CA Nimsoft Monitor

Probe Guide for Active Directory Server

ad_server v1.5 series

Legal Notices

Warranty

The material contained in this document is provided "as is," and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Nimsoft LLC disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Nimsoft LLC shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Nimsoft LLC and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Nimsoft LLC as governed by United States and international copyright laws.

Restricted Rights Legend

If software is for use in the performance of a U.S. Government prime contract or subcontract, Software is delivered and licensed as "Commercial computer software" as defined in DFAR 252.2277014 (June 1995), or as a "commercial item" as defined in FAR 2.101(a) or as "Restricted computer software" as defined in FAR 52.22719 (June 1987) or any equivalent agency regulation or contract clause. Use, duplication or disclosure of Software is subject to Nimsoft LLC's standard commercial license terms, and nonDOD Departments and Agencies of the U.S. Government will receive no greater than Restricted Rights as defined in FAR 52.22719(c)(12) (June 1987). U.S. Government users will receive no greater than Limited Rights as defined in FAR 52.22714 (June 1987) or DFAR 252.2277015 (b)(2) (November 1995), as applicable in any technical data.

Trademarks

Nimsoft is a trademark of CA.

Adobe®, Acrobat®, Acrobat Reader®, and Acrobat Exchange® are registered trademarks of Adobe Systems Incorporated.

Intel® and Pentium® are U.S. registered trademarks of Intel Corporation.

Java(TM) is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Netscape(TM) is a U.S. trademark of Netscape Communications Corporation.

Oracle® is a U.S. registered trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of the Open Group.

ITIL® is a Registered Trade Mark of the Office of Government Commerce in the United Kingdom and other countries.

All other trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

For information on licensed and public domain software, see the *Nimsoft Monitor ThirdParty Licenses and Terms of Use* document at: http://docs.nimsoft.com/prodhelp/en_US/Library/index.htm?toc.htm?1981724.html.

Contact CA

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

Send comments or questions about CA Technologies Nimsoft product documentation to nimsoft.techpubs@ca.com.

To provide feedback about general CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Documentation Changes

This table describes the version history for this document.

Version	Date	What's New?
1.5	January 2014	Initial web-based GUI version of this probe. (Previous versions of this probe are configured using Infrastructure Manager).

Chapter 1: Overview

The Active Directory Server probe monitors the selected checkpoints on Active Directory. These checkpoints measure the availability and response time of the active directory server and perform the health checks to prevent outage and degradation conditions.

Active Directory is the directory service included with the Windows servers to manage the identities and relationships that make up network environments.

The probe uses monitoring profiles, which are classified in the following seven predefined groups or categories:

- **Event Logs:** Monitoring the event logs for specific event IDs contents. For example, messages.
- **Filesystems:** Monitoring the file systems for specific patterns.
- **Files:** Monitoring for specific files.
- **Performance Counters:** Monitoring the performance counters for a wide range of system objects. For example, disk, CPU performance, and memory print queues.
- **Processes:** Monitoring the wide range of counters for the different processes running on the system.
- **Services:** Monitoring the services outside the Active Directory that are essential to the proper operation of Active Directory.
- **WMI:** Checking authentication failures and the inability to access resources.

  Note: The probe does not support the WMI of Datatype Reference.

Each of these categories can contain several profiles. The Active Directory Server probe is delivered with a default configuration with a selected set of profiles to be monitored. You can define your own profiles containing more than one counter.

This section contains the following topics:

About This Guide

This guide is for the CA Nimsoft Monitor Administrator to help understand the configuration of the Active Directory Server probe.

This guide contains the following information:

- An overview of the Active Directory Server probe.
- The related documentation for previous probe versions, release notes, and so on.
- The configuration details of the probe including information for the fields that are required to configure the probe.
- The common procedures that can be used in the probe configuration.
- Field description with their default values.

Important! The field description for intuitive terms in the GUI has not been included in the document.

