

# Integrating Dell server hardware alerts into SBS 2008 report

By Perumal Raja  
Dell | Enterprise Product Group



## CONTENTS

---

Introduction:	3
SBS Management Console in SBS 2008:	3
Monitoring and Reporting feature in SBS 08:	4
Dell OpenManage tool	5
Adding OpenManage Alerts into SBS Report	6
Creating custom alerts:	7
Procedure to add a custom alerts file to the installed SBS	9
Sample Script	10
Reference	12

---

## Introduction:

This white paper provides information on the Monitoring and Reporting feature in the Microsoft Windows Small Business Server 2008 SBS Console and the alert mechanism in Dell OpenManage systems management tool. It includes instructions to integrate the OpenManage alerts into the SBS System Report. This white paper is ideal for users who have a Windows SBS-based infrastructure deployed and wants to generate a comprehensive report with both software and hardware alerts.

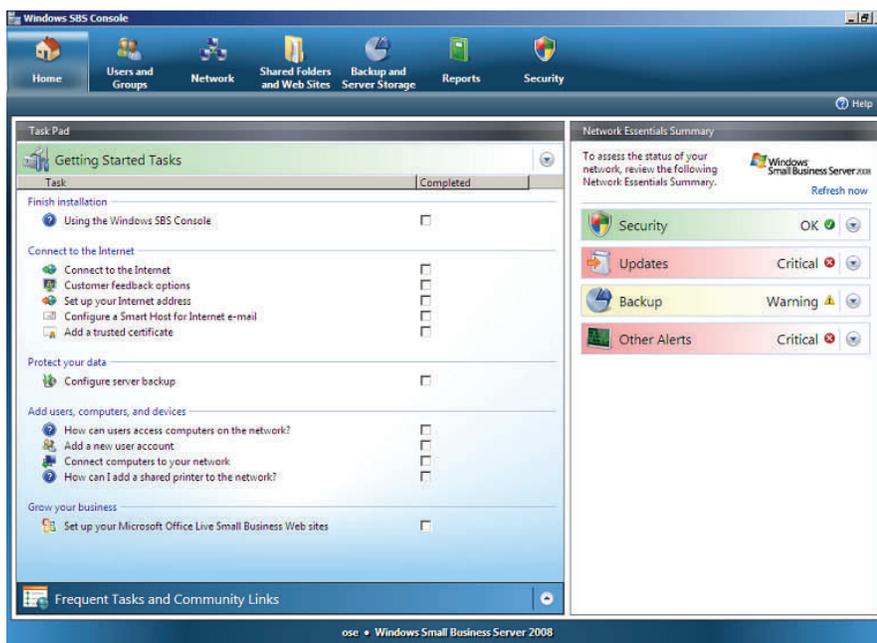
## SBS Management Console in SBS 2008:

Windows Small Business Server 2008 includes a new streamlined administration and management console called Windows SBS Console (fig 1) which makes it easy to configure and manage your Small Business network. By using the Windows SBS Console, you can:

- View high-level network status.
- Manage users and groups on your network.
- Manage computers, printers, faxes, and network connectivity.
- Manage access and settings for shared folders and Web sites.
- Manage backup, restore, and data storage.
- Add and customize server reports.
- Manage updates, antispyware, anti-spam, antivirus, and file-system antivirus settings.

Windows SBS Console provides base operational monitoring and policy definitions for SBS server, second server (if you have Premium Edition), and all domain joined clients. It gives a daily view of PC's and servers and makes it easier to manage common IT tasks.

Figure 1 Windows SBS Console



## Monitoring and Reporting feature in SBS 08:

One of the significant new features in Small Business Server 2008 is to monitor the health of the system & generate alerts and overall reports if a system has a problem. These reports can be emailed to the administrator or save it in a different location for future analysis.

