

**Report title:** Event Log health report

**Description:** The report is based on important events in the system log, with source EventLog. It displays events like log full, log file corrupt, Event Log service stopping /starting, and unexpected system shutdowns. Use this report to determine failures in the auditing process. These failures may be exploited by attackers and usually lead to loss of audit entries.

**Generated on:** 13-Sep-2006 16:35

**Generated by:** Calin

**Date filter:** 9/7/2006 12:00:00AM to 9/13/2006 11:59:59PM

**Event logs:** System

**Other filters:** event ID= 6000 from System log with source 'EventLog'  
and event ID= 6002 from System log with source 'EventLog'  
and event ID= 6005 from System log with source 'EventLog'  
and event ID= 6006 from System log with source 'EventLog'  
and event ID= 6008 from System log with source 'EventLog'

**Reviewed by:** \_\_\_\_\_

**Reviewed date:** \_\_\_\_\_

**Signature:** \_\_\_\_\_

## Event Log full

Computer	User	Description	Event ID	Source	Time	Date
CALDEV	N/A	The (1): test log file is full.	6000	eventlog	1:47:05PM	9/8/2006
CALDEV	N/A	The (2): test log file is full.	6000	eventlog	1:47:05PM	9/8/2006
CALDEV	N/A	The (3): test log file is full.	6000	eventlog	1:47:05PM	9/8/2006
CALDEV	N/A	The (1): application log file is full.	6000	eventlog	1:54:21PM	9/8/2006
CALDEV	N/A	The (2): application log file is full.	6000	eventlog	1:54:21PM	9/8/2006
CALDEV	N/A	The (3): application log file is full.	6000	eventlog	1:54:21PM	9/8/2006
CALDEV	N/A	The (1): system log file is full.	6000	eventlog	1:54:24PM	9/8/2006
CALDEV	N/A	The (2): system log file is full.	6000	eventlog	1:54:24PM	9/8/2006
CALDEV	N/A	The (3): system log file is full.	6000	eventlog	1:54:24PM	9/8/2006
CALDEV	N/A	The (1): test log file is full.	6000	eventlog	1:47:05PM	9/12/2006
CALDEV	N/A	The (2): test log file is full.	6000	eventlog	1:47:05PM	9/12/2006
CALDEV	N/A	The (3): test log file is full.	6000	eventlog	1:47:05PM	9/12/2006
CALDEV	N/A	The (1): application log file is full.	6000	eventlog	1:54:21PM	9/12/2006
CALDEV	N/A	The (2): application log file is full.	6000	eventlog	1:54:21PM	9/12/2006
CALDEV	N/A	The (3): application log file is full.	6000	eventlog	1:54:21PM	9/12/2006
CALDEV	N/A	The (1): system log file is full.	6000	eventlog	1:54:24PM	9/12/2006
CALDEV	N/A	The (2): system log file is full.	6000	eventlog	1:54:24PM	9/12/2006
CALDEV	N/A	The (3): system log file is full.	6000	eventlog	1:54:24PM	9/12/2006
CALDEV	N/A	The (1): test log file is full.	6000	eventlog	1:47:05PM	9/13/2006
CALDEV	N/A	The (2): test log file is full.	6000	eventlog	1:47:05PM	9/13/2006

Computer	User	Description	Event ID	Source	Time	Date
CALDEV	N/A	The (3): test log file is full.	6000	eventlog	1:47:05PM	9/13/2006
CALDEV	N/A	The (1): application log file is full.	6000	eventlog	1:54:21PM	9/13/2006
CALDEV	N/A	The (2): application log file is full.	6000	eventlog	1:54:21PM	9/13/2006
CALDEV	N/A	The (3): application log file is full.	6000	eventlog	1:54:21PM	9/13/2006
CALDEV	N/A	The (1): system log file is full.	6000	eventlog	1:54:24PM	9/13/2006
CALDEV	N/A	The (2): system log file is full.	6000	eventlog	1:54:24PM	9/13/2006
CALDEV	N/A	The (3): system log file is full.	6000	eventlog	1:54:24PM	9/13/2006

