

CLEAR CHOICE TEST Group policy management tools

NetIQ best at moving Microsoft group policy along

BY MANDY ANDRESS, NETWORK WORLD LAB ALLIANCE

For better or worse, Microsoft's Active Directory frequently serves as a central repository for security policy information for organizations that widely deploy Windows 2000 and 2003 as a core server operating system. Yet, Microsoft's out-of-the-box policy administration tools are limited in scope and do not meet the rigorous security auditing requirements of today's compliance-driven corporate atmosphere.

In this Clear Choice test, we examine sets of tools that greatly expand Active Directory Group Policy administration, providing assistance with access control, reporting, change management and security auditing functionality.

Of the four vendor submissions to this test — GPOVault from Desktop Standard; Group Policy Guardian (GPG) and Group Policy Administrator (GPA) from NetIQ; Group Policy Manager and Intrust for Active Directory from Quest Software; and Active Administrator from ScriptLogic Corporation — NetIQ's package is our Clear Choice winner based on its breadth of features, with specific prowess in auditing and change management.

Quest was our runner-up because it was

easier to use than the NetIQ products, but lacked some of the major components, such as what-if analysis for offline/test policies and snapshot-in-time reports.

Our testing honed in on how well these products assisted with policy administration and tracking security compliance via change management, reporting, auditing and administration functions. Our assessment of change management focused on how well the products maintained a controlled, trusted state for each policy with mechanisms such as version control, approval workflow, change notification and rollback.

We looked for format flexibility in reporting tools beyond what Microsoft offers with its Microsoft Management Console (MMC)

snap-in. For example, we wanted the ability to create comparisons between Group Policy versions, view current policy settings and run Resultant Set of Policies (RSOP) reports, analysis information showing the full implementation of a policy.

A successful audit for this test meant we could see a complete trail of changes. We also wanted the ability to see what policy was in effect at a specific point in time. Administration focused on core functionality to manage Group Policy, including detailed access control, offline or what-if analysis, policy backup/archive and overall ease of use.

Each product contains similar base reporting, change history and change control functionality, but all were implemented differently. Some, such as DesktopStandard, add directly onto Microsoft administration tools, while others, such as NetIQ, provide a completely different administration console. NetIQ watches existing audit logs while Quest watches the Active Directory events directly. NetIQ uses its own internal access-control system, while ScriptLogic relies on native Active Directory permissions. Finally, ScriptLogic makes changes directly to Active Directory, while Desktop Standard implements a proxy. No approach is right or wrong, but each has a different effect on an environment.

NetIQ

NetIQ submitted two products: GPA, which provides group policy and change management functions; and GPG, which relies on native Active Directory auditing to monitor group policy changes and sends alerts on the activity as configured.

We installed GPA and GPG on an Active Directory domain member server running SQL Server and all required prerequisites. The console is an MMC snap-in with all the Windows look and feel that implies. We imported the full Group Policy for our test domain via the command-line tool provided with GPA. We would like to see this functionality be directly available via the product's GUI. Policies are then copied to an offline SQL Server repository, so changes can be tested and approved before moving to production.

GPG comprises several components — database, reporting, server, collector and console. The reporting module analyzes the data in the database and renders the request reports. The server analyzes the changes made to Active Directory and sends them to the database. The collector watches the raw Active Directory events (specifically Microsoft event IDs 560, 565 and 566) and determines whether they should be sent to the server. Finally, the console provides the administration interface. GPG also includes connectors to monitoring products such as Microsoft Operations Manager and NetIQ's Security Manager and AppManager.

GPG provided the best audit trail. GPG can also integrate with GPA to alert on authorized and unauthorized changes to Active Directory to further boost the audit trail.

Version control, handled via GPA, is excellent because it creates specific version numbers for each policy check-in. We were able to easily identify checked-out policies by noticing an icon change. Change notifications are available in GPA, but only by e-mail. GPG adds additional alerting functionality.

GPA uses its own internal security model for setting up and maintaining access control. GPA reports are easy to access, but generated only in HTML. We would like to see PDFs offered. It also was difficult to quickly tell what changes were made in differential reports.

