

Data Solutions from Bradmark



Bradmark Surveillance 4.7 OS Guide

Notice

Disclaimer and Copyright

This guide contains information protected by copyright. No part of this guide may be photocopied or reproduced, in any form, without prior permission from Bradmark Technologies, Inc. (or Bradmark's Business Partners). BRADMARK TECHNOLOGIES, INC. SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN; NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL.

This guide, as well as the software described herein, is furnished under a license agreement and may only be used or copied in accordance with the terms of that agreement. The information contained in this guide is for informational use only and is subject to change without notice. The software described in this guide is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of that license agreement.

NORAD is a trademark of Bradmark Technologies, Inc. All other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

© 2001, 2020 Bradmark Technologies, Inc.

All rights reserved. Printed in the U.S.A.

Contents

Chapter 1: Views.....	9
Global.....	10
Processes.....	10
Device IO.....	12
File System Usage.....	13
Processors.....	13
Script Execution Monitor.....	14
System Status Monitor.....	15
 Chapter 2: Rules By Category.....	 17
Storage.....	18
OS_DEVIO_IO_RATE.....	18
OS_DEVIO_READ_RATE.....	18
OS_DEVIO_WRITE_RATE.....	19
OS_FILESYSTEM_USAGE_PCNT.....	20
OS_FILESYSTEM_USAGE_PCNT_DELTA.....	20
OS_GLOBAL_DISKIO.....	21
Other.....	21
OS_EXECSRIPT_ERREXIT.....	21
OS_GLOBAL_CPU_PCNT.....	22
OS_GLOBAL_MEMORY_PCNT.....	23
OS_GLOBAL_PROCESS_CNT.....	23
OS_GLOBAL_SWAP_USAGE.....	24
OS_LOGFILE_ERROR.....	24
OS_MSEVTLOG_ERROR.....	25
OS_PROCESSES_CPU.....	25
OS_PROCESSES_KMEM_DELTA.....	26
OS_PROCESSES_KMEM_USAGE.....	26
OS_PROCESSORS_CPU_PCNT.....	27
OS_PROCMON_MEM_GT.....	28
OS_PROCMON_PROCCNT_GT.....	28
OS_PROCMON_PROCCNT_LT.....	29
OS_W32SERVICE_CHANGED_STATE.....	29
OS_W32SERVICE_STARTED.....	30
OS_W32SERVICE_STOPPED.....	30
 Chapter 3: Rules.....	 33
OS_DEVIO_IO_RATE.....	34
OS_DEVIO_READ_RATE.....	34
OS_DEVIO_WRITE_RATE.....	35
OS_EXECSRIPT_ERREXIT.....	36
OS_FILESYSTEM_USAGE_PCNT.....	36
OS_FILESYSTEM_USAGE_PCNT_DELTA.....	37
OS_GLOBAL_CPU_PCNT.....	38
OS_GLOBAL_DISKIO.....	38
OS_GLOBAL_MEMORY_PCNT.....	39
OS_GLOBAL_PROCESS_CNT.....	39

OS_GLOBAL_SWAP_USAGE.....	40
OS_LOGFILE_ERROR.....	40
OS_MSEVTLOG_ERROR.....	41
OS_PROCESSES_CPU.....	41
OS_PROCESSES_KMEM_DELTA.....	42
OS_PROCESSES_KMEM_USAGE.....	43
OS_PROCESSORS_CPU_PCNT.....	43
OS_PROCMON_MEM_GT.....	44
OS_PROCMON_PROCCNT_GT.....	45
OS_PROCMON_PROCCNT_LT.....	45
OS_W32SERVICE_CHANGED_STATE.....	46
OS_W32SERVICE_STARTED.....	46
OS_W32SERVICE_STOPPED.....	47

Chapter 4: Stores By Category..... 49

Storage.....	50
DEVIO.....	50
FILESYSTEM.....	50
Other.....	51
EXECSCRIPT.....	51
GLOBALSTATS.....	51
LOGFILE.....	52
MSEVENTLOG.....	53
PROCESSES.....	53
PROCESSES_SOL.....	54
PROCESSORS.....	54
PROCMON.....	55
SQLSERVER_CPU_UTIL.....	55
SQLSERVER_MEMORY_USAGE.....	56
SQLSERVER_STATUS.....	56
SYSMON.....	56
W32SERVICES.....	57

Chapter 5: Stores..... 59

DEVIO.....	60
EXECSCRIPT.....	60
FILESYSTEM.....	61
GLOBALSTATS.....	61
LOGFILE.....	62
MSEVENTLOG.....	63
PROCESSES.....	63
PROCESSES_SOL.....	64
PROCESSORS.....	64
PROCMON.....	65
SQLSERVER_CPU_UTIL.....	65
SQLSERVER_MEMORY_USAGE.....	66
SQLSERVER_STATUS.....	66
SYSMON.....	67
W32SERVICES.....	67

Chapter 6: Collections By Category..... 69

Storage.....	70
DEVIO.....	70

FILESYSTEM.....	71
Other.....	72
EXECSCRIPT.....	72
GLOBALSTATS.....	72
LOGFILE.....	74
MSEVENTLOG.....	74
PROCESSES.....	75
PROCESSES_SOL.....	76
PROCESSORS.....	78
PROCMON.....	79
SQLSERVER_CPU_UTIL.....	80
SQLSERVER_MEMORY_USAGE.....	81
SQLSERVER_STATUS.....	81
SYSMON.....	82
W32SERVICES.....	83

Chapter 7: Collections.....85

DEVIO.....	86
EXECSCRIPT.....	87
FILESYSTEM.....	88
GLOBALSTATS.....	88
LOGFILE.....	90
MSEVENTLOG.....	90
PROCESSES.....	91
PROCESSES_SOL.....	93
PROCESSORS.....	94
PROCMON.....	95
SQLSERVER_CPU_UTIL.....	96
SQLSERVER_MEMORY_USAGE.....	97
SQLSERVER_STATUS.....	98
SYSMON.....	98
W32SERVICES.....	99

Chapter 8: Central Repository Schema..... 101

Chapter 1

Views

Topics:

- [Global](#)
 - [Processes](#)
 - [Device IO](#)
 - [File System Usage](#)
 - [Processors](#)
 - [Script Execution Monitor](#)
 - [System Status Monitor](#)
-

Global

Global statistics view

Columns

Name	Description
(First Column)	MetricName
Current	Current metric value, based on metric type
Average	Average of current metric value, since collection started
High	Maximum current metric value, since collection started
Total	Total of current metric values, since collection started, if applicable

Entity Requirements

Attributes: None

Minimum OS version: 2.0

Sample

	Current	Average	High	Total
CPU %	1.144	1.089	2.124	0.000
Disk I/Osec	1.400	9.772	27.955	574.000
Memory Usage %	36.687	36.719	36.811	0.000
Swap Usage %	7.006	7.006	7.006	0.000
Process Count	281.000	281.000	281.000	0.000
Memory Buffer %	0.000	0.000	0.000	0.000
Memory Cached %	66.163	66.160	66.163	0.000



Related reference

[GLOBALSTATS](#) on page 72

Global statistics collection

[GLOBALSTATS](#) on page 51

GLOBALSTATS store

Processes

OS processes activity view

Columns

Name	Description
PID	Process ID
Parent	Parent process ID

Name	Description
CPU %	Graph of CPU % used, in interval
CPU Time	Total CPU time for the process
Memory (KB)	Virtual memory size (UNIX / Linux) or working set memory size (Windows), in kilobytes Note: Currently, this value is ambiguously-defined, so it's best to compare this value relative to other processes or relative to historical values for this process. Using this value to exactly account for memory usage is not supported.
Mem Change (KB)	Delta memory usage, in kilobytes Note: See MemSizeK for special considerations.
Process Name	Process name, typically the executable name
User	User name
Command	Process command-line

Entity Requirements

Attributes: None

Minimum OS version: 2.0

Sample

PID	Parent	CPU %	CPU Time	Memory (KB)	Mem Change (KB)	Process Name	User	Command
25272	1	0.321%	3m 34m 38s	343440	0.000	dbgsm	bradmank	/home/bradmank/bradmank47/surveillance
25331	25272	0.101%	1h 52m 58s	156872	0.000	dbgrepos	bradmank	.jdbgrepos
25279	1	0.016%		711968	0.000	nsmservice	bradmank	/home/bradmank/bradmank47/surveillance
25203	25272	0.016%	570ms	105480	0.000	dbggy	bradmank	.jdbgy
25301	25272	0.016%	5m 27s	171748	0.000	dbgcps	bradmank	dbgcps
25293	25272	0.016%	7m 20s	157156	0.000	dbghist	bradmank	.jdbghist
9	2	0.016%	16m 2s	0	0.000	rcu_sched	root	
283	2	0.016%	58m 26s	0	0.000	rcu_sched	root	
25289	25272	0.016%	16m 36s	163652	0.000	dbghist	bradmank	.jdbghist
3217	25272	0.016%	45s	190516	0.000	dbghana	bradmank	.jdbghana
833	1	0.016%	27m 7s	573616	0.000	tuned	root	usr/bin/python
13	2	0%	4s 440ms	0	0.000	migration/1	root	
12	2	0%	43s	0	0.000	watchdog/1	root	

Related reference

[PROCESSES](#) on page 75

OS processes activity collection

[PROCESSES](#) on page 53

PROCESSES store

[OS_PROCESSES_CPU](#) on page 25

Interval CPU usage exceeds value rule

[OS_PROCESSES_KMEM_DELTA](#) on page 26

Interval KMem delta exceeds value rule

[OS_PROCESSES_KMEM_USAGE](#) on page 26

Interval KMem usage exceeds value rule

[OS_PROCESSORS_CPU_PCNT](#) on page 27

Processor CPU% exceeds value rule

Device IO

Device I/O activity view

Columns

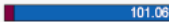
Name	Description
Device ID	Device ID
IO / Sec	Graph of number of I/Os per second, broken down by reads per second (blue) and writes per second (red); values are shown proportionate to Max IO Rate
Ovr % Total IO	% of total number of disk I/Os (reads + writes) over all devices, since collection started
Read Rate	Number of disk reads per second, in interval
Write Rate	Number of disk writes per second, in interval
Avg IO Rate	Average number of disk I/Os (reads + writes) per second, since collection started
Max IO Rate	Maximum number of disk I/Os (reads + writes) per second, since collection started
Ovr Read %	Disk read % of total number of disk I/Os (reads + writes) over all devices, since collection started

Entity Requirements

Attributes: None

Minimum OS version: 2.0

Sample

Device ID	IO / Sec	Ovr % Total IO	Read Rate	Write Rate	Avg IO Rate	Max IO Rate
fs0	0	0.000%	0	0	0	0
sda	 101.06	33.151%	95.4	5.66	21.96	101.06
sda1	 0.03	0.010%	0	0.03	0.01	0.03
sda2	 101.03	33.140%	95.4	5.63	21.96	101.03
sr0	0	0.000%	0	0	0	0
dm-0	0	0.000%	0	0	0	0
dm-1	 101.83	33.512%	95.93	5.9	22.21	101.83
sdb	 0.1	0.092%	0.03	0.07	0.06	0.19
sdb1	 0.1	0.092%	0.03	0.07	0.06	0.19