## Event log service started

Computer	User	Description	Event ID	Source	Time	Date
CALDEV	N/A	The Event log service was started.	6005	eventlog	1:47:05PM	9/8/2006
CALDEV	N/A	The Event log service was started.	6005	eventlog	1:47:05PM	9/8/2006
CALDEV	N/A	The Event log service was started.	6005	eventlog	1:47:05PM	9/8/2006
CALDEV	N/A	The Event log service was started.	6005	eventlog	1:47:05PM	9/12/2006
CALDEV	N/A	The Event log service was started.	6005	eventlog	1:47:05PM	9/12/2006
CALDEV	N/A	The Event log service was started.	6005	eventlog	1:47:05PM	9/12/2006
CALDEV	N/A	The Event log service was started.	6005	eventlog	1:47:05PM	9/13/2006
CALDEV	N/A	The Event log service was started.	6005	eventlog	1:47:05PM	9/13/2006
CALDEV	N/A	The Event log service was started.	6005	eventlog	1:47:05PM	9/13/2006

## Event Log service stopped

Computer	User	Description	Event ID	Source	Time	Date
CALDEV	N/A	The Event log service was stopped.	6006	eventlog	1:47:05PM	9/8/2006
CALDEV	N/A	The Event log service was stopped.	6006	eventlog	1:47:05PM	9/8/2006
CALDEV	N/A	The Event log service was stopped.	6006	eventlog	1:47:05PM	9/8/2006
CALDEV	N/A	The Event log service was stopped.	6006	eventlog	1:47:05PM	9/12/2006
CALDEV	N/A	The Event log service was stopped.	6006	eventlog	1:47:05PM	9/12/2006
CALDEV	N/A	The Event log service was stopped.	6006	eventlog	1:47:05PM	9/12/2006
CALDEV	N/A	The Event log service was stopped.	6006	eventlog	1:47:05PM	9/13/2006
CALDEV	N/A	The Event log service was stopped.	6006	eventlog	1:47:05PM	9/13/2006
CALDEV	N/A	The Event log service was stopped.	6006	eventlog	1:47:05PM	9/13/2006

## Log file corrupt

Computer	User	Description	Event ID	Source	Time	Date
CALDEV	N/A	The (4): test log file is corrupted and will be cleared.	6002	eventlog	1:47:05PM	9/8/2006
CALDEV	N/A	The (5): test log file is corrupted and will be cleared.	6002	eventlog	1:47:05PM	9/8/2006
CALDEV	N/A	The (6): test log file is corrupted and will be cleared.	6002	eventlog	1:47:05PM	9/8/2006
CALDEV	N/A	The (4): test log file is corrupted and will be cleared.	6002	eventlog	1:47:05PM	9/12/2006
CALDEV	N/A	The (5): test log file is corrupted and will be cleared.	6002	eventlog	1:47:05PM	9/12/2006
CALDEV	N/A	The (6): test log file is corrupted and will be cleared.	6002	eventlog	1:47:05PM	9/12/2006
CALDEV	N/A	The (4): test log file is corrupted and will be cleared.	6002	eventlog	1:47:05PM	9/13/2006
CALDEV	N/A	The (5): test log file is corrupted and will be cleared.	6002	eventlog	1:47:05PM	9/13/2006
CALDEV	N/A	The (6): test log file is corrupted and will be cleared.	6002	eventlog	1:47:05PM	9/13/2006

## Unexpected system shutdown

Computer	User	Description	Event ID	Source	Time	Date
CALDEV	N/A	The previous system shutdown at (13): test on (13): test was unexpected.	6008	eventlog	1:47:05PM	9/8/2006
CALDEV	N/A	The previous system shutdown at (14): test on (14): test was unexpected.	6008	eventlog	1:47:05PM	9/8/2006
CALDEV	N/A	The previous system shutdown at (15): test on (15): test was unexpected.	6008	eventlog	1:47:05PM	9/8/2006
CALDEV	N/A	The previous system shutdown at (13): test on (13): test was unexpected.	6008	eventlog	1:47:05PM	9/12/2006
CALDEV	N/A	The previous system shutdown at (14): test on (14): test was unexpected.	6008	eventlog	1:47:05PM	9/12/2006
CALDEV	N/A	The previous system shutdown at (15): test on (15): test was unexpected.	6008	eventlog	1:47:05PM	9/12/2006
CALDEV	N/A	The previous system shutdown at (13): test on (13): test was unexpected.	6008	eventlog	1:47:05PM	9/13/2006
CALDEV	N/A	The previous system shutdown at (14): test on (14): test was unexpected.	6008	eventlog	1:47:05PM	9/13/2006
CALDEV	N/A	The previous system shutdown at (15): test on (15): test was unexpected.	6008	eventlog	1:47:05PM	9/13/2006