

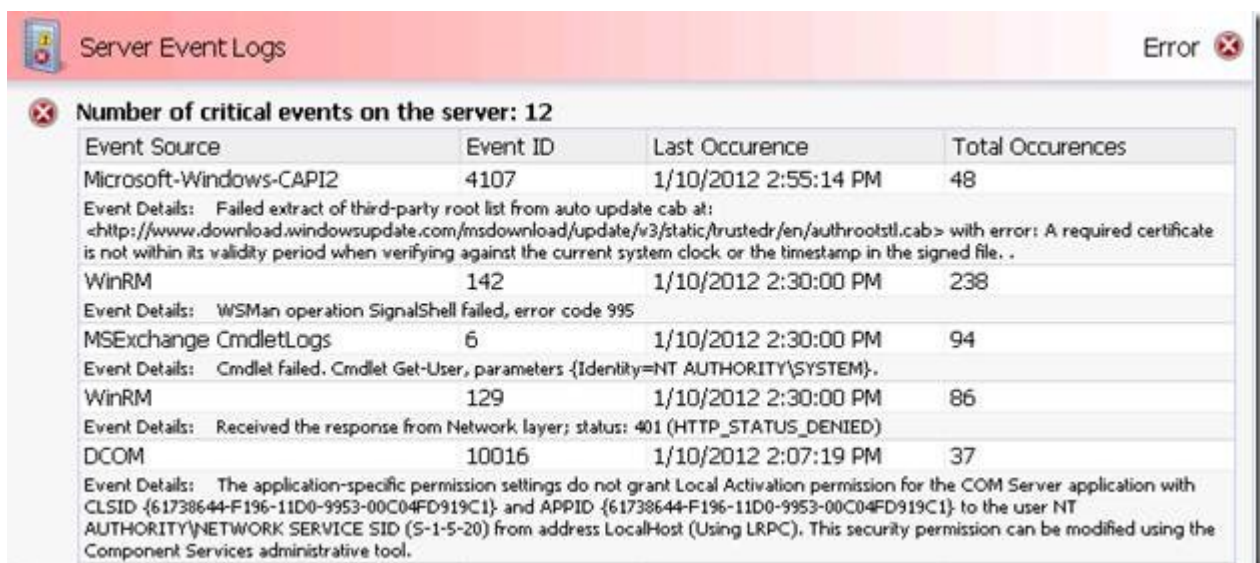
Managing Event Alerts in Your Reports - An SBS Monitoring Feature Enhancement

One of the most requested features for the SBS Monitoring component of Windows SBS 2008 and Windows SBS 2011 Standard is the ability to control and filter unwanted errors from the event logs section of the reports.

There are a number of known events that can be safely ignored. Also depending on the particular environment you might have your own list of events you want to ignore. You cannot accomplish this with the built-in, out-of-box, functionality.

This, as-is solution, was built by engineers from the SBS support team and is aimed at improving the functionality and effectiveness of the SBS Monitoring reports.

The relevant portion of a detailed report from SBS 2011 standard before installing the new functionality:

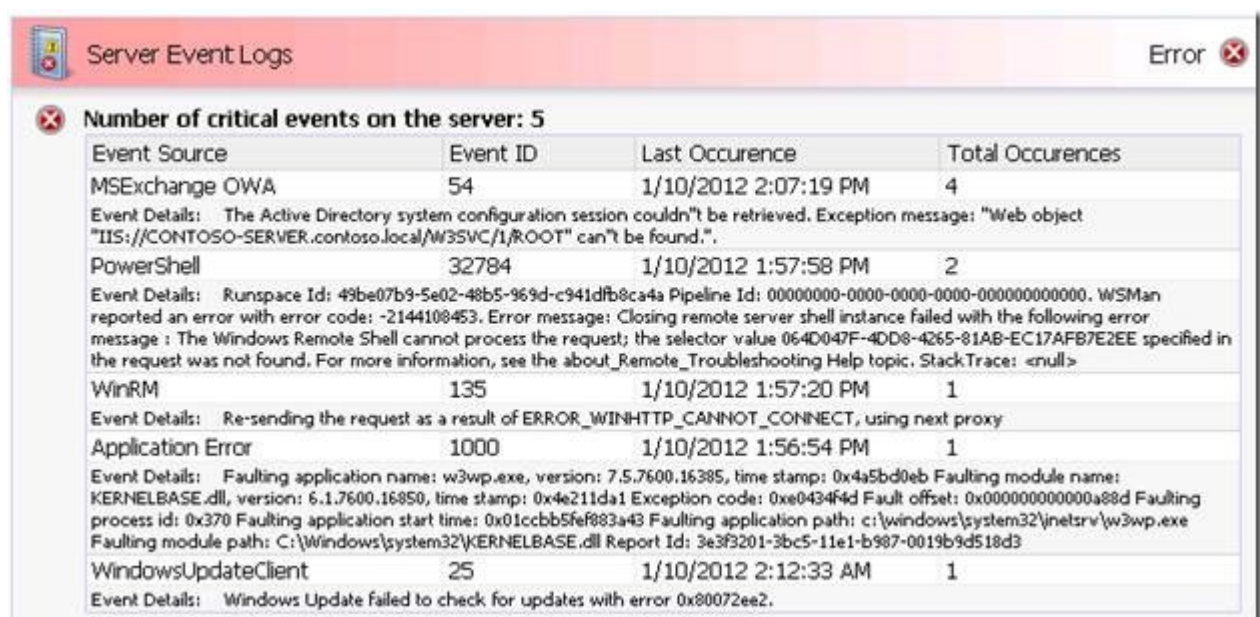


Server Event Logs Error

Number of critical events on the server: 12

| Event Source | Event ID | Last Occurrence | Total Occurrences |
|--|----------|----------------------|-------------------|
| Microsoft-Windows-CAPI2 | 4107 | 1/10/2012 2:55:14 PM | 48 |
| Event Details: Failed extract of third-party root list from auto update cab at: <http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab> with error: A required certificate is not within its validity period when verifying against the current system clock or the timestamp in the signed file. . | | | |
| WinRM | 142 | 1/10/2012 2:30:00 PM | 238 |
| Event Details: WSMAN operation SignalShell failed, error code 995 | | | |
| MSEExchange CmdletLogs | 6 | 1/10/2012 2:30:00 PM | 94 |
| Event Details: Cmdlet failed. Cmdlet Get-User, parameters {Identity=NT AUTHORITY\SYSTEM}. | | | |
| WinRM | 129 | 1/10/2012 2:30:00 PM | 86 |
| Event Details: Received the response from Network layer; status: 401 (HTTP_STATUS_DENIED) | | | |
| DCOM | 10016 | 1/10/2012 2:07:19 PM | 37 |
| Event Details: The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {61738644-F196-11D0-9953-00C04FD919C1} and APPID {61738644-F196-11D0-9953-00C04FD919C1} to the user NT AUTHORITY\NETWORK SERVICE SID (S-1-5-20) from address LocalHost (Using LRPC). This security permission can be modified using the Component Services administrative tool. | | | |

The same report with the feature installed using the default exclusions:



Server Event Logs Error

Number of critical events on the server: 5

| Event Source | Event ID | Last Occurrence | Total Occurrences |
|--|----------|----------------------|-------------------|
| MSEExchange OWA | 54 | 1/10/2012 2:07:19 PM | 4 |
| Event Details: The Active Directory system configuration session couldn't be retrieved. Exception message: "Web object "IIS://CONTOSO-SERVER.contoso.local/W3SVC/1/ROOT" can't be found." | | | |
| PowerShell | 32784 | 1/10/2012 1:57:58 PM | 2 |
| Event Details: Runspace Id: 49be07b9-5e02-48b5-969d-c941dfb8ca4a Pipeline Id: 00000000-0000-0000-0000-000000000000. WSMAN reported an error with error code: -2144108453. Error message: Closing remote server shell instance failed with the following error message : The Windows Remote Shell cannot process the request; the selector value 064D047F-4DD8-4265-81AB-EC17AFB7E2EE specified in the request was not found. For more information, see the about_Remote_Troubleshooting Help topic. StackTrace: <null> | | | |
| WinRM | 135 | 1/10/2012 1:57:20 PM | 1 |
| Event Details: Re-sending the request as a result of ERROR_WINHTTP_CANNOT_CONNECT, using next proxy | | | |
| Application Error | 1000 | 1/10/2012 1:56:54 PM | 1 |
| Event Details: Faulting application name: w3wp.exe, version: 7.5.7600.16385, time stamp: 0x4a5bd0eb Faulting module name: KERNELBASE.dll, version: 6.1.7600.16850, time stamp: 0x4e211da1 Exception code: 0xe0434f4d Fault offset: 0x000000000000a88d Faulting process id: 0x370 Faulting application start time: 0x01ccbb5fef883a43 Faulting application path: c:\windows\system32\inetrv\w3wp.exe Faulting module path: C:\Windows\system32\KERNELBASE.dll Report Id: 3e3f3201-3bc5-11e1-b987-0019b9d518d3 | | | |
| WindowsUpdateClient | 25 | 1/10/2012 2:12:33 AM | 1 |
| Event Details: Windows Update failed to check for updates with error 0x80072ee2. | | | |

Notice how the critical event count went from 12 to 5, and unimportant DCOM and WinRM events have been hidden.

How it works

This solution configures a database table with a number of source:event combinations (known as exclusions) that need not be collected from the event logs, for example: DCOM 10016. Upon installing the solution a default set of exclusions are added depending on the version of SBS and the existing instances that have already been collected are removed. The same is true when a new exclusion is added manually, existing source:events instances will be deleted.