Related reference

[DEVIO](#) on page 70

Device I/O activity collection

[DEVIO](#) on page 50

DEVIO store

[OS_DEVIO_IO_RATE](#) on page 18

IO Rate exceeds value rule

[OS_DEVIO_READ_RATE](#) on page 18

Read Rate exceeds value rule

[OS_DEVIO_WRITE_RATE](#) on page 19

Write Rate exceeds value rule

File System Usage

Filesystem space usage view

Columns

Name	Description
Filesystem	Device path (UNIX / Linux) or filesystem type (Windows)
Mount Point	Mount point of filesystem
Usage %	Graph with % of total capacity space that is used
Used (MB)	Amount of space used, in megabytes
Capacity (MB)	Total capacity size, in megabytes
Delta (MB)	Delta amount of space used, in megabytes

Entity Requirements

Attributes: None

Minimum OS version: 2.0

Sample

Filesystem	Mount Point	Usage %	Used (MB)	Capacity (MB)	Delta (MB)
/dev/mapper/cic-root	/	 49.777%	38632.635	77410.191	0.000
/dev/sda1	/boot	 26.147%	129.867	496.667	0.000

Related reference

[FILESYSTEM](#) on page 71

Filesystem space usage collection

[FILESYSTEM](#) on page 50

FILESYSTEM store

[OS_FILESYSTEM_USAGE_PCNT](#) on page 20

Filesystem usage % exceeds value rule

[OS_FILESYSTEM_USAGE_PCNT_DELTA](#) on page 20

Filesystem usage delta exceeds value rule

Processors

Processors activity view

Columns

Name	Description
#	Processor # (starting with 0)

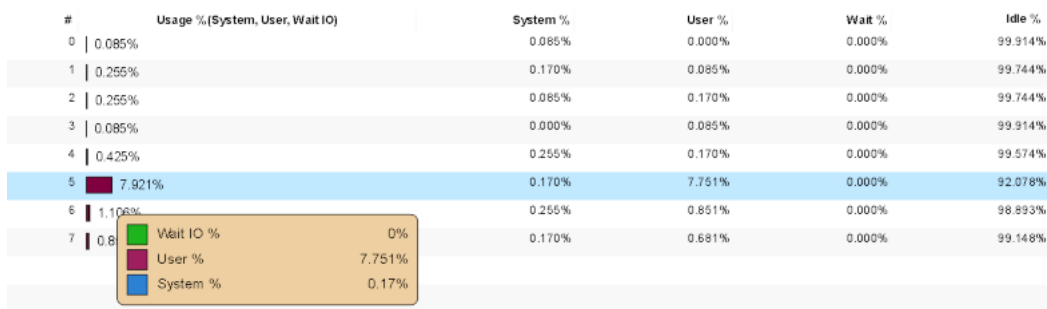
Name	Description
Usage % (System, User, Wait IO)	Graph of (non-idle) CPU % used, in interval, broken down by system (blue), user (red), and wait I/O (green) % used
System %	System CPU % used, in interval
User %	User CPU % used, in interval
Wait %	Wait I/O CPU % used, in interval
Idle %	Idle %, in interval

Entity Requirements

Attributes: None

Minimum OS version: 2.0

Sample



Related reference

[PROCESSORS](#) on page 78
Processors activity collection

[PROCESSORS](#) on page 54
PROCESSORS store

Script Execution Monitor

Custom OS script view

Columns

Name	Description
Application	Application name, as defined in the UDC
Script Name	Script name, as defined in the UDC
Exit Status	Script exit status
Result Num 1	User-defined result number #1, as defined in the UDC
Result Num 2	User-defined result number #2, as defined in the UDC
Result String 1	User-defined result string #1, as defined in the UDC
Result String 2	User-defined result string #2, as defined in the UDC

Name	Description
Exec Time	Execution time

Entity Requirements

Attributes: None

Minimum OS version: 2.0

Sample

Application	Script Name	Exit Status	Result Num 1	Result Num 2	Result String 1
Test exec app1	Test script 1	0	100.000	200.000	100
Test exec app2	Test script 2	0	1000.000	2000.000	2:1000

Related reference

[EXECSCRIPT](#) on page 72

Custom OS script collection

[EXECSCRIPT](#) on page 51

EXECSCRIPT store

[OS_EXECSCRIPT_ERREXIT](#) on page 21

Script had Bad exitstatus rule

System Status Monitor

System status / heartbeat monitoring view

Columns

Name	Description
Domain	SAM domain name
SAM	SAM name
Status	Description of the status: NORMAL The SAM is responding normally. NORAD DOWN The SAM is not responding, but the server can be pinged. SERVER DOWN The server is unreachable and appears offline.
Heartbeat Interval	Heartbeat message interval
Overdue Timeout	Heartbeat overdue timeout
Connect String	Connect string to the SAM

Entity Requirements

Attributes: None

Minimum OS version: 2.0

Sample

Domain	SAM	Status	Heartbeat Interval	Overdue Timeout	Connect String
US	FTEA45	NORAD DOWN	1m	2m	SOCKET,STREAM,C
US	WSTRA	NORMAL	1m	2m	SOCKET,STREAM,C
WORLD	EM	NORAD DOWN	1m	2m	SOCKET,STREAM,C

Related reference

[SYSMON](#) on page 82

System status / heartbeat monitoring collection

[SYSMON](#) on page 56

SYSMON store

Chapter

2

Rules By Category

Topics:

- [Storage](#)
- [Other](#)

Storage

OS_DEVIO_IO_RATE

IO Rate exceeds value rule

Alert Message

@DEVICEID@ IO Rate @IO_RATE@/sec > @VALUE@

Detail View

[Device IO](#) on page 12

Default Rule Properties

Severity	20
Event Type	STD
Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

DEVIO

Related reference

[DEVIO](#) on page 70

Device I/O activity collection

[DEVIO](#) on page 50

DEVIO store

[Device IO](#) on page 12

Device I/O activity view

OS_DEVIO_READ_RATE

Read Rate exceeds value rule

Alert Message

@DEVICEID@ Read Rate @READ_RATE@/sec > @VALUE@

Detail View

[Device IO](#) on page 12

Default Rule Properties

Severity	20
Event Type	STD

Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

DEVIO

Related reference

[DEVIO](#) on page 70

Device I/O activity collection

[DEVIO](#) on page 50

DEVIO store

[Device IO](#) on page 12

Device I/O activity view

OS_DEVIO_WRITE_RATE

Write Rate exceeds value rule

Alert Message

@DEVICEID@ Write Rate @WRITE_RATE@/sec > @VALUE@

Detail View

[Device IO](#) on page 12

Default Rule Properties

Severity	20
Event Type	STD
Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

DEVIO

Related reference

[DEVIO](#) on page 70

Device I/O activity collection

[DEVIO](#) on page 50

DEVIO store

[Device IO](#) on page 12

Device I/O activity view

OS_FILESYSTEM_USAGE_PCNT

Filesystem usage % exceeds value rule

Alert Message

fs "@MOUNTPOINT@" usage @USAGEPCT@% > @VALUE@

Detail View

[File System Usage](#) on page 13

Default Rule Properties

Severity	20
Event Type	STD
Refresh	600 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

FILESYSTEM

Related reference

[FILESYSTEM](#) on page 71

Filesystem space usage collection

[FILESYSTEM](#) on page 50

FILESYSTEM store

[File System Usage](#) on page 13

Filesystem space usage view

OS_FILESYSTEM_USAGE_PCNT_DELTA

Filesystem usage delta exceeds value rule

Alert Message

fs "@MOUNTPOINT@" usage delta @USAGEPCT_DELTA@% > @VALUE@

Detail View

[File System Usage](#) on page 13

Default Rule Properties

Severity	20
Event Type	STD
Refresh	600 seconds
Occurrence Window	1 / 1
Enabled	No

Attributes	None
------------	------

Source Collection

FILESYSTEM

Related reference

[FILESYSTEM](#) on page 71

Filesystem space usage collection

[FILESYSTEM](#) on page 50

FILESYSTEM store

[File System Usage](#) on page 13

Filesystem space usage view

OS_GLOBAL_DISKIO

Diskio/sec exceeds value rule

Alert Message

Diskio @ "Disk IO/sec".current@/sec > @VALUE@

Default Rule Properties

Severity	20
Event Type	STD
Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

GLOBALSTATS

Related reference

[GLOBALSTATS](#) on page 72

Global statistics collection

[GLOBALSTATS](#) on page 51

GLOBALSTATS store

Other

OS_EXECSCRIPT_ERREXIT

Script had Bad exitstatus rule

Alert Message

Script @SCRIPTNAME@ had Exitstatus @EXITSTATUS@

Detail View

[Script Execution Monitor](#) on page 14

Default Rule Properties

Severity	10
Event Type	STD
Refresh	600 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

EXECSCRIPT

Related reference

[EXECSCRIPT](#) on page 72

Custom OS script collection

[EXECSCRIPT](#) on page 51

EXECSCRIPT store

[Script Execution Monitor](#) on page 14

Custom OS script view

OS_GLOBAL_CPU_PCNT

Overall CPU % exceeds value rule

Alert Message

Overall CPU usage at @"CPU %".current@% > @VALUE@

Default Rule Properties

Severity	20
Event Type	STD
Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

GLOBALSTATS

Related reference

[GLOBALSTATS](#) on page 72

Global statistics collection

[GLOBALSTATS](#) on page 51

GLOBALSTATS store

OS_GLOBAL_MEMORY_PCNT

Memory usage % exceeds value rule

Alert Message

Memory usage at @"Memory Usage %".current@% > @VALUE@

Default Rule Properties

Severity	20
Event Type	STD
Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

GLOBALSTATS

Related reference

[GLOBALSTATS](#) on page 72

Global statistics collection

[GLOBALSTATS](#) on page 51

GLOBALSTATS store

OS_GLOBAL_PROCESS_CNT

Process count exceeds value rule

Alert Message

Process count at @"Process Count".current@ > @VALUE@

Default Rule Properties

Severity	20
Event Type	STD
Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

GLOBALSTATS

Related reference

[GLOBALSTATS](#) on page 72

Global statistics collection

[GLOBALSTATS](#) on page 51

GLOBALSTATS store

OS_GLOBAL_SWAP_USAGE

Swap usage % exceeds value rule

Alert Message

Swap usage at @"Swap Usage %".current@% > @VALUE@

Default Rule Properties

Severity	20
Event Type	STD
Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

GLOBALSTATS

Related reference

[GLOBALSTATS](#) on page 72

Global statistics collection

[GLOBALSTATS](#) on page 51

GLOBALSTATS store

OS_LOGFILE_ERROR

Logfile contains ERROR rule

Alert Message

Logfile for @APPNAME@ had an Error

Default Rule Properties

Severity	10
Event Type	STD
Refresh	600 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

LOGFILE

Related reference[LOGFILE](#) on page 74

Log file parsing collection

[LOGFILE](#) on page 52

LOGFILE store

OS_MSEVTLOG_ERROR

MS EventLog contains ERROR rule

Alert Message

@Servername@:@LogName@ had Event Error @Description@

Default Rule Properties

Severity	10
Event Type	STD
Refresh	300 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	WIN32;

Source Collection

MSEVENTLOG

Related reference[MSEVENTLOG](#) on page 74

Windows Event Log collection

[MSEVENTLOG](#) on page 53

MSEVENTLOG store

OS_PROCESSES_CPU

Interval CPU usage exceeds value rule

Alert Message

@PID@/@USER@/@COMMAND@ CPU usage of @CPU_RATE@ > @VALUE@.

