

Monitoring Windows Event Logs



ManageEngine
OpManager

Powering IT ahead

Monitoring Windows Event Logs

Using OpManager

The Windows event logs are files serving as a placeholder of all occurrences on a Windows machine. This includes logs on specific occurrence on the system, an application or the operating system. Be it an incorrect login attempt, a hack, an application failure, or a system failure- all these happenings are 'logged' here, helping troubleshoot a fault, and also monitor the system's health. All Windows events include information on the occurrence such as the event time, the source of the event, the type of fault, and a unique ID for the event type. The event logs contain a wealth of information, which helps an administrator troubleshoot and manage the system. The Event Viewer utility on the Windows device helps in viewing all the events on that machine.

Why should Event Logs be monitored?

Prevention is better than cure. This applies perfectly for network monitoring too! In this era of the Internet, where hacking is commonplace, being a smart proactive administrator is a must. Securing network information, ensuring data integrity, assuring 100% uptime of important services etc is critical to business. Juggling with multiple tools to address different monitoring needs only compounds to the stress. Let us consider the following two possibilities:

1. Daily Backup

Periodic backup of your network data is the first step for disaster recovery. Assume you have an application like Veritas doing the backup job for you. Ensuring a smooth backup is a critical task, specially, in environments where you hold important customer data. It needs little imagination to say what will happen if the backup fails and you end up finding it out only the next morning!

2. ISA Firewall Service

The objective of enabling a firewall for security, goes for a toss when the firewall service goes down or is unwilling to start and you discover hours later! Of all things, no administrator would like to fail in safeguarding the network. A quick warning over an SMS or email, or a popup on your machine for the ISA firewall failure will save a lot of time. Monitoring specific event logs like with the ID 11000 will solve this problem.

An event log is the first call for help! Naturally, as an administrator, the responsibility of watching out for the help calls lies with you and you need to choose and put in place a proper solution to track the important events. Both the above situations could have been avoided, or at least, mended in time by monitoring the event logs 57751, 34113 for the backup failures.

Though the Windows Event Viewer gives an exhaustive account of the events, the problem however is the lack of a centralized view of these events across machines. Moreover, a huge

number of event logs are 'information' events and can be conveniently ignored. Automating the monitoring of important event logs is the next logical step and therefore calls for an effective monitoring tool. That said; let us see how OpManager helps you achieve this in addition to monitoring all other network resources.

OpManager - The Guardian Angel

We understand the importance of simplified, centralized monitoring. There can be nothing cooler than an application intelligently filtering important event logs and notifying it periodically. This apart from monitoring the devices, applications, and other hardware resources!

OpManager provides a set of about 50 pre-defined event log rules. Besides, you can configure as many rules as required to address your [event log monitoring](#) need and assign appropriate severity. The default rules can be modified or removed too. Based on the rules, the event logs are converted into OpManager alarms and you can be notified also using an email or sms. The ability to define rules based on any or all of the windows event log properties is of sure plus!

OpManager acts as the guardian angel for your network by keeping a watch on the important event logs of the entire Windows environment as discussed above. For instance, a user who is restricted access to specific machines is trying to access a network drive on one of the machines, a cause for security concern. A failure audit event is triggered in the event logs and you will see the event listed in the Security event log category. With just a few clicks, you will be able to configure this Failure audit event log monitoring for all your windows machines. When there is a security event of this nature, OpManager generates a corresponding meaningful alarm and also notifies immediately over SMS or email.

It is highly impossible for an administrator to keep a watch for a security breach on each and every machine's event logs. Life is easier when he can view all the problems from a single console. And this is possible if OpManager is deployed in this network.

Some typical Windows events that need monitoring

Security Events

Often, securing the network from internal user becomes a daunting task. Users restricted from accessing critical servers try logging in. Hackers at times meddle with the audit service so that the login attempts are not traced. Security events are logged for all these.

Application Events

Any application failure raises an event. Highly critical services like Active Directory, and its related services, failure of critical services startup like that of ISA, more than the allowed number of users trying to access an application, insufficient system resources for an application

to run etc require round-the-clock monitoring. All these are critical to business and will prove costly if unattended. You will find event logs for all these.