Alerts that are generated are listed under four categories:

- **Security** – Displays the status of the security components: Anti-spam, anti-spyware, e-mail anti-virus, and file system anti-virus
- **Updates** – Displays the status of the software updates for the computers on your network.
- **Backup** – Displays the status of the server backup(s).
- **Other Alerts** – Displays remaining server and computer related alerts.

Apart from these pre-defined alerts, you can also create additional customized alerts.

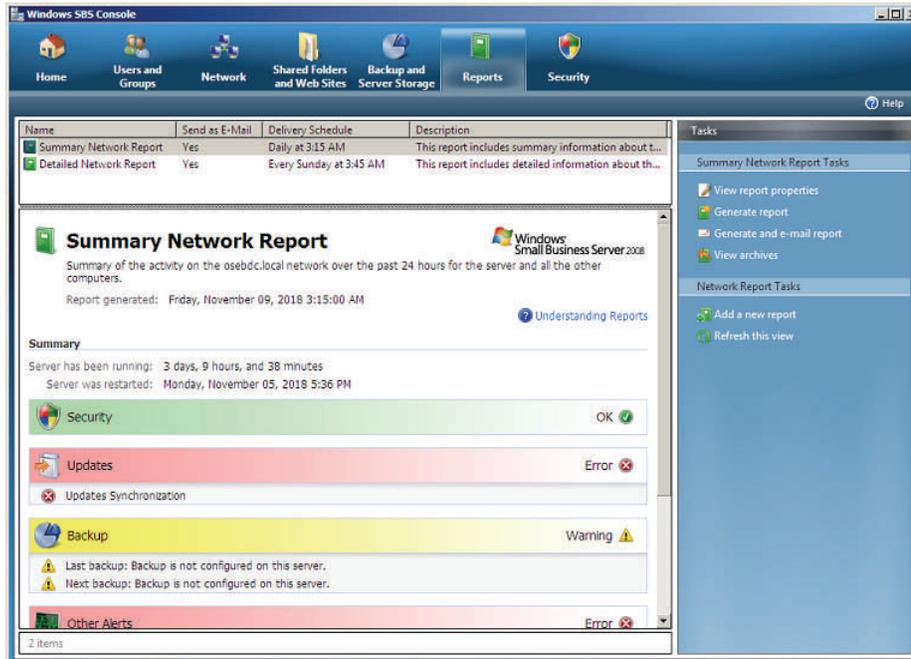
The **Home** tab in the Windows SBS Console provides you with the current status of the SBS network. Administrators can browse to **Security**, **Backup** and **Server Storage & Network** tabs in Windows SBS Console to find the exact information of the generated alerts.

An SBS Report is generated by pulling the network or application error events logged in the Event Viewer. Administrators can periodically generate reports and archive them for future reference or analysis. By default, Small Business Server 2008 comes with two core reports that cannot be deleted but can be modified.

- **Summary Network Report** – Displays a summary of the activity on the SBS network over the past 24 hours. This includes both server and computers.
- **Detailed Network Report** – Provides detailed information concerning the performance of your network.

Apart from the Microsoft provided reports, you can also add a new report with your custom actions.

