Monitoring Active Directory Environment

Share:

solarwinds
Unexpected Simplicity™

Effectively Manage Users Accounts in Active Directory

Any large enterprise which uses a Windows® environment uses Microsoft® Active Directory®. With just a single sign-on, users can access their computers, group accounts, email, VPN, shared drives, printers, servers, etc. System administrators will find Active Directory to be a great application for managing user accounts and login access management.

Take the case of login access management, when users get locked out of their accounts, SysAdmins are expected to reset the user password and unlock the account immediately. This happens very often in organizations. SysAdmins are then expected to oblige – no matter what time of day it is – this task and attended to it immediately. Even though it's only a simple task of unlocking a user account, this issue can unfortunately take up some of the SysAdmin's time. In addition to user account lockouts, there can be other issues related to performance of AD servers.

Comprehensive monitoring of the Active Directory environment is critical because it helps you detect problems before they're reported by your users, and before they impact productivity.

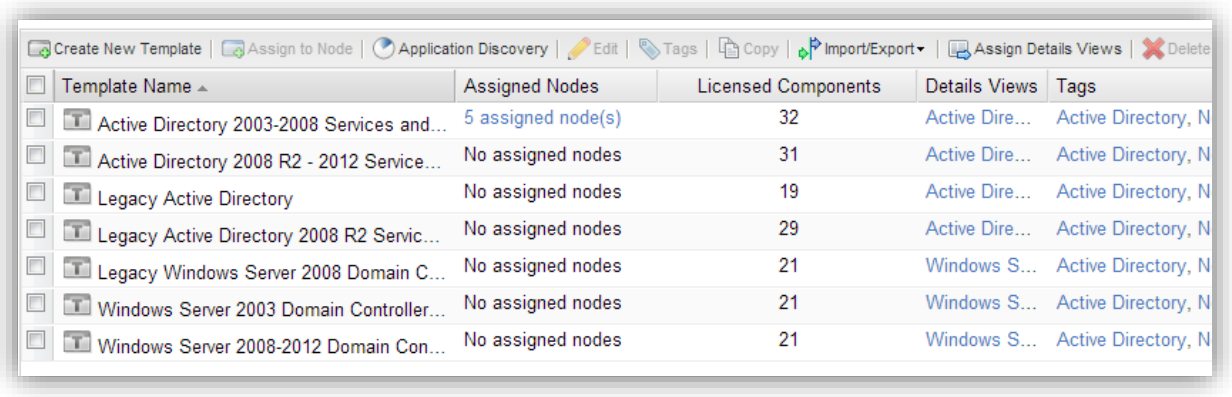
Importance of Monitoring Active Directory

Active Directory monitoring will ensure user accounts, application availability, and optimum performance levels are maintained. Active Directory monitoring tools will help you track whenever issues arise within your directory services. In order to effectively and efficiently go about monitoring your Active Directory applications, you should consider monitoring a few key performance metrics:

- **Directory Services:** Monitoring directory services are critical to ensure addresses, email, and phone contacts are always in sync.
- **Service Outages:** All new alerts in each domain controller have to be monitored on an on-going basis to avoid any type of service outage. This could be within DNS servers and clients, servers and workstations, distributed file systems, Intersite messaging, etc.
- **Mission Critical Processes:** Monitor critical processes to check whether the system/server is able to handle all processing requests.
- **Reporting:** Generate reports to gain visibility into critical processes in order to consistently monitor the frequent services and alerts that occur over a period of time. Reporting may also include authentication for failed log-ins, number of logged in users for a given period, etc.
- **Domain Controllers:** Monitoring domain controllers will let you know whether the CPU usage has reached its threshold, whether a user account is locked out, or identify the cause of a log-on issue. Set thresholds and monitor the drive that contains NTDS files; monitoring this prevents the drive from running out of disk space and prevents the domain controller from not functioning.
- **Lightweight Directory Access Protocol (LDAP) Client Sessions:** Monitoring NTDS object counter will indicate the number of clients connected to an LDAP session. It also provides statistics on other performances, such as speed and response times of particular sessions.
- **Replication:** Monitoring replication shows if there's a failure on a replication link or if there's an issue with the network leading to slow replication rates between websites.

