Blackout Knowledge Module® for PATROL® by Sentry Software™

Reference Guide

Supporting

Blackout Knowledge Module® for PATROL® by Sentry Software™ version 1.1

October, 2006

Contents

Blackout KM for PATROL - Reference Guide

Blackout Knowledge Module® for PATROL® is a Knowledge Module for BMC Software® PATROL® that allows the administrators to temporarily and under certain conditions suspend the monitoring of some part of their IT infrastructure. A blackout can be useful when a monitored system (a database or an application) encounters abnormal but planned activities like back-ups. Such unusual activities will lead PATROL® to trigger false positives. Thanks to the Blackout KM, administrators can dramatically reduce the false alerts that operators have to process.

SEN_BO_BLACKOUT_MANAGER

Icon

PATROL Classic Console	PATROL Central
	

Parameters

Name	Description	Polling interval
removeOlderFilesColl	Deletes files that are over 21 days old from the %PATROL_HOME/SEN_BO_LOG" directory.	Runs every day at 2 am
selfCheckColl	Performs a check of the Blackout KM status (privileges, access rights, preloaded, etc.)	60 minutes
serviceColl	Collects information on Windows services	1 minute
processColl	Collects information on processes	1 minute
fileColl	Collects information on files	1 minute

InfoBox

None.

SEN_BO_BLACKOUT

Icon

PATROL Classic Console	PATROL Central
	

Parameters

Name	Description	Value set by
Status	Blackout status. May trigger and alert if an incident occurs at the start of a blackout *Unit: 0 = OK, 1 = Warning, 2 = Alarm*	BlackoutColl every 2 minutes
blackoutColl	Evaluates the blackout status	
Active	Blackout activation Status *Unit: 0 = Stopped, 1 = Started*	BlackoutColl every 2 minutes

InfoBox

Name	Description
PATROL ID	Blackout PATROL internal identifier
Current status	Blackout current status
Last started on	Date and time at which the blackout was last started
Last stopped on	Date and time at which the blackout was last stopped

Regular expressions

A regular expression is a string formatted with a specific syntax. It is intended to select some lines in a text, which will match the regular expression.

Regular expressions are commonly used in pattern matching, and especially on UNIX systems with the grep, awk and sed commands.

The following table describes the regular expression syntax that is supported in Blackout KM for PATROL.

Character	Meaning
`. (dot)`	Match any single character Example: *Err.*. will match *Err01*, *Err02* or *ErrAB*, etc.
`[xyz]`	Match any character in the brackets Example: *Err[123]* will match *Err1*, *Err2* or *Err3* *[Ee]rror* will match either *error* or *Error*
`[^xyz]`	Match any character not in the brackets Example: *Err[^12345]* will match *Err0*, *Err6*, *Err7*, etc. but not *Err1*
`[a-z]`	Match any character in the range in the brackets Example: *Err[0-9]* will match *Err0*, *Err1*, etc. and *Err9* *Err[A-Z][0-9]* will match *ErrA0*, *ErrA1*, *ErrS9*, *ErrZ0*, etc. but not *Err1A* *Err[A-Z0-9]* will match *ErrA0*, *ErrA1*, etc. and *Err1A*
`[^a-z]`	Match any character not in the range in the brackets Example: *Application[^0-9]* will match *ApplicationA*, *ApplicationB*, *Application!* but not *Application1*
`*`	Match zero or more repetitions of the preceding Example: *Err[0-9A-F]** will match *Err*, *Err0*, *ErrA*, *Err11*, *ErrBF0001*, etc. *Error.*ApplicationABC* will match all lines that contains *Error* and *ApplicationABC* further (*Critical Error 0x000295F0 on ApplicationABC*)
`+`	Match one or more repetitions of the preceding Example: *Err[0-9A-F]+* will match *Err0*, *ErrA*, *Err11*, *ErrBF0001*, etc. but not *Err*

^	Match the beginning of the line Example: *^Err* will match all lines that begin with *Err*
$	Match the end of the line Example: *[0-9]+ connections$* will match all lines that end with *xxx connections* where *xxx* is an integer
\<	Match the beginning of a word Example: \<*set* will match any line that contains a word that begins with *set*. It will not match a line that only contains the word *unset*
\>	Match the end of a word Example: *[Aa]pplication*\> will match all lines that contain the word *Application* or *application* but not *ApplicationAA*
\(expression\)	Defines an expression which has to be processed as a unit regarding the modifier *, + and | Example: \(*_[a-zA-Z0-9]*\)+ will match only sequences like *_patrol*, *_patrol_agent*, *_patrol_console*, etc.
exprA|exprB	Match either exprA or exprB Example: \(*firewall*\)|\(*antivirus*\) will match all lines that contains either the word *firewall* or the word *antivirus*
****	Avoid the meaning of the following character Example: \. will match the single character dot (.) *C:**Program Files* will match *C:**Program Files*

Configuration variables

The following table recapitulates the general configuration variables used by Blackout KM for PATROL. These variables are stored in the PATROL Agent configuration and can be managed through PATROL Configuration Manager (PCM), WPCONFIG.EXE (Windows) or xpconfig (UNIX/Linux).

All configuration variables are stored under the /SENTRY/BLACKOUT1 folder in the configuration tree. By default, none of them are set.

Variable	Description
debugMode	When set to '1', enables the debug mode of Blackout KM for PATROL. Default: OFF
debugFile	Optional file name and path of the debug output when the debug mode is enabled. Default: No file output
lsCommand	Command used to get a directory file list on UNIX systems Default: ls -atp1 %{FOLDERPATH}
dirCommand	Command used to get a directory file list on Windows systems Default: dir /A:-D /B /O:-D /T:W %{FOLDERPATH} 2>nul
vmsDirCommand	Command used to get a directory file list on Windows systems Default: directory /columns=1 /notrailing /SELECT=(FILE=(NAME,NOVERSION)) /noheading %{FOLDERPATH}
psCommand	Command used to get the list of processes running Default: ps -A -o args
processPollingInterval	Polling interval, in seconds, at which the list of running processes is updated. This is most useful on UNIX systems for which there is no real-time process monitoring. Default: 60
noRealTimeMonitoring	Set it to '1' to turn off all real-time monitoring in Blackout KM for PATROL and '1' to enable it. Default: ON
noRealTimeProcessMonitoring	Set it to '1' to turn off processes real-time monitoring in Blackout KM for PATROL and '1' to enable it. Default: ON
noRealTimeServiceMonitoring	Set it to '1' to turn off NT services real-time monitoring in Blackout KM for PATROL and '1' to enable it. Default: ON
noRealTimeFileMonitoring	Set it to '1' to turn off files real-time monitoring in Blackout KM for PATROL and '1' to enable it. Default: ON
timeToDeletion	Number of seconds since the last modification of any file found under %PATROL_HOME/SEN_BO_LOG will be deleted. Default: 1814400 (21 days)
noPrefix	Set it to '1' to disable the use of the "Blackout: " prefix in blackout instance labels. Default: ON