

The White Papers

Advanced Security Management of Active Directory in Windows 2000

by

**Dung Hoang Khac, Principal Consultant,
Hewlett Packard Consulting and Integration**

**Keith Millar, Director of Product Management,
Microsoft Solutions, Quest Software**

**Joe Baguley, Product Manager,
Microsoft Solutions, EMEA, Quest Software**

May 15, 2002

Contents

Abstract.....	3
Introduction	4
Access Controls within Active Directory	4
Understanding the Active Directory	5
Exploiting the Active Directory.....	6
Access Control Management Challenges.....	7
<i>Granting Autonomy to Business Units.....</i>	<i>8</i>
<i>Auditing within Active Directory.....</i>	<i>9</i>
AD Architecture Realities	10
<i>Providing Alternate Views on AD.....</i>	<i>10</i>
<i>Content Management of AD Data</i>	<i>12</i>
Group Policy and Active Directory	13
<i>Overview</i>	<i>13</i>
<i>Resultant Set of Policy (RSOP).....</i>	<i>13</i>
<i>Multiple-domain Policies.....</i>	<i>14</i>
The Future of Active Directory	15
Conclusions.....	15
About the Authors	16

Advanced Security Management of Active Directory in Windows 2000

By **Dung Hoang Khac, Keith Millar & Joe Baguley**

Abstract

As the cornerstone of a Windows 2000 network, Active Directory provides a unified repository of corporate users, groups and network assets when it is deployed completely in the enterprise. The security management challenges of Active Directory are profoundly different than the challenges experienced with Windows NT domains. The new challenges are a result of the complexity and flexibility of Active Directory and Windows 2000. Microsoft offers this flexibility to meet the enterprise requirements of large networks.

Deployments of Active Directory have been slower than expected due to the complexity of Active Directory and other Windows 2000 concepts such as Group Policy and DNS integration, as well as normal deployment planning delays. However, Active Directory's value proposition has driven many projects, and 2002 will be a year of accelerated Windows 2000 deployment. The integrity of the data stored inside Active Directory will determine the true value of the directory and will ultimately drive a quantifiable ROI for customers. Maintaining this data requires diligent attention to the security management of Active Directory.

Quest Software's FastLane[®] ActiveRoles was designed specifically to address the security management challenges encountered when managing a large Windows 2000 deployment. Companies deploying Windows 2000 will need to acquire best of breed solutions and employ widely used best practices to maximize their return on investment in Microsoft technologies.

Introduction

Active Directory and Windows 2000 are critical components of Microsoft networks. Many large companies and organizations are adopting these technologies to overcome the limitations of Windows NT. Active Directory will allow an enterprise to build a unified IT infrastructure that will reflect the structure of the business.

Windows NT domains have several limitations. By necessity, Windows NT networks are segmented into domains. Each NT domain is a security and administrative boundary and can easily be kept isolated from other NT domains. Active Directory brings the management of diverse domains together into one structure. This enables flexibility in management: IT departments can centralize the management of the core infrastructure while allowing distributed administration of day-to-day operations to local personnel. Flexibility in the management model also enables reducing the cost of operations, but it raises the requirement for enhanced security management. Enterprises need the ability to effectively manage AD permissions to ensure that only appropriate people can access corporate data.

Access Controls within Active Directory

Microsoft offers a very granular administrative delegation model within Active Directory. Administrative delegation is defined as the ability to delegate part of the administrative task to another administrator. This type of delegation is made possible thanks to enhancements in the Windows 2000 Access Control List (ACL) model and the inclusion of a container, called the Organizational Unit (OU). The same mechanism used to grant permissions to file objects can now be applied to Active Directory objects.

The OU offers a convenient way of grouping objects and provides a hierarchical view of objects within a domain. Administrative delegation mainly consists of grouping managed objects into an OU, then assigning permissions on the OU that correspond to specific administrative tasks. Thus, Active Directory enables a very granular level of delegation that provides a vast array of flexibility for delegating administrative privileges. All of the following delegation options are possible with Active Directory:

Level of Administration	Full Access – Read and Modify	Restricted Access – Read Only
Entire AD Forest	•	•
Part of the AD Forest	•	•
Entire AD tree	•	•
Part of AD tree	•	•
Entire domain	•	•
Part of an AD domain - multiple OUs	•	•
Single OU and contents	•	•
Specific object types (users, groups, computers, etc)	•	•
Single objects (Joe’s User Account, Marketing Global Group, etc.)	•	•
Single object attributes (password, name, group members, phone number, etc.)	•	•

The above table shows the fine level of granularity available natively with Active Directory's security model. The challenge for most organizations lies in managing these permissions to the finest possible level of granularity.