Agentless Performance Monitoring

Your application monitoring tool should deliver agentless monitoring for performance and availability for Active Directory. Application monitoring tools today use templates for monitoring Active Directory environments. Templates give you the flexibility to monitor the current status of directory services. With the template-based approach, you can set baseline thresholds to each performance metric to indicate if the metric has reached a warning or a critical state.



Template Name	Assigned Nodes	Licensed Components	Details Views	Tags
Active Directory 2003-2008 Services and...	5 assigned node(s)	32	Active Dire...	Active Directory, N
Active Directory 2008 R2 - 2012 Service...	No assigned nodes	31	Active Dire...	Active Directory, N
Legacy Active Directory	No assigned nodes	19	Active Dire...	Active Directory, N
Legacy Active Directory 2008 R2 Servic...	No assigned nodes	29	Active Dire...	Active Directory, N
Legacy Windows Server 2008 Domain C...	No assigned nodes	21	Windows S...	Active Directory, N
Windows Server 2003 Domain Controller...	No assigned nodes	21	Windows S...	Active Directory, N
Windows Server 2008-2012 Domain Con...	No assigned nodes	21	Windows S...	Active Directory, N

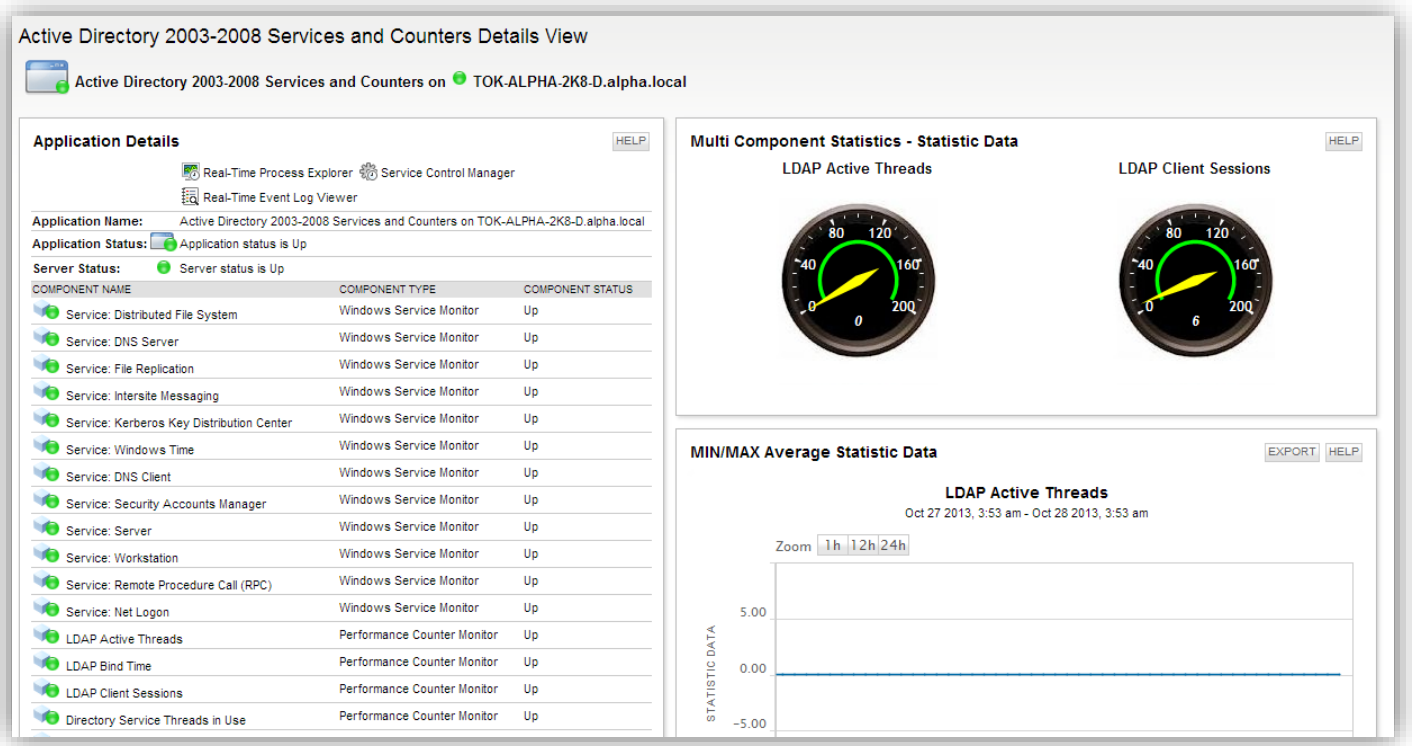
SolarWinds Server & Application Monitor (SAM) offers agentless monitoring using expert templates

