Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Addressing Network Security through Windows 2000 Active Directory: Designing a Single Domain Structure

Windows 2000 provides a remedy for the all-powerful NT Domain Admin group, where traditionally excessive powers were given to groups of users, thereby violating the security principal of least privilege. Microsoft's answer is Windows 2000's Active Directory. However, the complexity of Active Directory makes it difficult to understand how best to design a secure directory structure. This paper provides security design considerations for locating users, computers and groups in the Windows 2000 network environment.

Copyright SANS Institute

Author Retains Full Rights

AD

Addressing Network Security through Windows 2000 Active Directory: *Designing a Single Domain Structure*

Written by Les McCarter
MCSE, MCT, Master CNE, CNI, CCNA, A+

February 11, 2002

Abstract

Windows 2000 provides a remedy for the all-powerful NT Domain Admin group, where traditionally excessive powers were given to groups of users, thereby violating the security principal of least privilege.

Microsoft's answer is Windows 2000's Active Directory. However, the complexity of Active Directory makes it difficult to understand how best to design a secure directory structure.

This paper provides security design considerations for locating users, computers and groups in the Windows 2000 network environment.

Introduction: *Active Directory Complexity Breeds Confusion*

As reported in ENTNews December 12, 2001 news article, Microsoft's Active Directory manager Stuart Kwans admits that Microsoft did a poor job of educating administrators on how to implement Windows 2000.

> "We gave you the 1,500 pages of the distributed systems guide and said go do it. That was probably not the best way to do it," Kwan said Tuesday.[1]

Approaching the two-year anniversary of the release of Windows 2000, Microsoft is recognizing how difficult it is to understand the complexities of its core security element: the Active Directory. Surprisingly enough, Microsoft did not learn from Novell's earlier mistake in their misguided rollout of their directory services of NetWare 4.x.[2] Microsoft is repeating history: lack of customer education results in customer confusion.

If Microsoft, with all its resources, is having a difficult time explaining Active Directory, then it is understandable the daunting task facing network architects and LAN administrators in constructing their own Windows 2000 network.

---

[1] Bekker, Scott. "Active Directory: Microsoft Buttressing Best Practices Docs." *ENTNews from 101Communications*. December 12, 2001. http://www.entmag.com/news/article.asp?EditorialsID=5120 (February 8, 2002)

[2] Spivak, Wayne. "Has Microsoft Ever Read the History Books? Windows 2000 Server--a repeat of Novell 4.x?" *VARBusiness*. July 13, 2001. http://guide.sbanetweb.com/press/varbiz07116001.html (February 8, 2002)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

This paper will provide some guideposts on creating a secure network through Active Directory design.

Premise: *Complexity Equals Security Concerns*

Windows 2000 is the most complex network operating system from Microsoft. Where there is complexity, this is the possibility of incorrect configuration. Where there are mistakes in configuration, there is the possibility of security lapse. And where there are security lapses, there is the possibility of security breaches.

A solid understanding of Active Directory is required when building networks of any substantial size. Networks under 20 users can function well with the standard, out-of-the-box install. However, for larger networks, an in depth knowledge of Active Directory gives tools to the LAN designer that enhances the security beyond the capabilities of any previous desktop network.

Microsoft's Windows 2000 feature of Active Directory provides the opportunity to bring structure and organization to our network objects. While the design of our Active Directory can be influenced by many competing business needs, security is a major factor in the creation of our Windows 2000 Active Directory. It is also important to note that this design process is more an art, not a science. There can often be multiple good solutions to any design problems; and their can also be disastrous layouts.

We will focus on the design of a single domain. While multiple domains, trees and forests introduce more complexity, they potentially bring more control over the security design, but these additional elements are beyond the scope of this paper.

Technical Level: this paper will provide a quick overview of the various elements of the Active Directory; this however is not intended as a primer to the Active Directory. This a more advanced design theory subject matter.

