




Recommended Sentry-go Monitoring Settings

© 3Ds (UK) Limited, December, 2013
<http://www.Sentry-go.com>

Be Proactive, Not Reactive!

Automated monitoring with Sentry-go Quick Monitors or Sentry-go Plus! provides a powerful way of ensuring your Windows server environment is performing as designed to its optimum. However, any such solution is only ever as good as the options you've asked it to check. Understanding these settings and the values returned is therefore key to getting the best out of it.

In the notes that follow, we outline the settings you might consider using in a typical monitored environment.

-  Some of these options are dependent on the Quick Monitor or Plus! monitoring components installed. Suggested values are a guide only; you should always consider your specific needs when determining thresholds or monitored values.

Full details showing how to configure Sentry-go monitors can be found in the appropriate product documentation.

Recommended alerting settings

Alerts are very much dependent on your setup and how you wish to be notified of events or errors. However, a typical installation might include the following ...

- **E-mail**

E-mails are a great way of being notified of issues detected by the monitor, at any time of day. If you have different teams looking after aspects of your environment – e.g. web team, DBA, network etc., consider using “alert groups” and configuring an e-mail address for each. Details of specific errors can then be forwarded to the appropriate group.

- **SMS/Text message**

SMS is a much more immediate way of being notified of errors, even more so when you're away from the office environment, such as overnight or weekends. You might configure Sentry-go to notify by SMS during these times only, through an alert schedule.

- **Network message**

When you're in the office, at a logged on PC, network messaging is an ideal (and free) way of being notified immediately a fault is detected.

- **Scripting**

If you have third party software or wish to perform some custom action, such as automatically print an error, you can use a custom script. Scripts available on-line at <http://www.Sentry-go.com>, you can provide your own or we can help develop them for you. Please contact us for more information at <http://www.3Ds.co.uk>.

Recommended monitoring

<i>Monitored Area</i>	<i>Monitored Item</i>	<i>Recommended Settings</i>
Heartbeat monitoring	All monitors	<p>From a single monitor (monitor "A"), check for a response from all other monitors.</p> <p>From one of the others, also check for a response from monitor "A".</p>
Network monitoring	All servers in the domain	Check for a response from all "important" servers. If necessary, ignore less critical ones by overriding the default setting.
	Critical "IP" devices	Add any specific IP addresses of critical TCP/IP network resources. Check for a response from these.

<p>Performance monitoring <i>(the Sentry-go Performance Wizard can help configure initial settings)</i></p>	<p>For all servers ...</p> <p>For Terminal Services ...</p> <p>For Terminal Services ...</p>	<p>Check overall loading and health of the server ...</p> <ul style="list-style-type: none"> • Continually high (> 80%) CPU • Available memory • No. running processes • No. open files • % paging file used • % registry database used <p>Check for error conditions & suspect activity ...</p> <ul style="list-style-type: none"> • No. recent internal server errors (> 1, cumulative count) • No. suspect access attempts (> 1, cumulative count) • No. suspect logon attempts (> 1, cumulative count) <p>Check loading ...</p> <ul style="list-style-type: none"> • No. T/server sessions (> designed max.) • High no. inactive sessions <p>Check loading ...</p> <ul style="list-style-type: none"> • No. T/server sessions (> designed max.) • High no. inactive sessions
---	--	---

Event Logs	System event log	<p>Monitor all messages of type “error”.</p> <p>Monitor all messages of type “warning”, mapping out less important messages based on keywords.</p>
	Application event log	<p>Monitor all messages of type “error”.</p> <p>Monitor all messages for specific applications (“sources”) or based on keywords as required.</p>
	Security event log	For servers where security is critical, monitor all “failed audit” records.
Text-based log files	SQL Server log file	<p>If SQL Server is installed, monitor the SQL Server log file. Use “Unicode” text file monitoring, based on keywords or the phrase “[All Records]” to monitor all entries.</p> <p>#### Path</p>
	IIS & FTP log files	<p>If IIS web/FTP servers are installed, monitor the appropriate log files. Use date-based naming where needed and HTTP errors codes as keywords to detect specific errors such as 500 or 404s. Alternatively record or the phrase “[All Records]” and map out successful codes such as 200.</p> <p>####</p>
	Custom log files	If you have custom software installed that writes to its own log files, monitor these for errors using keywords & phrases – e.g. error, warning, fault, exception etc.
Available disk space	All local hard disks	Check for at least 10% of disc capacity free space available
Windows services	All services configured to “auto start” when Windows is booted	<p>Periodically ensure that these are running. If they’re not, configure the monitor to automatically respond by restarting it.</p> <p>Additionally trigger an alert so you’re aware of the automatic response being taken.</p>
	Critical services	If you have other services that are critical to the system’s operation but not automatically started, configure these to be monitored. Automatically restart these, or alert if they’re not running.