Related Documentation

For related information that may be of interest, see the following material:

Related Documentation

Documentation for other versions of the ad_server probe

The Release Notes for the ad_server probe

User documentation for the Admin Console

Monitor Metrics Reference Information for CA Nimsoft Probes (http://docs.nimsoft.com/prodhelp/en_US/Probes/ProbeReference/index.htm)

Preconfiguration Requirements

This section contains the preconfiguration requirements for the Active Directory Server probe.

Supported Platform

Refer to the Nimsoft Compatibility Support Matrix for the latest information about supported platforms. See also the Support Matrix for Nimsoft Probes for more specific information about the Active Directory Server probe.

Chapter 2: Configuration Details

The Active Directory Server probe is configured to monitor health and performance of the Active Directory (AD) server by configuring the threshold parameters for counters. This probe is delivered with a default configuration with a selected set of monitoring counters.

Note: The Active Directory Server probe is a local probe, which monitors the AD Server of the host system only.

This section contains the following topics:

ad_server Node (see page 9)

ad_server Node

In this node, you can view the probe information and can configure the general properties of the Active Directory Server probe. You can also configure the log level of the probe.

Navigation: ad_server

Set or modify the following values that are based on your requirement:

ad_server > Probe Information

This section provides information about the probe name, probe version, start time of the probe, and the vendor who created the probe.

ad_server > General Config

This section is used to configure the log level of the probe.

Note: Recommendation is to select a lower log level during the normal operation and minimize the disk consumption. You can increase the log level while debugging.

Event Logs Node

The **Event Logs** node is used to create and configure the monitoring profiles for monitoring the event logs of the host system. Each monitoring profile is displayed as the child node of the **Event Logs** node.

<Profile Name> Node

The *profile name* is used to configure properties for monitoring the event logs of the host system.

Note: This node is referred as the *profile name* node in this document as it displays the name of the monitoring profile, which is user-configurable.

Navigation: ad_server > Event Logs > *profile name*

Set or modify the following values that are based on your requirement:

***profile name* > General**

This section displays the properties which are defined at time of creating a profile. You can configure these properties when the changes are required.

- Sample Data Every: Defines the time interval for executing the profile and collecting data.
- Sample Data Every (Unit): Specifies a unit of time interval. The valid units are seconds, minutes, hours, or days.
- Startup Delay: Defines a time delay after activating the profile for start collecting data from the AD Server.
- Startup Delay (Unit): Specifies a unit of time delay. The valid units are seconds, minutes, hours, or days.

***profile name* > Event Log**

This section defines the criteria for monitoring the Windows Event Logs.

- Log: Specifies the log file from which the probe fetches the events for monitoring.
- Computer: Defines the computer name on which the event has occurred.
- Source/Publisher: Defines the source or the publisher from where the event has logged.
- Severity: Specifies the severity of the event.
- User: Defines the Windows user account for whom the event was generated.
- Category: Defines the event category. For example, Service State Event.
- Event ID: Defines the unique identification number of the event.
- Message: Defines the message text of the event. You can use the regular expressions for matching the message string.

***profile name* > Counter: Counter Name**

This section is used for configuring the thresholds for the counter and displays a list of counters that are configured earlier. The **New** and **Delete** options are used for managing the list of thresholds for the counter. A separate section is displayed for each counter, which is added to the profile for monitoring.

- Publish Data: Allows the probe for generating the QoS messages.

  Default: Not selected

  Note: This field appears if the counter generates the QoS messages.
- Threshold: Defines the threshold value of the counter for generating alarms.
- Operator: Specifies the threshold operator for comparing the actual value with the threshold value.
- Severity: Specifies the severity of the alarm message.
- Message: Specifies the alarm message to be issued when the threshold value is breached.

File Node

The **File** node is used for monitoring files of the host system. Each monitoring profile is displayed as the child node of the **File** node.

<Profile Name> Node

This node allows you to define files, which the profile monitors.

