

Change and Configuration Management for AD

Focus

Go a step **beyond** basic AD auditing

Out of the box, Windows Server 2003 and Windows 2000 let you perform basic auditing of Active Directory (AD)-related machines. For example, you can determine who logged on to AD and who manipulated a file on a server. You can even determine when someone created a new Group Policy Object (GPO) or granted AD privileges to a new user.

AD's out-of-the-box auditing capabilities come up short, however. Some sensitive areas, such as the Default Domain Policy GPO and the Default Domain Controllers Policy GPO, need to be handled with kid gloves. If someone manipulates either of these GPOs, your entire domain could be at risk. Getting to the heart of who made the change, what the change was, and when the change was made are paramount to getting that domain back to its normal functioning state.

At times, the out-of-the-box functionality can't give you all the answers, and you'll require more advanced functionality. To take the GPO example a bit further, AD auditing tells you when a specific GPO has changed but not which part of the GPO changed. (For more information about AD auditing, see "Group Policy Logging," March 2002, <http://www.winnetmag.com>, InstantDoc ID 23832.)

Being able to determine when AD changes occur and—more importantly—who made them can help you quickly and easily restore the system should you need to. That's where Change and Configuration Management (CCM) products come in.

AD CCM Products

CCM products for AD go a step beyond simply auditing the directory. These tools provide a way to locate errant changes and implement sanctioned changes to your environment. This Buyer's Guide lists products that perform CCM for AD.

Because AD comprises so many functions, each vendor—and thus each product—has a slightly different idea of what the goals of AD CCM should be and implements that vision in its own way.

If your primary objective is to comprehensively manage your environment through Group Policy and prevent inadvertent changes from being applied to AD, consider a tool that performs check-in/check-out to stage proposed GPO configurations. The idea behind a tool such as this is simple: First, someone creates a proposed GPO to use in the domain or within an organizational unit (OU). That person then simply checks in the GPO to the library of potential GPOs. Then, after a corporate approval process (ideally through some centralized authority), the GPO is set to go live. In addition, some GPO management tools can help you determine who changed a GPO and the precise changes that person made—an especially valuable function if a user bypasses the approval process.

AD maintains user accounts and delegated security settings. Many corporations have corporate computing standards that stipulate user- and group-naming standards, OU naming standards and structure, and delegation of security rights. But AD's out-of-the-box toolset doesn't ensure that objects or attributes conform to your standard corporate configuration or naming standards. If you want to ensure that your AD deployment is consistent, look for a tool that can help flush out objects and

Being able to determine when AD changes are made and—more importantly—who made them can give you the information you need for a fast and easy system restore.

security rights that don't match your corporation-developed naming and configuration standards. If you want to go the extra mile, consider a tool that can enforce corporate configuration and naming standards and adjust and reset those misconfigured objects to your company's standards.

When you evaluate CCM for AD tools, look for products that can help you determine AD's current state as well as identify changes that have been made to it. Throughout your deployment and ongoing AD maintenance, the best tool is one that works hand in hand with your ongoing processes. You'll want to wrap all the changes you make around a renewable process that makes sense for the way you work.

InstantDoc ID 41099

—Jeremy Moskowitz

Contact Information	Product Name	Price	Description
Aelita Software 614-336-9223 800-263-0036 http://www.aelita.com	Enterprise Directory Reporter (EDR)	Contact vendor for pricing	Provides directory reporting, pre- and post-migration analysis, configuration change auditing, security assessment, and inventory management for Windows-centric networks; includes the Aelita Reporting Console, which features hundreds of predefined reports and the ability to tailor specific reports
	InTrust	Contact vendor for pricing	Consolidates event, performance, and other IT audit data across multiple directory services, applications, and systems for use in monitoring, security assessment, capacity planning, and performance optimization; archives audit data; InTrust for Events complements real-time monitoring by enabling a historical view of events and activity patterns
BindView 713-561-4000 800-813-5869 http://www.bindview.com	bv-Control for Windows	Contact vendor for pricing	Offers comprehensive security, availability, policy management, automated administration, and computer-configuration management for Windows OSs; includes share and NTFS configuration for assessing shared permissions, service configuration for ensuring that only approved services are installed and properly configured, and flexible registry and event-log reporting for performing detailed auditing and forensic analysis
Ecora Software 603-436-1616 877-923-2672 http://www.ecora.com	Ecora Enterprise Auditor 3.0 Suite	Platform-specific pricing starts at \$650 per license and is volume discounted	Provides flexible cross-platform configuration reporting and change management; collects critical configuration data from Windows, UNIX, Linux, Novell NetWare, Cisco Systems, Microsoft SQL Server, Exchange Server, IIS, AD, Citrix, Oracle, and Lotus Domino platforms into a SQL Server database (or Microsoft SQL Server Desktop Engine—MSDE) with cross-platform configuration repositories; uses collected data for change identification and tracking, auditing, reporting, and disaster recovery
FullArmor 617-457-8100 800-653-1783 http://www.fullarmor.com	FAZAM 2000 4.0	\$10 per user	Features GPO CCM capabilities, including check-in/check-out, version control, granular delegation, difference and comparison reports, baselining, and GPO Health Check; tracks GPO change history; performs general administration, including Resultant Set of Policies (RSOP), restore and backup, reporting, searching, and scripting; provides knowledge taskpads and wizards; interoperates with Group Policy Management Console (GPMC) backup files and report and migration map formats
NetIQ 408-856-3000 888-323-6768 http://www.netiq.com	NetIQ Group Policy Administrator 4.0	\$10 per user account	Provides Group Policy change management for AD environments including GPO change and release management, backup and restore GPOs, GPO troubleshooting and remote diagnostics, RSOP, and GPO change history; copies GPOs from test to production
Quest Software 949-754-8000 800-306-9329 http://www.quest.com	FastLane ActiveRoles 5.0	\$20 per managed user	Amplifies and automates Windows and Exchange security by providing centralized management of all AD security and content across the entire enterprise; ActiveRoles leverages AD to distribute all its application data across the network for virtually unlimited scalability and enhances the security of Windows 2003, Win2K, Exchange Server 2003, and Exchange 2000 Server