Detail View[Processes](#) on page 10**Default Rule Properties**

Severity	20
Event Type	STD
Refresh	120 seconds
Occurrence Window	1 / 1

Enabled	No
Attributes	None

Source Collection

PROCESSES

Related reference

[PROCESSES](#) on page 75

OS processes activity collection

[PROCESSES](#) on page 53

PROCESSES store

[Processes](#) on page 10

OS processes activity view

OS_PROCESSES_KMEM_DELTA

Interval KMem delta exceeds value rule

Alert Message

@PID@/@USER@/@COMMAND@ KMem delta of @MEMK_DELTA@ > @VALUE@.

Detail View

[Processes](#) on page 10

Default Rule Properties

Severity	20
Event Type	STD
Refresh	120 seconds
Occurrence Window	5 / 5
Enabled	No
Attributes	None

Source Collection

PROCESSES

Related reference

[PROCESSES](#) on page 75

OS processes activity collection

[PROCESSES](#) on page 53

PROCESSES store

[Processes](#) on page 10

OS processes activity view

OS_PROCESSES_KMEM_USAGE

Interval KMem usage exceeds value rule

Alert Message

@PID@/@USER@/@COMMAND@ KMem usage of @MEMSIZEK@ > @VALUE@.

Detail View

[Processes](#) on page 10

Default Rule Properties

Severity	20
Event Type	STD
Refresh	120 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

PROCESSES

Related reference

[PROCESSES](#) on page 75

OS processes activity collection

[PROCESSES](#) on page 53

PROCESSES store

[Processes](#) on page 10

OS processes activity view

OS_PROCESSORS_CPU_PCNT

Processor CPU% exceeds value rule

Alert Message

Processor @ProcNum@ using @CPUPCNT@ > @VALUE@

Detail View

[Processes](#) on page 10

Default Rule Properties

Severity	20
Event Type	STD
Refresh	120 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

PROCESSORS

Related reference[PROCESSORS](#) on page 78

Processors activity collection

[PROCESSORS](#) on page 54

PROCESSORS store

[Processes](#) on page 10

OS processes activity view

OS_PROCMON_MEM_GT

Procgroup MemoryMB exceeds value rule

Alert Message

@APPNAME@/@PROCGROUP@ MemSizeK = @MemSizeK@ > @VALUE@.

Default Rule Properties

Severity	20
Event Type	STD
Refresh	120 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

PROCMON

Related reference[PROCMON](#) on page 79

Application process monitoring collection

[PROCMON](#) on page 55

PROCMON store

OS_PROCMON_PROCCNT_GT

Process count exceeds value rule

Alert Message

@APPNAME@/@PROCGROUP@ count = @count@ exceeded @VALUE@.

Default Rule Properties

Severity	20
Event Type	STD
Refresh	120 seconds

Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

PROCMON

Related reference

[PROCMON](#) on page 79

Application process monitoring collection

[PROCMON](#) on page 55

PROCMON store

OS_PROCMON_PROCCNT_LT

Process count < value rule

Alert Message

@APPNAME@/@PROCGROUP@ count = @count@ < @VALUE@.

Default Rule Properties

Severity	10
Event Type	STD
Refresh	120 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

PROCMON

Related reference

[PROCMON](#) on page 79

Application process monitoring collection

[PROCMON](#) on page 55

PROCMON store

OS_W32SERVICE_CHANGED_STATE

Win32 Service has changed state rule

Alert Message

Service @service_name@ changed state to "@state@"

Default Rule Properties

Severity	10
-----------------	----

Event Type	STD
Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	WIN32;

Source Collection

W32SERVICES

Related reference[W32SERVICES](#) on page 83

Windows services collection

[W32SERVICES](#) on page 57

W32SERVICES store

OS_W32SERVICE_STARTED

Win32 Service was started rule

Alert Message

Service @service_name@ was started!

Default Rule Properties

Severity	10
Event Type	STD
Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	WIN32;

Source Collection

W32SERVICES

Related reference[W32SERVICES](#) on page 83

Windows services collection

[W32SERVICES](#) on page 57

W32SERVICES store

OS_W32SERVICE_STOPPED

Win32 Service was stopped rule

Alert Message

Service @service_name@ was stopped!

Default Rule Properties

Severity	10
Event Type	STD
Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	WIN32;

Source Collection

W32SERVICES

Related reference

[W32SERVICES](#) on page 83

Windows services collection

[W32SERVICES](#) on page 57

W32SERVICES store

Chapter

3

Rules

Topics:

- OS_DEVIO_IO_RATE
- OS_DEVIO_READ_RATE
- OS_DEVIO_WRITE_RATE
- OS_EXECSCRIPT_ERREXIT
- OS_FILESYSTEM_USAGE_PCNT
- OS_FILESYSTEM_USAGE_PCNT_DELTA
- OS_GLOBAL_CPU_PCNT
- OS_GLOBAL_DISKIO
- OS_GLOBAL_MEMORY_PCNT
- OS_GLOBAL_PROCESS_CNT
- OS_GLOBAL_SWAP_USAGE
- OS_LOGFILE_ERROR
- OS_MSEVTLOG_ERROR
- OS_PROCESSES_CPU
- OS_PROCESSES_KMEM_DELTA
- OS_PROCESSES_KMEM_USAGE
- OS_PROCESSORS_CPU_PCNT
- OS_PROCMON_MEM_GT
- OS_PROCMON_PROCCNT_GT
- OS_PROCMON_PROCCNT_LT
- OS_W32SERVICE_CHANGED_STATE
- OS_W32SERVICE_STARTED
- OS_W32SERVICE_STOPPED

OS_DEVIO_IO_RATE

IO Rate exceeds value rule

Alert Message

@DEVICEID@ IO Rate @IO_RATE@/sec > @VALUE@

Detail View

[Device IO](#) on page 12

Default Rule Properties

Severity	20
Event Type	STD
Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

DEVIO

Related reference

[DEVIO](#) on page 70

Device I/O activity collection

[DEVIO](#) on page 50

DEVIO store

[Device IO](#) on page 12

Device I/O activity view

OS_DEVIO_READ_RATE

Read Rate exceeds value rule

Alert Message

@DEVICEID@ Read Rate @READ_RATE@/sec > @VALUE@

Detail View

[Device IO](#) on page 12

Default Rule Properties

Severity	20
Event Type	STD
Refresh	60 seconds

Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

DEVIO

Related reference

[DEVIO](#) on page 70

Device I/O activity collection

[DEVIO](#) on page 50

DEVIO store

[Device IO](#) on page 12

Device I/O activity view

OS_DEVIO_WRITE_RATE

Write Rate exceeds value rule

Alert Message

@DEVICEID@ Write Rate @WRITE_RATE@/sec > @VALUE@

Detail View

[Device IO](#) on page 12

Default Rule Properties

Severity	20
Event Type	STD
Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

DEVIO

Related reference

[DEVIO](#) on page 70

Device I/O activity collection

[DEVIO](#) on page 50

DEVIO store

[Device IO](#) on page 12

Device I/O activity view

OS_EXECSCRIPT_ERREXIT

Script had Bad exitstatus rule

Alert Message

Script @SCRIPTNAME@ had Exitstatus @EXITSTATUS@

Detail View

[Script Execution Monitor](#) on page 14

Default Rule Properties

Severity	10
Event Type	STD
Refresh	600 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

EXECSCRIPT

Related reference

[EXECSCRIPT](#) on page 72

Custom OS script collection

[EXECSCRIPT](#) on page 51

EXECSCRIPT store

[Script Execution Monitor](#) on page 14

Custom OS script view

OS_FILESYSTEM_USAGE_PCNT

Filesystem usage % exceeds value rule

Alert Message

fs "@MOUNTPOINT@" usage @USAGEPCT@% > @VALUE@

Detail View

[File System Usage](#) on page 13

Default Rule Properties

Severity	20
Event Type	STD
Refresh	600 seconds

Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

FILESYSTEM

Related reference

[FILESYSTEM](#) on page 71

Filesystem space usage collection

[FILESYSTEM](#) on page 50

FILESYSTEM store

[File System Usage](#) on page 13

Filesystem space usage view

OS_FILESYSTEM_USAGE_PCNT_DELTA

Filesystem usage delta exceeds value rule

Alert Message

fs "@MOUNTPOINT@" usage delta @USAGEPCT_DELTA@% > @VALUE@

Detail View

[File System Usage](#) on page 13

Default Rule Properties

Severity	20
Event Type	STD
Refresh	600 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

FILESYSTEM

Related reference

[FILESYSTEM](#) on page 71

Filesystem space usage collection

[FILESYSTEM](#) on page 50

FILESYSTEM store

[File System Usage](#) on page 13

Filesystem space usage view

OS_GLOBAL_CPU_PCNT

Overall CPU % exceeds value rule

Alert Message

Overall CPU usage at @"CPU %".current@% > @VALUE@

Default Rule Properties

Severity	20
Event Type	STD
Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

GLOBALSTATS

Related reference

[GLOBALSTATS](#) on page 72

Global statistics collection

[GLOBALSTATS](#) on page 51

GLOBALSTATS store

OS_GLOBAL_DISKIO

Diskio/sec exceeds value rule

Alert Message

Diskio @"Disk IO/sec".current@/sec > @VALUE@

Default Rule Properties

Severity	20
Event Type	STD
Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

GLOBALSTATS

Related reference

[GLOBALSTATS](#) on page 72

Global statistics collection

[GLOBALSTATS](#) on page 51

GLOBALSTATS store

OS_GLOBAL_MEMORY_PCNT

Memory usage % exceeds value rule

Alert Message

Memory usage at @"Memory Usage %".current@% > @VALUE@

Default Rule Properties

Severity	20
Event Type	STD
Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

GLOBALSTATS

Related reference

[GLOBALSTATS](#) on page 72

Global statistics collection

[GLOBALSTATS](#) on page 51

GLOBALSTATS store

OS_GLOBAL_PROCESS_CNT

Process count exceeds value rule

Alert Message

Process count at @"Process Count".current@ > @VALUE@

Default Rule Properties

Severity	20
Event Type	STD
Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No

Attributes	None
------------	------

Source Collection

GLOBALSTATS

Related reference[GLOBALSTATS](#) on page 72

Global statistics collection

[GLOBALSTATS](#) on page 51

GLOBALSTATS store

OS_GLOBAL_SWAP_USAGE

Swap usage % exceeds value rule

Alert Message

Swap usage at @"Swap Usage %".current@% > @VALUE@

Default Rule Properties

Severity	20
Event Type	STD
Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

GLOBALSTATS

Related reference[GLOBALSTATS](#) on page 72

Global statistics collection

[GLOBALSTATS](#) on page 51

GLOBALSTATS store

OS_LOGFILE_ERROR

Logfile contains ERROR rule

Alert Message

Logfile for @APPNAME@ had an Error

Default Rule Properties

Severity	10
----------	----

Event Type	STD
Refresh	600 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

LOGFILE

Related reference[LOGFILE](#) on page 74

Log file parsing collection

[LOGFILE](#) on page 52

LOGFILE store

OS_MSEVTLOG_ERROR

MS EventLog contains ERROR rule

Alert Message

@Servername@:@LogName@ had Event Error @Description@

Default Rule Properties

Severity	10
Event Type	STD
Refresh	300 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	WIN32;

Source Collection

MSEVENTLOG

Related reference[MSEVENTLOG](#) on page 74

Windows Event Log collection

[MSEVENTLOG](#) on page 53

MSEVENTLOG store

OS_PROCESSES_CPU

Interval CPU usage exceeds value rule

Alert Message

@PID@/@USER@/@COMMAND@ CPU usage of @CPU_RATE@ > @VALUE@.