Navigation: ad_server > Files > *profile name*

Set or modify the following values that are based on your requirement:

***profile name* > File**

This section allows you to define the complete path of the file to be monitored.

Note: The field descriptions for the **General** and the **Counter: Counter Name** sections are same as described in the **Event Logs** node.

File System Node

The **File System** node defines the file system (for example, **C:** and **C:\program Files**) and allows you to create a monitoring profile. The Active Directory Server probe checks the directory existence, file existence, size of the directory, and age of the oldest and newest file.

<Profile Name> Node

This node allows you to configure the file system, which the profile monitors.

Navigation: ad_server > File System > *profile name*

Set or modify the following values that are based on your requirement:

***profile name* > File System**

This section allows you to define the complete path of the directory to be monitored.

- Directory: Defines the complete path of the directory or file system for monitoring.
- Pattern: Defines the pattern (for example, the name of a file) to be searched for within the file system.
- Include Subdirectories: Allows you to include sub directories to be searched for within the file system.

Note: The field descriptions for the **General** and the **Counter: Counter Name** sections are same as described in the **Event Logs** node.

Performance Counter Node

The **Performance Counter** node allows you to create a monitoring profile for providing and consuming performance data from the performance counters. This data provides health information about Operating System, Network, Applications, Services, and so on.

<Profile Name> Node

The *profile name* node configures a monitoring profile for consuming data from the performance counters. This data is used for comparing actual values with the threshold values and generate alarms and QoS.

Navigation: ad_server > Performance Counters > *profile name*

Set or modify the following values that are based on your requirement:

***profile name* > Performance Counter**

This section allows you to define the object and instance that the profile monitors.

- Object: Specifies the performance object that is available on the host for monitoring.
- Instance: Specifies an instance of the object.

Note: The field descriptions for the **General** and the **Counter: Counter Name** sections are same as described in the **Event Logs** node.

Process Node

The **Process** node allows you to monitor the processes that are running on the host system (for example, **notepad.exe**).

<Profile Name> Node

The *profile name* node allows you to configure the monitoring parameters of the process, which the probe is monitoring.

Navigation: ad_server > Process > *profile name*

Set or modify the following values that are based on your requirement:

***profile name* > Process**

This section allows you to specify the process that the profile is monitoring.

Note: The field descriptions for the **General** and the **Counter: Counter Name** sections are same as described in the **Event Logs** node.

Service Node

The **Service** node allows you to monitor the services that are running on the host system (for example, **Dnscache**).

<Profile Name> Node

The *profile name* node allows you to configure the monitoring parameters of the service, which the probe is monitoring.

Navigation: ad_server > Service > *profile name*

Set or modify the following values that are based on your requirement:

***profile name* > Service**

This section allows you to specify the process that the profile is monitoring.

Note: The field descriptions for the **General** and the **Counter: Counter Name** sections are same as described in the **Event Logs** node.

WMI Node

The **WMI** node is used for creating a monitoring profile for getting WMI-related data from the host system. The WMI is used for consolidating the management of devices and applications in a network from the Windows environment.

<Profile Name> Node

The *profile name* node allows you to configure the WMI parameters for getting status of the local and remote systems.

Navigation: ad_server > WMI > *profile name*

Set or modify the following values that are based on your requirement:

***profile name* > WMI**

This section allows you to specify the process that the profile is monitoring.

- Namespace: Specifies the namespace of the WMI for monitoring. For example, **CIMV2**.
- Class: Specifies a class of the selected namespace for monitoring. For example, **Win32_process**.
- Instance: Specifies the instance of the selected class for monitoring, when more than one are found. For example, **notepad.exe**.

Note: The field descriptions for the **General** and the **Counter: Counter Name** sections are same as described in the **Event Logs** node.

Configure a Node

This procedure provides the information to configure a particular section within a node.

Each section within the node allows you to configure the properties of the probe. You can monitor the health and performance of the AD Server by gathering data about the monitoring checkpoints.