A command-line tool is available to create a report showing the GPA policy in place at any time — a useful feature that should be incorporated into the GUI front end. RSoP reporting is also available.

Back-up policies were very flexible, providing the ability to back up full policies or specific objects. Additionally, a full backup was taken before any new policies were pushed to production should we have needed to facilitate a rollback. We could roll back any

policy through viewing the history GPA provided.

One especially appealing feature of the NetIQ product is the export override service account, which gives a directory administrator the ability to give permissions to modify a production Active Directory to a limited account set. NetIQ also has the unique ability to perform health checks against the Active Directory.

Quest Software

Quest submitted Group Policy Manager and Intrust for Active Directory. Group Policy Manager provides directory administration tools. Intrust for Active Directory — which is based on Quest's log collection and alerting product Intrust for Windows — stores group policy events in a SQL Server database and generates alerts and reports on the entries when queried to do so. Quest's approach does not require Active Directory auditing to be enabled to gather logs, but relies on its own agent sitting on the domain controller that sees the events and sends them to the database.

We installed both products on a domain member server without issue.

Quest could improve the detail of its access control within Group Policy Manager. As many as four groups are assigned to particular roles with varying privileges when it comes to policy management. Other products we tested let us set access control per object down to a specific user.

The version control and check-in/check-out functionality of Group Policy Manager was the best we tested. Version numbers are assigned to each modified policy in increments of .1 until a new version is officially approved and rolled to production, and is registered as a full version number. Checked-out policies are moved to a separate folder, where they sit while changes await approval. Policies can be exported for offline testing, but the test functionality is not built in to the product.

You can tap into the rollback functionality via the compliance wizard program within the Group Policy Manager interface. Running this wizard compares the current GPO against the offline version expected to be in production. If any discrepancies are identified and reported by the wizard, you can choose to roll back to previous versions of the policy listed in the history tab.

The reports served up by Group Policy

Manager in an HTML format could be easier to read, and we found that identifying differential information is not as clear as it could be. With Group Policy Manager, you select comparison reports from a drop-down list; with other products we tested, you highlight two policies with the mouse. While not a significant difference, the latter method is easier to use.

Intrust for Active Directory provides a full audit trail of changes, but you can get a snapshot of data only by reviewing individual policy history. You have to review the history of each group policy to see what is in place at any point in time. You then have to perform differential analysis on each policy to see what has changed from point to point. RSoP reports are available, but testing what-if scenarios are not.

ScriptLogic

Active Administrator, while a strong product overall, lacks workflow for approving policy changes and uses a tabbed console that is more cluttered and not as intuitive as other products we tested.


We installed Active Administrator on a domain member server and installed the necessary agent on the domain controller without issue. We used the built-in Microsoft SQL Server 2000 Desktop Engine database for storing log events.

Active Administrator requires that Active Directory auditing be enabled on the domain controllers and agent software running on those machines then collect and read entries from the security event log. Administrators determine which events trigger alerts that then can be sent by e-mail to designated addresses.

Version control is tracked by date/time stamp and is accessed through the policy history interface. Versions are not assigned easily referenced labels or numbers. Policies can be checked out to the offline repository stored on the local file system for testing, but GPO Vault does not include a workflow process to approve changes before they are submitted to production. Policy changes are made directly in Active Directory with standard access rights limiting who has the ability to make those changes.

Rollback is available and proved to be very detailed, providing support to rollback down to specific objects. Backups can be made at the individual object level and automated to run at set intervals. Both processes were very

NetResults GROUP POLICY MANAGEMENT TOOLS

Product	Group Policy Guardian 2.0, Group Policy Administrator 4.6	Group Policy Manager 2.0, InTrust for Active Directory 8.5	Active Administrator 4.02	GPOVault 2.1
Vendor	NetIQ www.netiq.com	Quest Software www.quest.com	ScriptLogic www.scriptlogic.com	Desktop Standard www.desktopstandard.com
Price	Group Policy Administrator starts at \$900 per 100-user pack; Group Policy Guardian starts at \$1,000 per 100-user pack.	Group Policy Manager is \$8 per user account. InTrust for Active Directory is \$12 per managed user account.	\$12 per seat.	GPOVault Enterprise Edition starts at \$1,400 per managed domain.
				