Detail View

[Processes](#) on page 10

Default Rule Properties

Severity	20
Event Type	STD
Refresh	120 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

PROCESSES

Related reference

[PROCESSES](#) on page 75

OS processes activity collection

[PROCESSES](#) on page 53

PROCESSES store

[Processes](#) on page 10

OS processes activity view

OS_PROCESSES_KMEM_DELTA

Interval KMem delta exceeds value rule

Alert Message

@PID@/@USER@/@COMMAND@ KMem delta of @MEMK_DELTA@ > @VALUE@.

Detail View

[Processes](#) on page 10

Default Rule Properties

Severity	20
Event Type	STD
Refresh	120 seconds
Occurrence Window	5 / 5
Enabled	No
Attributes	None

Source Collection

PROCESSES

Related reference[PROCESSES](#) on page 75

OS processes activity collection

[PROCESSES](#) on page 53

PROCESSES store

[Processes](#) on page 10

OS processes activity view

OS_PROCESSES_KMEM_USAGE

Interval KMem usage exceeds value rule

Alert Message

@PID@/@USER@/@COMMAND@ KMem usage of @MEMSIZEK@ > @VALUE@.

Detail View[Processes](#) on page 10**Default Rule Properties**

Severity	20
Event Type	STD
Refresh	120 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

PROCESSES

Related reference[PROCESSES](#) on page 75

OS processes activity collection

[PROCESSES](#) on page 53

PROCESSES store

[Processes](#) on page 10

OS processes activity view

OS_PROCESSORS_CPU_PCNT

Processor CPU% exceeds value rule

Alert Message

Processor @ProcNum@ using @CPUPCNT@ > @VALUE@

Detail View

[Processes](#) on page 10

Default Rule Properties

Severity	20
Event Type	STD
Refresh	120 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

PROCESSORS

Related reference

[PROCESSORS](#) on page 78

Processors activity collection

[PROCESSORS](#) on page 54

PROCESSORS store

[Processes](#) on page 10

OS processes activity view

OS_PROCMON_MEM_GT

Progroup MemoryMB exceeds value rule

Alert Message

@APPNAME@/@PROCGROUP@ MemSizeK = @MemSizeK@ > @VALUE@.

Default Rule Properties

Severity	20
Event Type	STD
Refresh	120 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

PROCMON

Related reference[PROCMON](#) on page 79

Application process monitoring collection

[PROCMON](#) on page 55

PROCMON store

OS_PROCMON_PROCCNT_GT

Process count exceeds value rule

Alert Message

@APPNAME@/@PROCGROUP@ count = @count@ exceeded @VALUE@.

Default Rule Properties

Severity	20
Event Type	STD
Refresh	120 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	None

Source Collection

PROCMON

Related reference[PROCMON](#) on page 79

Application process monitoring collection

[PROCMON](#) on page 55

PROCMON store

OS_PROCMON_PROCCNT_LT

Process count < value rule

Alert Message

@APPNAME@/@PROCGROUP@ count = @count@ < @VALUE@.

Default Rule Properties

Severity	10
Event Type	STD
Refresh	120 seconds
Occurrence Window	1 / 1
Enabled	No

Attributes	None
------------	------

Source Collection

PROCMON

Related reference

[PROCMON](#) on page 79

Application process monitoring collection

[PROCMON](#) on page 55

PROCMON store

OS_W32SERVICE_CHANGED_STATE

Win32 Service has changed state rule

Alert Message

Service @service_name@ changed state to "@state@"

Default Rule Properties

Severity	10
Event Type	STD
Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	WIN32;

Source Collection

W32SERVICES

Related reference

[W32SERVICES](#) on page 83

Windows services collection

[W32SERVICES](#) on page 57

W32SERVICES store

OS_W32SERVICE_STARTED

Win32 Service was started rule

Alert Message

Service @service_name@ was started!

Default Rule Properties

Severity	10
----------	----

Event Type	STD
Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	WIN32;

Source Collection

W32SERVICES

Related reference[W32SERVICES](#) on page 83

Windows services collection

[W32SERVICES](#) on page 57

W32SERVICES store

OS_W32SERVICE_STOPPED

Win32 Service was stopped rule

Alert Message

Service @service_name@ was stopped!

Default Rule Properties

Severity	10
Event Type	STD
Refresh	60 seconds
Occurrence Window	1 / 1
Enabled	No
Attributes	WIN32;

Source Collection

W32SERVICES

Related reference[W32SERVICES](#) on page 83

Windows services collection

[W32SERVICES](#) on page 57

W32SERVICES store

Chapter

4

Stores By Category

Topics:

- [Storage](#)
- [Other](#)

--	--

Storage

DEVIO

DEVIO store

Default Store Properties

Refresh	600 Seconds
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 01:00:00

Related reference

[Device IO](#) on page 12

Device I/O activity view

[DEVIO](#) on page 70

Device I/O activity collection

[OS_DEVIO_IO_RATE](#) on page 18

IO Rate exceeds value rule

[OS_DEVIO_READ_RATE](#) on page 18

Read Rate exceeds value rule

[OS_DEVIO_WRITE_RATE](#) on page 19

Write Rate exceeds value rule

FILESYSTEM

FILESYSTEM store

Default Store Properties

Refresh	30 Minutes
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate

Export Repeat Interval	00 10:00:00
-------------------------------	-------------

Related reference

[File System Usage](#) on page 13

Filesystem space usage view

[FILESYSTEM](#) on page 71

Filesystem space usage collection

[OS_FILESYSTEM_USAGE_PCNT](#) on page 20

Filesystem usage % exceeds value rule

[OS_FILESYSTEM_USAGE_PCNT_DELTA](#) on page 20

Filesystem usage delta exceeds value rule

Other

EXECSCRIPT

EXECSCRIPT store

Default Store Properties

Refresh	30 Minutes
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 10:00:00

Related reference

[Script Execution Monitor](#) on page 14

Custom OS script view

[EXECSCRIPT](#) on page 72

Custom OS script collection

[OS_EXECSCRIPT_ERREXIT](#) on page 21

Script had Bad exitstatus rule

GLOBALSTATS

GLOBALSTATS store

Default Store Properties

Refresh	120 Seconds
Enabled	Yes

Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 00:30:00

Related reference

[Global](#) on page 10

Global statistics view

[GLOBALSTATS](#) on page 72

Global statistics collection

[OS_GLOBAL_CPU_PCNT](#) on page 22

Overall CPU % exceeds value rule

[OS_GLOBAL_DISKIO](#) on page 21

Diskio/sec exceeds value rule

[OS_GLOBAL_MEMORY_PCNT](#) on page 23

Memory usage % exceeds value rule

[OS_GLOBAL_PROCESS_CNT](#) on page 23

Process count exceeds value rule

[OS_GLOBAL_SWAP_USAGE](#) on page 24

Swap usage % exceeds value rule

LOGFILE

LOGFILE store

Default Store Properties

Refresh	600 Seconds
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 01:00:00

Related reference

[LOGFILE](#) on page 74

Log file parsing collection

[OS_LOGFILE_ERROR](#) on page 24

Logfile contains ERROR rule

MSEVENTLOG

MSEVENTLOG store

Default Store Properties

Refresh	30 Minutes
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 06:00:00

Related reference

[MSEVENTLOG](#) on page 74

Windows Event Log collection

[OS_MSEVTLOG_ERROR](#) on page 25

MS EventLog contains ERROR rule

PROCESSES

PROCESSES store

Default Store Properties

Refresh	600 Seconds
Enabled	Yes
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 01:00:00

Related reference

[Processes](#) on page 10

OS processes activity view

[PROCESSES](#) on page 75

OS processes activity collection

[OS_PROCESSES_CPU](#) on page 25

Interval CPU usage exceeds value rule

[OS_PROCESSES_KMEM_DELTA](#) on page 26

Interval KMem delta exceeds value rule

[OS_PROCESSES_KMEM_USAGE](#) on page 26

Interval KMem usage exceeds value rule

PROCESSES_SOL

PROCESSES_SOL store

Default Store Properties

Refresh	600 Seconds
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 01:00:00

Related reference

[PROCESSES_SOL](#) on page 76

OS processes activity (Solaris extension) collection

PROCESSORS

PROCESSORS store

Default Store Properties

Refresh	30 Minutes
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 06:00:00

Related reference

[Processors](#) on page 13

Processors activity view

[PROCESSORS](#) on page 78

Processors activity collection

[OS_PROCESSORS_CPU_PCNT](#) on page 27

Processor CPU% exceeds value rule

PROCMON

PROCMON store

Default Store Properties

Refresh	60 Minutes
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 10:00:00

Related reference

[PROCMON](#) on page 79

Application process monitoring collection

[OS_PROCMON_MEM_GT](#) on page 28

Progroup MemoryMB exceeds value rule

[OS_PROCMON_PROCCNT_GT](#) on page 28

Process count exceeds value rule

[OS_PROCMON_PROCCNT_LT](#) on page 29

Process count < value rule

SQLSERVER_CPU_UTIL

SQLSERVER_CPU_UTIL store

Default Store Properties

Refresh	120 Seconds
Enabled	Yes
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 00:30:00

Related reference

[SQLSERVER_CPU_UTIL](#) on page 80

Multi-instance SQL Server CPU utilization collection

SQLSERVER_MEMORY_USAGE

SQLSERVER_MEMORY_USAGE store

Default Store Properties

Refresh	120 Seconds
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 00:30:00

Related reference

[SQLSERVER_MEMORY_USAGE](#) on page 81

Multi-instance SQL Server memory usage collection

SQLSERVER_STATUS

SQLSERVER_STATUS store

Default Store Properties

Refresh	120 Seconds
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 00:30:00

Related reference

[SQLSERVER_STATUS](#) on page 81

Multi-instance SQL Server status collection

SYSMON

SYSMON store

Default Store Properties

Refresh	600 Seconds
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 01:00:00

Related reference

[System Status Monitor](#) on page 15

System status / heartbeat monitoring view

[SYSMON](#) on page 82

System status / heartbeat monitoring collection

W32SERVICES

W32SERVICES store

Default Store Properties

Refresh	600 Seconds
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 02:00:00

Related reference

[W32SERVICES](#) on page 83

Windows services collection

[OS_W32SERVICE_CHANGED_STATE](#) on page 29

Win32 Service has changed state rule

[OS_W32SERVICE_STARTED](#) on page 30

Win32 Service was started rule

[OS_W32SERVICE_STOPPED](#) on page 30

Win32 Service was stopped rule

Chapter

5

Stores

Topics:

