

# 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 OpManager interface with the 'Alarms' tab selected. On the left, there is a 'Device Search' box with 'buddy' entered and a 'Search' button. Below it, an 'Alarms' sidebar lists options: 'Devices to watch', 'Unsolicited Traps', 'All Alarms', 'Active Alarms', and 'Windows Events' with a link 'Click here'. The main area displays a list of alarms. The first alarm is from 'akarthik.india.adventn...' with ID=680, Source=Security, Type=5, and Message='Logon attempt by: MICROSOFT AUTHENTICATION PACKAGE V1.0 Logon account: Administrator Source Workstation: SDP-TEST1 Error Code: 0xC000006A'. The second alarm is from 'vidvavasu.india.advent...' with ID=1517, Source=Userenv, Type=2, and Message='Windows saved user ADVENTNET\vidvavasu registry while an application or service was still using the registry during log off. The memory used by the user's registr...'. The interface also shows 'Showing 1 to 4 of 4' and 'Page: [1]'.

### Event Logs Processed into OpManager Alarms:

Source	Alarm Message	Status
<input type="checkbox"/> advw2k-server.india.ad...	ID=3 Source=Active Server Pages Type=3 Message=Service started.	Critical
<input type="checkbox"/> advw2k-server.india.ad...	ID=1 Source=WinVNC4 Type=3 Message=Connections: accepted: 192.168.111.196::49046	Critical
<input type="checkbox"/> mnageanyware.com	ID=2102 Source=MSExchangeDSAccess Type=1 Message=Process MAD.EXE (PID=3344). All Domain Controller Servers in use are not responding: mail.mnageanyware.com For more information, click <a href="http://www.microsoft.com/contentredirect.asp">http://www.microsoft.com/contentredirect.asp</a> .	Critical
<input type="checkbox"/> mnageanyware.com	ID=2003 Source=Perflib Type=2 Message=The configuration information of the performance library "C:\WINDOWS\system32\inetsrv\w3ctrs.dll" for the "W3SVC" service does not match the trusted performance library information stored in the registry. The functio	Critical
<input type="checkbox"/> mnageanyware.com	ID=14120 Source=Microsoft Web Proxy Type=1 Message=The ISA Server services cannot create a packet filter 60.43.155.132. This event occurs when there is a conflict between the Local Address Table (LAT) configuration and the Windows 2000 routing table. Che	Critical

**Intuitive Pre-defined Event Log Rules in OpManager:**

<input checked="" type="checkbox"/> Monitor Event Log For this device		Monitoring Interval : <input type="text" value="300"/> seconds	
<b>Application</b> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Any Application failure</li> <li><input type="checkbox"/> An ISA service failed to start</li> <li><input type="checkbox"/> Disk restriction in place for ISA Server</li> <li><input type="checkbox"/> ISA cannot send data across the data line route</li> <li><input type="checkbox"/> Cache initialization fail for ISA</li> <li><input type="checkbox"/> Transaction log full for a SQL database</li> <li><input type="checkbox"/> Insufficient memory available for MS SQL</li> <li><input type="checkbox"/> Database backup failed for MS SQL</li> <li><input type="checkbox"/> Windows Installer : Install operation</li> <li><input type="checkbox"/> Windows Installer : Application Installed Successfully</li> <li><input type="checkbox"/> Windows Installer : Application uninstalled</li> <li><input type="checkbox"/> Chasis intrusion</li> <li><input type="checkbox"/> Norman antivirus found infected file</li> <li><input type="checkbox"/> Dameware remote control</li> </ul>		<b>Security</b> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Any Security failure</li> <li><input type="checkbox"/> Object Deletion failure due to restricted permissions</li> <li><input type="checkbox"/> Logon Failure : NetLogon inactive or not available for this user</li> <li><input type="checkbox"/> Logon Failure : Unknown / Unexpected error</li> <li><input type="checkbox"/> Server Shutting Down</li> <li><input type="checkbox"/> Event Log Resouces exhausted</li> <li><input type="checkbox"/> Computer Account Created</li> <li><input type="checkbox"/> Computer Account Changed</li> <li><input type="checkbox"/> Computer Account Deleted</li> <li><input type="checkbox"/> New program or process has been launched</li> <li><input type="checkbox"/> A program or process has exited</li> </ul>	
<b>System</b> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Any System failure</li> <li><input type="checkbox"/> System file replacement attempt</li> <li><input type="checkbox"/> Eventlog Service stopped</li> </ul>		<b>DNS Server</b> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Any DNS Server failure</li> <li><input type="checkbox"/> DNS Server started</li> <li><input type="checkbox"/> Bad DNS Zone Transfer</li> </ul>	

**Notifying an Event Log through an email or SMS:**

**Define Criteria for profile EventLogProfile**

**Select all**

- when the Device misses  poll(s)
- When an **interface or switch port is down**
- when any [selected...] **Service is down**
- when any [selected...] **Windows Service is down**
- when a **SNMP trap is received** from the device
- when any assigned **Threshold rule** is violated.
- when any [selected...] **Event Log Rules** generates alarm
- notify when the **alarm is cleared**

**Selecting the Rules for which Notification should be sent:**

Application			
<input checked="" type="checkbox"/> Any Application failure	<input checked="" type="checkbox"/> An ISA service failed to start	<input checked="" type="checkbox"/> Disk restriction in place for ISA Server	<input checked="" 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 checked="" 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 checked="" type="checkbox"/> Any Security failure	<input type="checkbox"/> Object Deletion failure due to restricted permissions	<input checked="" 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	

  

System			
<input checked="" type="checkbox"/> Any System failure	<input type="checkbox"/> System file replacement attempt	<input checked="" type="checkbox"/> Eventlog Service stopped	<input type="checkbox"/> Disk : Bad Sector detected
<input type="checkbox"/> Save Dump:	<input type="checkbox"/> Network adapter	<input type="checkbox"/> Network	<input type="checkbox"/> DHCP : Out of

We recommend monitoring the following event logs. Please note that

Category	Event IDs
Security	<ul style="list-style-type: none"> <li>• 564- Object Deletion failure due to restricted permissions</li> <li>• 536 - NetLogon inactive or not available for this user</li> <li>• 537 - Unknown/Unexpected error</li> <li>• 513 - Server shutting down</li> </ul>
Application	<ul style="list-style-type: none"> <li>• 11000 - ISA Service failure</li> <li>• 17052 - Insufficient memory available for MS SQL</li> <li>• 5774, 5775, 5781, 5783, 5805 - Netlogon service events</li> <li>• 40960, 40961 - LDAP service events</li> </ul>

Category	Event IDs
System	<ul style="list-style-type: none"> <li>• 64001- System file replacement</li> <li>• 7 - Disk : Bad Sector detected</li> <li>• 4202 - Network adaptor disconnected</li> </ul>
DNS Server	<ul style="list-style-type: none"> <li>• 6004 - Bad DNS Zone Transfer</li> <li>• 4016 - DNS Server has timed out</li> <li>• 6527 - DNS Zone has been shut down</li> </ul>
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.