COURSE TECHNOLOGY
CENGAGE Learning

Hands-On Microsoft Windows Server 2008

Chapter 10

Managing System Reliability and Availability

Using and Configuring Event Viewer

- Event Viewer
  - Houses the event logs that record information about all types of server events, in the form of errors, warnings, and informational events
- Windows Server 2008 event logs are divided into three general categories:
  1. Windows logs
  2. Applications and services logs
  3. Microsoft logs

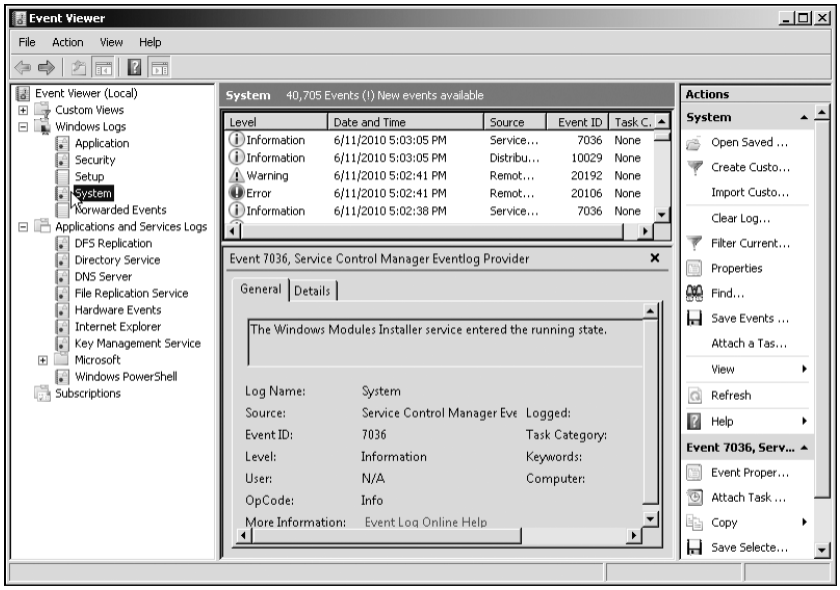


Figure 12-7 Event Viewer

Using and Configuring Event Viewer (continued)

1. **<u>Windows Logs:</u>** generates four logs for reporting general operating system and software application events:
   - System log
     - Hardware errors, driver problems, and hard drive errors.
   - Security log
     - Access and security information about logon accesses, and system policy changes.
   - Application log
     - Records information about how software applications are performing
   - Setup log
     - Contains a record of installation events, such as installing a role or feature through Server Manager.

Using and Configuring Event Viewer (continued)

2. **Applications And Services Logs:** Combined of Operational and Admin log as follows:
   - **Operational log**
     - Tracks occurrences of specific operations.
       - Example: such as when a disk drive is added
   - **Admin logs**
     - Help to give the system administrator information about a specific problem and its causes and may suggest how to solve the problem
       - Example: Reporting that the DFS Replication service has failed and that this might be caused by the Windows Firewall configuration.

Using and Configuring Event Viewer (continued)

- Applications and services logs available in Event Viewer include:
  - DFS Replication log
    - Records events for the Distributed File System Replication services
  - Directory Service log
    - Records events that are associated with Active Directory
  - DNS Server log
    - Records events that are associated with Domain Name System services
  - Hardware Events
    - Records events related to hardware including the CPU, disk drives, memory, and other hardware
  - Internet Explorer
    - Records events related to Internet Explorer

Using and Configuring Event Viewer (continued)

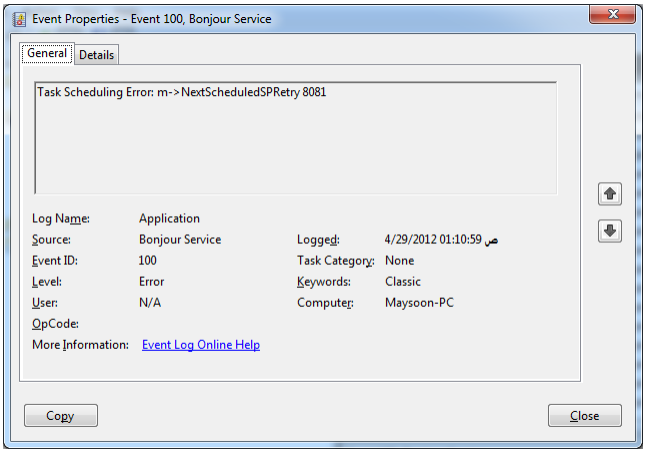
For more complex detailed application and services logs:

- **Analytic logs**
  - Relate to how programs are operating and are typically used by application or system programmers
- **Debug logs**
  - Used by application developers to help trace problems in programs so they can fix program code or program structures

Viewing Log Events

- Log events are displayed in Event Viewer with an icon that indicates the seriousness of the event
- Each log displays descriptive information about individual events, including the following:
  - Description of the event
  - Name of the log in which the event is recorded
  - Source of the event
  - Event ID
  - Level of the event—information, warning, error
  - User associated with the event, if any