Understanding the Active Directory

Another key aspect of Active Directory ACL-based permissions is the architecture of the delegation model. Active Directory permissions are set on the individual objects or containers within Active Directory. The native AD delegation model is built into Active Directory itself and is replicated throughout AD along with AD objects and attributes, providing for a robust, distributed, secure directory.

An Active Directory domain keeps synchronized, read-write copies of the directory on all Domain Controllers within a domain. For instance, all of the user and group accounts within a domain can be accessed and edited on any DC within the domain. Having multiple read-write copies of the AD is a great improvement in flexibility over the single read-write copy available on the PDC of a Windows NT domain, and it allows administrators to access any local DC to perform administration tasks.

Example: See Figure 1 below. An Active Directory domain can span across North America. A helpdesk person can access a local DC in Miami to make edits, as can a helpdesk person in Vancouver. Active Directory security permissions are also propagated throughout the Domain Controllers using the native replication of Active Directory. Furthermore, an administrator in Vancouver can grant a helpdesk person the right to reset passwords over the Marketing OU by setting the ACLs on the Domain Controller, DC-Vancouver. After the AD replication has taken place, the Miami helpdesk person can reset a user's password in the Marketing OU by accessing a local DC, DC-Miami.

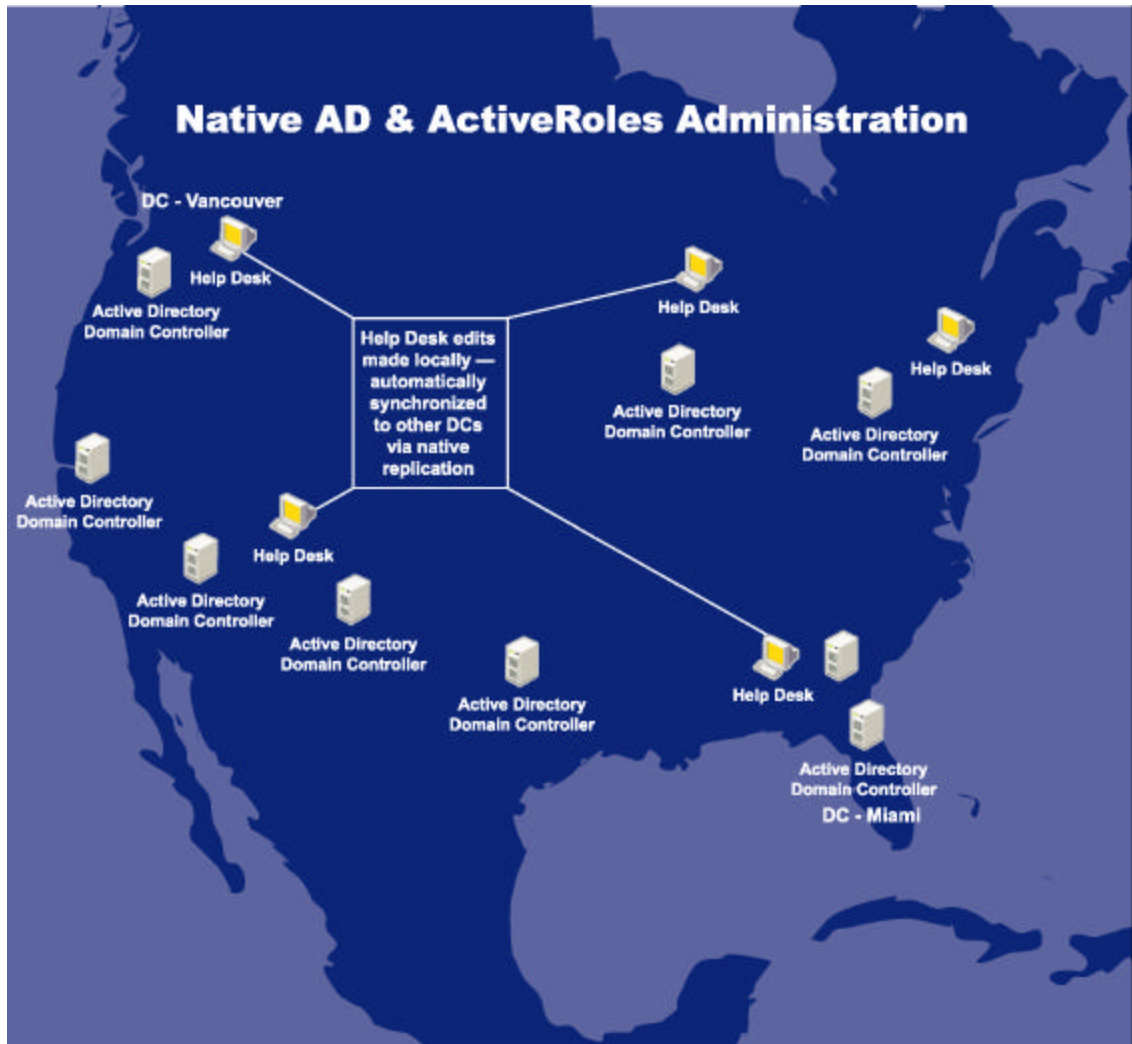


Figure 1

Exploiting the Active Directory

Active Directory is not simply a Network Operating System (NOS) directory used for authentication and authorization, but it also provides a central repository for other applications that need to store information. For example, Exchange 2000 and Mobile Information Server are AD-enabled applications from Microsoft. They extend the schema in defining new classes and attributes of objects, and, therefore, they use AD to store new objects or attributes. Administrators can apply the delegation model to these new objects.

Other vendors will also be leveraging AD for their identity requirements. SAP, PeopleSoft® and J.D. Edwards have already stated their intent to leverage Active Directory instead of their own proprietary data stores.

Access Control Management Challenges

