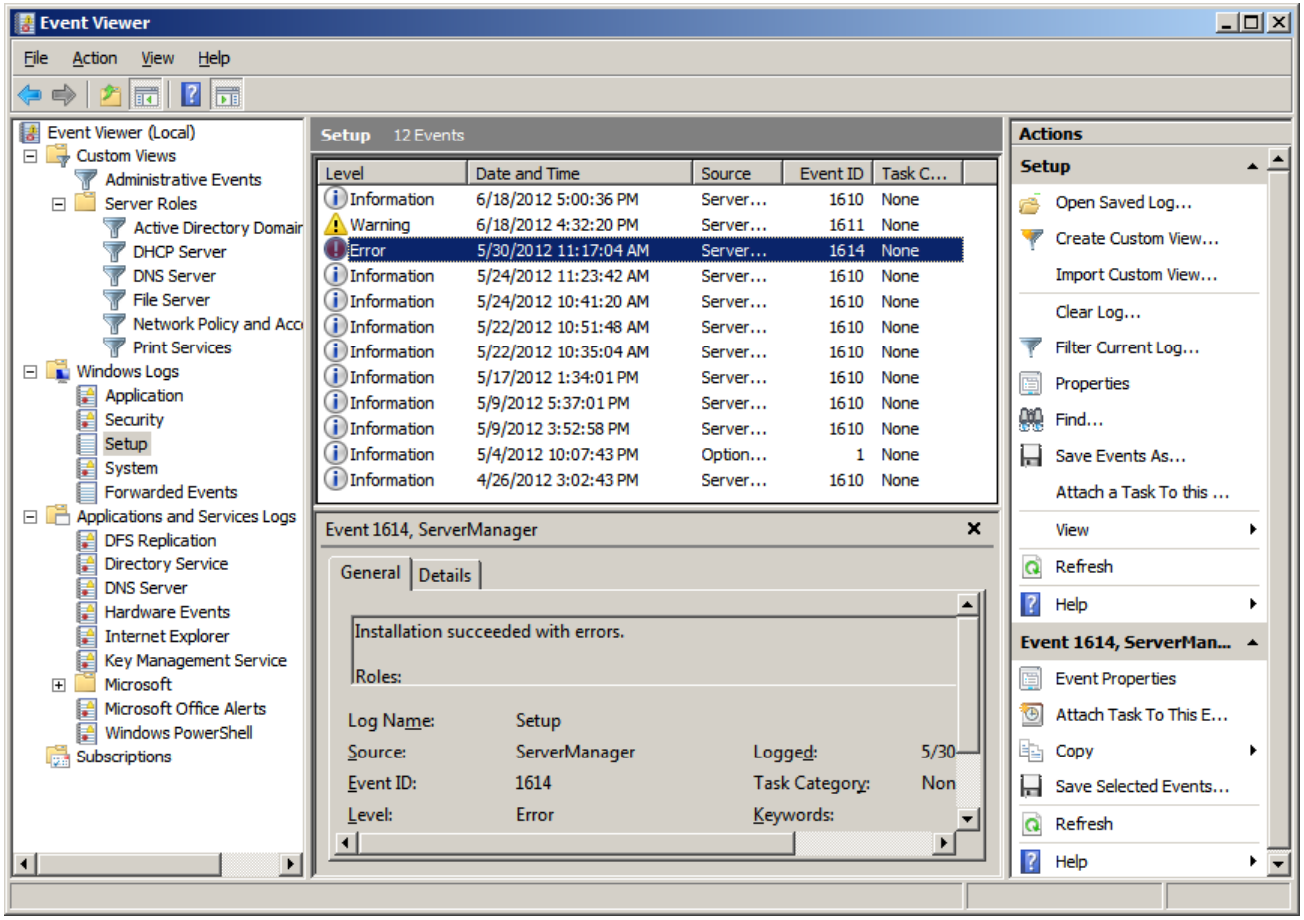
Security Log Property

Again, administrators can receive directives from senior managers to change the Windows Server log size. We right click on Security in the left pane and we pick properties from the menu and the Security log properties window will appear. To change the maximum log size, we would enter the number of kilobytes in the textbox. By default, when the log is filled, the oldest record is deleted.