- [DEVIO](#)
- [EXECSCRIPT](#)
- [FILESYSTEM](#)
- [GLOBALSTATS](#)
- [LOGFILE](#)
- [MSEVENTLOG](#)
- [PROCESSES](#)
- [PROCESSES_SOL](#)
- [PROCESSORS](#)
- [PROCMON](#)
- [SQLSERVER_CPU_UTIL](#)
- [SQLSERVER_MEMORY_USAGE](#)
- [SQLSERVER_STATUS](#)
- [SYSMON](#)
- [W32SERVICES](#)

DEVIO

DEVIO store

Default Store Properties

Refresh	600 Seconds
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 01:00:00

Related reference

[Device IO](#) on page 12

Device I/O activity view

[DEVIO](#) on page 70

Device I/O activity collection

[OS_DEVIO_IO_RATE](#) on page 18

IO Rate exceeds value rule

[OS_DEVIO_READ_RATE](#) on page 18

Read Rate exceeds value rule

[OS_DEVIO_WRITE_RATE](#) on page 19

Write Rate exceeds value rule

EXECSCRIPT

EXECSCRIPT store

Default Store Properties

Refresh	30 Minutes
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate

Export Repeat Interval	00 10:00:00
-------------------------------	-------------

Related reference

[Script Execution Monitor](#) on page 14

Custom OS script view

[EXECSCRIPT](#) on page 72

Custom OS script collection

[OS_EXECSCRIPT_ERREXIT](#) on page 21

Script had Bad exitstatus rule

FILESYSTEM

FILESYSTEM store

Default Store Properties

Refresh	30 Minutes
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 10:00:00

Related reference

[File System Usage](#) on page 13

Filesystem space usage view

[FILESYSTEM](#) on page 71

Filesystem space usage collection

[OS_FILESYSTEM_USAGE_PCNT](#) on page 20

Filesystem usage % exceeds value rule

[OS_FILESYSTEM_USAGE_PCNT_DELTA](#) on page 20

Filesystem usage delta exceeds value rule

GLOBALSTATS

GLOBALSTATS store

Default Store Properties

Refresh	120 Seconds
Enabled	Yes
Overdue Timeout	1 Minutes

Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 00:30:00

Related reference

[Global](#) on page 10

Global statistics view

[GLOBALSTATS](#) on page 72

Global statistics collection

[OS_GLOBAL_CPU_PCNT](#) on page 22

Overall CPU % exceeds value rule

[OS_GLOBAL_DISKIO](#) on page 21

Diskio/sec exceeds value rule

[OS_GLOBAL_MEMORY_PCNT](#) on page 23

Memory usage % exceeds value rule

[OS_GLOBAL_PROCESS_CNT](#) on page 23

Process count exceeds value rule

[OS_GLOBAL_SWAP_USAGE](#) on page 24

Swap usage % exceeds value rule

LOGFILE

LOGFILE store

Default Store Properties

Refresh	600 Seconds
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 01:00:00

Related reference

[LOGFILE](#) on page 74

Log file parsing collection

[OS_LOGFILE_ERROR](#) on page 24

Logfile contains ERROR rule

MSEVENTLOG

MSEVENTLOG store

Default Store Properties

Refresh	30 Minutes
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 06:00:00

Related reference

[MSEVENTLOG](#) on page 74

Windows Event Log collection

[OS_MSEVTLOG_ERROR](#) on page 25

MS EventLog contains ERROR rule

PROCESSES

PROCESSES store

Default Store Properties

Refresh	600 Seconds
Enabled	Yes
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 01:00:00

Related reference

[Processes](#) on page 10

OS processes activity view

[PROCESSES](#) on page 75

OS processes activity collection

[OS_PROCESSES_CPU](#) on page 25

Interval CPU usage exceeds value rule

[OS_PROCESSES_KMEM_DELTA](#) on page 26

Interval KMem delta exceeds value rule

[OS_PROCESSES_KMEM_USAGE](#) on page 26

Interval KMem usage exceeds value rule

PROCESSES_SOL

PROCESSES_SOL store

Default Store Properties

Refresh	600 Seconds
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 01:00:00

Related reference

[PROCESSES_SOL](#) on page 76

OS processes activity (Solaris extension) collection

PROCESSORS

PROCESSORS store

Default Store Properties

Refresh	30 Minutes
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 06:00:00

Related reference

[Processors](#) on page 13

Processors activity view

[PROCESSORS](#) on page 78

Processors activity collection

[OS_PROCESSORS_CPU_PCNT](#) on page 27

Processor CPU% exceeds value rule

PROCMON

PROCMON store

Default Store Properties

Refresh	60 Minutes
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 10:00:00

Related reference

[PROCMON](#) on page 79

Application process monitoring collection

[OS_PROCMON_MEM_GT](#) on page 28

Progroup MemoryMB exceeds value rule

[OS_PROCMON_PROCCNT_GT](#) on page 28

Process count exceeds value rule

[OS_PROCMON_PROCCNT_LT](#) on page 29

Process count < value rule

SQLSERVER_CPU_UTIL

SQLSERVER_CPU_UTIL store

Default Store Properties

Refresh	120 Seconds
Enabled	Yes
Overdue Timeout	1 Minutes
Partition Interval	1 Days

Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 00:30:00

Related reference

[SQLSERVER_CPU_UTIL](#) on page 80

Multi-instance SQL Server CPU utilization collection

SQLSERVER_MEMORY_USAGE

SQLSERVER_MEMORY_USAGE store

Default Store Properties

Refresh	120 Seconds
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 00:30:00

Related reference

[SQLSERVER_MEMORY_USAGE](#) on page 81

Multi-instance SQL Server memory usage collection

SQLSERVER_STATUS

SQLSERVER_STATUS store

Default Store Properties

Refresh	120 Seconds
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	

Export	No
Export Start	immediate
Export Repeat Interval	00 00:30:00

Related reference

[SQLSERVER_STATUS](#) on page 81

Multi-instance SQL Server status collection

SYSMON

SYSMON store

Default Store Properties

Refresh	600 Seconds
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No
Export Start	immediate
Export Repeat Interval	00 01:00:00

Related reference

[System Status Monitor](#) on page 15

System status / heartbeat monitoring view

[SYSMON](#) on page 82

System status / heartbeat monitoring collection

W32SERVICES

W32SERVICES store

Default Store Properties

Refresh	600 Seconds
Enabled	No
Overdue Timeout	1 Minutes
Partition Interval	1 Days
Partitions	7
Filter	
Export	No

Export Start	immediate
Export Repeat Interval	00 02:00:00

Related reference

[W32SERVICES](#) on page 83

Windows services collection

[OS_W32SERVICE_CHANGED_STATE](#) on page 29

Win32 Service has changed state rule

[OS_W32SERVICE_STARTED](#) on page 30

Win32 Service was started rule

[OS_W32SERVICE_STOPPED](#) on page 30

Win32 Service was stopped rule

Chapter

6

Collections By Category

Topics:

- [Storage](#)
- [Other](#)

Storage

DEVIO

Device I/O activity collection

ROWID

(DeviceID)

Columns

Name	Data Type	Description
DeviceID	string(32)	Device ID
DiskReads	double	Number of disk reads
DiskWrites	double	Number of disk writes
MERGESTATUS	long	Internal-use merge status; created by Surveillance
READS_DELTA	double	Delta number of disk reads
WRITES_DELTA	double	Delta number of disk writes
READ_RATE	double	Number of disk reads per second, in interval
WRITE_RATE	double	Number of disk writes per second, in interval
IO_RATE	double	Number of disk I/Os (reads + writes) per second, in interval
IO_RATE_AVG	double	Average number of disk I/Os (reads + writes) per second, since collection started
IO_RATE_MAX	double	Maximum number of disk I/Os (reads + writes) per second, since collection started
READS_TOTAL	double	Total number of disk reads, since collection started
WRITES_TOTAL	double	Total number of disk writes, since collection started
IO_TOTAL	double	Total number of disk I/Os (reads + writes), since collection started
IO_PCT_TOTAL	double	% of total number of disk I/Os (reads + writes) over all devices, since collection started
READ_PCT	double	Disk read % of total number of disk I/Os (reads + writes) over all devices, since collection started

Requirements

Attributes: None

Minimum OS version: 2.0

Related reference

[Device IO](#) on page 12

Device I/O activity view

[DEVIO](#) on page 50

DEVIO store

[OS_DEVIO_IO_RATE](#) on page 18

IO Rate exceeds value rule

[OS_DEVIO_READ_RATE](#) on page 18

Read Rate exceeds value rule

[OS_DEVIO_WRITE_RATE](#) on page 19

Write Rate exceeds value rule

FILESYSTEM

Filesystem space usage collection

ROWID

(MountPoint)

Columns

Name	Data Type	Description
FileSystem	string(128)	Device path (UNIX / Linux) or filesystem type (Windows)
MountPoint	string(128)	Mount point of filesystem
KBytesUsage	double	Amount of space used, in kilobytes
KBytesCapacity	double	Total capacity size, in kilobytes
MERGESTATUS	long	Internal-use merge status; created by Surveillance
USAGEPCT	double	% of total capacity space that is used
USAGEPCT_DELTA	double	Delta % of total capacity space that is used
KBUSAGE_DELTA	double	Delta amount of space used, in kilobytes
MBUSAGE	double	Amount of space used, in megabytes
MBCAPACITY	double	Total capacity size, in megabytes
MBUSAGE_DELTA	double	Delta amount of space used, in megabytes

Requirements

Attributes: None

Minimum OS version: 2.0

Related reference

[File System Usage](#) on page 13

Filesystem space usage view

[FILESYSTEM](#) on page 50

FILESYSTEM store

[OS_FILESYSTEM_USAGE_PCNT](#) on page 20

Filesystem usage % exceeds value rule

[OS_FILESYSTEM_USAGE_PCNT_DELTA](#) on page 20

Filesystem usage delta exceeds value rule

Other

EXECSCRIPT

Custom OS script collection

Comments

This is a sample user-defined collection (UDC). Edit or copy EXECSCRIPT.COL to customize which script outputs are included.

Any user-declared columns will appear following the predefined columns (below). Derived columns appear after any user-declared columns.

