Keeping Active Directory Healthy and Fine-Tuned

Written by Chris Ashley, product manager, Quest

INTRODUCTION

Active Directory (AD) is the heart of every Windows-based infrastructure, responsible for coordinating both network administration and security management. Many applications and services your organization depends on every day, from Exchange to SharePoint to Oracle and SQL Server, rely on AD in one way or another. Many organizations have even extended the power of AD to control authentication and access to non-Windows systems such as Linux, UNIX, Mac OS X and third-party applications (on-premises and cloud).

Maintaining the health of your AD, therefore, is essential to powering your business, protecting your intellectual property, keeping employees productive and much more. After all, a healthy AD is critical for ensuring that users can authenticate properly and promptly, and that they can access the resources they need to do their jobs — and only those resources.

But what's the best way to go about keeping your AD healthy? In this white paper, I'll detail the critical components and services to monitor, explore the strengths and limitations of native tools, and explain why third-party solutions can be a sound investment.

CRITICAL COMPONENTS AND SERVICES TO MONITOR

Active Directory is nothing if not complex. Here are the critical components and services you'll want to monitor to keep it healthy.

Replication

AD is a distributed directory service — objects in the directory are distributed across the domain controllers (DCs) in a forest. Changes made on one DC are replicated to all other DCs that store copies of the same information, keeping the DCs in sync and ensuring data integrity.

Therefore, replication failures, and even replication slowdowns, can lead to a wide range of issues. For example, if an update to a Group Policy Object (GPO) is not promptly replicated out to all DCs, users might be able to read or modify documents they should no longer be able to access, putting security and compliance at risk. Similarly, until the deletion of a user profile is replicated to all DCs, a terminated employee might retain access to sensitive systems and data. If a password change is not replicated, the user might not be able to log on, hurting productivity and increasing help desk costs.

Domain Name System (DNS)

DNS is the name resolution protocol for TCP/IP networks. It is an essential part of the internet, enabling us to use memorable, alphanumeric URLs instead of cryptic IP addresses, and enabling providers to change the IP address associated with a URL without affecting end users.

DNS is also a critical component of Active Directory. Network hosts and services are configured with DNS names so that they can be located in the network, and they are also configured with DNS servers that resolve the names of AD domain controllers.

> Maintaining the health of your AD is essential to powering your business, protecting your intellectual property, keeping employees productive and much more.

There are many ways DNS can fail, and any of them can cause serious problems for the organization. Users and processes may be unable to access the servers, file shares, printers and other resources they need. Moreover, DNS problems can cause AD replication failures, leading to any of the issues I just discussed.

Therefore, it's critical to ensure that DNS servers are properly provisioned, especially with RAM, and to monitor DNS server authentication, basic connectivity, configuration of forwarders, delegation, dynamic registration and resource record registration.

Group Policy

Group Policy is a powerful tool that provides centralized management of DCs, member servers and desktops — but it can be complex to design and implement. Monitoring its health is critical to security, performance, productivity and more. Configuration errors or other dependency failures can prevent settings or features from functioning as expected. You need to ensure that all Group Policies are correctly synced across all DCs, and keep an eye out for unlinked, disabled and orphaned Group Policies.

Site topology

Your site topology significantly affects the performance of your network and the ability of users to access network resources. For example, DNS servers must be placed appropriately on your network for traffic load, replication and fault tolerance. (Usually, DNS servers are installed on all DCs.) In addition, primary and secondary DNS servers need to be correctly set to resolve to each other.

More broadly, you need to ensure that sites are contacting the nearest DC in order to prevent issues such as slow logon times and slow access to email. You also need to keep tabs on your site link schedule, preferred bridgehead configuration, and IP subnet definition and mapping to sites. For instance, you need to make sure you do not have any unmapped subnets.

Domain controllers

Domain controllers are arguably a part of site topology, but they merit their own discussion. Clearly, you need to know how many DCs you have, including both physical and virtualized. You also need to be aware of the location of each DC and its physical security, and you need to ensure that time is properly synchronized across all DCs. If you are using a global catalog, you need to monitor the configuration of the DCs designated as global catalog servers and the replication of the catalog between them.