System Events

The health of a system needs to be good to serve important applications. Any system failure needs monitoring. It can be a bad disk, attempt by a user to replace a system file. Again, the first clue to the failure comes from the event logs.

DNS Server

Active Directory depends extensively on the DNS service availability. Needless to say that it needs monitoring. The Domain Controllers have a specific category to log the system events specific to DNS.

File Replication Server

This service is responsible for replicating data across the Domain Controllers. Failure of this service leads to critical issues such as logon. This too, therefore needs monitoring. Like DNS, a separate category is provided for FRS too for quicker troubleshooting.

OpManager monitors the event logs in all the above categories and in fact you can define your own event log rules! Here are some screenshots showing what OpManager can do:

Separate view to see Windows event logs:



The screenshot shows the 'Active Alarms' interface in OpManager. At the top, there are buttons for 'Acknowledge', 'UnAcknowledge', 'Clear', and 'Delete'. Below these is a table of active alarms. The table has columns for Source, Alarm Message, Status, Technician, Category, and Date / Time. Two alarms are visible: one for 'Linux-Server-I' and one for 'W2k-Server-II'. The 'Date / Time' column for the second alarm has a dropdown arrow, and a red arrow points to the 'Windows Events' option in the dropdown menu.

Source	Alarm Message	Status	Technician	Category	Date / Time
Linux-Server-I	Device not responding: Probably down or busy	Attention	UnAssigned	Server	16 Dec 2011 11:11:11
W2k-Server-II	Device not responding: Probably down or busy	Attention	demoadmin	Server	13 Dec 2011 10:39:53 PM

Availability threshold limit violated (< 100%), 100 % of requests sent from cisco2800Router failed to reach 203.199.211.77.
Command Output: □

Event Logs Processed into OpManager Alarms:

Windows Events RSS Windows Events

Show Page size 25 1 to 6 of 6 [1]

Source	Alarm Message	Status	Technician	Category	Date / Time
<input type="checkbox"/> W2k8R2-Server-1	ID=1111 Source=Microsoft-Windows-TerminalServices-Printers Type=1 Message=Driver HP LaserJet M5035 MFP PCL 6 required for printer !!AV-SERVER!dif-printer is unknown. Contact the administrator to install the driver before you log in again.	Critical	UnAssigned	Server	12 Dec 2011 10:48:54 AM
<input type="checkbox"/> W2k8R2-Server-1	ID=4321 Source=NetBT Type=1 Message=The name "OPMAN-K8R2S-64-:0" could not be registered on the interface with IP address 172.18.161.66. The computer with the IP address 172.18.170.47 did not allow the name to be claimed by this computer.	Critical	UnAssigned	Server	6 Dec 2011 09:42:59 PM
	ID=4029 Source=Microsoft-Windows-TelnetServer				

Intuitive Pre-defined Event Log Rules in OpManager:

Event Log Rules Add Custom Event log

Application	Rule Name	Edit	Delete
	Any Application failure		
	An ISA service failed to start		
	Disk restriction in place for ISA Server		
	ISA cannot send data across the data line route		
	Cache initialization fail for ISA		
	Transaction log full for a SQL database		
	Insufficient memory available for MS SQL		
	Database backup failed for MS SQL		
	Windows Installer : Install operation		
	Windows Installer : Application Installed Successfully		
	Windows Installer : Application uninstalled		
	Chasis intrusion		
	Norman antivirus found infected file		
	Dameware remote control		
	New Rule...		

DNS Server	Rule Name	Edit	Delete
	Any DNS Server failure		
	DNS Server started		
	Bad DNS Zone Transfer		
	DNS Server has timed out		
	DNS Server is being updated		
	DNS Zone has been shut down		
	New Rule...		

File Replication Service	Rule Name	Edit	Delete
	Any File Replication Service failure		
	File Replication Service is starting		
	New Rule...		

Directory Service	Rule Name	Edit	Delete
	Any Directory Service failure		
	Active Directory is started		
	Active Directory is stopped		
	NTDS database engine is started		
	NTDS database engine is stopped		
	NTDS Defragmentation is started		
	NTDS Defragmentation is complete		
	New Rule...		