For an overview of Active Directory, the reader is referred to Johnny L. Waddell's June 11, 2001 SANS Reading Room article: *Basic Security Issues of Active Directory*

- http://rr.sans.org/win2000/active_dir.php

Another introductory article by Emmett Dulaney, Vijay Sankar and Sharon E. Sankar entitled *Active Directory: An Overview*, can be found at:

- http://www.windowsitlibrary.com/Content/155/07/1.html

To quote from their web page:

> Active Directory is a *directory service*. The term directory service refers to two things — a directory where information about users and resources is stored and a service or services that let you access and manipulate those resources. Active Directory is a way to manage all elements of

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

your network, including computers, groups, users, domains, security policies, and any type of user-defined objects. [3]

Introduction: *The Cast of Characters*

While Windows NT has the concept of a domains and trusts, Windows 2000 expands the number network elements and how they can be configured. *Table 1* provides a brief introduction to the match up between NT and Windows 2000.

Table 1: Contrasting NT and Windows 2000 Networking Elements

Windows NT 4.0 Element	Windows 2000 Active Directory Element	Purpose
Domain	Domain	Collection of users and computers.
Primary Domain Controller (PDC)	Domain Controller (DC)	Holds a modifiable list of users, computers and security policies.
Backup Domain Controller (DC)	None. [W2K deploys multiple DCs]	Holds read only copy of NT's PDC database.
Groups [Local, Global]	Groups [Local, Domain Local, Global, Universal]	A collection of users to facility the secure sharing of resources, such as printers or files and folders.
One Way Non-Transitive Trusts	Two Way Transitive Trust	The logical security link between separate domains.
	Schema	The database that holds the structure of a specific organization's Active Directory.
	Tree	A collection of W2k Domains that share the same root parent domain.
	Forest	A collection of Trees sharing the same schema.
	Site	A physical grouping of computers and servers in the same "geographical area" based on IP subnets.
	Organization Units	A logical collection of users and/or computers for delegation of management and other organization purposes.
	Group Policies	A way to roll out security policies or software or desktop configurations to either: 1) domains, 2) sites or 3) organization units.

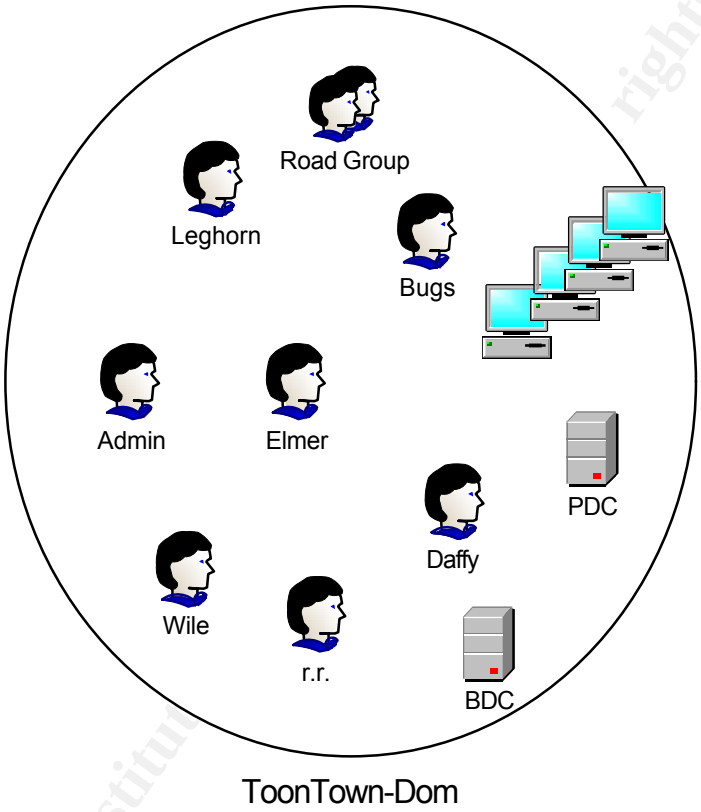
[3] Dulaney, Emmett; Sankar, Vijay; Sankar, Sharon E. *Active Directory: An Overview* http://www.windowsitlibrary.com/Content/155/07/1.html (February 8, 2002)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

As we can see there are many more players with Windows 2000's Active Directory. These elements also have a very specific way of organizing our network.

