Dealing with Event Viewer

Event Viewer is a troubleshooting tool in Microsoft Windows 2000. This how-to article will describe how to use Event Viewer.

Event Viewer displays detailed information about system events.

This information includes

- Event type.
- The date and time that the event occurred.
- The source of the event.
- The category for the event.
- The Event ID.
- The user who was logged on when the event occurred, and the computer on which the event occurred.

Here we will discuss about the ABC of Event Viewer.

Starting Event Viewer:

Event Viewer can be started from

Start→ Programs→ Administrative Tools→ Event Viewer. Or



Run	<u>?×</u>
<u></u>	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	eventvwr.msc
	OK Cancel Browse

Selecting Computers:

With appropriate administrative authority, you can select any computer in your network to view that computer's Event logs.

To select computers in Event Viewer

1. In the top of the console tree, right-click **Event Viewer (local)**, and then click **Connect to another computer**.

😽 Event Viewer					×
<u>A</u> ction <u>V</u> iew] ⇐ ⇒ 🖿 🖪	1 🗟 😫			
Tree		Event Viewer (Lo	ocal)		
🗑 Event Viewer (L	ocal)	Name		Туре	De
Application	Connect to anothe	er computer	g	Log	Aţ
Security Lc	Open Log File			Log	Se
System Loc	View	•		Log	Sγ
DNS Serve				Log	Q
	Export List				
	Help				▶
View logs on a diffe	rent computer				

- 2. Either browse to the computer name or type the computer name in the dialog box to view the Event log on that computer.
- 3. Click OK.

Select the computer you want this Snap-in to manage.	
🗆 This snap-in will always manage:	
C Local computer: (the computer this console is running on)	
Another computer: Browse	
OK Cancel	

Adjusting Event Viewer Settings:

In Windows 2000, you can adjust Event Viewer settings for a specific log file like display name, max log file size etc.

To adjust the settings for a log file.

- 1. In the console tree, right-click the appropriate log file, and then click **Properties**.
- 2. Click the General tab.

Application Log Pro	operties	<u>?</u> ×
General Filter		
Display name:	Application Log	
Log name:	C:\WINNTS\system32\conf	ig\AppEvent.Evt
Size:	448.0 KB (458,752 bytes)	
Created:	Monday, February 17, 2003 3	3:05:44 PM
Modified:	Thursday, March 06, 2003 10	0:12:04 AM
Accessed:	Thursday, March 06, 2003 10	0:12:04 AM
Log size		
Maximum log s	ize: 512 🔺 KB	
When maximur	m log size is reached:	
O Overwrite e	events as needed	
Overwrite e	events older than 7 📑	days
C Do not ove (clear log r	erwrite events nanually)	Restore Defaults
Using a low-sp	peed connection	Clear Log
		Cancel Apply

Saving Event Logs:

You can save Event Logs for later analysis or for use as historical data. The log files are saved to a file name and location that you choose, with a file name extension that is determined by the format of the saved log file.

To save Event logs

1. In the console tree, right-click the appropriate log file, and then click **Save Log File** As.

😽 Event Vie	wer			. 🗆 🗙
<u>A</u> ction <u>V</u>	jew 📙 🗢 🔿 🖪	1 😭 🕼 🖪	ß	
Tree		Application Log	1,698 event(s)	
Event View	wer (Local)	Туре	Date	Tim 🔺
- 🕑 Applic	ation Lon	Information	3/6/2003	11:
Secu	Open Log File	Information	3/6/2003	11:
Syste	Save Log File As	Information	3/6/2003	11:
DNS	New Log View	Information	3/6/2003	11:
	Clear all Events	Information	3/6/2003	11:
	View 🕨	Information	3/6/2003	11:0
		Information	3/6/2003	10:
	Rename	Information	3/6/2003	10:
	Refresh	Information	3/6/2003	10:
	Export List	Information	3/6/2003	10:
	Properties		3/6/2003	10: 💌
Create a cop	Help			

2. Navigate to the subfolder in which you want to save the file, type a name for the file, click the file type, and then click **Save**.

Save "Applicatio	n Log" As				<u>? ×</u>
Save in:	🔁 templates		•	+ 🗈 💣 🎟 -	
History History Desktop My Documents My Computer					
My Network P	J File name: Save as type:	ApplicationLog3rdM Event Log (*.evt)	arch2003	•	Save Cancel

Clearing Event Logs:

You can manually clear all of the events from an Event log when necessary. On heavily used servers, it is a good idea to save data from the Event log for later administrative use before you clear all of the events.