ROWID

None

Columns

Name	Data Type	Description
AppName	string(64)	Application name, as defined in the UDC
ScriptName	string(64)	Script name, as defined in the UDC
ExitStatus	long	Script exit status
ResultStr1	string(128)	User-defined result string #1, as defined in the UDC
ResultNum1	double	User-defined result number #1, as defined in the UDC
ResultStr2	string(128)	User-defined result string #2, as defined in the UDC
ResultNum2	double	User-defined result number #2, as defined in the UDC
ExecTimeMS	double	Execution time, in milliseconds

Requirements

Attributes: None

Minimum OS version: None

Related reference

[Script Execution Monitor](#) on page 14

Custom OS script view

[EXECSCRIPT](#) on page 51

EXECSCRIPT store

[OS_EXECSCRIPT_ERREXIT](#) on page 21

Script had Bad exitstatus rule

GLOBALSTATS

Global statistics collection

ROWID

(MetricName)

Columns

Name	Data Type	Description
MetricName	string(64)	Metric name
MetricType	long	Metric type: 1 Counter = sum(Value) 2 Run Level = Value 3 Ratio 4 Rate = Value / Elapsed time
MetricID	long	Metric ID; ID < 100 = displayable metric
Value	double	Metric value
MERGESTATUS	long	Internal-use merge status; created by Surveillance
CURRENT	double	Current metric value, based on metric type
AVG	double	Average of current metric value, since collection started
MAX	double	Maximum current metric value, since collection started
VALUE_DELTA	double	Delta metric value (regardless of metric type)
TOTAL	double	Total of current metric values, since collection started, if applicable

Requirements

Attributes: None

Minimum OS version: 2.0

Related reference

[Global](#) on page 10

Global statistics view

[GLOBALSTATS](#) on page 51

GLOBALSTATS store

[OS_GLOBAL_CPU_PCNT](#) on page 22

Overall CPU % exceeds value rule

[OS_GLOBAL_DISKIO](#) on page 21

Diskio/sec exceeds value rule

[OS_GLOBAL_MEMORY_PCNT](#) on page 23

Memory usage % exceeds value rule

[OS_GLOBAL_PROCESS_CNT](#) on page 23

Process count exceeds value rule

[OS_GLOBAL_SWAP_USAGE](#) on page 24

Swap usage % exceeds value rule

LOGFILE

Log file parsing collection

Comments

This is a sample user-defined collection (UDC). Edit or copy LOGFILE.COL to customize which error log entries are included.

Any user-declared columns will appear following the predefined columns (below). Derived columns appear after any user-declared columns.

ROWID

None

Columns

Name	Data Type	Description
Timestamp	string(32)	Time when the message was parsed
Seq#	long	Sequence #, within a timestamp
AppName	string(64)	Application name, as defined in the UDC
FilePath	string(256)	Error log file path
ErrorCode	string(128)	Error code, as defined in the UDC
ErrorLevel	string(128)	Error level, as defined in the UDC
ErrorText	string(256)	Error text, as defined in the UDC

Requirements

Attributes: None

Minimum OS version: None

Related reference

[LOGFILE](#) on page 52

LOGFILE store

[OS_LOGFILE_ERROR](#) on page 24

Logfile contains ERROR rule

MSEVENTLOG

Windows Event Log collection

Comments

This is a user-defined collection (UDC). Edit MSEVENTLOG.COL to customize which Windows events are included.

Any user-declared columns will appear following the predefined columns (below). Derived columns appear after any user-declared columns.

ROWID

(ServerName, LogName, RecordNum, EventTime)

Columns

Name	Data Type	Description
ServerName	string(64)	Server name
LogName	string(64)	Name of the event log (i.e. Security, System, Application)
RecordNum	long	Record # in the event log
ClosingRecordNum	long	If this event closes a previous one: record # of the opening event in the event log
EventTime	time	Time when the event was observed
EventID	long	Event number
EventType	string(32)	Type of event (i.e. Error, Warning)
EventCategory	string(64)	Event category
User	string(64)	User which generated the event
Domain	string(64)	Domain of the user which generated the event
Source	string(64)	Source of the event (i.e. program, component)
Computer	string(64)	Computer name
Description	string(1024)	Event description

Requirements

Attributes: WIN32

Minimum OS version: None

Related reference

[MSEVENTLOG](#) on page 53

MSEVENTLOG store

[OS_MSEVTLOG_ERROR](#) on page 25

MS EventLog contains ERROR rule

PROCESSES

OS processes activity collection

ROWID

(Pid)

Columns

Name	Data Type	Description
Pid	long	Process ID
PPid	long	Parent process ID
MemSizeK	long	Virtual memory size (UNIX / Linux) or working set memory size (Windows), in kilobytes

Name	Data Type	Description
		Note: Currently, this value is ambiguously-defined, so it's best to compare this value relative to other processes or relative to historical values for this process. Using this value to exactly account for memory usage is not supported.
CPUsecs	double	Number of CPU seconds for the process
User	string(64)	User name
Command	string(256)	Process command-line
ProcessName	string(256)	Process name, typically the executable name
ProcCnt	long	Internal-use number of processors on the machine; created by Surveillance
MERGESTATUS	long	Internal-use merge status; created by Surveillance
CPU_DELTA	double	Delta number of CPU seconds
CPU_RATE	double	CPU % used, in interval
CPU_RATE_AVG	double	Average CPU % used, since collection started
CPU_RATE_MAX	double	Maximum CPU % used, since collection started
MEMK_DELTA	double	Delta memory usage, in kilobytes Note: See MemSizeK for special considerations.

Requirements

Attributes: None

Minimum OS version: 2.0

Related reference

[Processes](#) on page 10

OS processes activity view

[PROCESSES](#) on page 53

PROCESSES store

[OS_PROCESSES_CPU](#) on page 25

Interval CPU usage exceeds value rule

[OS_PROCESSES_KMEM_DELTA](#) on page 26

Interval KMem delta exceeds value rule

[OS_PROCESSES_KMEM_USAGE](#) on page 26

Interval KMem usage exceeds value rule

PROCESSES_SOL

OS processes activity (Solaris extension) collection

ROWID

(Pid)

Columns

Name	Data Type	Description
Pid	long	Process ID
PPid	long	Parent process ID
MemSizeK	long	Virtual memory size, in kilobytes Note: Currently, this value is ambiguously-defined, so it's best to compare this value relative to other processes or relative to historical values for this process. Using this value to exactly account for memory usage is not supported.
CPUsecs	double	Number of CPU seconds for the process
User	string(64)	User name
Command	string(256)	Process command-line
ProcCnt	long	Internal-use number of processors on the machine; created by Surveillance
MemVirtK	double	Virtual memory size, in kilobytes
MemResK	double	Resident memory (private + shared) used, in kilobytes
MemSharedK	double	Resident shared memory used, in kilobytes
MemPrivK	double	Resident private memory used, in kilobytes
MinFaults	double	Number of minor faults
MajFaults	double	Number of major faults (reclaims)
Swaps	double	Number of swaps
BlocksIn	double	Number of input blocks
BlocksOut	double	Number of output blocks
MsgSent	double	Number of messages sent
MsgRcvd	double	Number of messages received
VolCtxSwitches	double	Number of voluntary context switches
InvCtxSwitches	double	Number of involuntary context switches
SystemCalls	double	Number of system calls
CharIO	double	Number of character I/Os
MERGESTATUS	long	Internal-use merge status; created by Surveillance
CPU_DELTA	double	Delta number of CPU seconds
CPU_RATE	double	CPU % used, in interval
CPU_RATE_AVG	double	Average CPU % used, since collection started
CPU_RATE_MAX	double	Maximum CPU % used, since collection started
MEMK_DELTA	double	Delta memory usage, in kilobytes Note: See MemSizeK for special considerations.

Name	Data Type	Description
PRIVK_DELTA	double	Delta resident private memory used, in kilobytes
BLOCKIO_DELTA	double	Delta number of block I/Os (input + output)
MSG_DELTA	double	Delta number of messages (sent + received)
CHARIO_DELTA	double	Delta number of character I/Os

Requirements

Attributes: SOLARIS

Minimum OS version: 2.0

Related reference

[PROCESSES_SOL](#) on page 54

PROCESSES_SOL store

PROCESSORS

Processors activity collection

ROWID

(ProcNum)

Columns

Name	Data Type	Description
ProcNum	long	Processor # (starting with 0)
UserTicks	double	Number of user ticks
SystemTicks	double	Number of system ticks
WaitIOTicks	double	Number of wait I/O ticks
IdleTicks	double	Number of idle ticks
UsageTicks	double	Number of non-idle (user + system + wait I/O) ticks
TotalTicks	double	Number of ticks (any kind)
MERGESTATUS	long	Internal-use merge status; created by Surveillance
CPUPCNT	double	(Non-idle) CPU % used, in interval
USERPCNT	double	User CPU % used, in interval
SYSTEMPCNT	double	System CPU % used, in interval
WAITIOPCNT	double	Wait I/O CPU % used, in interval
IDLEPCNT	double	Idle %, in interval

Requirements

Attributes: None

Minimum OS version: 2.0

Related reference

[Processors](#) on page 13

Processors activity view

[PROCESSORS](#) on page 54

PROCESSORS store

[OS_PROCESSORS_CPU_PCNT](#) on page 27

Processor CPU% exceeds value rule

PROCMON

Application process monitoring collection

Comments

This is a user-defined collection (UDC). Edit PROCMON.COL to customize which application processes are included.

ROWID

(AppName, ProcGroup)

Columns

Name	Data Type	Description
AppName	string(64)	Application name, as defined in the UDC
ProcGroup	string(64)	Process group name, as defined in the UDC
Count	long	Number of processes observed in the group; 0 = no processes in the group
MemSizeK	long	Total virtual memory size (UNIX / Linux) or working set memory size (Windows), in kilobytes, for all processes in the group Note: Currently, the memory value for each individual process is ambiguously-defined, and the sum over the processes in the group most likely double-counts memory. Using this value to exactly account for memory usage is not supported.
CPUsecs	double	Total number of CPU seconds for the processes
Pid	long	Process ID of the first matching process in the group
MERGESTATUS	long	Internal-use merge status; created by Surveillance
MEM_KBYTES_DELTA	double	Delta total memory usage, in kilobytes Note: See MemSizeK for special considerations.
MEM_MBYTES	double	Total memory usage, in megabytes Note: See MemSizeK for special considerations.
MEM_MBYTES_AVG	double	Average total memory usage, in megabytes, since collection started Note: See MemSizeK for special considerations.