To help illustrate the differences, we will employ the imaginary company, Acme LLP.[4] *Illustration 1* represents the company in a Windows NT environment.

Illustration 1: Sample NT Domain



Note that all users, domain controllers and computers are in one collective "bucket." This is no organizing structure to manage users or computers. This structure becomes cumbersome as the number of users grows. A thirty-person network is manageable under NT's domain structure. A 10,000 user network becomes complex and, at times, almost unmanageable.

The other major problem with NT is that this is not a true enterprise solution. It is difficult to separate out management powers from the Domain Admins group. However, Microsoft has created an enterprise networking system with Windows 2000 and Active Directory: it gives us a better way to organize our users, and as we will see, better separations of powers.

Window 2000's Active Directory gives the ability to put users, computers and groups into Organization Units. This gives the administrators a tool to organize their user base even in the

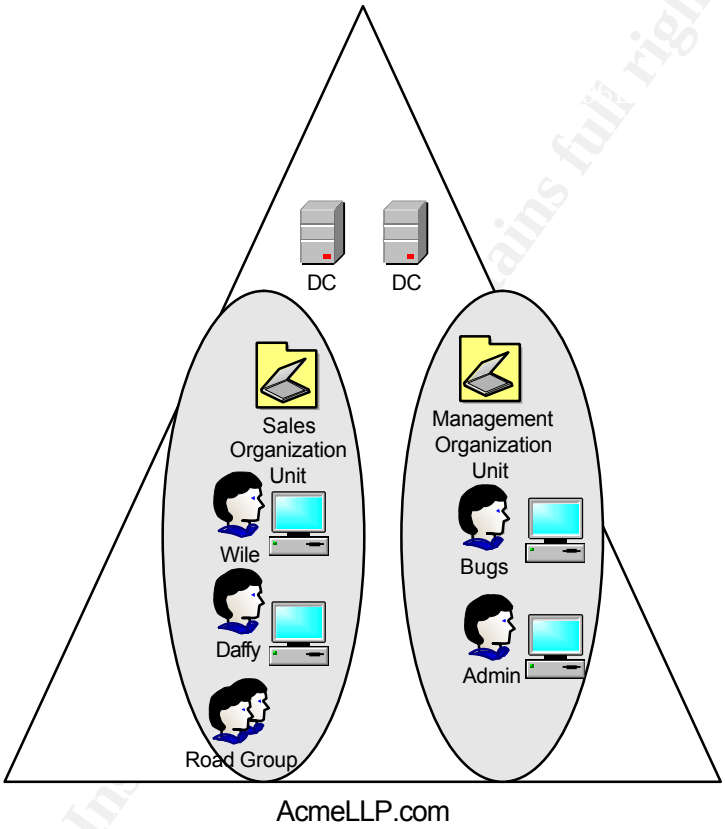
[4] Acme LLP is no relation to any real company. As of the writing of this paper, February 2002, AcmeLLP.com was not registered on the Net.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

confines of a single domain. With a structured organization, we can better document and manage a large network. With a properly designed network, we can confidently managed tens of thousands of users.[5]

Looking at *Illustration 2*, we can now see a more structured approach as we put our users into one of two OUs: the Sales Organization Unit or the Management Organization Unit.

Illustration 2: Sample Active Directory Domain



At first glance, this structure looks like a corporate organization chart, but this is an incorrect way to design a network, especially when considering security. The Active Directory organization units are used to match users and computers that have similar network requirements, not to list who they report to in the corporate political structure.