Security	Rule Name	Edit	Delete
	Any Security failure		
	Object Deletion failure due to restricted permissions		
	Logon Failure : NetLogon inactive or not available for this user		
	Logon Failure : Unknown / Unexpected error		
	Server Shutting Down		
	Event Log Resources exhausted		
	Computer Account Created		

Notifying an Event Log through an email or SMS:

Define Criteria for profile EventLog

Select all

when the Device misses poll(s)

when an **interface or switch port has some problems**

when any [selected...] **Service is down**

when any [selected...] **Windows Service is down**

when any [selected...] **SNMP trap is received** from the device.

when any assigned **Threshold rule** is violated.

when the **URL is down**

when any [selected...] **Script Monitor is down or has violated a threshold**

when any [selected...] **Process is down or has violated a threshold**

when any [selected...] **File Monitors has violated a threshold**

when any [selected...] **Folder Monitors has violated a threshold**

when any [selected...] **Event Log Rules** generates alarm

when any [selected...] **Syslog Rules** generates alarm

when any [selected...] **Virtual Device has problem**

when any **Agent is down**

notify when the **alarm is cleared**

Advanced <<

Notify only when severity is

<input checked="" type="checkbox"/> Any	<input checked="" type="checkbox"/> Trouble
<input checked="" type="checkbox"/> Critical	<input checked="" type="checkbox"/> Service down
<input checked="" type="checkbox"/> Attention	

Selecting the Rules for which Notification should be sent:

Event Log Rules

Select all

Application

<input type="checkbox"/> Any Application failure	<input type="checkbox"/> An ISA service failed to start	<input type="checkbox"/> Disk restriction in place for ISA Server	<input type="checkbox"/> ISA cannot send data across the data line route
<input type="checkbox"/> Cache initialization fail for ISA	<input type="checkbox"/> Transaction log full for a SQL database	<input type="checkbox"/> Insufficient memory available for MS SQL	<input type="checkbox"/> Database backup failed for MS SQL
<input type="checkbox"/> Windows Installer : Install operation	<input type="checkbox"/> Windows Installer : Application Installed Successfully	<input type="checkbox"/> Windows Installer : Application uninstalled	<input type="checkbox"/> Chasis intrusion
<input type="checkbox"/> Norman antivirus found infected file	<input type="checkbox"/> Dameware remote control		

Security

<input type="checkbox"/> Any Security failure	<input type="checkbox"/> Object Deletion failure due to restricted permissions	<input type="checkbox"/> Logon Failure : NetLogon inactive or not available for this user	<input type="checkbox"/> Logon Failure : Unknown / Unexpected error
<input type="checkbox"/> Server Shutting Down	<input type="checkbox"/> Event Log Resources exhausted	<input type="checkbox"/> Computer Account Created	<input type="checkbox"/> Computer Account Changed
<input type="checkbox"/> Computer Account Deleted	<input type="checkbox"/> New program or process has been launched	<input type="checkbox"/> A program or process has exited	

We recommend monitoring the following event logs. Please note

Category	Event IDs
Security	<ul style="list-style-type: none">• 564- Object Deletion failure due to restricted permissions• 536 - NetLogon inactive or not available for this user• 537 - Unknown/Unexpected error• 513 - Server shutting down
Application	<ul style="list-style-type: none">• 11000 - ISA Service failure• 17052 - Insufficient memory available for MS SQL• 5774, 5775, 5781, 5783, 5805 - Netlogon service events• 40960, 40961 - LDAP service events
System	<ul style="list-style-type: none">• 64001- System file replacement• 7 - Disk : Bad Sector detected• 4202 - Network adaptor disconnected
DNS Server	<ul style="list-style-type: none">• 6004 - Bad DNS Zone Transfer• 4016 - DNS Server has timed out• 6527 - DNS Zone has been shut down
File Replication Server	13508, 13509, 13511, 13522, 13526

Summary

OpManager is a comprehensive monitoring solution monitoring all resources on your network and comes with extensive windows event logs monitoring capabilities. Managing event logs centrally cannot be easier!! Stop by at our support portal for any queries.