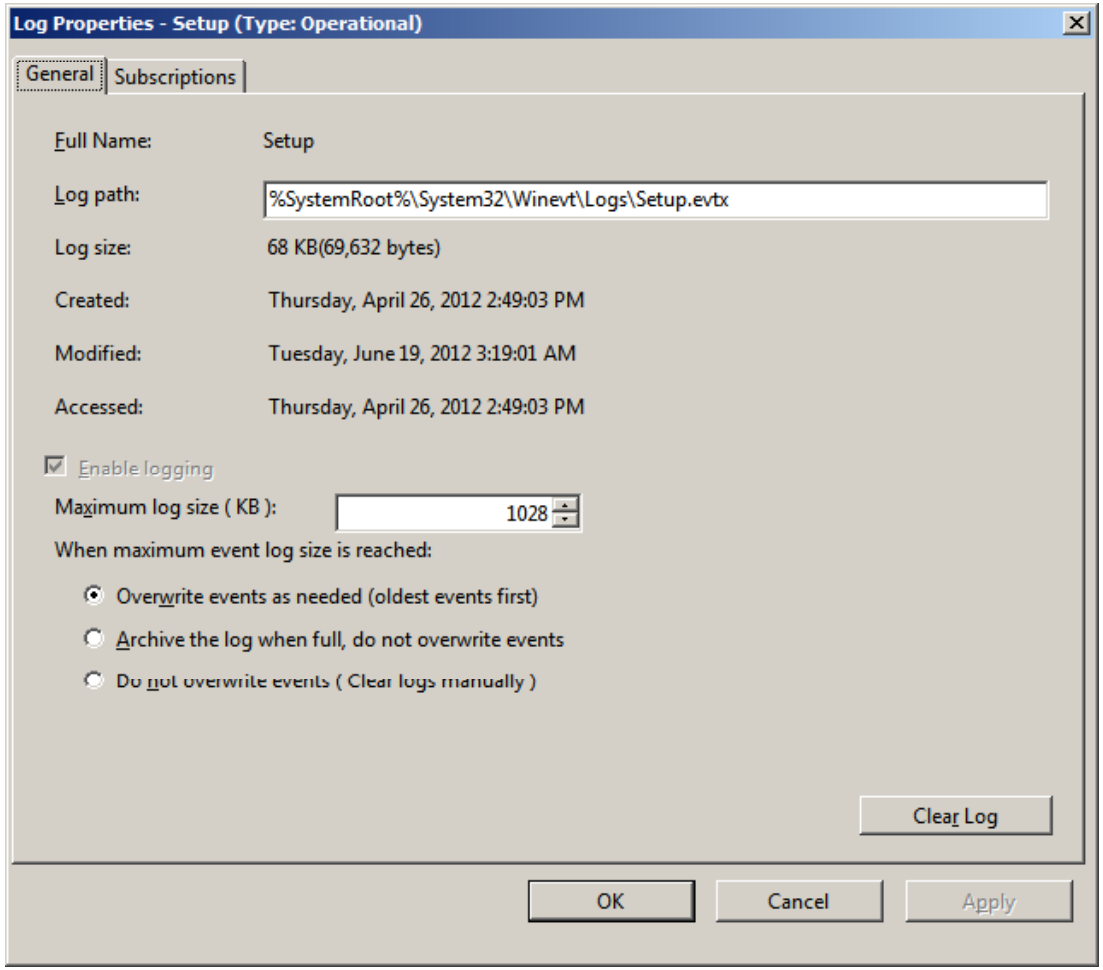
Windows Logs - Setup

Open the Windows Log folder and highlight Setup. These events shown in the middle pane are logged from setup on the Windows Server.