The challenges of managing AD access controls are almost identical to challenges encountered when managing NTFS permissions. Whereas on a file server it is very easy to grant “Everyone - Full Control” to a parent folder, in Active Directory, it is equally easy to grant “Everyone – Full Control” to a parent OU and its contents. Similarly, on a file server, it is difficult to grant and maintain granular rights to specific people to manage different folders and files based on their access requirements, while in Active Directory, it is just as difficult to grant and maintain specific rights to different helpdesk personnel to manage OUs and user/group objects. In both scenarios, the security implications are profound: inappropriate Active Directory access can lead to significant AD data loss or unauthorized access to corporate resources, meaning that implementing AD in and of itself is no assurance that security will be enhanced.

The main challenge that large organizations face is the lack of role-based administration within the Active Directory. AD Access Controls allow an administrator to allow or deny access to any attribute of any AD object. While this is no challenge for one object, it becomes very unwieldy when a large number of AD objects need to be secured. Using role based administration allows an administrator to build re-usable collections of permissions (or “roles”) to reflect the business requirements of the enterprise. These roles can be deployed, modified or removed and can provide significant savings by automating a task that would be very expensive and error-prone if done manually. Without role-based administration in place, the administrator cannot efficiently audit permissions or make changes to common delegated rights in a timely manner.

Example: A large US Government deployment of AD involves 3000 delegation points. A delegation point is defined as a location in AD where certain administrative rights are delegated to allow for efficient administration – this can be a person or a group of people with similar admin responsibilities. Managing discrete access control entries over thousands of delegation points was not feasible for this institution. Fortunately, role-based administration provided through Quest Software’s FastLane® ActiveRoles product allowed the IT staff to quickly build common administrative roles, accelerate the deployment of rights and tightly manage AD security on an ongoing basis. Some roles were used in 40 or 50 different locations. In a role-based environment, expected changes to permissions are simple to perform and require minimal labor, while modifying discrete Access Control settings manually would involve a massive amount of labor.

Granting Autonomy to Business Units

The non-hierarchical or ‘flat’ architecture of Windows NT generated a highly autonomous administration model where each domain represented an administrative boundary. Contrary to this model, Active Directory and its flexible delegation model enable both centralized and distributed administrative operations. Centralized administration can reduce the cost of operations, while distributed administration provides necessary autonomy to Business Units and eases management burdens.