**Figure 2 Report Tab in Windows SBS Console**



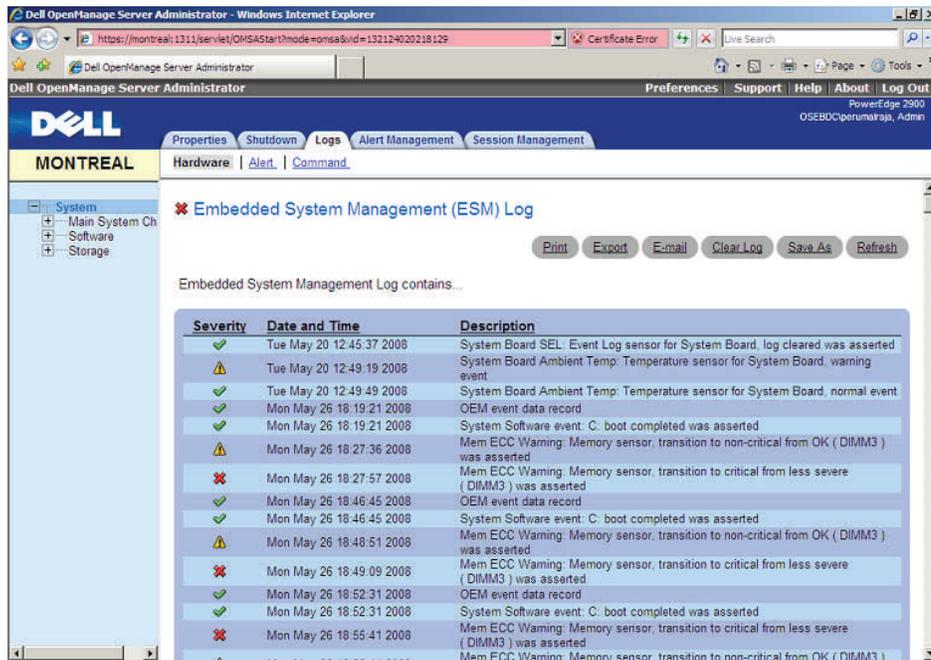
## Dell OpenManage tool:

The Dell PowerEdge servers in combination with Dell OpenManage systems management tools provide alerting mechanisms that proactively notify system administrators about abnormalities of system hardware before failure occurs. It is critical that system administrators be notified before hardware failures occur or as soon as possible.

You can configure Dell PowerEdge servers managed through Dell OpenManage tools to generate and send Simple Network Management Protocol (SNMP) traps, trigger local alert actions, or generate

and send Platform Event Traps (PETs) when they detect system error events or status changes. It logs the alert messages in the Operating system through Event viewer as Error event. You can configure these alerting mechanisms using Dell OpenManage Server Administrator (OMSA), a software tool that allows administrators to manage individual servers locally or remotely using a graphical user interface (GUI), or locally using the OMSA command-line interface (CLI). Figure 3 displays the list of hardware alerts generated in the local system which can also be saved for later analysis.

**Figure 3 Hardware Alerts Logged by OpenManage Tool**



## Adding OpenManage Alerts into SBS Report:

By default, the report provided by the Microsoft pulls only the software-related error events in the SBS network to the report. Any of the hardware (System) related error events generated by the OpenManage (OM) tool is not recorded in the Report. The OM tool has its own error logging mechanism and options to archive the Hardware related error events generated, integrating both error events (alerts) into one report reduces complexity. A one-time job for the administrator to set up the integration provides value if they plan to archive the report in addition to reviewing it.

To have this customized report, Microsoft provides a way to have custom alerts to add the hardware alerts to the SBS report. Administrators can view these alerts in the Windows SBS Console, under **Other Alerts** section in the **Home** Tab. By installing OpenManage, you get the advantage of pulling critical hardware error events into the report.

## Creating custom alerts:

Custom alerts are configured in XML files and copied into “*C:\Program Files\Windows Small Business Server\Data\Monitoring\ExternalAlerts*” folder of the Windows SBS 2008 operating system at any time after the installation is completed. These alert files contain references to events that are already being logged in Event Viewer by OpenManage tools, and contain enough information to display these events as part of the Windows SBS Console reports.

The following xml script can be used as an example for creating your own custom alerts file.

```
<AlertDefinitions>
  <AlertDefinition ID="469ADADA-0000-1111-9999-ADADADADA001"
    Default="1"
    Title="OpenManage Log"
    Source="Server Administrator">
    <Parameters>
      <Path>System</Path>
      <Provider>Server Administrator</Provider>
      <SetEventID>2335</SetEventID>
      <ClearEventID />
    </Parameters>
  </AlertDefinition>
</AlertDefinitions>
```

Table 1 provides the description of the parameters required for creating a custom alert.