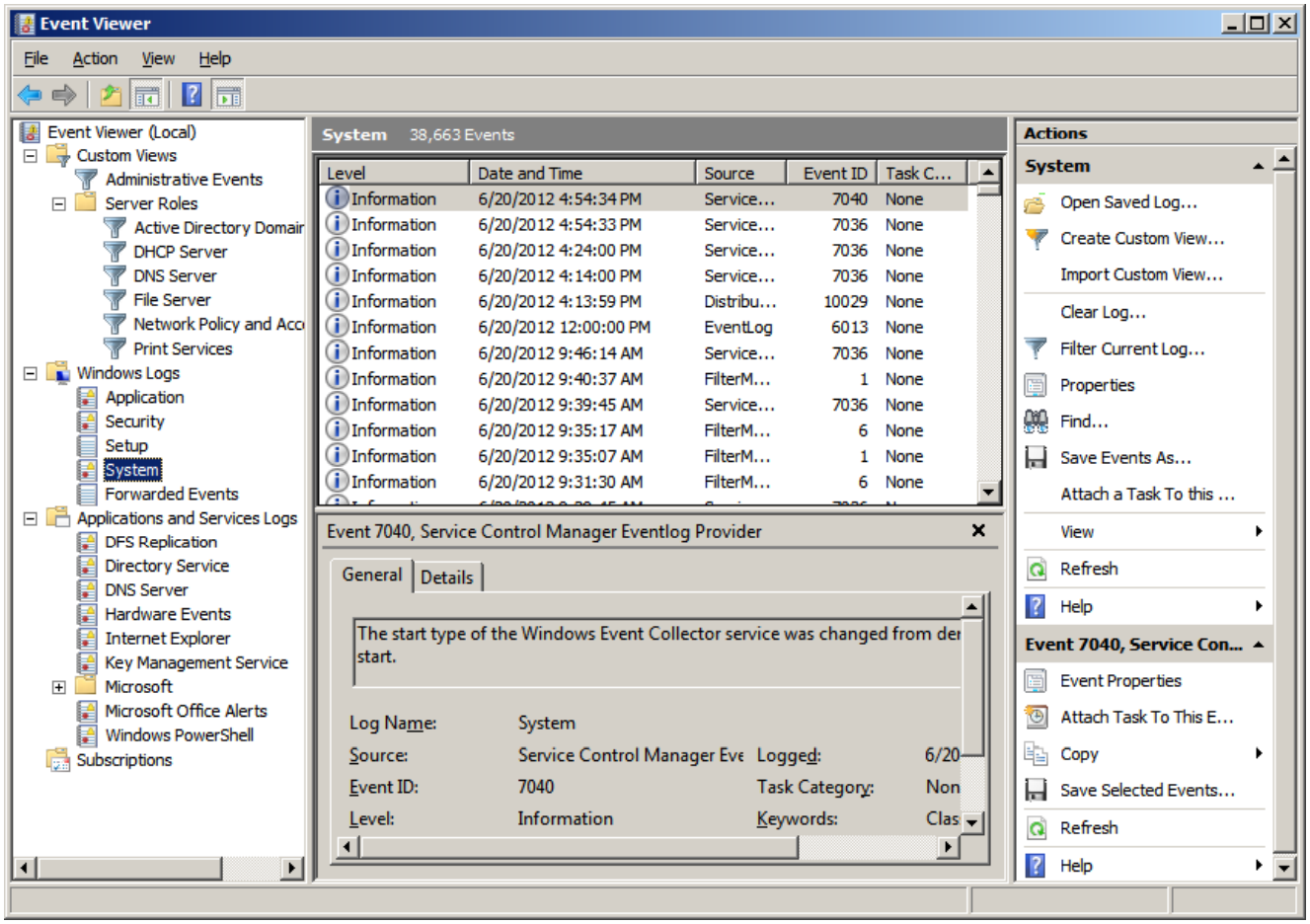
Setup Log Property

We right click on the Setup Log in the left pane and we pick properties from the menu and the Setup log properties window will appear. To change the maximum log size, we would enter the number of kilobytes in the textbox. We can opt to archive a log and do not overwrite the existing log or we can manually clear the log and have no overwrite.