Name	Data Type	Description
MEM_MBYTES_MAX	double	Maximum total memory usage, in megabytes, since collection started Note: See MemSizeK for special considerations.
CPU_SECS_DELTA	double	Delta total number of CPU seconds for the processes
CPU_SECS_AVG	double	Average of delta total number of CPU seconds, since collection started
CPU_SECS_MAX	double	Maximum of delta total number of CPU seconds, since collection started

Requirements

Attributes: None

Minimum OS version: None

Related reference

[PROCMON](#) on page 55
PROCMON store

[OS_PROCMON_MEM_GT](#) on page 28
Procgroup MemoryMB exceeds value rule

[OS_PROCMON_PROCCNT_GT](#) on page 28
Process count exceeds value rule

[OS_PROCMON_PROCCNT_LT](#) on page 29
Process count < value rule

SQLSERVER_CPU_UTIL

Multi-instance SQL Server CPU utilization collection

ROWID

(process_name)

Columns

Name	Data Type	Description
pid	long	
countertype	long	
dvalue	double	
hrperftime100nsec	double	
process_type	long	
process_name	string(128)	
MERGESTATUS	long	Internal-use merge status; created by Surveillance
RAW_CPU_PCT_CURRENT	double	
CPU_PCT_CURRENT	double	

Name	Data Type	Description
CPU_PCT_AVG	double	
CPU_PCT_MAX	double	

Requirements

Attributes: SQLSERVER

Minimum OS version: 2.0

Related reference

[SQLSERVER_CPU_UTIL](#) on page 55

SQLSERVER_CPU_UTIL store

SQLSERVER_MEMORY_USAGE

Multi-instance SQL Server memory usage collection

ROWID

(process_name)

Columns

Name	Data Type	Description
pid	long	
working_set_private	double	
working_set_total	double	
private_bytes	double	
process_type	long	
process_name	string(128)	
MERGESTATUS	long	Internal-use merge status; created by Surveillance
WORKING_SET_SHARED	double	
OTHER_PRIVATE	double	

Requirements

Attributes: SQLSERVER

Minimum OS version: 2.0

Related reference

[SQLSERVER_MEMORY_USAGE](#) on page 56

SQLSERVER_MEMORY_USAGE store

SQLSERVER_STATUS

Multi-instance SQL Server status collection

ROWID

(instance_name)

Columns

Name	Data Type	Description
pid	long	Process ID
status	string(16)	SQL Server instance status
instance_name	string(128)	SQL Server instance name

Requirements**Attributes:** SQLSERVER**Minimum OS version:** 2.0**Related reference**[SQLSERVER_STATUS](#) on page 56

SQLSERVER_STATUS store

SYSMON

System status / heartbeat monitoring collection

ROWID

(Serial#)

Columns

Name	Data Type	Description
Serial#	long	SAM ID (unique)
SamName	string(32)	SAM name
DomainName	string(32)	SAM domain name
Connect	string(128)	Connect string to the SAM
BeatRate	long	Heartbeat message interval, in seconds
Overdue	long	Heartbeat overdue timeout, in seconds
Expiration	long	Heartbeat subscription lease expiration, in seconds
Status	long	Heartbeat status: 1 Normal 0 Unknown -1 NORAD DOWN -2

Name	Data Type	Description
		SERVER DOWN
StatusDesc	string(32)	Description of the status: NORMAL The SAM is responding normally. NORAD DOWN The SAM is not responding, but the server can be pinged. SERVER DOWN The server is unreachable and appears offline.
Duration	long	Number of seconds observed in the current state

Requirements

Attributes: None

Minimum OS version: 2.0

Related reference

[System Status Monitor](#) on page 15

System status / heartbeat monitoring view

[SYSMON](#) on page 56

SYSMON store

W32SERVICES

Windows services collection

Comments

This is a user-defined collection (UDC). Edit W32SERVICES.COL to customize which Windows services are included.

ROWID

(service_name)

Columns

Name	Data Type	Description
service_name	string(64)	
display_name	string(128)	
state	string(32)	
numstate	long	
ExitStatus	long	
MERGESTATUS	long	Internal-use merge status; created by Surveillance
NUMSTATE_DELTA	double	

Requirements

Attributes: WIN32

Minimum OS version: 2.0

Related reference

[W32SERVICES](#) on page 57

W32SERVICES store

[OS_W32SERVICE_CHANGED_STATE](#) on page 29

Win32 Service has changed state rule

[OS_W32SERVICE_STARTED](#) on page 30

Win32 Service was started rule

[OS_W32SERVICE_STOPPED](#) on page 30

Win32 Service was stopped rule

Chapter

7

Collections

Topics:

- [DEVIO](#)
- [EXECSCRIPT](#)
- [FILESYSTEM](#)
- [GLOBALSTATS](#)
- [LOGFILE](#)
- [MSEVENTLOG](#)
- [PROCESSES](#)
- [PROCESSES_SOL](#)
- [PROCESSORS](#)
- [PROCMON](#)
- [SQLSERVER_CPU_UTIL](#)
- [SQLSERVER_MEMORY_USAGE](#)
- [SQLSERVER_STATUS](#)
- [SYSMON](#)
- [W32SERVICES](#)

DEVIO

Device I/O activity collection

ROWID

(DeviceID)

Columns

Name	Data Type	Description
DeviceID	string(32)	Device ID
DiskReads	double	Number of disk reads
DiskWrites	double	Number of disk writes
MERGESTATUS	long	Internal-use merge status; created by Surveillance
READS_DELTA	double	Delta number of disk reads
WRITES_DELTA	double	Delta number of disk writes
READ_RATE	double	Number of disk reads per second, in interval
WRITE_RATE	double	Number of disk writes per second, in interval
IO_RATE	double	Number of disk I/Os (reads + writes) per second, in interval
IO_RATE_AVG	double	Average number of disk I/Os (reads + writes) per second, since collection started
IO_RATE_MAX	double	Maximum number of disk I/Os (reads + writes) per second, since collection started
READS_TOTAL	double	Total number of disk reads, since collection started
WRITES_TOTAL	double	Total number of disk writes, since collection started
IO_TOTAL	double	Total number of disk I/Os (reads + writes), since collection started
IO_PCT_TOTAL	double	% of total number of disk I/Os (reads + writes) over all devices, since collection started
READ_PCT	double	Disk read % of total number of disk I/Os (reads + writes) over all devices, since collection started

Requirements

Attributes: None

Minimum OS version: 2.0

Related reference

[Device IO](#) on page 12

Device I/O activity view

[DEVIO](#) on page 50

DEVIO store

[OS_DEVIO_IO_RATE](#) on page 18

IO Rate exceeds value rule

[OS_DEVIO_READ_RATE](#) on page 18

Read Rate exceeds value rule

[OS_DEVIO_WRITE_RATE](#) on page 19

Write Rate exceeds value rule

EXECSCRIPT

Custom OS script collection

Comments

This is a sample user-defined collection (UDC). Edit or copy EXECSCRIPT.COL to customize which script outputs are included.

Any user-declared columns will appear following the predefined columns (below). Derived columns appear after any user-declared columns.

ROWID

None

Columns

Name	Data Type	Description
AppName	string(64)	Application name, as defined in the UDC
ScriptName	string(64)	Script name, as defined in the UDC
ExitStatus	long	Script exit status
ResultStr1	string(128)	User-defined result string #1, as defined in the UDC
ResultNum1	double	User-defined result number #1, as defined in the UDC
ResultStr2	string(128)	User-defined result string #2, as defined in the UDC
ResultNum2	double	User-defined result number #2, as defined in the UDC
ExecTimeMS	double	Execution time, in milliseconds

Requirements

Attributes: None

Minimum OS version: None

Related reference

[Script Execution Monitor](#) on page 14

Custom OS script view

[EXECSCRIPT](#) on page 51

EXECSCRIPT store

[OS_EXECSCRIPT_ERREXIT](#) on page 21

Script had Bad exitstatus rule

FILESYSTEM

Filesystem space usage collection

ROWID

(MountPoint)

Columns

Name	Data Type	Description
FileSystem	string(128)	Device path (UNIX / Linux) or filesystem type (Windows)
MountPoint	string(128)	Mount point of filesystem
KBytesUsage	double	Amount of space used, in kilobytes
KBytesCapacity	double	Total capacity size, in kilobytes
MERGESTATUS	long	Internal-use merge status; created by Surveillance
USAGEPCT	double	% of total capacity space that is used
USAGEPCT_DELTA	double	Delta % of total capacity space that is used
KBUSAGE_DELTA	double	Delta amount of space used, in kilobytes
MBUSAGE	double	Amount of space used, in megabytes
MBCAPACITY	double	Total capacity size, in megabytes
MBUSAGE_DELTA	double	Delta amount of space used, in megabytes

Requirements

Attributes: None

Minimum OS version: 2.0

Related reference

[File System Usage](#) on page 13

Filesystem space usage view

[FILESYSTEM](#) on page 50

FILESYSTEM store

[OS_FILESYSTEM_USAGE_PCNT](#) on page 20

Filesystem usage % exceeds value rule

[OS_FILESYSTEM_USAGE_PCNT_DELTA](#) on page 20

Filesystem usage delta exceeds value rule

GLOBALSTATS

Global statistics collection

ROWID

(MetricName)

Columns

Name	Data Type	Description
MetricName	string(64)	Metric name
MetricType	long	Metric type: 1 Counter = sum(Value) 2 Run Level = Value 3 Ratio 4 Rate = Value / Elapsed time
MetricID	long	Metric ID; ID < 100 = displayable metric
Value	double	Metric value
MERGESTATUS	long	Internal-use merge status; created by Surveillance
CURRENT	double	Current metric value, based on metric type
AVG	double	Average of current metric value, since collection started
MAX	double	Maximum current metric value, since collection started
VALUE_DELTA	double	Delta metric value (regardless of metric type)
TOTAL	double	Total of current metric values, since collection started, if applicable

Requirements

Attributes: None

Minimum OS version: 2.0

Related reference

[Global](#) on page 10

Global statistics view

[GLOBALSTATS](#) on page 51

GLOBALSTATS store

[OS_GLOBAL_CPU_PCNT](#) on page 22

Overall CPU % exceeds value rule

[OS_GLOBAL_DISKIO](#) on page 21

Diskio/sec exceeds value rule

[OS_GLOBAL_MEMORY_PCNT](#) on page 23

Memory usage % exceeds value rule

[OS_GLOBAL_PROCESS_CNT](#) on page 23

Process count exceeds value rule

[OS_GLOBAL_SWAP_USAGE](#) on page 24

Swap usage % exceeds value rule

LOGFILE

Log file parsing collection

Comments

This is a sample user-defined collection (UDC). Edit or copy LOGFILE.COL to customize which error log entries are included.

Any user-declared columns will appear following the predefined columns (below). Derived columns appear after any user-declared columns.

ROWID

None

Columns

Name	Data Type	Description
Timestamp	string(32)	Time when the message was parsed
Seq#	long	Sequence #, within a timestamp
AppName	string(64)	Application name, as defined in the UDC
FilePath	string(256)	Error log file path
ErrorCode	string(128)	Error code, as defined in the UDC
ErrorLevel	string(128)	Error level, as defined in the UDC
ErrorText	string(256)	Error text, as defined in the UDC

Requirements

Attributes: None

Minimum OS version: None

Related reference

[LOGFILE](#) on page 52

LOGFILE store

[OS_LOGFILE_ERROR](#) on page 24

Logfile contains ERROR rule

MSEVENTLOG

Windows Event Log collection

Comments

This is a user-defined collection (UDC). Edit MSEVENTLOG.COL to customize which Windows events are included.

Any user-declared columns will appear following the predefined columns (below). Derived columns appear after any user-declared columns.