To clear Event logs:

1. In the console tree, right-click the appropriate log file, and then click **Clear all Events**.

😽 Event 🕈	🔢 Event Viewer							
<u>A</u> ction	<u>A</u> ction ⊻iew ← → 🔁 📧 😭 🔂 🗔 😭							
Tree		Application Log	1,698 event(s)					
Event \	/iewer (Local)	Туре	Date	Tim				
🔚 🚯 Ap		Information	3/6/2003	11:				
🛛 📓 Sei	Open Log File	Information	3/6/2003	11:				
🛛 🔤 Sy:	Save Log File As	Information	3/6/2003	11:				
- 😼 DN	New Log View	Information	3/6/2003	11::				
Clear all Events	Clear all Events	Information	3/6/2003	11:				
	View 🕨	Information	3/6/2003	11:0				
Re		Information	3/6/2003	10:				
	Rename	Information	3/6/2003	10:				
	Rerresh	Information	3/6/2003	10:				
-	Export List	Information	3/6/2003	10:				
	Properties	Information	3/6/2003	10: 👻				
Delete all re	Help			•				

- 2. You are prompted for whether you want to save the log to a file before clearing it.
- 3. Click **Yes** to save a log and clear all events. If you click **No**, the log is not saved, but all events are cleared from the selected Event log. If you click **Cancel**, the request to clear the log is canceled.

Event Vie	wer					×
?	Do you want t	o save "App	lication Lo	og" before	e clear	ing it?
	Yes	No		Cancel		

Viewing Event Details

After you select a log in the Event Viewer, you can search, filter, sort and view details about events.

To view events:

- 1. In the console tree, right-click the appropriate log file. A list of events in the log file is displayed in the details pane of Event Viewer.
- 2. Click a specific event in the details pane to display the **Event Properties** dialog box and details about the event.

Event Prope	ties				? ×
Event					
Date: Time: Type: User: Computer:	3/6/2003 11:32 Information N/A SERVER	Source: Category: Event ID:	ESENT General 101		 ↑ ↓ □
Description	1:				
Data: ©	2) The databa Bytes C Wa	se engine s	topped.		
					×
			IK	Cancel	Apply

Filtering Events:

You can specify a filter that limits the type of information that you want Event Viewer to display. These filters only affect which event log items are displayed in the viewer.

To filter events:

- 1. In the console tree, right-click the appropriate log file, and then click **Properties**.
- Click the Filter tab.
 Type the appropriate information that you would like to filter.
 Click OK.

Application Log Proper	ties
General Filter	
Event types Information Warning Error	 Success audit Failure audit
Event source:	(All)
Category:	(All)
Event ID:	
User:	
Computer:	
From: First Event	▼ 2/20/2003 ▼ 4:00:45 PM ÷
To: Last Event	💌 3/ 6/2003 💌 11:33:54 AM 🚍
	Restore Defaults
	Cancel Apply

Finding Events

Event Viewer provides the option to search for events. Searches can be useful when you are viewing large logs.

To find an event:

- In the console tree, right-click the appropriate log file.
 On the View menu, click Find.

😽 Event V	/iewer				
Action	⊻iew 📙 🗢 🔿 🔁 🗍	I	1 🗗 🕼 🗟	l 😫	
Tree	Choose Columns		Application Log	1,698 event(s)	
Event \	All Records	F	Туре	Date	Tim
- 🚯 Apr	Filter		Information	3/6/2003	11:
Sec	A Newest First		Information	3/6/2003	11:
Sys	Oldest First		Information	3/6/2003	11:
			Information	3/6/2003	11::
	Find		Information	3/6/2003	11:
	Customize		Information	3/6/2003	110
Cascomize			Information	3/6/2003	10:
			Information	3/6/2003	10:
			Information	3/6/2003	10:
			Information	3/6/2003	10:
			Information	3/6/2003	10: 👻
			•		►
Search the l	og for specific records		_		

3. Type the appropriate information that you would like to find in the dialog box, and then click **Find Next**.

Find in local Application Log	?)	<
Event types		
Information	🔽 Success audit	
🔽 Warning	🔽 Failure audit	
Error		
Event source: (All)	-	
Category: (All)	•	
Event ID:		
User:		
Computer:		
Description:		
Search direction		
C Up 💿 Down	Find Next	
	Restore Defaults Close	

4. Click **Close** when you are finished.