Out-of-the-box Dashboards

Maintaining consistent Active Directory performance is a big task. In order to address this task, you need accurate performance data. Your application monitoring tool should offer you not just performance statistics, but provide meaningful insights into why those numbers are affecting your Active Directory performance. Having out-of-the-box dashboards in your application monitoring tool will give you the status and performance of Active Directory servers.

If you can't access a shared drive or a group account, then you most likely will end up looking at user rights and settings that are related to fixing the issue. An application monitoring tool will precisely lead you to your Active Directory settings, where the issue can be modified and fixed.

In addition, the dashboard should give you vital statistics using a range of graphs, charts, and gauges. All with the ability to drill down into historical data.



SAM's interactive dashboard offers critical information about key performance metrics

Monitor Key Performance Metrics for Optimal Active Directory Health

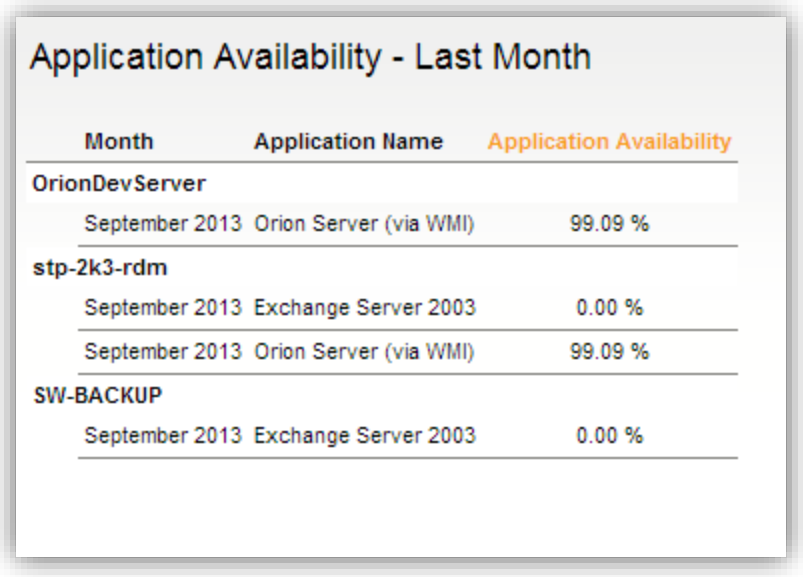
In addition to the key metrics mentioned above, you should also leverage a range of out-of-the-box monitors to manage various components of the Active Directory server. A list of performance metrics you should monitor are:

- Distributed File System Service
- DNS Server Service
- Filer Replication Service
- Intersite Messaging Service
- Kerberos Key Distribution Service
- Windows Time Service
- DNS Client Service
- Security Accounts Manager Service
- Server Service
- Workstation Service
- Remote Procedure Call (RPC) Service
- Net Logon Service
- LDAP Version Script
- LDAP Active Threads
- LDAP Bind Time
- LDAP Client Sessions
- Directory Service Threads in Use
- Address Book Client Sessions
- Directory Service Notify Queue Size

Advanced Reporting Capabilities

Having a built-in reporting engine which is easy to use, customizable, and provides the ability to share historical performance data on Active Directory performance and availability is an added advantage to a SysAdmin. You should also be able to create reports based on specific user groups, business units, and departments. An automated reporting system allows you to fix reporting schedules. Additionally, a pre-set list of reports can be utilized for generating a variety of reports about Active Directory performance. A few examples of pre-set reports are:

- Active Directory availability and performance
- Status of critical performance metrics
- Historical CPU and memory usage
- Hardware health and performance
- Weekly reports on user access management – failed logins, access denied to shared folders, etc.