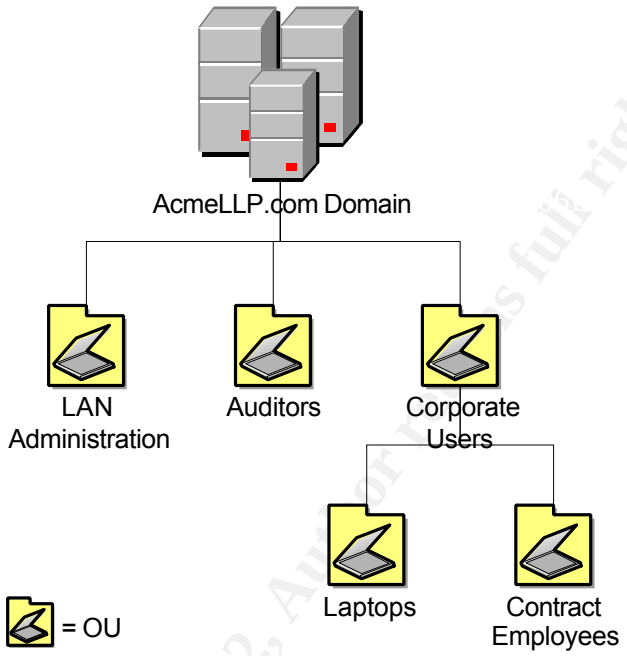
Examine *Illustration 3: Basic Active Directory for Security With Organization Units*. Unlike a traditional org chart, executive management is not at the top of the structure. Instead we have broken the organization units into groups of security levels. Both "LAN Administration" and "Auditors" are towards the top of the structure, where each group can have independent security policies, as explained below.

[5] While it seems excessive, Microsoft claims that the number of objects can reach into the millions.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The large majority of users and computers will be placed in the "Corporate Users" organization unit. And below, "Laptops" and "Contract Employee" can be used to apply the strictest security policies. (Corporate executives could be in either "Corporate Users" or "Laptops" Organization Units.)

Illustration 3: Basic Active Directory for Security with Organization Units (OU)



Note: Users, computers and groups are placed in the OU folders.

W2k's Security Toolbox: *Delegation, Policies & Software Rollout*

With the basics of the components now defined, let's examine the three tools Active Directory provides for security: Delegation of Power, Group Policies and Software Rollouts.

1. Delegation of Power

One of the major drawbacks of NT4 was the lack of administration delegation. Either you were "masters of the universe" by virtue of belonging to the Domain Admins group, or you had little power. While it is true that other management groups do exist (Account Admin, Power User, to name two), it was limited and many organization resorted to giving out membership in the prized Domain Admins group much too easily. This breaks the rule of Powers of Least Privilege, which states that a user should only have enough security permissions to perform their job, and no more.

Windows 2000 gives the ability to delegate powers and rights. With this capability we can now remove all everyday administrators from the Domain Admins group. Instead we will delegate their responsibilities to either specific portions of our network or to specific duties.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Delegation of Full Powers Over Portions of the Network

The first step is to delegate responsibility for only portions of the network as opposed to granting complete control over the entire network. By breaking our Active Directory into Organization Units, we can then delegate the management of that Organization Unit to specific LAN administrators.

Using our previous *Illustration 3* as an example, we would create a new group called "Network Admin" and place all our day-to-day administrators in this group. We would then give this group full management rights to the Corporate Users OU, which would flow down to the two other OUs: Laptops and Contract Employees.

With this design, the new group "Network Admin" could do all their necessary day-to-day tasks of managing the corporate network (add users, reset passwords, and more), but would have NO power over the OUs holding other LAN Administrators or the Auditors. Nor could this group change the powers of any other LAN Administrator, nor any of the built in groups.

[Note: While this paper is a discussion of design considerations, the steps to actually delegate the powers is found with the following steps. Click on **START** / **PROGRAMS** / **ADMINISTRATION TOOLS** / **ACTIVE DIRECTORY USERS AND COMPUTERS**. Then right click on the Organization User object and select **DELEGATE CONTROL** . . . . Next follow the wizard.[6]]

To manage the LAN Administrators group, we would create a second group called "LAN Administrators OU Admin Group." This group would contain only a single user account, which our most trusted Administrator had rights to use. (Depending on our internal security policy, this may be an account with the difficult password locked in a safe.)

We can expand upon this idea by creating independent auditors. In this case we would grant administrative control over this OU to a non-LAN administrator. Then we could grant a specially created Auditors Group, read access to key portions of the network.