**Table 1 Parameters for Creating a Custom Alert**

Element	Description
AlertDefinition	<p>This element identifies a unique event source from an installed driver or application (OpenManage). The AlertDefinition contains the following values:</p> <ul style="list-style-type: none"> <li>• <b>ID</b> – The GUID assigned to the event being described. The column in the database for this entity is the SQL type "unique identifier" so any other format does not work. You can choose any hexadecimal number you want, so long as it is unique, follows the format provided in the example and does not already exist in Windows SBS 2008. Best option is to create a GUID of the format provided in the example and increment the values for subsequent alerts. Alternatively you can use the command “[System.Guid]::NewGuid().ToString()” in Windows PowerShell available in the SBS 2008 to get unique ID.</li> <li>• <b>Default</b> – A value of 1 means the alert is included by default when the application (OpenManage tool) is installed, and is restored if you click Restore Defaults on the Reports page.</li> <li>• <b>Title</b> – A string of text to be displayed as a title for the alert in the Notification Settings.</li> <li>• <b>Source</b> – A text string representing the name of the application or module that generated the alert.</li> </ul>

Element	Description
Parameters	<p>The Parameters element contains the data to populate the event within the Windows SBS 2008 report. It contains the following values:</p> <ul style="list-style-type: none"> <li>• <b>Path</b> – Represents the name of the event log where the event appears. OpenManage tool populates the error event in the “System” section in the Event Viewer. So always use “System” as provider for any OpenManage logs.</li> <li>• <b>Provider</b> – A display name for the module that generates the alert. Server Administrator is the provider for any of the OpenManage logs.</li> <li>• <b>SetEventID</b> – This is the ID number (within the Path and Source parameters) of the event that triggers the alert.</li> <li>• <b>ClearEventID</b> – This is the ID number of the event that signals the alert has been cleared. This is an optional parameter. If there is no ClearEventID parameter, the event is considered to be cleared after 30 minutes.</li> </ul>

## Procedure to add a custom alerts file to the installed SBS 08 system:

1. Create a new XML file to contain your custom alert definitions using Notepad or XML editor.
2. Add your custom alerts, and then save the file. Give a meaningful name to the file. For eg. “SBSCustomAlerts1.xml”.
3. Copy the file into the “*C:\Program Files\Windows Small Business Server\Data\Monitoring\ExternalAlerts*” folder after completing the Small Business Server 2008 installation.
4. Restart the Windows SBS Manager Service.

To restart the Windows SBS Manager Service

A. Click **Start**, point to **Administrative Tools**, and then click **Services**

B. Right-click the **Windows SBS Manager Service**, and then click **Restart**.

**Note :**

You can copy new custom alerts files into the ExternalAlerts folder at any time. But, you must restart the Windows SBS Manager Service in order to have the new alerts file read. The custom alert files are only read during the startup of the Windows SBS Manager Service and it takes around 30 minutes to get displayed in the Report.

**Note:**

To get the list of Event ID's for the alerts generated by the OpenManage Tool, see *Dell™ OpenManage™ Messages Reference Guide* on the Dell Support website at **support.dell.com**. Administrators can choose which OpenManage hardware alerts to be logged into SBS report from the list of Event ID provided in the document.

## Sample Script:

Below is list of OpenManage alerts that gets into the Server Event Logs section of the SBS report as displayed in the Fig 4 using the sample script provided here.