Viewing Log Events (continued)

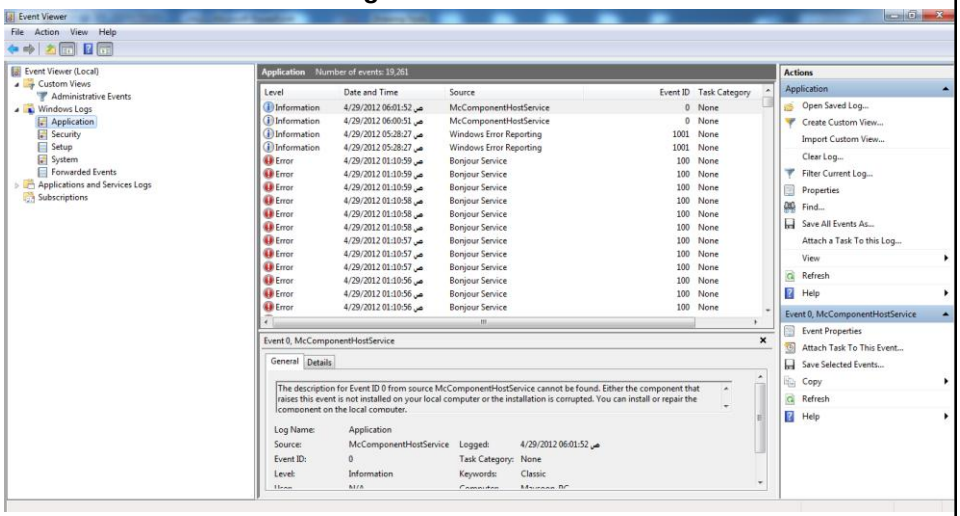


Viewing Log Events (continued)

- Event Viewer can be opened from:
  - Administrative Tools menu
  - Computer Management tool
  - Server Manager
- To view the contents of a log, click that log in the tree under Event Viewer
  - To view the detailed information about an event, double-click the event
- The event logs are a good source of information to help you troubleshoot a software or hardware problem

Viewing The Content a Log

In the following example we double clicked on the **Application** log that is included inside **Windows Logs**



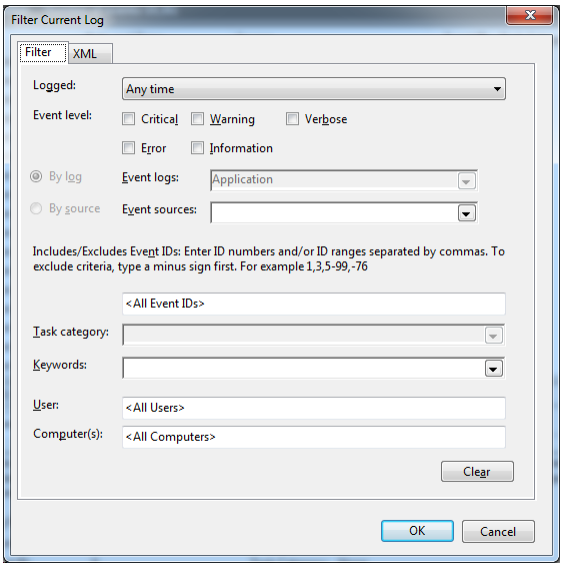
Using the Event Viewer Filter Option

- All of the event logs in Event Viewer have a filter option to help you quickly locate a problem
- The events can be filtered on the basis of the following criteria:
  - When the event was Logged, such as in the last seven days
  - Event level, such as information, warning, error, critical, and verbose
  - By log, such as the application, system or security log
  - By source of the event, such as a particular service or software component

Using the Event Viewer Filter Option (continued)

- The events can be filtered on the basis of the following criteria: (continued)
  - Task category of the event, such as a security change
  - Keywords, such as Audit Failure and Audit Success
  - User associated with the event
  - Computer associated with the event
  - Date range
  - Time of day range

Example: Using the Filter Option with the Application log



Maintaining Event Logs

- Event logs can be quickly filled with information
- Logs can be maintained using several methods, as follows:
  - Size each log to prevent it from filling too quickly
  - Overwrite the oldest events when the log is full
  - Archive the log when it is full
  - Clear the log manually (does not overwrite events)
- It is recommended that you develop a maintenance schedule
  - To save the log contents for a designated time period

Maintaining Event Logs (continued)

- To tune the event logs, open Event Viewer and right-click each log you want to tune, one at a time
  - And click Properties
- On the General tab, set the log size in the *Maximum log size (KB):* box
- You can save the log as one of the following kinds of files:
  - Microsoft Event Viewer logs (.evtx)
  - EXtensible Markup Language (.xml)
  - Text File (.txt)
  - Comma Delimited File (.csv) can be opened from Microsoft Excel.

Maintaining Event Logs