Follow these steps:

1. Select the appropriate navigation path.
2. Update the field information and click **Save**.

   The specified section of the probe is configured.

The probe is now ready for monitoring the health and performance of the AD Server.

Manage Profiles

In the probe GUI, the navigation pane consists of a parent node. Under the parent node, there are some predefined groups, which are Event Logs, Files, File System, Performance Counter, Process, Service, and WMI. You can add child nodes under these predefined groups. These child nodes correspond to the unique profiles, which are configured for the probe to start monitoring. To configure a profile, information is entered or selected in the fields, appearing for the selected profile.

Follow these steps:

1. Click the **Options** icon next to the appropriate group node in the navigation pane.
2. Click the **Add Profile** option.
3. Enter profile details in the **New Profile** dialog and click **Submit**.

   The profile is saved and you can configure the profile properties for monitoring the AD Server.

Delete Profile

You can delete an existing profile of a predefined group when you no longer want the probe to monitor it.

Follow these steps:

1. Click the **Options** icon next to the *profile name* node that you want to delete.
2. Click the **Delete Profile** option.

   The profile is deleted. Alternatively, deactivate a monitoring profile for avoiding a reconfiguration of the profile when the requirement comes again.

Add Counter

You can add a counter for a monitoring profile. A counter defines the area, which the profile monitors. For each type of profile, there is a list of predefined counters. You can add one or more of these counters to the profile.

Follow these steps:

1. Click the **Options** icon next to the *profile name* node in the navigation pane.
2. Click the **Add Counter** option.

3. Select the counter from the **Name** drop-down menu and click **Submit**.

   The new counter is added as a separate section in the right pane.

Note: You can add counters for every predefined group or category. The option to add a counter for a profile appears only when certain selection criteria are met, depending on which predefined group is selected.

Add Threshold for Counter

The probe GUI allows you to add a threshold for a counter that defines the performance criteria to raise alarm when the threshold value breaches.

Follow these steps:

1. Select the *profile name* node in the navigation pane.
2. Click the **New** button in the **Counter** section for which you want to add a threshold.
3. Update the field information and click **Save**.

   The threshold details are added, which defines the performance criteria to raise alarm with the specific severity and message.

Delete Threshold for Counter

You can delete a threshold for a counter when you no longer require it.

Follow these steps:

1. Select the *profile name* node in the left navigation pane.
2. Select the threshold in the table of the **Counter** section, which you want to delete.
3. Click the **Delete** button in the **Counter** section.
4. Click **Save**.

   The selected threshold is deleted.

Chapter 3: QoS Threshold Metrics

Many Nimsoft Monitor probes are shipped with some default QoS threshold values set. The default threshold values provide an idea of the type of values to be entered in the fields. These default values are not necessarily recommended best practice values. To aid in tuning thresholds and reducing false-positive alarms, this section describes the QoS metrics and provides the default QoS thresholds.

This section contains the following topics:

ad_server QoS Metrics

The following table describes the checkpoint metrics that can be configured using the ad_server probe.

Monitor Name	Units	Description
Eventlogs		
QOS_NUMBEROFEVENTSFOUND	-	Number of events found
Files		
QOS_CHANGED	-	Changed
QOS_CREATED	-	Created
Filesystems		
QOS_DIRECTORIES	-	Directories
QOS_FILEAGENEWEST	-	File Age Newest
QOS_FILEAGEOLDEST	-	File Age Oldest
QOS_FILES	-	Files
QOS_TOTALSIZE	-	Total Size
Performance Counters		
QOS_SQLCLIENT:_CURRENT_#_CONNECTION_POOLS	-	Sql Client: Current # of connection pools
QOS_SQLCLIENT:_CURRENT_#_POOLED_AND_NONPOOLED_CONNECTIONS	-	Sql Client: Current # of pooled and nonpooled connections
QOS_SQLCLIENT:_CURRENT_#_POOLED_CONNECTIONS	-	Sql Client: Current # of pooled connections