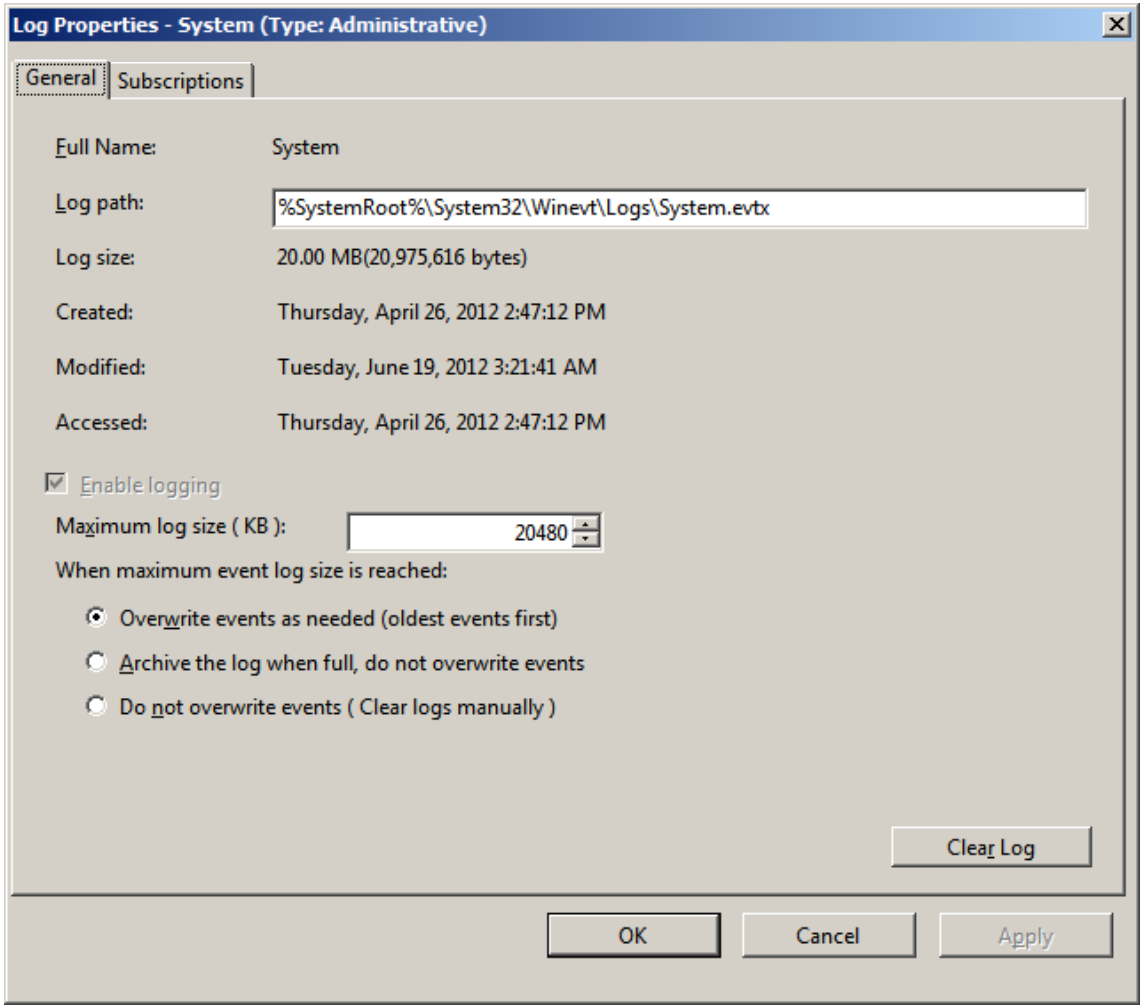
Windows Logs - System

Open the Windows Log folder and highlight System. These events shown in the middle pane are logged from system problems on the Windows Server.



