Enterprise Administrator for NT

BY GUY C. YOST

Last month, I examined Hyena, a product from Adkins Resource, Inc., that integrates the functionality of Explorer/File Manager, Server Manager, User Manager, and Print Manager into one program and management interface, all while presenting NT domain objects in an organized and manageable manner.

Although Hyena does a good job of presenting an administrative interface, it does not function beyond NT's basic and dated domain-based NOS principles. The next generation of Enterprise NT administration will need to redefine how network resources are organized, grouped, and how security permissions are assigned. The clear direction that the NOS industry is headed will leverage X.500 compatible directory services not only for typical directory "look-up" functions, but also for managing the logic, security, and control of network resources. Microsoft is busy catching up to the Directory Services world with its forever-pending formal release of NT 5 (now called, no joke, NT 2000!), while Novell, Banyan, and others in the UNIX world have been using Directory Services to streamline network management for several years.

In the meantime, administrators of large NT network deployments are looking for immediate solutions to ease the pains of maintaining large-scale multi-domain, multi-location networks. One company that offers a "directory-service-like" approach to NT administration is MCS (Mission Critical Software) in Houston, Texas. MSC currently offers two flagship products, Enterprise Administrator (EA) and SeNTry. EA addresses general network administration efforts, while SeNTry focuses on collecting Event Viewer information across several servers and generating reports, alarms, etc., based on event log content. On MCS's web page, they boast reaching 2 million Windows NT user accounts under administration at more than 360 of the world's largest NT deployments. Even Microsoft uses EA internally to make their large NT network more manageable.

The next generation of Enterprise NT administration will need to redefine how network resources are organized, grouped, and how security permissions are assigned.

EA uses an Old West analogy to organize NT users, groups, and network resources. God-like powers still belong to the native NT administrator who designates one or more user accounts to be "Marshals." Marshals can then define "Territories" and appoint "Deputies" to manage specific functions over user accounts, groups, and resources within their Territory. To better understand how EA works, MCS defines the terms as follows:

Territory - A set of user accounts, groups and resources in a domain. A Territory also defines one or more Deputies and the powers that each Deputy has over the user accounts, groups and resources in that Territory.

Marshal - A user authorized to use EA to define Territories. A Marshal can also create Deputies in a Territory and delegate powers to each Deputy. EA allows a Windows NT administrator to create one or more Marshals in a domain. A Marshal does not have to be a Windows NT administrator.

Deputy - A set of user accounts or groups defined by a Marshal that have one or more powers over the user accounts, groups and resources in a Territory. By defining Deputies in each Territory, a Marshal can delegate administrative tasks to one or more users.

Power - A granular subset of Windows NT administrator authority. A power allows a Deputy to perform specific system management or maintenance tasks related to that power. For example, a Deputy with the UserDelete power can delete user accounts in that Territory.

Resources - A set of computer systems or Windows NT network components, including printers, shares, services, devices, connected users, open files, event logs, domain controllers, and domain members.

So, what does this buy you? In practice, administrative privileges are all or nothing using the base NT security model, despite the fact that "rights" for managing users, servers, printers, and backup services can be assigned to specific users or groups. An NT Account Operator has rights enough to create, delete and modify users and groups, whereas EA divides administrative privileges into task-oriented permissions granted to Deputies. Using this approach, it's possible to have several Deputies work together to manage a Territory. The downside of this, however, is that communication between Deputies must be clear and constant.

Although EA allows you to create a hierarchy of administrative power, it doesn't replace the NT security structure. Instead, it uses the native NT SAM (Security Account

Manager) database, so changes made by EA utilities will be reflected when using conventional NT admin tools. Like Hyena, EA uses a main console utility that consolidates the functions of inherent NT tools including Server Manager, User Manager and Print Manager. EA includes a comprehensive command-line interface that allows you to perform network management functions using batch files. The MCS SE who assisted me in setting up EA indicated that any function that can be performed in the GUI console has a command-line equivalent. This allows automation of routine tasks, which can be triggered manually as needed or scheduled to occur at present times using NT's AT.EXE scheduler service.

EA also includes a Domain Consolidation Toolkit that consists of an Account Replicator and a File Security Translator. These utilities simplify moving users, groups or other resources from one domain to another, or consolidating multiple domains.

SUMMARY

EA's real strength is in its ability to group network resources within domains and distribute administrative powers to as many people required to make large-scale NT networks manageable. It's reminiscent of the Tom Sawyer white wash routine, beckoning unknowing souls into the world of network administration.

The clear direction that the NOS industry is headed will leverage X.500 compatible directory services not only for typical directory "look-up" functions, but also for managing the logic, security, and control of network resources.

Although EA is a fully functional administrative suite with notable depth, I'm disappointed that MCS uses Old West terminology and concepts as the foundation of their product. Not that I have anything against the Wild West, however, MSC would see a much broader acceptance of EA "terminology" had they used industry standard definitions, preferably based on X.500 culture. That is, territories could have as easily been called OUs (Organizational Units) and the idea of hierarchical administration used in the current Directory Services world would cover the roles of Marshals and Deputies. Of course, for MSC to use industry standard x.500 terms would imply to most consumers that the product indeed provides true directory services and full LDAP support. That too, would be a nice addition, because much of the MCS EA marketing material claims that the product readies organizations for NT 2000 deployment. For more information contact Mission Critical Software at (713) 548-1700 or www.missioncritical.com. ts

NaSPA member Guy C. Yost is the owner of Redstone Consulting, an IT management consulting firm in New York. He has authored several books on networking for Que Publishing, including Learning NetWare 4.1, *and* NetWare 4.1 SmartStart, *and contributes to* Technical Support *magazine as an author, columnist and technical editor. Guy also develops and conducts seminars on networking with Windows NT, UNIX, NetWare and Internet/intranet technologies across the United States and Canada. He can be reached at (518) 674-5606 or gyost@logical.net.*