Monitor Name	Units	Description
QOS_SQLCLIENT:_PEAK_#_POOLED_CONNECTIONS	-	Sql Client: Peak # of pooled connctions
QOS_SQLCLIENT:_TOTAL_#_FAILED_COMMANDS	-	Sql Client: Total # of failed commands
QOS_SQLCLIENT:_TOTAL_#_FAILED_CONNECTS	-	Sql Client: Total # of failed connects
QOS_WORKFLOWS_ABORTED	-	Workflows Aborted
QOS_WORKFLOWS_ABORTED/SEC	-	Workflows Aborted per second
QOS_WORKFLOWS_COMPLETED	-	Workflows Completed
QOS_WORKFLOWS_COMPLETED/SEC	-	Workflows Completed per second
QOS_WORKFLOWS_CREATED	-	Workflows Created
QOS_WORKFLOWS_CREATED/SEC	-	Workflows Created per second
QOS_WORKFLOWS_EXECUTING	-	Workflows Executing
QOS_WORKFLOWS_IDLE/SEC	-	Workflows Idle per second
QOS_WORKFLOWS_IN_MEMORY	-	Workflows in Memory
QOS_WORKFLOWS_LOADED	-	Workflows Loaded
QOS_WORKFLOWS_LOADED/SEC	-	Workflows Loaded per second
QOS_WORKFLOWS_PENDING	-	Worklfows Pending
QOS_WORKFLOWS_PERSISTED	-	Workflows Persisted
QOS_WORKFLOWS_PERSISTED/SEC	-	Workflows Persisted per second
QOS_WORKFLOWS_RUNNABLE	-	Workflows Runnable
QOS_WORKFLOWS_SUSPENDED	-	Workflows Suspended
QOS_WORKFLOWS_SUSPENDED/SEC	-	Workflows Suspended per second
QOS_WORKFLOWS_TERMINATED	-	Workflows Terminated
QOS_WORKFLOWS_TERMINATED/SEC	-	Workflows Terminated per second
QOS_WORKFLOWS_UNLOADED	-	Workflows Unloaded
QOS_WORKFLOWS_UNLOADED/SEC	-	Workflows Unloaded per second
QOS_FRAGMENTATION_FAILURES	-	Fragmentation Failures
Processes		
QOS_EXECUTIONSTATE	-	Execution State
QOS_HANDLECOUNT	-	Handle Count
QOS_KERNELMODETIME	100ns	Kernel Mode Time
QOS_MAXIMUMWORKINGSETSIZE	Kilobytes	Maximum Working Set Size

Monitor Name	Units	Description
QOS_MINIMUMWORKINGSETSIZE	Kilobytes	Minimum Working Set Size
QOS_OTHEROPERATIONCOUNT	-	Other Operation Count
QOS_OTHERTRANSFERCOUNT	Bytes	Other Transfer Count
QOS_PAGEFAULTS	-	Page Faults
QOS_PAGEFILEUSAGE	Kilobytes	Page File Usage
QOS_PARENTPROCESSID	-	Parent Process Id
QOS_PEAKPAGEFILEUSAGE	Kilobytes	Peak Page File Usage
QOS_PEAKVIRTUALSIZE	Bytes	PeakVirtualSize
QOS_PEAKWORKINGSETSIZE	Kilobytes	Peak Working Set Size
QOS_PRIORITY	-	Priority
QOS_PRIVATEPAGECOUNT	-	Private Page Count
QOS_PROCESSID	-	Process ID
QOS_QUOTANONPAGEDPOOLUSAGE	-	Quota Nonpaged Pool Usage
QOS_QUOTAPAGEDPOOLUSAGE	-	Quota Paged Pool Usage
QOS_QUOTAPEAKNONPAGEDPOOLUSAGE	-	Quota Peak Nonpaged Pool Usage
QOS_QUOTAPEAKPAGEDPOOLUSAGE	-	Quota Peak Paged Pool Usage
QOS_READOPERATIONCOUNT	-	Read Operation Count
QOS_READTRANSFERCOUNT	Bytes	Read Transfer Count
QOS_SESSIONID	-	Session ID
QOS_THREADCOUNT	-	Thread Count
QOS_USERMODETIME	100ns	User Mode Time
QOS_VIRTUALSIZE	Bytes	Virtual Size
QOS_WORKINGSETSIZE	-	Working Set Size
QOS_WORKINGOPERATIONCOUNT	-	Write Operation Count
QOS_WRITETRANSFERCOUNT	-	Write Transfer Count
WMI		
QOS_COUNTERVALUE	-	Counter Value