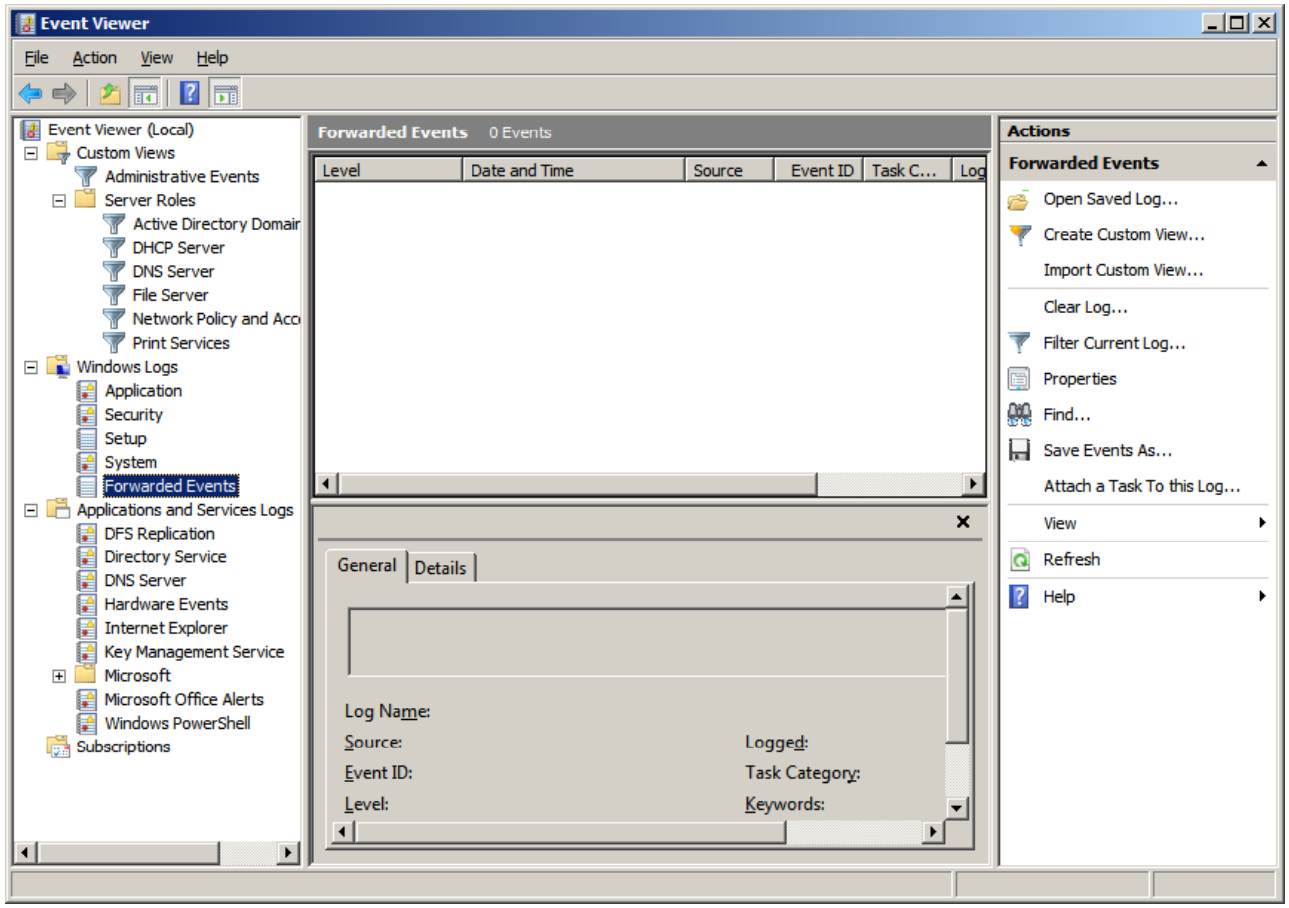
System Log Property

We right click on the System Log in the left pane and we pick properties from the menu and the System log properties window will appear. To change the maximum log size, we would enter the number of kilobytes in the textbox. After setting up a new server in the lab, we can clear the logs right before putting the machine into action. Then we will not have setup events in the history.