Windows processes	Critical (non-service) processes	<p>Check critical processes – e.g. anti-virus software is running. If not, automatically start it.</p> <p>Additionally trigger an alert so you’re aware of the problem and can see if it continues to fail (and continually needs restarting).</p>
	Restricted processes	<p>Check for unauthorised processes being run – e.g. Setup routines. Alert when run, optionally terminating them automatically.</p> <p><i>If a process is terminated, beware that data may be lost. Additionally some files may remain for applications such as Setup where temporary files may have been copied.</i></p>
Printers <i>(the Sentry-go Printer Wizard can help configure initial settings)</i>	All connected “critical” printers	<p>For each printer, monitor ...</p> <ul style="list-style-type: none"> • Error conditions being reported • Queue length less than 10 • Individual jobs do not exceed 30 pages (for smaller or specialised printers etc.) <p>If found, automatically pause or delete the document in response.</p> <p><i>You can use the Wizard to quickly set up initial settings for all defined printers.</i></p>

Files & directories	As required for the server.	<p>Example 1. Verify the no. files in the TEMP directory ...</p> <ul style="list-style-type: none">• Check count of all files (*.*) in the folder, or the overall size of all files (*.*) in the folder.• If exceeds number, initiate auto-response to delete files. <p>Example 2. Verify the size of log files ...</p> <ul style="list-style-type: none">• Check file size of individual (or all *.log) files in the folder.• Alert if exceeds expected maximum. <p>Example 3. Be notified if no updated files found within a folder ...</p> <ul style="list-style-type: none">• Check required (or all) files in the folder.• Alert if not updated within a given timeframe. <p>Example 4. Be notified if critical files are accessed within a directory ...</p> <ul style="list-style-type: none">• Configure a file or folder access check.• Configure the appropriate folder(s) and file(s)• Configure the access check to return user and/or process details when files are accessed.• Configure logging to save file access information for analysis or reporting.
---------------------	-----------------------------	---

Windows firewall & TCP/IP ports	Window firewall	Ensure the firewall is enabled. If not, automatically enable it in response and trigger an alert.
Windows firewall & TCP/IP ports	E-mail SMTP – e.g. port 25	If SMTP server installed, ensure server is listening for inbound requests. Optionally ensure server response. Alert if expected initial result “220” is not returned.
	E-mail POP3 – e.g. port 110	If POP3 is in use, ensure server is listening for inbound requests. Alert if expected initial result “OK” is not returned.
	E-mail IMAP – e.g. port 143	If IMAP is in use, ensure server is listening for inbound requests.
	HTTP (80) and HTTPS (443)	If a web server is installed, ensure inbound HTTP and/or HTTPS requests are being handled.
	FTP – e.g. port 21	If an FTP server installed, ensure server is listening for inbound requests. Alert if expected initial result “220” is not returned.
	Custom ports	Depending on installed software, ensure the appropriate TCP/IP listen ports are active & available.
	HTML availability	All key web sites/pages

FTP	All critical FTP sites	<p>For each site, check one or more of the following ...</p> <ul style="list-style-type: none"> • The monitor can connect to the site via FTP. • If files are being downloaded, ensure the remote directories are accessible via FTP and/or named remote files exist. • If files are being downloaded from the server, ensure a test file can be downloaded to the client (monitor) (GET). • If files are being uploaded to the server, ensure a test file can be uploaded to the server from the client (monitor) (PUT).
E-mail send/receive	Critical e-mail domains	<p>For each e-mail domain – e.g. @Company.com ...</p> <ul style="list-style-type: none"> • Set up a dummy e-mail address at the domain – e.g. Sentry-go@YourDomain. • Configure a test to ensure a message can be sent from System@YourDomain to the test address using either POP3 or IMAP, or both depending on your typical usage . • Ensure the e-mail can be sent & arrives within an expected timeframe – e.g. 3 minutes.
SQL Connectivity	All critical databases	<p>For each database ...</p> <ul style="list-style-type: none"> • Create a “system” ODBC entry • Configure a check to use the above ODBC entry <p>Optionally ...</p> <ul style="list-style-type: none"> • Run a test to INSERT or UPDATE a dummy row to ensure the SQL operation can be completed successfully. Configure the check to ROLLBACK after completing. • Run a test to retrieve data from a table and verify either the result, or the number of rows returned.

SQL Server Locking	Critical SQL Server instances	<p>For each SQL Server instance ...</p> <ul style="list-style-type: none"> • Create a “system” ODBC entry • Create a SQL user that can access the “MASTER” database • Configure a connection to use the above ODBC entry and user. <p>Then ...</p> <ul style="list-style-type: none"> • Configure monitoring to ensure locks are not waiting for longer than 10 to 15 seconds. • Record suspect queries to a log file. • Automatically terminate <i>blocking</i> queries if detected.
Custom/script	Any custom actions not covered elsewhere	<p>Example 1. Verify broken links on a web site using a command line tool ...</p> <ul style="list-style-type: none"> • Create a .BAT file to call the command line tool. • Ensure the “current directory” is set appropriately for the tool. • If required, pass any required parameters. • Specify the expected result for success (e.g. “Syntax OK,0 errors found”). Alert if not found in output. <p>Example 2. Verify a SQL Server database with DBCC ...</p> <ul style="list-style-type: none"> • Create a .SQL file containing the appropriate DBCC commands. • Create a .BAT file to call “SQLCMD”, connect to the database and run the SQL script created above • Specify the expected DBCC output result for success (e.g. “0 allocation errors,0 consistency errors”). Alert if not found in output.

More Information

If you need more help or information on this topic ...

- Read all [papers/documents on-line](#).
- Watch [demonstrations & walkthrough videos on-line](#).
- Visit <http://www.Sentry-go.com>.
- Contact our [Support Team](#).



*Sentry-go, © 3Ds (UK) Limited, 2000-2013
East Molesey, Surrey, United Kingdom
T. 0208 144 4141
W. <http://www.Sentry-go.com>*