ad_server Alert Metrics Default Settings

This section contains the alert metric default settings for the ad_server probe.

Alert Metric	Warning Threshold	Warning Severity	Error Threshold	Error Severity	Description
Eventlogs					
Event Found	-	-	TRUE	Critical	Event matched
Number of Events Found	-	-	-	Critical	Event matched
Files					
Not Found	-	-	TRUE	Critical	File failure
Changed	-	-	-	Critical	File failure
Created	-	-	-	Critical	File failure
Filesystems					
Directories	-	-	-	Critical	File system failure
File Age Newest	-	-	-	Critical	File system failure
File Age Oldest	-	-	-	Critical	File system failure
Files	-	-	-	Critical	File system failure
Total Size	-	-	-	Critical	File system failure
Not Found	-	-	TRUE	Critical	File system failure
Performance Counters					
Sql Client: Current # of connection pools	-	-	-	Critical	Performance failure
Sql Client: Current # of pooled and nonpooled connections	-	-	-	Critical	Performance failure
Sql Client: Current # of pooled connections	-	-	-	Critical	Performance failure
Sql Client: Peak # of pooled connections	-	-	-	Critical	Performance failure
Sql Client: Total # of failed commands	-	-	-	Critical	Performance failure
Sql client: Total # of failed connects	-	-	-	Critical	Performance failure
% Processor Time	50	Warning	-	-	Performance failure

Alert Metric	Warning Threshold	Warning Severity	Error Threshold	Error Severity	Description
IO Read Bytes per second	-	-	100000	Major	Performance failure
IO Write Bytes per second	-	-	100000	Major	Performance failure
Page Faults per second	-	-	1000	Major	Performance failure
Fragmentation failures	-	-	-	Critical	Performance failure
Active Lines	-	-	-	Critical	Performance failure
Active Telephones	-	-	-	Critical	Performance failure
Client Apps	-	-	-	Critical	Performance failure
Current Incoming Calls	-	-	-	Critical	Performance failure
Current Outgoing Calls	-	-	-	Critical	Performance failure
Incoming Calls per second	-	-	-	Critical	Performance failure
Lines	-	-	-	Critical	Performance failure
Outgoing Calls per second	-	-	-	Critical	Performance failure
Telephone Devices	-	-	-	Critical	Performance failure
Active Sessions	-	-	-	Critical	Performance failure
Inactive Sessions	-	-	-	Critical	Performance failure
Total Sessions	-	-	-	Critical	Performance failure
Datagrams No Port per second	-	-	-	Critical	Performance failure
Datagrams Received Errors	-	-	-	Critical	Performance failure
Datagrams Received per second	-	-	-	Critical	Performance failure
Datagrams Sent per second	-	-	-	Critical	Performance failure
Datagrams per second	-	-	-	Critical	Performance failure
Workflows Aborted	-	-	-	Critical	Performance failure
Workflows Aborted per second	-	-	-	Critical	Performance failure
Workflows Completed	-	-	-	Critical	Performance failure
Workflows Completed per second	-	-	-	Critical	Performance failure
Workflows Created	-	-	-	Critical	Performance failure
Workflows Created per second	-	-	-	Critical	Performance failure
Workflows Executing	-	-	-	Critical	Performance failure
Workflows Idle per second	-	-	-	Critical	Performance failure

