CA Nimsoft Monitor

Probe Guide for Active Directory Server

ad_server v1.7 series

CA Nimsoft Monitor Copyright Notice

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?
1.7	June 2014	■ Added the **Enhancements**, **Software Requirements**, and **Upgrades and Migrations** topic. ■ Updated all the **<Profile Name> Node** topics. ■ Updated the **Manage Profiles** topic procedure. ■ Removed the **Add Threshold for Counter** and **Delete Threshold for Counter** topics.
1.6	March 2014	■ Added the **Health Monitor Node** topic. ■ Updated the **ad_server QoS Metrics** topic. ■ Updated the **ad_server Alert Metrics Default Settings** topic. ■ Updated the document for language and style consistency.
1.5	January 2014	Documentation on the initial web-based GUI version of this probe. (Previous versions of this probe are configured using Infrastructure Manager).

Chapter 1: Overview

Active Directory is the directory service included with the Windows servers to manage the identities and relationships for managing network environments.

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

The probe uses monitoring profiles, which are classified in the following eight predefined groups:

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

  Note: The probe does not support the WMI of Datatype Reference.
- **Health Monitor:** monitors status and response time for all the objects. For example, monitor the operations master schema, fetch number of lost and found objects, and fetch AD replication partner synchronization status.

Each of these groups can have more than one monitoring profile. The Active Directory Server probe is delivered with a default configuration of a selected set of profiles to be monitored. You can also 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 and provides the following information:

- Overview of the Active Directory Server probe and related documentation for previous probe versions.
- Configuration detail of the probe.
- Field information and common procedures for configuring the probe.

Important! Description for the intuitive GUI fields is not included in the document.

Related Documentation

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.

Enhancements

Active Directory Server probe now supports the following locale:

- Simplified Chinese
- Japanese
- Korean
- Spanish
- Italian
- German
- Portuguese

Software Requirements

The ad_server probe requires the following software environment:

- Nimsoft Monitor Server 5.1.1 or later
- Nimsoft Robot 5.23 or later
- Probe Provisioning Manager (PPM) probe version 2.34 or later (for Web GUI only)
- Java Virtual Machine 1.6 or later (typically installed with NMS 5.0 and above)
- .Net Framework 4.5, if Nimsoft Robot is installed
- .Net Framework 2.0, if Nimsoft Monitor Server is installed

  Note: .Net Framework 4.5 is required if Nimsoft Robot and Nimsoft Monitor Server are installed on the same machine.

Chapter 2: Upgrades and Migrations

While upgrading the probe from a previous version to 1.70 in the non-English locale, take a back-up of your existing **ad_server.cfg** file in UTF-8 encoding. The process ensures that the configuration file is not corrupt and the upgraded probe reads the non-English characters correctly.

Follow these steps:

1. Copy the existing **ad_server.cfg** file to any other location of your system.
2. Open the copied **ad_server.cfg** file and save it to UTF-8 without BOM. If the file is with BOM, the probe throws an error while reading the file.

   BOM is a special text at the beginning of the text file for identifying the file encoding. You can use a text editor, like **Notepad++** on Windows system and **gedit** on Linux system, for defining your file encoding. You can also use the **iconv** command on Linux for changing the character encoding. Alternatively, edit the configuration file on Windows system and copy it back to the Linux system.
3. Upgrade the probe to 1.70 version.
4. Deactivate the probe after upgrade.
5. Replace the new **ad_server.cfg** file with the UTF-8 encoded configuration file.
6. Activate the probe.

   The probe reads the Japanese characters of the **ad_server.cfg** file correctly.

In case, the probe is already upgraded to version 1.70 without taking a back-up of the configuration file, you can delete all such profiles and can recreate them.

Chapter 3: Configuration Details

The Active Directory Server probe is configured to monitor health and performance of the AD server by configuring the threshold parameters for counters. This probe is delivered with a default configuration of 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 13)

ad_server Node

The ad_server node lets you view the probe information and configure log level of the probe.

Navigation: ad_server

Set or modify the following values as required:

ad_server > Probe Information

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

ad_server > General Config

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

- Log Level: specifies the detail level of the log file.

  Default: 0 - Fatal

Event Logs Node

The **Event Logs** node is used to create and configure profiles for monitoring event logs of the host system. Each monitoring profile is displayed under 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 user-configurable and is named as the *profile name* node.

Navigation: ad_server > Event Logs > *profile name*

Set or modify the following values as required:

***profile name* > General**

This section lets you edit the properties which are defined at time of creating a profile.

- Sample Data Every: defines the time interval for executing the profile and collecting data.
- Sample Data Every (Unit): specifies a time interval unit.
- Startup Delay: defines a time delay for collecting data from the AD server after activating the profile.
- Startup Delay (Unit): specifies a unit of time delay.

***profile name* > Event Log**

This section defines the criteria for monitoring the Windows event logs.