NATIVE TOOLS

Command-line tools

Microsoft provides a number of command-line tools to help administrators troubleshoot problems with AD. Here are some of the most useful:

- **repadmin/replsummary** — Provides a summary of the replication status from each DC in a forest
- **repadmin/queue** — Displays inbound replication requests that the DC has to issue to become consistent with its source replication partners
- **repadmin/showoutcalls** — Displays calls that have been made by the specified directory server to other directory servers that have not yet been answered

- **repadmin/bridgeheads** — Lists the directory servers acting as bridgehead servers for a specified site
- **dsquery server** — Lists all the domain controllers in AD
- **dcdiag** — Analyzes the state of DCs in a forest or enterprise and reports problems
- **GPOtool.exe** — Provides information about GPO replication
- **w32tm.exe** — Is used to configure Windows time service settings and diagnose problems with the time service

This list provides just the tip of the iceberg. Most of these commands have multiple parameters to learn, and they can change with each new release of Windows Server.

Scripting

Each of the tools listed above — and the many other parameters not listed — can be useful for troubleshooting problems, but running them manually to keep tabs on the health of AD simply isn't practical. Some admins attempt to work around this problem by combining the commands they need into scripts, which they can run either as needed or on schedule.

However, creating effective scripts requires specialized skills and significant time. For example, one AD health check script offered on Microsoft TechNet includes more than 250 lines of code — code that not only has to be tailored to your environment, but maintained over time through changes in your environment as well as software updates.

In addition, the output from command-line tools, whether run manually or scripted, is cryptic and incomplete. To really understand a problem, you need the history and context. Was the issue a one-time aberration or is it a recurring problem? Is it getting worse? If so, how fast? What else was happening at the time? With native tools, you still have to dig through event logs from individual DCs and try to piece together this information. And you'll get no suggestions for how to find the root cause or remediate the problem.

Other native tools

Microsoft also offers a few tools that offer a graphical user interface and more functionality than the command-line tools:

- **Active Directory Domain Services Management Pack for System Center Operations Manager (SCOM)** — Enhances the SCOM Operator Console with additional views, tasks and reports related to AD.
- **Active Directory Replication Status Tool (ADREPLSTATUS)** — Checks the replication status of an entire forest, a single domain in the forest or a specific set of DCs in a domain, and highlights DCs experiencing replication problems. You can review each unique replication error and even get the recommended troubleshooting content from Microsoft. However, this read-only utility cannot make changes to AD objects or AD configuration.
- **Group Policy Management Console** — Provides information about Group Policy for Windows Server 2012 and later.

While these tools are far easier to use than command-line tools, they still share some of the same limitations. In particular, they are point solutions that provide insight into a particular aspect of AD health at a given time, rather than providing ongoing monitoring across the environment with historical context.

Services

For premier customers, Microsoft also offers RAP (Risk Assessment Program) as a Service. You run the assessment on your Active Directory and upload the data through the cloud. Microsoft will assess the data and provide an online report of any issues it finds. Then, a Microsoft-accredited engineer will review the report and offer recommendations for remediation.

Although this service will likely uncover important issues in your environment, it provides only a one-time snapshot and analysis, rather than ongoing monitoring of AD health.

> Command-line tools can be useful for troubleshooting problems, but running them manually to keep tabs on the health of Active Directory simply isn't practical.

Third-party solutions can monitor your Active Directory continuously, providing you with real-time insight into its overall health and the health of its various components.

HOW THIRD-PARTY TOOLS HELP IT AND THE BUSINESS

Fortunately, there are third-party solutions that overcome the limitations of the native options. Given the importance of keeping Active Directory healthy, that can make them an extremely wise investment. In particular, third-party tools can:

- **Provide AD health monitoring, not just AD health checks** — Third-party solutions can monitor your Active Directory continuously, providing you with real-time insight into its overall health and the health of its various components.
- **Reduce workload through automation** — Third-party tools eliminate the need to manually formulate and issue commands or build and maintain complex scripts.
- **Empower junior admins** — Intuitive interfaces eliminate the need to learn arcane commands and dig through cryptic logs.
- **Alert you to emerging problems** — Third-party tools can help you discover and address problems before they affect users by highlighting issues in the dashboard display or issuing text or email alerts. Some tools provide an indicator of the severity of an issue and the flexibility to set your own thresholds.
- **Provide a holistic view** — Instead of having to compare logs from multiple servers and try to reconstruct a string of events, you can easily see the context you need to understand a problem across time and across the environment.
- **Speed troubleshooting and remediation** — Third-party tools can automate troubleshooting steps and provide expert advice to help you quickly resolve problems.
- **Reduce maintenance work and reliability issues** — Third-party tools are regularly updated and tested as Active Directory technology changes, removing the burden of manually changing and testing scripts.

