

The Finer Points of Domain Planning

By John Jacobs

AT A GLANCE

Key Point: Beyond rules of thumb, choosing a domain model requires understanding the impacts of each model.

Detail: Medium

Task: Planning, implementation

Article Section

What's There

Introduction

Domain planning is the foundation of Windows NT security, but the choice of a domain model can be complicated.

Domain Overview

Often useful in choosing a domain model, a selection matrix can be inconclusive because organizations are hard to accurately categorize.

Account Management

The best domain model is often the one that best fits the organization's personnel management.

Resource Management

Domain models that centralize resource management are usually best for organizations that concentrate hardware support in one IT group.

IT Centralization

Managing several domains from one administrative account helps centralized IT groups, and may also work for decentralized security-conscious IT groups.

Conclusion

More Information

Pointers to related articles and URLs on TechNet and the Web.

Introduction

Windows NT domains are the foundation of network security: they define which servers can share resources, and which users have access to those resources. In addition, they are the basic unit of network administration, and the larger a network gets, the more impact the domain model has on administrative efficiency. Domains can be designed in various ways to best match an organization's IT group, but this flexibility complicates the choice of a domain model. The Windows NT Resource Kit and various white papers help simplify the choice with rules of thumb that apply to most organizations, most of the time. But when the rules are inconclusive, administrators need to understand the models, specifically the impact each has on administrative labor. This article explains their terminology, benefits, and costs.

Domain Overview

Domains are essentially a security arrangement between a group of computers. The heart of the arrangement is a directory database containing information on user accounts, groups of users, and computer accounts. That database controls users' access to shared resources. Each user has one account in the domain database, instead of one account on each of the servers. This simplifies user access: the user logs onto the domain, and once validated, has whatever permissions the administrator assigned on the domain's file, print, and application servers. Also, it eliminates the need to log on separately to each server. Administrators benefit as well: they create and manage one account in the domain instead of one on each server.

Each domain includes at least one Domain Controller (DC), which maintains the master copy of the directory database, and usually one or more backup domain controllers (BDCs) to which the DC replicates database changes. BDCs provide fault tolerance in case the DC is taken off line, and they divide the user authentication workload among several systems.

Administrators can establish trust relationships between domains wherein the machines in one domain "trust" the authority of another domain's directory database. Trust relationships benefit administrators—especially in large organizations—by letting them divide users into small, easily manageable groups. Some obvious division criteria are job function (Marketing, Engineering, and so on) and geographic area (North America, Europe, and so on). A less obvious division is by type of account: user accounts in one domain, computer accounts in another. This allows division of administrative labor between a group that manages users (such as Security, or Human Resources) and one that manages computers (such as IT).

The four major domain models are defined by the number of domains involved, whether those domains' databases hold user accounts or machine accounts or both, and how the domains trust one another:

- Single Domain—All user and machine accounts reside in one directory database.
- Single Master Domain—All user accounts reside in one database in the "master domain," and machine accounts are split among one or more databases in resource domains that trust the master.
- Multiple Master Domain—User accounts are split among several master domains, which usually trust one another. Machine accounts are typically split among several domains, each of which trusts all master domains.
- Independent Domains—User and machine accounts for a subset of the organization may be stored in the same database. Some domains trust each other, but (unlike the Single Master and Multiple Master models) some domains do not.

The following domain planning matrix provides rules of thumb for choosing the best domain model.

Domain selection matrix

<u>Domain Attribute</u>	<u>Single Domain</u>	<u>Single Master Domain</u>	<u>Multiple Master Domain</u>	<u>Independent Single Domains with Trusts</u>
Fewer than 40,000 users per domain	X	X	X	
More than 40,000 users per domain			X	
Centralized account management	X	X		
Centralized resource management	X		X	X
Decentralized account management			X	X
Decentralized resource management		X	X	
Centralized MIS	X	X		

Decentralized MIS				X
-------------------	--	--	--	---

This matrix often helps planners find the best domain model. For example, if the organization has fewer than 40,000 users, and wants to manage user permissions centrally but manage servers locally at each of several sites, the single master domain model is the best choice. For many organizations this matrix makes the choice simple and certain.

However, the matrix is not conclusive if, for example, an enterprise has a decentralized MIS group that wants to centralize account management, or one that wants to centralize account or resource management in some ways and decentralize it in others. To help with these sorts of real-world problems, the rest of this article explains the attributes in the matrix's leftmost column, and provides examples that help the administrator decide which attributes are most beneficial to a given organization.

Number of Users

This is the only attribute in the matrix that administrators must accept at face value. For performance reasons, Windows NT Server stores the directory database in nonpaged pool memory (RAM that is reserved and cannot be paged out to disk to free up space for other data). Up to 32 MB of system RAM can be allotted to the nonpaged pool. A directory database with 40,000 user accounts is roughly 26 MB in size, leaving only 6 MB of nonpaged pool for other system processes. Additional user accounts would consume too much nonpaged pool for the other processes to function correctly, so domain models that store all user accounts in one domain (single, and single master) are not supported with more than 40,000 users.

Account Centralization

User accounts can be stored in one or a few databases (centralized) or in many databases (decentralized). The terms are somewhat subjective: obviously, the single and single master models are centralized, but there is no universal rule for how many databases it takes before you can consider a multiple master or independent trust model decentralized. The real questions are which (if either) model is more useful to your organization, and how much decentralization is too much.

Account centralization reduces administration effort because it:

- Minimizes the number of directory databases to manage and back up
- Minimizes the number of trust relationships to maintain
- Avoids duplication of effort when creating or deleting user accounts, and when changing user permissions
- Simplifies creation of user groups that can be managed as a single unit

These changes benefit users. Administrators can respond more quickly to domain-related requests, such as creating new shares, creating accounts for new users, and changing permissions for existing users. It also frees administrators for other tasks unrelated to domain management.

