

SOLARWINDS TECHNICAL REFERENCE

APM Active Directory Template Pack

This document describes the template included in the APM Active Directory Template Pack.

Copyright© 1995-2011 SolarWinds. All rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds. All right, title and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its licensors. SolarWinds Orion™, SolarWinds Cirrus™, and SolarWinds Toolset™ are trademarks of SolarWinds and SolarWinds.net® and the SolarWinds logo are registered trademarks of SolarWinds All other trademarks contained in this document and in the Software are the property of their respective owners.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Microsoft® and Windows 2000® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Graph Layout Toolkit and Graph Editor Toolkit © 1992 - 2001 Tom Sawyer Software, Oakland, California. All Rights Reserved.

Portions Copyright © ComponentOne, LLC 1991-2002. All Rights Reserved.

Document Revised: 03/24/2011

Active Directory 2003-2008 Services and Counters

This template assesses the overall health of Active Directory 2003-2008 services and counters on a domain controller. It is recommended to use this template in conjunction with the Windows Server 2003-2008 Services and Counters template.

Prerequisites: RPC and WMI access to the domain controller.

Credentials: Windows Administrator on the domain controller.

Monitored Components

Note: Components without predetermined threshold values have guidance such as "use the lowest threshold possible" or "use the highest threshold possible" to help you find a threshold appropriate for your application. For more information, see <http://knowledgebase.solarwinds.com/kb/questions/2415>.

Service: Distributed File System

Enables you to group shared folders located on different servers into one or more logically structured namespaces. Each namespace appears to users as a single shared folder with a series of subfolders.

Service: DNS Server

Enables DNS clients to resolve DNS names by answering DNS queries and dynamic DNS update requests. If this service is stopped, DNS updates will not occur. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: File Replication

Synchronizes folders with file servers that use File Replication Service (FRS) instead of the newer DFS Replication technology.

Service: Intersite Messaging

Enables messages to be exchanged between computers running Windows Server sites. If this service is stopped, messages will not be exchanged, nor will site routing information be calculated for other services. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: Kerberos Key Distribution Center

On domain controllers, this service enables users to log on to the network using the Kerberos authentication protocol. If this service is stopped on a domain controller, users will be unable to log on to the network. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: Windows Time

Maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: DNS Client

The DNS Client service (dnscache) caches Domain Name System (DNS) names and registers the full computer name for this computer. If the service is stopped, DNS names will continue to be resolved. However, the results of DNS name queries will not be cached and the computer's name will not be registered. If the service is disabled, any services that explicitly depend on it will fail to start.

Service: Security Accounts Manager

The startup of this service signals other services that the Security Accounts Manager (SAM) is ready to accept requests. Disabling this service will prevent other services in the system from being notified when the SAM is ready, which may in turn cause those services to fail to start correctly. This service should not be disabled.

Service: Server

Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these functions will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: Workstation

Creates and maintains client network connections to remote servers using the SMB protocol. If this service is stopped, these connections will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: Remote Procedure Call (RPC)

The RPCSS service is the Service Control Manager for COM and DCOM servers. It performs object activation requests, object exporter resolutions, and distributed garbage collection for COM and DCOM servers. If this service is stopped or disabled, programs using COM or DCOM will not function properly. It is strongly recommended that you have the RPCSS service running.

Service: Net Logon

Maintains a secure channel between this computer and the domain controller for authenticating users and services. If this service is stopped, the computer may not authenticate users and services, and the domain controller cannot register DNS records. If this service is disabled, any services that explicitly depend on it will fail to start.

LDAP Active Threads

The current number of threads in use by the LDAP subsystem of the local directory service.

Note: You can provide a value for the warning and critical thresholds based on your current environment and your requirements.

LDAP Bind Time

The time (in milliseconds) required for the completion of the last successful LDAP binding.

This counter should be as low as possible. If it is not, it usually indicates that hardware or network-related problems are occurring.

LDAP Client Sessions

The number of currently connected LDAP client sessions.

This counter should show activity over time. If it does not, it usually indicates that network-related problems are occurring.

Note: You can provide a value for the warning and critical thresholds based on your current environment and your requirements.

Directory Service Threads in Use

The current number of threads in use by the directory service.

This counter should show activity over time. If it does not, it usually indicates that network problems are hindering client requests.

Note: You can provide a value for the warning and critical thresholds based on your current environment and your requirements.

Address Book Client Sessions

The number of connected Address Book client sessions.

Directory Service Notify Queue Size

The number of pending update notifications that have been queued, but not yet transmitted to clients.

Note: This counter should be as low as possible.

DRA Inbound Full Sync Objects Remaining

The number of objects remaining until the full synchronization is completed (while replication is done).

Note: This counter should be as low as possible.

DRA Inbound Values (DNs only)/sec

The number of object property values received from inbound replication partners that are distinguished names (DNs) that reference other objects. DN values, such as group or distribution list memberships, are generally more expensive to apply than other types of values.

DRA Outbound Values (DNs only)/sec

The number of object property values containing DN's sent to outbound replication partners. DN values, such as group or distribution list memberships, are generally more expensive to read than other kinds of values.

LDAP Successful Binds/sec

The number of LDAP bindings (per second) that occurred successfully.

This counter should show activity over time. If it does not, it usually indicates that network-related problems are occurring.

LDAP Searches/sec

The number of search operations per second performed by LDAP clients.

This counter should show activity over time. If it does not, it usually indicates that network problems are hindering client requests.

DS Directory Reads/sec

The number of directory reads per second.

DS Directory Writes/sec

The number of directory writes per second.

DRA Pending Replication Synchronizations

The number of directory synchronizations that are queued for this server but not yet processed.

Replication: Change Orders Received

The number of change orders received. In an idle state this counter should be zero.

Replication: Change Orders Sent

The number of change orders sent. In an idle state this counter should be zero.

Replication: Usn Records Accepted

The number of USN records accepted. Replication is triggered by entries to the NTFS USN journal. A high value on this counter, such as one every five seconds, indicates heavy replication traffic and may result in replication latency.

System: Context Switches/sec

Used to determine whether or not the processor must handle too many applications.

Interpret the data cautiously. A thread that is heavily using the processor lowers the rate of context switches, because it does not allow much processor time for other processes' threads. A high rate of context switching means that the processor is being shared repeatedly—for example, by many threads of equal priority. It is a good practice to minimize the context switching rate by reducing the number of active threads on the system. The use of thread pooling, I/O completion ports, and asynchronous I/O can reduce the number of active threads. Consult your in-house developers or application vendors to determine if the applications you are running provide tuning features that include limiting the number of threads.

A context switching rate of 300 per second per processor is a moderate amount; a rate of 1000 per second or more is high. Values at this high level may be a problem.

Note: You can provide a value for the warning and critical thresholds based on your current environment and your requirements.

System: Processor Queue Length

Indicates whether or not the system is able to handle processing requests.

This counter is a rough indicator of the number of threads each processor is servicing. The processor queue length, sometimes called processor queue depth, reported by this counter is an instantaneous value that is representative only of a current snapshot of the processor, so it is necessary to observe this counter over a long period of time. Also this counter is reporting a total queue length for all processors, not a length per processor. For additional information on how to monitor this counter, refer to the following article: <http://technet.microsoft.com/en-us/library/cc938643.aspx>.