Alert Metric	Warning Threshold	Warning Severity	Error Threshold	Error Severity	Description
Workflows in Memory	-	-	-	Critical	Performance failure
Workflows Loaded	-	-	-	Critical	Performance failure
Workflows Loaded per second	-	-	-	Critical	Performance failure
Workflows Pending	-	-	-	Critical	Performance failure
Workflows Persisted	-	-	-	Critical	Performance failure
Workflows Persisted per second	-	-	-	Critical	Performance failure
Workflows runnable	-	-	-	Critical	Performance failure
Workflows suspended	-	-	-	Critical	Performance failure
Workflows suspended per second	-	-	-	Critical	Performance failure
Workflows Terminated	-	-	-	Critical	Performance failure
Workflows Terminated per second	-	-	-	Critical	Performance failure
Workflows Unloaded	-	-	-	Critical	Performance failure
Workflows Unloaded per second	-	-	-	Critical	Performance failure
HiPerf Classes	-	-	-	Critical	Performance failure
HiPerf Validity	-	-	-	Critical	Performance failure
Processes					
Caption	-	-	-	Critical	Process failed
Command line	-	-	-	Critical	Process failed
Creation Class Name	-	-	-	Critical	Process failed
CS Creation Class Name	-	-	-	Critical	Process failed
CS Name	-	-	-	Critical	Process failed
Description	-	-	-	Critical	Process failed
Executable Path	-	-	-	Critical	Process failed
Execution State	-	-	-	Critical	Process failed
Handle Count	-	-	-	Critical	Process failed
Kernel Mode Time	-	-	-	Critical	Process failed

Alert Metric	Warning Threshold	Warning Severity	Error Threshold	Error Severity	Description
Maximum Working Set Size	-	-	-	Critical	Process failed
Minimum Working Set Size	-	-	-	Critical	Process failed
Name	-	-	-	Critical	Process failed
OS Creation Class Name	-	-	-	Critical	Process failed
OS Name	-	-	-	Critical	Process failed
Other Operation Count	-	-	-	Critical	Process failed
Other Transfer Count	-	-	-	Critical	Process failed
Page Faults	-	-	-	Critical	Process failed
Page File Usage	-	-	-	Critical	Process failed
Parent Process ID	-	-	-	Critical	Process failed
Peak Page File Usage	-	-	-	Critical	Process failed
Peak Virtual Size	-	-	-	Critical	Process failed
Peak Working Set Size	-	-	-	Critical	Process failed
Priority	-	-	-	Critical	Process failed
Private Page Count	-	-	-	Critical	Process failed
Process ID	-	-	-	Critical	Process failed
Quota Nonpaged Pool Usage	-	-	-	Critical	Process failed
Quota Paged Pool Usage	-	-	-	Critical	Process failed
Quota Peak Nonpaged Pool Usage	-	-	-	Critical	Process failed
Quota Peak Paged Pool Usage	-	-	-	Critical	Process failed
Read Operation Count	-	-	-	Critical	Process failed
Read Transfer Count	-	-	-	Critical	Process failed
Session ID	-	-	-	Critical	Process failed
Status	-	-	Degraded	Critical	Process failed
Thread Count	-	-	-	Critical	Process failed
User Mode Time	-	-	-	Critical	Process failed
Virtual Size	-	-	-	Critical	Process failed
Windows Version	-	-	-	Critical	Process failed
Working Set Size	-	-	-	Critical	Process failed

Alert Metric	Warning Threshold	Warning Severity	Error Threshold	Error Severity	Description
Write Operation Count	-	-	-	Critical	Process failed
Write Transfer Count	-	-	-	Critical	Process failed
Services					
State	-	-	Continue Pending	Critical	Serivce is Continue Pending/Pause Pending/Paused/Running/ Start Pending/Stop Pending/Stopped/Unknown
WMI					
Counter Value	-	-	-	Critical	WMI failure