Decentralization is beneficial for groups that are part of the same organization but operate independently. Multinational corporations, for example, are often spread over several continents.

It makes more sense for them to have on-site administrators capable of resolving issues than to have to wait for business hours in a central office in another time zone.

The most common account management problems stem from excessive decentralization, which often allows independence to become anarchy. A typical warning sign is the breakdown of user account standards, such as those that define domain and username conventions, password specifications, and qualifications for inclusion in certain groups (such as Administrator). Creating these standards eases inter-domain administration (including adding or splitting domains), and it makes the domains transparent to users. If domain administrators exercise their freedom at the cost of usability, they probably have too much freedom.

Resource Centralization

Windows NT allows separation of machine accounts from user accounts by putting machine accounts into one or more resource domains. The IT group can centralize resource management by keeping all machine accounts in one domain, or decentralize it by splitting machine accounts among multiple resource domains. How to decide? The best fit is usually the one that forces the fewest changes to current procedures. For example, if the organization has a single point-of-contact who authorizes creation or renaming of each server, and this arrangement is working fine, don't fix it: use a domain model such as multiple master which supports centralized resource management. If each group has the authority to add its own servers to the network, then decentralized resource management may be the best fit, and the single or multiple master models might be the best choice.

Do current procedures require authorization to create a new server? If so, the domain models that centralize resource administration may offer the best fit for the IT group: the single, the independent, and sometimes the multiple master.

Centralized resource administration increases control but decreases flexibility. For example, if a group manages its own servers and needs to bring a new one on line quickly, centralized resource management can create bottlenecks that reduce efficiency. A typical decentralized approach is to create a "resource domain" for each group that manages its own hardware. One user in the group has a subset of administrative privileges in the resource domain, enough to create and manage servers and back-up files to a tape drive, but not enough to create new user accounts. Trust relationships with account domains give the users in those domains access to the resources shared by servers in the resource domain.

The major benefit of decentralizing resource management is the autonomy it provides. Although less important, autonomy can be beneficial for psychological reasons as well. If a group feels like a pawn in internal politics, giving it control of its own hardware may improve morale, and that improvement may offset the costs of additional administrative labor. Also, if a new group is created by combining several others, a resource domain gives the members something in common and can reinforce the feeling that they are now members of the same team..

The rule of thumb for resource management is similar to that for account management: stop decentralizing when users find it harder to do their work because their domains play by different rules. For example, server and share names can help users find information quickly. If each resource domain administrator chooses a different naming scheme, the user's job becomes harder, not easier. Curtail the administrators' freedom before it impacts user productivity.

IT Centralization

Centralization of the IT group is subtly different from account and resource management: it depends on whether an administrator in one domain can manage accounts and resources without logging off of one domain and logging into another one as a different user. Because administration usually concerns user accounts, and not machine accounts, the domain models with centralized account management (single, and single master) tend to be good choices for centralized IT groups. The selection matrix does not offer advice about the multiple master model because it may fit a centralized IT group, or may not, depending on the nature of the trust relationships defined between master domains. If each master domain trusts the others, an administrator in one master domain is effectively an administrator in the others as well. If not, then an administrator in one domain may or may not be an administrator in others.

Domain models that centralize administration are most valuable in organizations that maintain a single IT group, or that concentrate all security-related tasks on one part of the IT group. For example, suppose that a defense contractor has three sites and each is devoted to a single contract. IT staff at each site might be responsible for assisting the site's users and maintaining its hardware, but a small group at one site might be responsible for ensuring that all users have proper clearance, and all servers hold the right classified documents. In this case, the value of centralizing certain IT functions might outweigh the cost of decentralizing the others. An independent domain model might be the best solution. For example, user accounts could be split among three master domains, and machine accounts could be split among three resource domains. All six trust an "IT Security" domain, whose administrators can oversee all user and machine accounts. The three master domains have no trust relationships, and the resource domains trust only their respective master domains (plus IT Security), so administrators in one master domain can add user or machine accounts at their own site, but not in the other two, and not in the IT Security domain.

Conclusion

Choosing the right domain model is not always easy because several models may appear to be good choices. The domain selection matrix shows which models are best for centralized management of accounts, resources, and the IT group in general, and this information is often enough to help administrators decide. Centralization and decentralization are relative terms, as is the value of either strategy to a particular organization. Choosing the right domain model requires a deeper understanding of how each model affects administration. The section below contains pointers to articles that discuss domains in general, as well as the mechanics of planning them, rolling them out, and managing them.

More Information

First time administrators should be sure to read the Windows NT 4.0 Concepts and Planning Manual, especially the first four chapters:

- **Chapter 1 – Managing Domains**
- **Chapter 2 - Working with User and Group Accounts**
- **Chapter 3 - Managing User Work Environments**
- **Chapter 4 - Managing Shared Resources and Resource Security**

More advanced domain planning information can be found the Windows NT Server 4.0 Resource Kit, especially in the Networking Guide, Chapter 2 - Network Security and Domain Planning. In particular, see

- **Introduction, and Windows NT Server Domains**—Background information
- **Planning Your Domain Design**—Major issues, and examples of domain models used for various types of organizations
- **Tools and Checklist for Domain Planning**—Help choosing a model, and calculating the number and type of servers
- **Troubleshooting Problems**—Help with five typical problems that can occur when setting up a domain

In addition to these, the following query finds scores of domain planning articles on the TechNet CD or on Microsoft's Web site:

domain near planning

Microsoft TechNet
June 1997
Volume 5, Issue 6