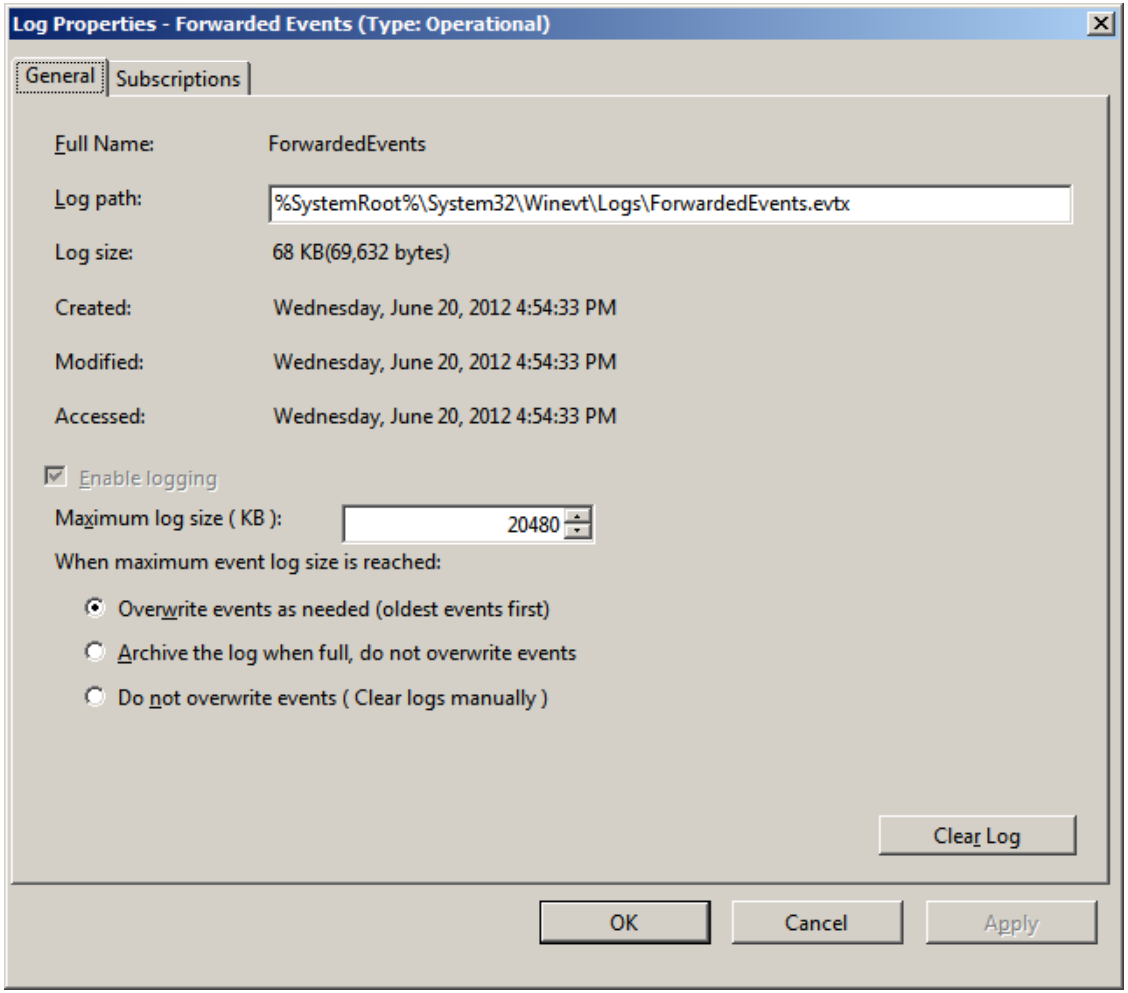
Windows Logs – Forwarded Events

Open the Windows Log folder and highlight Forward Events and we see there are none in the middle pane.