Active Directory enables several administrative models when its native security model is leveraged. Some companies require a very centrally managed environment where many helpdesk and higher-level administrative tasks are performed. However, a more common and emerging model is one that involves the delegation of a large amount of administrative autonomy down to the local business units. This ‘local autonomy’ model matches with the business structure of many companies.

Example: A large technology company has a geographically distributed business that spans the Americas, Europe, Middle East and the Pacific Rim. The company has chosen an AD structure that spans this entire area with a single forest containing multiple AD domains. From a security perspective, the company wishes to maintain central control over key infrastructure master components, so it has decided to go with a root domain housed in its central office in North America.

High-level administrative privileges are given to the geographically distributed domains, then to the OUs within those domains. This allows the local business units to manage helpdesk permissions, including group membership changes, password resets and computer account creations. The local tasks will also involve more complicated activities, such as creating new OUs and rolling out new Domain Controllers as needed regionally. Local activities can be monitored and documented by the central IT authority, but the administrative tasks will actually be performed locally.

The company chose FastLane[®] ActiveRoles to manage this environment because its design provided their IT organization with the flexibility to meet their needs. To provide autonomy to the local business units, the chosen solution would have to add value to the central IT group while also providing value to the local business units. ActiveRoles’ directory-enabled design made it a good fit because its application data lives inside AD itself, and therefore the data can be replicated to all corners of the AD infrastructure. This dynamic, directory-enabled behavior created multiple benefits:

- Role-based administration data would be available on every domain controller
 - Guaranteed local access to roles, even on newly created domain controllers which alleviated any scalability or availability concerns
- ActiveRoles would not require a deployment of any sort

- No proxy servers: An alternative solution, which required deployment of proprietary proxy servers to provide the role information, was untenable due to the large and geographically distributed nature of the network
- ActiveRoles' security relied entirely on the native AD security model
 - AD security leveraged: After an in-depth review of AD security, the company was satisfied that it was sufficient for their network
 - No additional security review: an overlay solution that ran under an elevated security context would have required a complete security review process before it could be seriously considered

Auditing within Active Directory

For security reasons, changes made to AD objects must be audited. Several types of changes can be made within AD that could constitute a security risk. Examples of this include additions to the Domain Admins group, granting password reset rights on company executive accounts and group membership modifications. The best way to prevent AD security risks is to be very selective in granting Access Control rights. Organizations should carefully scrutinize who will have the following:

- Schema Admin rights – this gives full rights over the AD schema
- Enterprise Admin rights – this gives full rights over the AD forest
- Domain Admin rights – this gives full rights over the AD forest
- Account Operator rights –this gives full control over groups and user accounts inside the entire domain
- Full Control anywhere inside a domain or OU –if a person needs to reset passwords only, do not give them Full Control
- Access to key/sensitive personal data – does the help desk need to have rights to edit “home phone number”, if they are not the authoritative source for that info? Typically, these attributes are managed by someone in Human Resources

Once the organization is confident that the access controls have been handed out appropriately, it is still important to follow a diligent auditing procedure for granting access to AD objects. As Active Directory involves a multi-mastered infrastructure, AD object modifications can occur on any domain controller. The audit events will be stored on the AD domain controller where the object was edited. Consequently, all AD Domain Controllers must be canvassed to get a complete picture of all object edits that occurred in the AD domain(s). The audit events are written into the directory services log on each DC, so object auditing must be enabled for each AD domain.

There are several ways to view the directory service logs:

- Use the native Event Viewer to connect the DC(s) to search for specific event IDs, or to review the entire log file, or to export that relevant log file
- Third-party reporting products, such as Quest Software's FastLane[®] Reporter, that leverage the local WMI engine to make intelligent queries of the existing logs on the local DC
- MOM – Microsoft Operations Manager provides event consolidation
- Home-grown scripts running locally or remotely to collect certain Events IDs

AD Architecture Realities

Providing Alternate Views on AD

Native Active Directory protocol only permits object to exist in a single location at any given time. From a security viewpoint, this is a blessing and a curse. The espoused major benefit is that since any one object only exists in one location, it is easier to lock down the directory and understand who has permissions on those objects. While this is essentially true, it also creates a number of security-related administrative challenges.