Upon removing an exclusion or uninstalling the solution, the process of collecting all events will resume and only after the event is experienced again it will then be collected and will appear on the report.

Installation and Usage

1. Download and extract the [SBSAlertsCleanup](#) package which is hosted on the SBS Support Team's SkyDrive.
2. Open the location of the extracted files and then the properties of **SBSAlertsCleanup.ps1** file.
3. **Unblock** the file if the option is shown. **Note:** you do not need to do this to the .sql files.
4. Launch an elevated PowerShell prompt.
5. From PowerShell, browse to the folder where you extracted the files.
6. From PowerShell, run:
.\SBSAlertsCleanup.ps1 -Action install [enter]

You will see "Changed database context to 'SBSMonitoring'

Listing current Exclusions

.\SBSAlertsCleanup.ps1 -Action ListExclusions

ID Event Source

```
1 129 WinRM
2 142 WinRM
3 4107 Microsoft-Windows-CAPI2
4 10016 DCOM
5 10009 DCOM
6 5586 SharePoint Foundation
7 6772 SharePoint Foundation
8 6398 SharePoint Foundation
9 8 MExchange CmdletLogs
10 6 MExchange CmdletLogs
```

Removing an Exclusion

This is a 2 part process, first you have to list the current exclusions, and then we can pick which one to remove.

.\SBSAlertsCleanup.ps1 -Action ListExclusions

ID Event Source

```
1 129 WinRM
2 142 WinRM
3 4107 Microsoft-Windows-CAPI2
```

4 10016 DCOM
5 10009 DCOM
6 5586 SharePoint Foundation
7 6772 SharePoint Foundation
8 6398 SharePoint Foundation
9 8 MExchange CmdletLogs
10 6 MExchange CmdletLogs

.\SBSAlertsCleanup.ps1 -Action RemoveExclusion -ID 1

Removing Exclusion for Source: WinRM, EventID: 129

To confirm:

.\SBSAlertsCleanup.ps1 -Action ListExclusions

ID Event Source

-- -----

2 142 WinRM
3 4107 Microsoft-Windows-CAPI2
4 10016 DCOM
5 10009 DCOM
6 5586 SharePoint Foundation
7 6772 SharePoint Foundation
8 6398 SharePoint Foundation
9 8 MExchange CmdletLogs
10 6 MExchange CmdletLogs

Adding an Exclusion

This is a 2 part process, first you have to list the available instances of events that have already been collected, and then we can pick which one to exclude.

.\SBSAlertsCleanup.ps1 -Action ListEvents

ID Event Source

-- -----

346141 11 Disk
349778 13 Server Infrastructure Licensing
349779 14 Server Infrastructure Licensing
349781 15 Server Infrastructure Licensing
349552 25 WindowsUpdateClient
349832 54 MExchange OWA
349827 135 WinRM
349795 502 Windows Small Business Server 2011 Standard
349809 1000 Application Error
343153 1016 DhcpServer
342822 2002 ESENT
348341 2007 ESE
342823 2007 ESENT

Let's say that the administrator was been receiving several events for WindowsUpdateClient 25 on a regular basis. The admin has investigated this event and determined that it is not cause for concern on their network and they would no longer like to be notified about this event. The admin can do the following to exclude this event from the report:

.\SBSAlertsCleanup.ps1 -Action AddExclusion -ID 349552

Adding Exclusion for Source: WindowsUpdateClient, EventID: 25

To confirm:

.\SBSAlertsCleanup.ps1 –Action ListExclusions

ID Event Source

2 142 WinRM
3 4107 Microsoft-Windows-CAPIC
4 10016 DCOM
5 10009 DCOM
6 5586 SharePoint Foundation
7 6772 SharePoint Foundation
8 6398 SharePoint Foundation
9 8 MExchange CmdletLogs
10 6 MExchange CmdletLogs
11 25 WindowsUpdateClient

Uninstalling

Upon removing an exclusion or uninstalling the product, the process of collecting all events will resume and only after the event is experienced again it will then be collected and will appear on the report.

.\SBSAlertsCleanup.ps1 –Action Uninstall

Default set of exclusions

We install a set of common exclusions for known events that are generally considered as ignorable. This may not be the case for each and every server so you might have to tweak the list of exclusions, removing and adding as needed as to make your reports show relevant errors that could be of interest for someone administering the health of the server.

SBS 2008

- 10016 DCOM
- 10009 DCOM

SBS 2011 Standard

- 129 WinRM
- 142 WinRM
- 4107 Microsoft-Windows-CAPIC
- 10016 DCOM
- 10009 DCOM
- 5586 SharePoint Foundation
- 6772 SharePoint Foundation
- 6398 SharePoint Foundation
- 8 MExchange CmdletLogs
- 6 MExchange CmdletLogs

Hopefully, this simple enhancement can help you regain control of the reports and fine tune them to your needs.