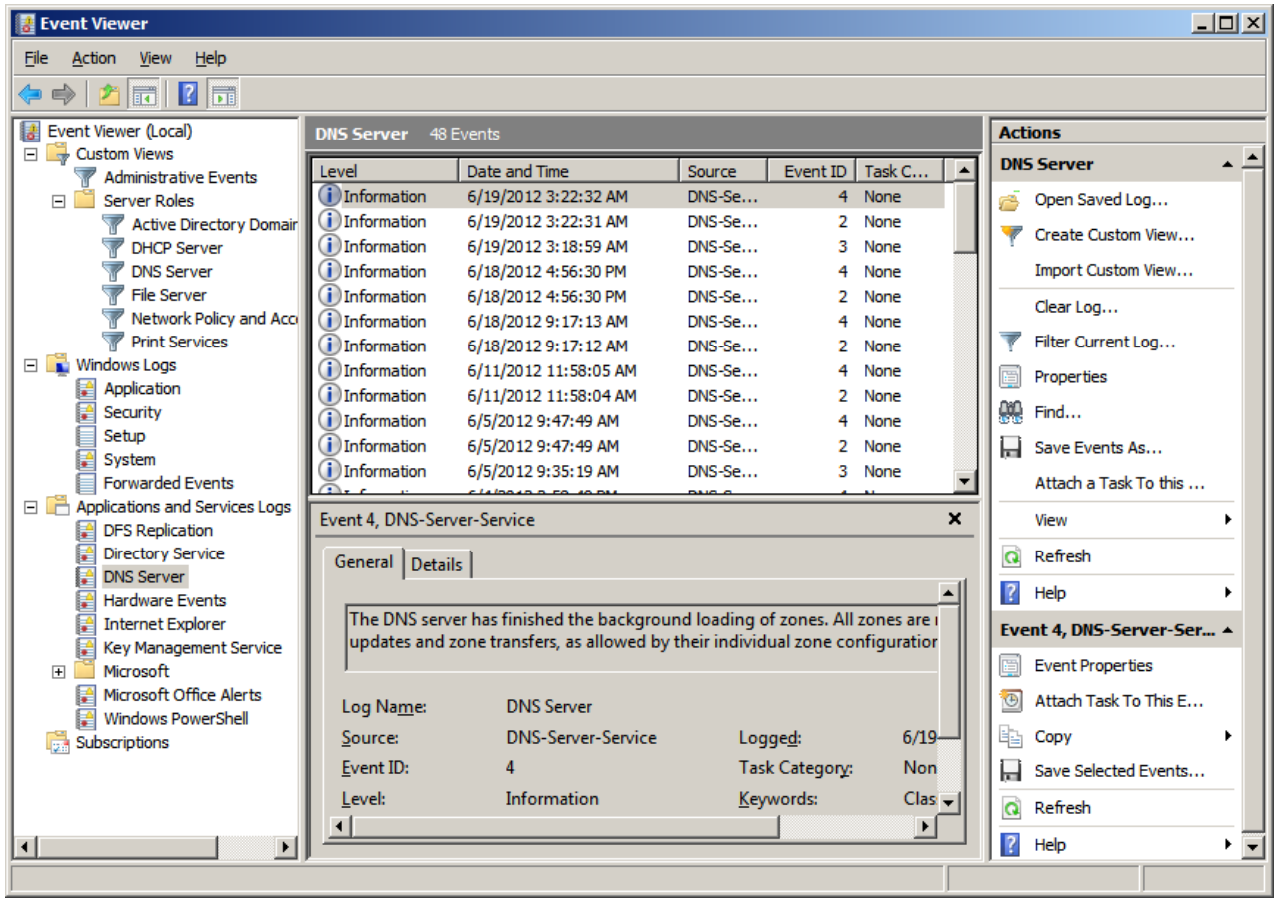
Forwarded Events Log Property

We right click on the Forwarded Events Log in the left pane and we pick properties from the menu and the Forwarded Events log properties window will appear. To change the maximum log size, we would enter the number of kilobytes in the textbox.