Pros	Best all-around functionality for group policy management; complete audit trail available in easy-to-understand format.	Excellent change management module; intuitive, easy-to-use.	Detailed rollback functionality.	Excellent report formats.
Cons	Report format could be improved.	Report format could be improved; access control not as detailed as other products.	Does not include workflow management.	Accessibility to audit trail could be greatly improved.
Score	4.38	3.88	3.75	2.88

The Breakdown	NetIQ	Quest Software	ScriptLogic	Desktop Standard
Change management 25%	5	4.5	3	4
Reporting 25%	3.5	4	4.5	3
Auditing 25%	5	4	4	2
Administration 25%	4	3	3.5	2.5
Total score	4.38	3.88	3.75	2.88

Scoring Key: **5:** Exceptional; **4:** Very good; **3:** Average; **2:** Below average; **1:** Subpar or not available

quick in our test environment.

Reports are available in multiple formats, but they are essentially formatted log entries and did not provide a means to quickly identify specific changes. RSoP reports are available and include what-if analysis.

The raw log file of changes is available as an audit trail, but we would like to see a more formatted report with easily identifiable information.

DesktopStandard

GPOVault shows a lot of promise, but needs some additional features, such as integrated RSoP reporting, what-if analysis, detailed audit trail reports and snapshot-in-time reports to compete in the enterprise.

GPOVault — which runs as a service on a

member server and acts as a proxy for making changes to Active Directory — focuses on extending the functionality of native Active Directory tools, even relying on Microsoft's standard group policy management console. GPOVault brings additional tabs to the standard Active Directory interface, including some that present historical data for policies, add extensions for all objects and offer a change control folder for each domain.

GPO Vault provides four access levels — Administrator, Approver, Reviewer and Editor — that give detailed access control options down to the per-policy level.

We found that date/time stamps number policy versions only. We'd prefer to have easily referenced unique version numbers

assigned. A separate number identifies computers and users that make changes, but we were not able to find a way to easily associate the number with a specific machine name.

Check-in/Check-out is available via icons that easily identify the state of a policy. A workflow mechanism is available that entails moving policies to a pending folder when they are ready for approval. Rollback is simply accomplished through the policy history tab. You select a policy and click deploy. Full policy backups are available, but must be run manually.

Differential reports are available and rated the best of the products tested. The items were color-coded, which allowed us to quickly identify changes made between ver-

sions. Reports are available in HTML or XML. RSoP reporting and what-if analysis are not available within the product. Audit trail and snapshot-in-time reports also are not readily available. You can piece together an audit log and snapshot in time by comparing different policy versions in the history section, but we would like to see specific reports created for this functionality.

Overall, the products we tested provide a basic level of functionality to improve group policy change management, administration and auditing. We would like to see improved reporting across all products, specifically the ability to create custom reports on changes made to a policy, using date range, user, object modified as options. NetIQ lets you find this information via a command-line utility, but we would like this function included in the

reporting engine.

We also would like to see improved, more flexible workflow processes in all products. It should be possible to customize workflows for different organizational processes. We would also like to see a different way to identify the changes that need approval.

Currently, the best way to see this information is to run a differential report. We would like to see improved alerting methods such as SNMP traps, and not rely solely on e-mail for notification.

Group Policy administration tools may not sit at the top of a security team's request list, but we found that these products can enable significant improvements to change management, access control and auditing of any Active Directory installation. Many of the changes made to this environment are criti-

cal to an organization's infrastructure and should be protected accordingly.

Andress is president of ArcSec Technologies, a security company focusing on product reviews and analysis. She can be reached at mandy@arcsec.com.

Lab Alliance

■ Andress also is a member of the Network World Lab Alliance, a cooperative of the premier testers in the network industry, each bringing to bear years of practical experience on every test. For more Lab Alliance information, including what it takes to become a partner, go to www.networkworld.com/alliance.



NetIQ Corporation
3553 N. First Street – San José, CA 95134
Tel: (408) 856-3000 – Fax: (408) 273-0578
Sales: 1-888-323-6768
Email: info@netiq.com