- Log: specifies the log file for fetching the events for monitoring.
- Computer: defines the computer name where the event has occurred.
- Source/Publisher: defines the source or the publisher of the event.
- Severity: specifies the event severity.
- User: defines the Windows user account for whom the event is generated.
- Category: defines the event category.
- Event ID: defines the unique identification number of the event.
- Message: defines the event message text. Use the regular expressions for identifying the message string.

  Note: Specify only those fields, which are required for filtering the event logs and keep all other fields blank. Do not use asterisk (*) in any other field because the regex is unsupported for filtering event logs.

***profile name* > Monitors**

This section lets you select the appropriate counters from the list and configure counter thresholds. The probe lets you configure two thresholds for each counter.

Note: Use the **Add Counter** option of the *profile name* node for adding any missing counter to the list.

- Severity 1: specifies the alarm message severity.
- Operator: specifies the threshold operator for comparing the actual and threshold value.
- Value: defines the counter threshold value for generating alarms.

- Message: specifies the alarm message when the threshold value breaches.

Similarly, you can configure the second threshold for the counter in the corresponding **Severity 2**, **Operator**, **Value**, and **Message** fields.

File Node

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

<Profile Name> Node

This node lets you define the files, which the profile monitors.

Navigation: ad_server > Files > *profile name*

Set or modify the following values as required:

***profile name* > File**

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

Note: The fields of the **General** and the **Monitors** sections are same as described in the *profile name* node under the **Event Logs** node.

File System Node

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

<Profile Name> Node

The *profile name* node lets you configure the file system, which the profile monitors.

Navigation: ad_server > File System > *profile name*

Set or modify the following values as required:

***profile name* > File System**

This section lets you define the directory path for monitoring.

- Directory: defines the directory path or file system for monitoring.
- Pattern: defines the pattern (for example, the name of a file) to search within the file system.

- Include Subdirectories: lets you search and include sub directories of the file system.

Note: The fields of the **General** and the **Monitors** sections are same as described in the *profile name* node under the **Event Logs** node.

Performance Counter Node

The **Performance Counter** node lets you fetch performance data from the performance counters. The performance 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 Counter > *profile name*

Set or modify the following values as required:

***profile name* > Performance Counter**

This section lets you define performance object and instance for monitoring.

- Object: specifies the performance object of the host for monitoring.
- Instance: specifies the performance object instance for fetching data.

Note: The fields of the **General** and the **Monitors** sections are same as described in the *profile name* node under the **Event Logs** node.

Process Node

The **Process** node lets you monitor the running processes of the host system (for example, **notepad.exe**).

<Profile Name> Node

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

Navigation: ad_server > Process > *profile name*

Set or modify the following values as required:

***profile name* > Process**

This section lets you specify the process for monitoring.

Note: The fields of the **General** and the **Monitors** sections are same as described in the *profile name* node under the **Event Logs** node.

Service Node

The **Service** node lets you monitor running services of the host system (for example, **Dnscache**).

<Profile Name> Node

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

Navigation: ad_server > Service > *profile name*

Set or modify the following values as required:

***profile name* > Service**

This section lets you specify the service for monitoring.

Note: The fields of the **General** and the **Counter: Counter Name** sections are same as described in the *profile name* node under 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 data is used for consolidating the management of devices and applications in a network from the Windows environment.

<Profile Name> Node

The *profile name* node lets you 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 as required:

***profile name* > WMI**

This section lets you specify the process that the profile is monitoring.

- Namespace: specifies the WMI namespace 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 instance is found. For example, **notepad.exe**.

Note: The fields of the **General** and the **Monitors** sections are same as described in the *profile name* node under the **Event Logs** node.

Health Monitor Node

The **Health Monitor** node lets you configure counters for monitoring the AD Server health. These counters help you understand that current activities of the AD Server are within normal and healthy parameters. The **Health Monitor** node contains the following counters:

- Response Time: calculates the connection (bind) time for getting a response from the object. For example, use this counter for fetching the last bind time of the following objects:
  - Operations Master Infrastructure
  - Operations Master Domain naming
  - Operations Master Primary Domain Controller (PDC)
  - Operations Master Relative Identifier (RID)
  - Operations Master Schema

  Important! The Response Time counter is not applicable for replication profiles and returns a NULL value.
- Object Found: calculates the number of objects in the target root folder of the server. For example, use this counter for fetching the AD lost objects and number of domain controller replication partners.

- Status: monitors the object availability. For example, use this counter for fetching status of the lost and found object container and AD replication partners' synchronization status.

  Note: The probe contains a default set of health monitoring profiles for demonstrating counters usage. All monitoring profiles are deactivated, by default; you can activate them manually.

<Profile Name> Node

The *profile name* node lets you configure the health monitoring profile properties.

Navigation: ad_server > Health Monitor > *profile name*

Set or modify the following values as required:

***profile name* > Health Monitor**

This section lets you configure the search root criteria for identifying a monitoring object of the AD server.

- Search Root Criteria: specifies the search root criteria to fetch **Response Time**, **Objects Found**, and **status** counters value. Mention **replication** for a replication profile and for the PDC profile leave it blank. Enter search criteria for a normal profile in the **DC=demodomain,DC=local** format.