In fact, this one-object, one-place design creates a major problem. When organizations have designed their Active Directory on either political or geographic lines, there may be cases where they need to delegate responsibility differently – consider the following scenario:

Acme Corp. has selected a geographical design for their Active Directory because their administrative model is regionally based. They have decided to leverage the fact that a domain forms a security and replication boundary by having a placeholder root and regional domains managed by their regional IT teams. Their AD design is depicted below:

Acme Corp — Domain Structure

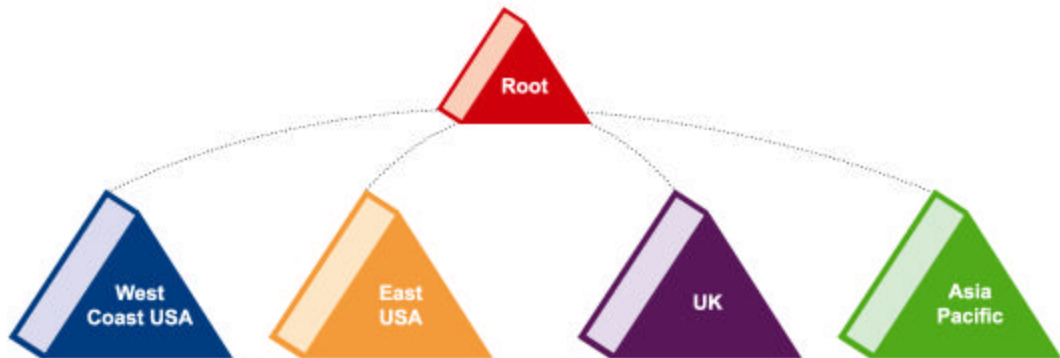


Figure 2

As shown in Figure 2, assume there is a sales OU in each of the four regional domains that includes the regional sales teams. The global VP of sales has decided that the administrative team should have access to modify various attributes of all sales people worldwide, including their address and manager information. To achieve this, an AD administrator must delegate permissions to the administrative team at the Sales OU level within each domain – not hard in itself, but when one considers scaling this for many different roles in many departments in a global company the enormous time investment required becomes clear.

The next problem is presenting these sales administrators with the appropriate information to do their jobs. In order to edit a Sales Person’s attributes, they will have to navigate through the AD tree to find the relevant OU and then edit the user. However, there is no mechanism provided to show them one simple list of all sales people worldwide.

From a security management aspect, even when using a role-based delegation system, this can create a long-term problem, because as the number of delegation points increases, there is no single view that shows where the Sales Admin team’s role applies. This issue is becoming more and more apparent to organizations as they go through the AD planning and deployment stages.

Many companies are relying on the “Business Views” functionality of FastLane ActiveRoles to solve this issue. With ActiveRoles’ directory-enabled functionality, administrators can create a Business View that contains many objects from across domains, and then delegate a role upon this Business View. This greatly simplifies delegation and solves the ‘one object, one location’ problem.

Content Management of AD Data

In Windows NT domains, the number of object attributes is considerably less than within Active Directory. Additionally, the importance of NT domain data is really restricted to the NOS environment. The profile of AD objects and content is much higher, since AD provides the backbone for Microsoft networked environments. Ensuring the integrity of AD data is key to the success of a directory deployment.

One of the drawbacks of the advanced, and more granular, rights delegation model in Active Directory is that as the administrators delegate control of objects and attributes to helpdesk staff, they have no control over the actual data being entered into AD. This can cause AD to become polluted with incorrect data unless strict controls are put in place. Examples of such are the corruption of a user's employee ID, the changing of a group description, non-compliance of naming conventions, etc.

The standard way to enforce such controls is by adopting strict procedures and scrutinizing who has access to this data, and then further instructing those individuals with rules about the population of objects and their attributes.

While for a small environment, this may seem feasible, as larger Active Directory implementations grow, the requirement for automated user creation and the enforcement of data standards becomes clear.

The "Business Rules" functionality of FastLane ActiveRoles is one solution to this issue. Business Rules allow administrators to exercise full control over the creation of objects and the population of their attributes through "Creation Templates." Additionally, through the use of "Ongoing Rules," an Administrator can ensure the enforcement of strict guidelines and rules for object content on an ongoing basis. All of this is achieved through Business Rules integration with the native tool, Active Directory Users and Computers. The Help Desk staff can still use the native tools that they are familiar with, while the Administrator can protect Active Directory against pollution. Additionally, ActiveRoles provides an alternative Web client that will also enforce Business Rules.