QUEST® ACTIVE ADMINISTRATOR® FOR ACTIVE DIRECTORY HEALTH

Active Administrator for Active Directory Health is an easy-to-use solution that helps you ensure the health and availability of your AD. Key features include:

- **Live AD topology view** — View the entire AD site and replication infrastructure to see an entire forest at a glance, view issues on DCs and quickly automate AD performance troubleshooting. Issues are divided into severity levels, prioritizing potential versus actual issues.
- **Centralized diagnostic console** — Discover the flow of data from the network through a domain controller using visual flow charts, graphs and icons. In this consolidated view of system status, resource bottlenecks are highlighted in yellow and red, and you can drill down on alerts for further analysis.
- **Simplified AD health analysis** — Proactively monitor and diagnose critical, directory-wide infrastructure issues, from replication latency to DNS inconsistencies. When a problem occurs, an alert notifies you immediately of the exact nature and location of the problem, saving you analysis and troubleshooting time. Following critical alerts, built-in or custom remediation actions run automatically to fix the problem.
- **Streamlined enterprise-wide troubleshooting** — Diagnose directory problems without server-by-server, test-by-test troubleshooting using a comprehensive set of troubleshooting tests and utilities. From domain controller health to DNS and replication, Active Administrator for Active Directory Health isolates and repairs problems and generates detailed reports for current use and historical reference.
- **Automated AD health checks and repairs** — Alleviate the pain of manual AD troubleshooting with more than 100 AD health check tests, including replication failure, queue length, DNS zone and SYSVOL consistency. Run multiple tests against selected DCs, sites, domains or naming contexts.

CONCLUSION

Keeping your Active Directory healthy is critical to your business. Problems in AD can hurt security, performance, availability, productivity and more. Instead of struggling with native tools that give you only a peep into the health of AD at a given moment in time, consider investing in a third-party solution such as Active Administrator for Active Directory Health. You'll be able to keep tabs on AD health, speed problem identification and resolution, and reduce IT workload.

ABOUT ACTIVE ADMINISTRATOR FOR ACTIVE DIRECTORY HEALTH

Active Administrator for Active Directory Health ensures the health and availability of AD with troubleshooting and diagnostics tools that monitor performance to maintain user productivity. With Active Administrator for AD Health, you get real-time diagnostic data from a centralized dashboard, eliminating the learning curve so you can identify the root cause of AD problems before they impact users. To learn more, visit quest.com/products/active-administrator-for-active-directory-health.

ABOUT THE AUTHOR

Chris Ashley is a senior advisor for product management at Quest. Since 2009, he has been responsible for the direction and innovation of Group Policy, Active Directory health and enterprise mobility solutions at Quest. Prior to that, he was a systems consultant for NetPro for more than five years.

Chris holds a degree from Montgomery College. He lives in Maryland and is married with two lovely children. When he's not cooking, hanging with his family or working, Chris co-hosts a regular podcast that covers a variety of consumer technologies, apps and games at smrpodcast.com.

> Active Administrator for Active Directory Health is an easy-to-use solution that helps you ensure the health and availability of your AD.

ABOUT QUEST

Quest helps our customers reduce tedious administration tasks so they can focus on the innovation necessary for their businesses to grow. Quest® solutions are scalable, affordable and simple-to-use, and they deliver unmatched efficiency and productivity. Combined with Quest's invitation to the global community to be a part of its innovation, as well as our firm commitment to ensuring customer satisfaction, Quest will continue to accelerate the delivery of the most comprehensive solutions for Azure cloud management, SaaS, security, workforce mobility and data-driven insight.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at www.quest.com/legal

Trademarks

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (www.quest.com) for regional and international office information.