ROWID

(ServerName, LogName, RecordNum, EventTime)

Columns

Name	Data Type	Description
ServerName	string(64)	Server name
LogName	string(64)	Name of the event log (i.e. Security, System, Application)
RecordNum	long	Record # in the event log
ClosingRecordNum	long	If this event closes a previous one: record # of the opening event in the event log
EventTime	time	Time when the event was observed
EventID	long	Event number
EventType	string(32)	Type of event (i.e. Error, Warning)
EventCategory	string(64)	Event category
User	string(64)	User which generated the event
Domain	string(64)	Domain of the user which generated the event
Source	string(64)	Source of the event (i.e. program, component)
Computer	string(64)	Computer name
Description	string(1024)	Event description

Requirements**Attributes:** WIN32**Minimum OS version:** None**Related reference**[MSEVENTLOG](#) on page 53

MSEVENTLOG store

[OS_MSEVTLOG_ERROR](#) on page 25

MS EventLog contains ERROR rule

PROCESSES

OS processes activity collection

ROWID

(Pid)

Columns

Name	Data Type	Description
Pid	long	Process ID
PPid	long	Parent process ID
MemSizeK	long	Virtual memory size (UNIX / Linux) or working set memory size (Windows), in kilobytes Note: Currently, this value is ambiguously-defined, so it's best to compare this value relative to other processes or relative to historical values for this process. Using this value to exactly account for memory usage is not supported.
CPUsecs	double	Number of CPU seconds for the process
User	string(64)	User name
Command	string(256)	Process command-line
ProcessName	string(256)	Process name, typically the executable name
ProcCnt	long	Internal-use number of processors on the machine; created by Surveillance
MERGESTATUS	long	Internal-use merge status; created by Surveillance
CPU_DELTA	double	Delta number of CPU seconds
CPU_RATE	double	CPU % used, in interval
CPU_RATE_AVG	double	Average CPU % used, since collection started
CPU_RATE_MAX	double	Maximum CPU % used, since collection started
MEMK_DELTA	double	Delta memory usage, in kilobytes Note: See MemSizeK for special considerations.

Requirements

Attributes: None

Minimum OS version: 2.0

Related reference

[Processes](#) on page 10

OS processes activity view

[PROCESSES](#) on page 53

PROCESSES store

[OS_PROCESSES_CPU](#) on page 25

Interval CPU usage exceeds value rule

[OS_PROCESSES_KMEM_DELTA](#) on page 26

Interval KMem delta exceeds value rule

[OS_PROCESSES_KMEM_USAGE](#) on page 26

Interval KMem usage exceeds value rule

PROCESSES_SOL

OS processes activity (Solaris extension) collection

ROWID

(Pid)

Columns

Name	Data Type	Description
Pid	long	Process ID
PPid	long	Parent process ID
MemSizeK	long	Virtual memory size, in kilobytes Note: Currently, this value is ambiguously-defined, so it's best to compare this value relative to other processes or relative to historical values for this process. Using this value to exactly account for memory usage is not supported.
CPUsecs	double	Number of CPU seconds for the process
User	string(64)	User name
Command	string(256)	Process command-line
ProcCnt	long	Internal-use number of processors on the machine; created by Surveillance
MemVirtK	double	Virtual memory size, in kilobytes
MemResK	double	Resident memory (private + shared) used, in kilobytes
MemSharedK	double	Resident shared memory used, in kilobytes
MemPrivK	double	Resident private memory used, in kilobytes
MinFaults	double	Number of minor faults
MajFaults	double	Number of major faults (reclaims)
Swaps	double	Number of swaps
BlocksIn	double	Number of input blocks
BlocksOut	double	Number of output blocks
MsgSent	double	Number of messages sent
MsgRcvd	double	Number of messages received
VolCtxSwitches	double	Number of voluntary context switches
InvCtxSwitches	double	Number of involuntary context switches
SystemCalls	double	Number of system calls
CharIO	double	Number of character I/Os
MERGESTATUS	long	Internal-use merge status; created by Surveillance

Name	Data Type	Description
CPU_DELTA	double	Delta number of CPU seconds
CPU_RATE	double	CPU % used, in interval
CPU_RATE_AVG	double	Average CPU % used, since collection started
CPU_RATE_MAX	double	Maximum CPU % used, since collection started
MEMK_DELTA	double	Delta memory usage, in kilobytes Note: See MemSizeK for special considerations.
PRIVK_DELTA	double	Delta resident private memory used, in kilobytes
BLOCKIO_DELTA	double	Delta number of block I/Os (input + output)
MSG_DELTA	double	Delta number of messages (sent + received)
CHARIO_DELTA	double	Delta number of character I/Os

Requirements

Attributes: SOLARIS

Minimum OS version: 2.0

Related reference

[PROCESSES_SOL](#) on page 54

PROCESSES_SOL store

PROCESSORS

Processors activity collection

ROWID

(ProcNum)

Columns

Name	Data Type	Description
ProcNum	long	Processor # (starting with 0)
UserTicks	double	Number of user ticks
SystemTicks	double	Number of system ticks
WaitIOTicks	double	Number of wait I/O ticks
IdleTicks	double	Number of idle ticks
UsageTicks	double	Number of non-idle (user + system + wait I/O) ticks
TotalTicks	double	Number of ticks (any kind)
MERGESTATUS	long	Internal-use merge status; created by Surveillance
CPUPCNT	double	(Non-idle) CPU % used, in interval
USERPCNT	double	User CPU % used, in interval

Name	Data Type	Description
SYSTEMPCNT	double	System CPU % used, in interval
WAITIOPCNT	double	Wait I/O CPU % used, in interval
IDLEPCNT	double	Idle %, in interval

Requirements

Attributes: None

Minimum OS version: 2.0

Related reference

[Processors](#) on page 13

Processors activity view

[PROCESSORS](#) on page 54

PROCESSORS store

[OS_PROCESSORS_CPU_PCNT](#) on page 27

Processor CPU% exceeds value rule

PROCMON

Application process monitoring collection

Comments

This is a user-defined collection (UDC). Edit PROCMON.COL to customize which application processes are included.

ROWID

(AppName, ProcGroup)

Columns

Name	Data Type	Description
AppName	string(64)	Application name, as defined in the UDC
ProcGroup	string(64)	Process group name, as defined in the UDC
Count	long	Number of processes observed in the group; 0 = no processes in the group
MemSizeK	long	Total virtual memory size (UNIX / Linux) or working set memory size (Windows), in kilobytes, for all processes in the group Note: Currently, the memory value for each individual process is ambiguously-defined, and the sum over the processes in the group most likely double-counts memory. Using this value to exactly account for memory usage is not supported.
CPUSecs	double	Total number of CPU seconds for the processes

Name	Data Type	Description
Pid	long	Process ID of the first matching process in the group
MERGESTATUS	long	Internal-use merge status; created by Surveillance
MEM_KBYTES_DELTA	double	Delta total memory usage, in kilobytes Note: See MemSizeK for special considerations.
MEM_MBYTES	double	Total memory usage, in megabytes Note: See MemSizeK for special considerations.
MEM_MBYTES_AVG	double	Average total memory usage, in megabytes, since collection started Note: See MemSizeK for special considerations.
MEM_MBYTES_MAX	double	Maximum total memory usage, in megabytes, since collection started Note: See MemSizeK for special considerations.
CPU_SECS_DELTA	double	Delta total number of CPU seconds for the processes
CPU_SECS_AVG	double	Average of delta total number of CPU seconds, since collection started
CPU_SECS_MAX	double	Maximum of delta total number of CPU seconds, since collection started

Requirements

Attributes: None

Minimum OS version: None

Related reference

[PROCMON](#) on page 55

PROCMON store

[OS_PROCMON_MEM_GT](#) on page 28

Procgroupp MemoryMB exceeds value rule

[OS_PROCMON_PROCCNT_GT](#) on page 28

Process count exceeds value rule

[OS_PROCMON_PROCCNT_LT](#) on page 29

Process count < value rule

SQLSERVER_CPU_UTIL

Multi-instance SQL Server CPU utilization collection

ROWID

(process_name)

Columns

Name	Data Type	Description
pid	long	
countertype	long	
dvalue	double	
hrperftime100nsec	double	
process_type	long	
process_name	string(128)	
MERGESTATUS	long	Internal-use merge status; created by Surveillance
RAW_CPU_PCT_CURRENT	double	
CPU_PCT_CURRENT	double	
CPU_PCT_AVG	double	
CPU_PCT_MAX	double	

Requirements

Attributes: SQLSERVER

Minimum OS version: 2.0

Related reference

[SQLSERVER_CPU_UTIL](#) on page 55

SQLSERVER_CPU_UTIL store

SQLSERVER_MEMORY_USAGE

Multi-instance SQL Server memory usage collection

ROWID

(process_name)

Columns

Name	Data Type	Description
pid	long	
working_set_private	double	
working_set_total	double	
private_bytes	double	
process_type	long	
process_name	string(128)	
MERGESTATUS	long	Internal-use merge status; created by Surveillance
WORKING_SET_SHARED	double	

Name	Data Type	Description
OTHER_PRIVATE	double	

Requirements

Attributes: SQLSERVER

Minimum OS version: 2.0

Related reference

[SQLSERVER_MEMORY_USAGE](#) on page 56

SQLSERVER_MEMORY_USAGE store

SQLSERVER_STATUS

Multi-instance SQL Server status collection

ROWID

(instance_name)

Columns

Name	Data Type	Description
pid	long	Process ID
status	string(16)	SQL Server instance status
instance_name	string(128)	SQL Server instance name

Requirements

Attributes: SQLSERVER

Minimum OS version: 2.0

Related reference

[SQLSERVER_STATUS](#) on page 56

SQLSERVER_STATUS store

SYSMON

System status / heartbeat monitoring collection

ROWID

(Serial#)

Columns

Name	Data Type	Description
Serial#	long	SAM ID (unique)

Name	Data Type	Description
SamName	string(32)	SAM name
DomainName	string(32)	SAM domain name
Connect	string(128)	Connect string to the SAM
BeatRate	long	Heartbeat message interval, in seconds
Overdue	long	Heartbeat overdue timeout, in seconds
Expiration	long	Heartbeat subscription lease expiration, in seconds
Status	long	Heartbeat status: 1 Normal 0 Unknown -1 NORAD DOWN -2 SERVER DOWN
StatusDesc	string(32)	Description of the status: NORMAL The SAM is responding normally. NORAD DOWN The SAM is not responding, but the server can be pinged. SERVER DOWN The server is unreachable and appears offline.
Duration	long	Number of seconds observed in the current state

Requirements

Attributes: None

Minimum OS version: 2.0

Related reference

[System Status Monitor](#) on page 15

System status / heartbeat monitoring view

[SYSMON](#) on page 56

SYSMON store

W32SERVICES

Windows services collection

Comments

This is a user-defined collection (UDC). Edit W32SERVICES.COL to customize which Windows services are included.

ROWID

(service_name)

Columns

Name	Data Type	Description
service_name	string(64)	
display_name	string(128)	
state	string(32)	
numstate	long	
ExitStatus	long	
MERGESTATUS	long	Internal-use merge status; created by Surveillance
NUMSTATE_DELTA	double	

Requirements

Attributes: WIN32

Minimum OS version: 2.0

Related reference

[W32SERVICES](#) on page 57

W32SERVICES store

[OS_W32SERVICE_CHANGED_STATE](#) on page 29

Win32 Service has changed state rule

[OS_W32SERVICE_STARTED](#) on page 30

Win32 Service was started rule

[OS_W32SERVICE_STOPPED](#) on page 30

Win32 Service was stopped rule

Chapter

8

Central Repository Schema

The table name in the Central Repository for a collection is a collector-specific prefix (i.e. OS), followed by an underscore (_), and then the collection name. For example, the OS collection GLOBALSTATS is exported to the table OS_GLOBALSTATS.

Column names are prefixed with "C_". Additional metadata columns are exported, as well: C_ENTITY_NAME, C_SAMPLE_HOST, C_SAMPLE_TIME. A few optional columns may be present to track various archive operations: IS_PEAK, ARCHIVES_STATUS.