- ESM log size is full.
- Failure of Fan 4 in the system chassis.
- Fan redundancy lost in the System chassis.

```
<AlertDefinitions>
  <AlertDefinition ID="469ADADA-0000-1111-9999-ADADADADA005"
    Default="1"
    Title="Open Manage Log"
    Source="Server Administrator">
    <Parameters>
      <Path>System</Path>
      <Provider>Server Administrator</Provider>
      <SetEventID>1104</SetEventID>
      <ClearEventID />
    </Parameters>
  </AlertDefinition>
```

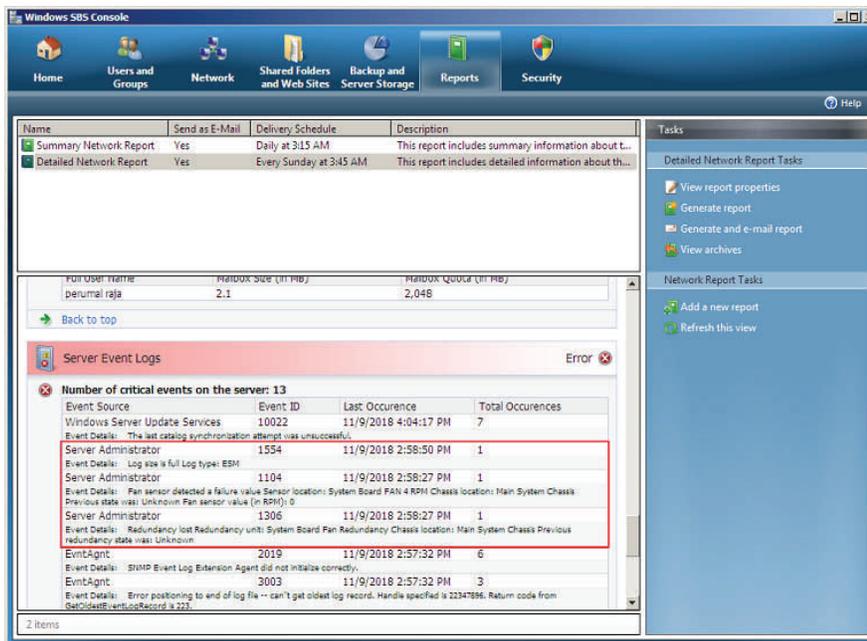
```

<AlertDefinition ID="469ADADA-0000-1111-9999-
ADADADADA006"
    Default="1"
    Title="Open Manage Log"
    Source="Server Administrator">
  <Parameters>
    <Path>System</Path>
    <Provider>Server Administrator</Provider>
    <SetEventID>1554</SetEventID>
    <ClearEventID />
  </Parameters>
</AlertDefinition>

<AlertDefinition ID="469ADADA-0000-1111-9999-
ADADADADA007"
    Default="1"
    Title="Open Manage Log"
    Source="Server Administrator">
  <Parameters>
    <Path>System</Path>
    <Provider>Server Administrator</Provider>
    <SetEventID>1306</SetEventID>
    <ClearEventID />
  </Parameters>
</AlertDefinition>
</AlertDefinitions>

```

Figure 4 OpenManage Tool Generated Alerts Listed in SBS Report



**Note:**

While creating the custom alert file, change only the values of **Alert-Definition ID & EventID** and keep all other fields constant.

**Reference:**

<http://support.dell.com/support/edocs/software/svradmin/>

<http://msdn.microsoft.com/en-us/library/cc721719.aspx>

<http://technet.microsoft.com/en-us/library/cc527559.aspx>

**Disclaimer:**

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT OF THIS WHITE PAPER ARE PROVIDED AS IS, WITH NO WARRANTIES, EXPRESS OR IMPLIED. DELL EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY. UNDER NO CIRCUMSTANCES, INCLUDING, BUT NOT LIMITED TO, NEGLIGENCE, SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOSS OF DATA OR PROFIT, ARISING OUT OF THE USE, OR THE INABILITY TO USE, THE INFORMATION, EVEN IF DELL OR A DELL AUTHORIZED REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

© 2008 Dell Inc. All rights reserved.

Trademarks used in this text: *Dell* and *PowerEdge* are trademarks of Dell, Inc.; *Microsoft*, *Windows Server*, and *Windows* are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to see to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.