Note: The fields of the **General** and the **Monitors** sections are same as described in the *profile name* node under 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. Navigate to the section within a node that you want to configure.
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.

How to Configure Alarm Thresholds

Some Quality of Service measurement probes allow you to set different types of alarm thresholds. These threshold options allow you to more broadly control when alarm messages are sent for each QoS probe.

For more information about the different alarm thresholds and their configuration requirements, refer to the *General Probe Configuration* section of the Admin Console Help.

Important! Alarm threshold settings are dependent on the baseline_engine probe. If you do not have the correct version of baseline_engine configured, you will not see the additional threshold options.

Manage Profiles

The navigation pane of the probe GUI consists of several predefined group nodes. These group nodes are Event Logs, Files, File System, Performance Counter, Process, Service, WMI, and Health Monitor where you can define monitoring profiles. Create a monitoring profile for each group node for start monitoring.

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 displayed under the selected node with all applicable counters.
4. Configure appropriate counters by defining thresholds and alarm message.
5. Click **Save**.

   The profile is added under the appropriate group node and all configured monitors list is displayed in the **Monitors** section of the *profile name* node.

Delete Profile

You can delete a monitoring profile 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.
3. Click **Save**.

   The profile is deleted.

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 more than one counter to the profile.

Important! The probe does not support those counters, which returns a **datetime** value. The probe GUI shows unexpected results when any such counter is added to the probe.

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 list and click **Submit**.

   The new counter is added in the list of **Monitors** section of the *profile name* node.

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 group is selected.

Chapter 4: 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 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	-	When was the file changed?
QOS_CREATED	-	When was the file created?
Filesystems		
QOS_DIRECTORIES	-	Total number of directories.
QOS_FILEAGENEWEST	-	Age of the newest file.
QOS_FILEAGEOLDEST	-	Age of the oldest file.
QOS_FILES	-	Number of files.
QOS_TOTALSIZE	-	Total size of all files.
Performance Counters		
QOS_SQLCLIENT:_CURRENT_#_CONNECTION_POOLS	-	Sql Client: Current number of connection pools.
QOS_SQLCLIENT:_CURRENT_#_POOLED_AND_NONPOOLED_CONNECTIONS	-	Sql Client: Current number of pooled and non-pooled connections.

Monitor Name	Units	Description
QOS_SQLCLIENT:_CURRENT_#_POOLED_CONNECTIONS	-	Sql Client: Current number of pooled connections.
QOS_SQLCLIENT:_PEAK_#_POOLED_CONNECTIONS	-	Sql Client: Peak number of pooled connections.
QOS_SQLCLIENT:_TOTAL_#_FAILED_COMMANDS	-	Sql Client: Total number of failed commands.
QOS_SQLCLIENT:_TOTAL_#_FAILED_CONNECTS	-	Sql Client: Total number 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	-	Workflows 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.

Monitor Name	Units	Description
QOS_KERNELMODETIME	100ns	Kernel mode time.
QOS_MAXIMUMWORKINGSETSIZE	Kilobytes	Maximum working set size.
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	Peak virtual size.
QOS_PEAKWORKINGSETSIZE	Kilobytes	Peak working set size.
QOS_PRIORITY	-	Process priority.
QOS_PRIVATEPAGECOUNT	-	Private page count.
QOS_PROCESSID	-	Process Id.
QOS_QUOTANONPAGEDPOOLUSAGE	-	Quota non-paged pool usage.
QOS_QUOTAPAGEDPOOLUSAGE	-	Quota paged pool usage.
QOS_QUOTAPEAKNONPAGEDPOOLUSAGE	-	Quota peak non-paged 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.
Health Monitor		

Monitor Name	Units	Description
QOS_RESPONSETIME	milliseconds	Total time for connecting to object.
QOS_OBJECTFOUND	count (number)	Number of objects found after connection.
QOS_STATUS	count (number)	Status of connection (4 indicates failure and 0 indicates success).

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

Alert Metric	Warning Threshold	Warning Severity	Error Threshold	Error Severity	Description
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
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

Alert Metric	Warning Threshold	Warning Severity	Error Threshold	Error Severity	Description
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
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

Alert Metric	Warning Threshold	Warning Severity	Error Threshold	Error Severity	Description
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
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

Alert Metric	Warning Threshold	Warning Severity	Error Threshold	Error Severity	Description
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
Write Operation Count	-	-	-	Critical	Process failed
Write Transfer Count	-	-	-	Critical	Process failed
Services					
State	-	-	Continue Pending	Critical	Service is Continue Pending/Pause Pending/Paused/Running/ Start Pending/Stop Pending/Stopped/Unknown
WMI					
Counter Value	-	-	-	Critical	WMI failure
Health Monitor					
ResponseTime	15000	Major	30000	Critical	Total time to connect
ObjectFound	10	Warning	100	Major	Total number of object found (thresholds are mentioned only for "Lost and Found" profiles)
status	4	Warning	-	-	Connection status