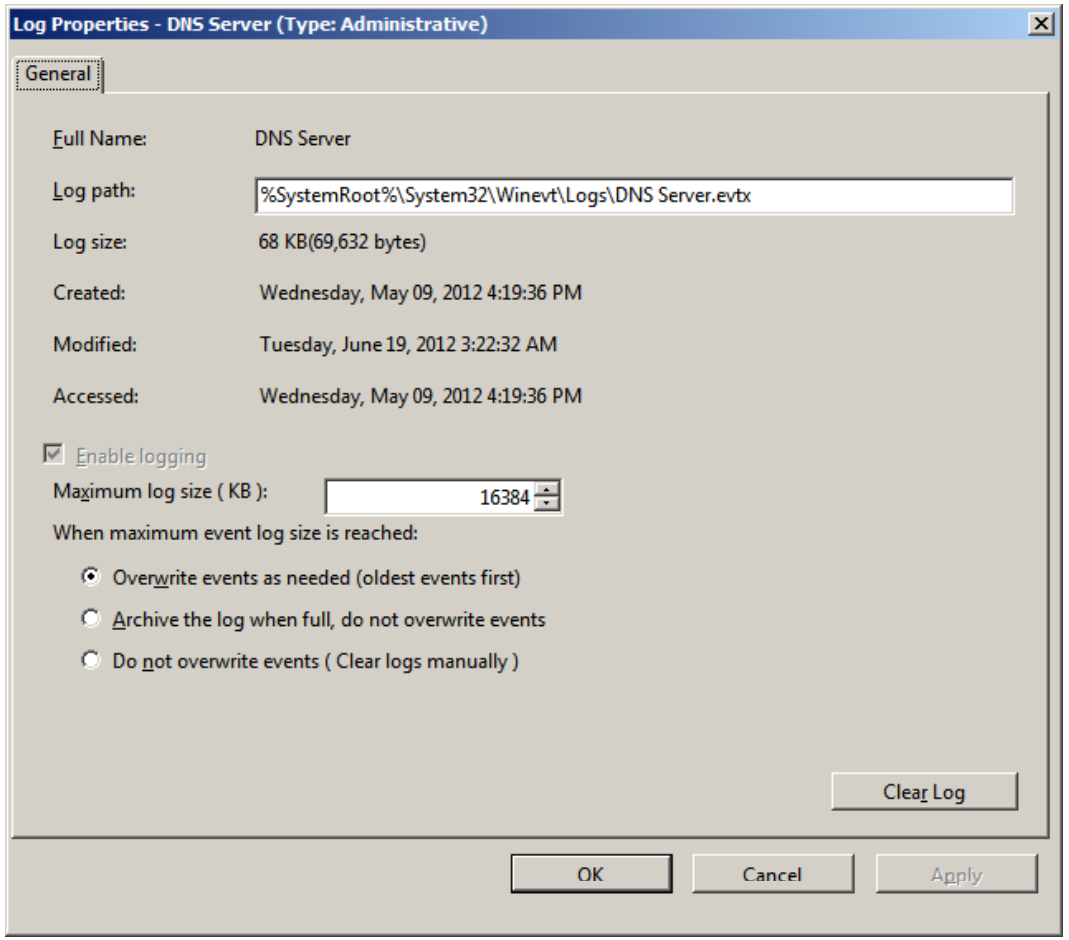
Application and Services Log - DNS Server

Open the Application and Services Log folder and highlight DNS Server and we see there are events in the middle pane.



DNS Server Log Properties

We right click on the DNS Server Log in the left pane and we pick properties from the menu and the DNS Server log properties window will appear. To change the maximum log size, we would enter the number of kilobytes in the textbox.



Recommended Log Sizes

Microsoft recommends these maximum log sizes on the http://support.microsoft.com/kb/957662 website that was released September 11, 2011

Operating system	Recommended maximum size for each log in kilobytes	Recommended maximum total size for all logs in kilobytes	Approximate maximum logging rate (events per second)	Recommended maximum log size to view in kilobytes
Windows Server 2008, 32-bit versions	4,194,240	16,776,960	2,000	4,194,240
Windows Server 2008, 64-bit versions	4,194,240	16,776,960	5,000	4,194,240

Recommended settings for event log sizes in Windows Server 2003, Windows XP, Windows Server 2008 and Windows Vista, September 11, 2011, Microsoft, June 21, 2012, < http://support.microsoft.com/kb/957662 >