Group Policy and Active Directory

Overview

Microsoft describes the function of Group Policy as “Enhancing the User Experience”. Administrators now have more control than ever before over the systems and applications that the users are permitted to use and how they use them.

Group Policy enables a significant amount of granularity of control over what users can and cannot do. Furthermore, Group Policy provides control over the behavior of the computers that are being used. The old favorites, such as disabling “Start, Run”, are now complemented by a considerable set of new features, such as allowing/restricting the running of certain MMC snap-ins, Internet Explorer configuration settings, desktop appearance, event log behavior and much more.

Resultant Set of Policy (RSoP)

Group Policy can be applied at the Site, Domain or OU level or locally to govern who receives the ‘benefits’ of these policies; they offer the additional ability to filter those effects by group membership. But their complexity depends on the topology of Active Directory. AD topologies are influenced by many factors: often, geographic distribution of the company drives the site and domain structure; moreover, administrative requirements drive OU structures within these AD domains. Deploying Group Policy Objects (GPOs) across Sites, Domains and OUs can result in quite complex hierarchies of Group Policy settings.

The resultant ‘experience’ a user receives could be a result of the application of many policies (e.g., a user logging in may receive a policy from his site, his domain and his OU), but there may also be a policy applied to his workstation at all of these points, in addition to a local computer policy. The subsequent resolution process is far too complex to discuss in this White Paper, but the immediate management challenges should be apparent. In any large organization, Group Policy management can very quickly become a full-time job.

The initial Group Policy interface is hierarchical and simple enough – it should be fairly familiar to those that have played with Policy in Windows NT. Unfortunately, it is very tedious to ascertain the exact effects of one particular policy and expanding all nodes to see what has been put into effect. Add to that the possibility that a user may be on the receiving end of *several* policies, and the task really starts to become daunting.

There are third-party tools available to assist with this process, one in particular being the ActiveRSoP application that ships with FastLane ActiveRoles. Using the ActiveRSoP tool, Administrators can quickly and easily view not only the effective components of one GPO, but also the resultant effects of many policies. For example, ActiveRSoP can show what would happen if User A, who is in Domain B, in OU C, logs onto workstation D in site E.

Additionally, ActiveRSoP can run ‘what-if?’ scenarios, showing the resultant effects of such actions as moving a user to another OU or group, moving their log-in computer, or authenticating against a DC in another site.

With an intuitive interface for managing and editing group policies, complete with export and import abilities, ActiveRSoP is a key tool for managing AD’s Group Policy.

Multiple-domain Policies

Microsoft’s design for Active Directory requires that GPOs should only be linked and housed inside a single domain. This means that GPOs are only *replicated* within a single domain. A GPO actually consists of two parts, the first part being an object held in the directory itself in the Domain Naming Context, and the second part being held in the SYSVOL share of every DC within a domain, as the full GPO itself was deemed too large to be stored in AD in its entirety.

This design can cause limitations in a multi-domain AD deployment. While GPOs can be ‘linked’ between domains, this has been proven to considerably slow the user logon process, because a client has to find a DC from the originating domain in order to read the GPO, and this DC may be in a completely different site over a slow link.

The more common practice has been to ‘copy’ that GPO and recreate it in the other domain. Recreating the GPO is a manual task that naturally lends itself to human error. Organizations must impose procedures to ensure that changes to that GPO are then synchronized over time.

Without adopting effective procedures for the reliable duplication of GPOs between domains, security holes can form rapidly. Consider the following example: a company uses Group Policy to determine the minimum password length across all domains; they decide to extend the minimum password length from 7 characters to 11 characters. If the company has multiple domains, they have to consistently modify this GPO setting across multiple domains or the old, shorter password length will remain in place.

Already, effective third-party tools are available to assist in this process. Quest Software’s FastLane ActiveRoles provides ActivePolicy functionality, which allows the creation of ‘policy templates’ that are stored in AD. These policy templates linked to new or existing GPOs, providing commonality and synchronization between GPOs within and across multiple domains, thereby removing the significant administrative burden of rolling out policy changes.

The Future of Active Directory

Because Active Directory is the cornerstone of a Windows 2000 network, the value proposition of Windows 2000 is greatly enhanced with the adoption of Active Directory. Many large companies are moving to AD from NT to provide a more consistent and unified structure for their network infrastructure. The adoption of Windows 2000 has been much slower than many industry observers predicted, due to the complexity of Active Directory and other Windows 2000 components. However, most large companies have plans in place and are moving forward on their AD deployment plans because the return on investment for Windows 2000 outweighs the cost of deployment.