Application Availability - Last Month

Month	Application Name	Application Availability
OrionDevServer		
September 2013	Orion Server (via WMI)	99.09 %
stp-2k3-rdm		
September 2013	Exchange Server 2003	0.00 %
September 2013	Orion Server (via WMI)	99.09 %
SW-BACKUP		
September 2013	Exchange Server 2003	0.00 %

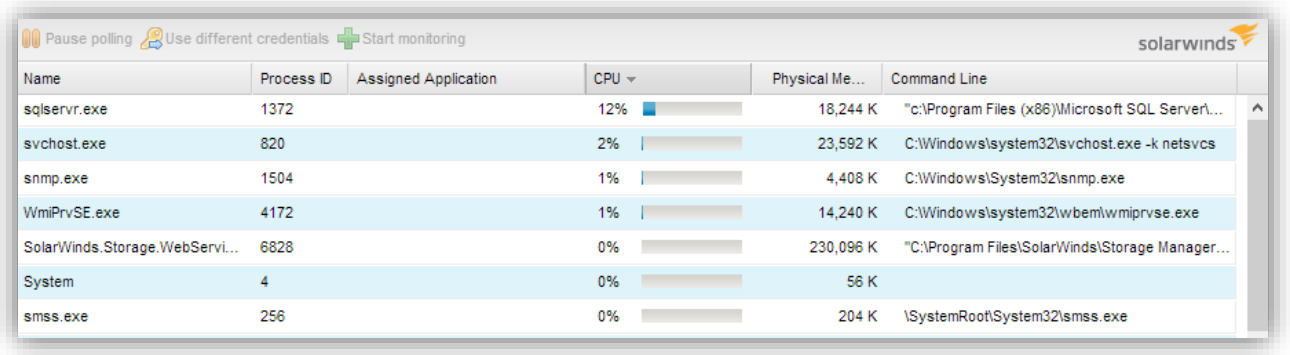
SolarWinds SAM report writer is a customizable reporting engine with pre-set reports which can be accessed anytime

Real-Time Process Explorer

When you have an Active Directory application running on multiple servers and in various locations, it helps to remotely monitor processes which are affecting the performance of the application. For example, if you have a real-time process explorer, you can remotely log in to a particular machine and check the machine's vital statistics. You can start and stop processes remotely without being physically present. Real-time process explorer allows you to monitor processes by:

- CPU utilization

- Virtual/Physical memory utilization
- Disk I/O performance



SolarWinds SAM provides real-time insights into your server and application performance

SolarWinds Server & Application Monitor

SolarWinds Server & Application Monitor (SAM) is an agentless server and application management software. SAM automatically discovers applications running in your servers, helps you monitor over 150 applications, alerts you in case there's an issue with an application, and generates hundreds of reports.

SAM helps you keep a close eye on directories and services in your Active Directory. SAM continuously and proactively alerts you to warnings or malfunctions inside Active Directory, its servers, services, and applications.

Some important features of SAM include:

- Identify and monitor critical application issues related to high CPU utilization, memory usage and availability
- Out-of-the-box dashboards for at-a-glance insights into Active Directory health and performance
- Application reporting engine offers built-in and customizable reports
- Monitor a range of performance counters that will keep your Active Directory servers healthy
- Leverage custom monitors for managing Active Directory servers
- Analyze Active Directory health to prevent downtime in the future
- Monitor a range of Microsoft applications like SQL server, IIS, Exchange, etc.

5 Reasons to Download Server & Application Monitor

1. Automatic discovery in SAM automatically scans and discovers your server infrastructure and applications that are running.
2. Leverage hundreds of out-of-the-box templates in SAM and thwack®. Apply these templates and start monitoring in less than an hour.
3. Monitors Windows, Linux®, AIX®, Solaris®, HP-UX®, and a range of other commercial applications.
4. Monitor hardware health and keep your server infrastructure healthy at all times.
5. Manage your IT assets using the automatic Asset Inventory Management capabilities that come with SAM.

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide - from Fortune 500 enterprises to small businesses. The company works to put its users first and remove the obstacles that have become “status quo” in traditional enterprise software. SolarWinds products are downloadable, easy to use and maintain, and provide the power, scale, and flexibility needed to address users’ management priorities. SolarWinds online user community, http://thwack.com, is a gathering place where tens of thousands of IT pros solve problems, share technology, and participate in product development for all of the company’s products. Learn more today at http://www.solarwinds.com.

Fully Functional for 30 Days

For additional information, please contact SolarWinds at 866.530.8100 or e-mail sales@solarwinds.com.

To locate an international reseller near you, visit http://www.solarwinds.com/partners/reseller_locator.aspx