Microsoft has shipped several directory-enabled applications such as Exchange 2000, Mobile Information Server and other .NET application servers, all of which will rely on Active Directory as a backbone. Third-party vendors have also shipped directory-enabled applications and the list of supporting vendors is growing. The allure of directory-enabled applications comes from the ability to unify the identity management and authentication behind the applications by leveraging Active Directory.

In late 2002, Microsoft will ship the next version of Windows, Windows .NET Server, which will provide a revised version of Active Directory. This new version will include many desirable features such as Domain and Domain Controller renames, schema deletes, multi-forest transitive trusts, cross-forest authentications and AD partitioning. All of these new features will make AD more configurable and more robust in the enterprise setting. Quest Software's FastLane ActiveRoles provides the same value for the new AD release as it does with the Windows 2000 version of Active Directory. The need for role-based administration, Business Views, Business Rules, GPO management and access control reporting still exists in Windows .NET Server.

Conclusions

As Active Directory adoption accelerates and becomes a critical part of production networks, employing effective security methodologies and tools becomes increasingly important. As more applications become directory-enabled and more information is stored in the Active Directory, including confidential HR information, the ability to effectively manage and lock down this directory will become business-critical.

The onus is on security specialists and administrators to deploy proven management tools and best practices to ensure that AD security is effectively managed throughout the entire lifecycle of the directory.

About the Authors

Dung Hoang Khac, Principal Consultant Hewlett Packard Consulting and Integration

Dung is member of the Applied Microsoft Technologies Group of HP Services Corporate. He provides technical support to HP Services, Professional Services Windows and Messaging Corporate Practice and to field consultants in providing enterprise infrastructure solutions. Dung is instrumental in designing and delivering the Windows 2000 and Exchange 2000 Academies, intensive 5-day lecture and lab exercises on how to approach the new technology. These Academies are delivered to both HP consultants and HP's customers in North America, Europe and Asia Pacific. In addition to this white paper, Dung co-authored various Windows 2000 migrations publications, is a regular contributor to the Exchange Administrator newsletter and regularly presents at Windows 2000 industry events. Dung recently moved from Europe to North America and is now based in Seattle, WA.

Keith Millar, Director of Product Management Microsoft Solutions, Quest Software

For years, Keith Millar, Quest's director of product management for Microsoft solutions, has been working with Global 2000 and other large enterprises to understand network challenges. Using this information, he has worked with the research and development team at Quest Software to develop Windows NT, Windows 2000 and Exchange solutions. Quest's experience with Windows networking produced the market's first integrated suite of domain management and reconfiguration, directory reporting, policy and security enforcement, and administration delegation applications. Keith has an MBA from the University of British Columbia, Canada and a BS in Mechanical Engineering from Queen's University, Canada.

Joe Baguley, Product Manager Microsoft Solutions EMEA, Quest Software

With a career architecting and supporting Microsoft enterprise networks with leading European consultancies, Joe Baguley was the consulting lead in Quest Software's European Microsoft Solutions Practice and is now product manager responsible for all Quest's Microsoft Solutions products in EMEA. By leveraging his extensive field experience of large-scale Microsoft Infrastructure deployments, Joe regularly presents and publishes on the migration, deployment and management of Microsoft technologies.



World Headquarters
8001 Irvine Center Drive
Irvine, CA 92618
www.quest.com
e-mail: info@quest.com
U.S. and Canada: 949.754.8000
Please refer to our Web site for regional
and international office information.

Mailing address: P.O. Box 692000
Houston, Texas 77269-2000
Street address: 20555 SH 249
Houston, Texas 77070-2698
www.hp.com
1.800.282.6672
281.370.0670

All content Copyright © 2002, Quest Software, Inc. and Hewlett Packard Corporation. The information in this publication is furnished for information use only and is subject to change without notice. Neither Quest Software, Inc. nor Hewlett Packard Corporation assume any responsibility or liability for any errors or inaccuracies that may appear in this publication. Other product or company names mentioned herein may be the trademarks of their respective owners.

FastLane is a registered trademark of Quest Software, Inc. FastLane ActiveRoles and FastLane Reporter are trademarks of Quest Software, Inc.