Security Design Philosophy: In this example, we have put the user base and the administrators one level down from the top of our domain. This gives us the ability to segment the security powers. The vast majority of our user base will be in the Corporate Users OU branch of the tree. In a larger organization, we would expand the number of OUs under the Corporate Users OU.

Another subtle design point of this example is that the LAN Admins would not have control over the Domain Controllers. Domain Controllers is a default Organization Unit.

[6] Sharick, Paula. "The Active Directory Delegation of Control Wizard." *Windows 2000 Magazine.* September 2000. http://www.win2000mag.com/Articles/Index.cfm?ArticleID=9646&pg=2 (February 8, 2002)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

We can elect to have a subset of our administrators manage these servers by delegating powers over this Domain Controller OU via a newly created security group.

We can take this a step further and elect to either drop our day-to-day servers in the Corporate Users OU, thereby giving our "Network Admin" group full Active Directory control, or we could create a new "Servers" OU at the same level as Corporate Users, LAN Administration and Auditors. Then delegate powers to a smaller server admin group.

It is important to recognize that we have removed almost everyone from the crucial built-in groups of Domain Admins, Administrators and Enterprise Admins. Once again, we may want to employee a user account with a 14-character difficult password controlled through physical access, such a double-keyed safe that would hold the password of these high-powered users in these special groups.

The Enterprise Admin group is new to Windows 2000 and is the most powerful group in the Active Directory. For more specific information on securing the prized Enterprise Domain Admin group, go to:

- http://researchcenter.zdnet.com/data/detail?id=992286116_292&type=RES&x=2083250870 [7]

Other than these special accounts, no one has total power over the whole domain. We have reduced the risk of a single administrator account bringing down our whole network.

Delegation of Partial Powers

Windows 2000 also lets us delegate only partial powers: such limited powers as adding users, managing computers, or reading user account information to name a few. With our same design as seen in *Illustration 3*, we can give a help desk group the ability to change all user account passwords, except for users in the LAN Administration and Auditor OUs. To accomplish this we use the same Microsoft delegation wizards and grant them "password reset" capabilities only on the Corporate Users OU.[8]

This concept can be expanded to our hardware technicians, giving them full Active Directory control over the computer objects in the Corporate Users OU, which still restricts them from managing our Domain Controllers or other servers, unless we have placed the servers in the Corporate Users OU.

---

[7] Barrett, James. "Windows 2000 Active Directory Design Restricting the Enterprise Administrators Group." Lucent Technology White Paper. June 1, 2001. http://researchcenter.zdnet.com/data/detail?id=992286116_292&type=RES&x=2083250870 (February 8, 2002)

[8] Smith, Randy Franklin. "Delegating Password Reset Control in Windows 2000." *Windows 2000 Magazine.* May 10, 2000. http://www.secadministrator.com/Articles/Index.cfm?ArticleID=9190 (February 8, 2002)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Security Design Philosophy This same structure lends itself well to delegating out specific powers to portions of our network. Note that the lower we go in the tree, we can grant additional powers. For example, if we have a sophisticated laptops user-base that needs to manage their own computers, we grant them additional computer rights to their computers in their Laptop OU. (One is then tempted to create two more OUs under Laptop: "Sophisticated Laptop Users" and "Basic Laptop Users." While this author recognizes how tempting it might be to classify our users by ability, he warns about the political sensitiveness of such a strategy.)

2. Group Policies

Group Policies play a central role in managing a Windows 2000 network. A full discussion of how to use Group Policies is beyond the scope of this paper. An excellent introduction can be found at Windows 2000 Magazine's web site[9]:

- http://www.win2000mag.com/Articles/Index.cfm?ArticleID=9169

With group policies, we can control:

- Auditing logs and policies
- Security registry changes
- Enforcement of the Encrypted File System
- Logon Warning Banners
- User's control over the configuration of their computers (such as granting or denying them access to various parts of the control panel).
- The running of logon and logoff scripts
- . . . and much more.

Using our same *Illustration 3*, we could assign a "corporate policy" of warning banners and required screen savers on our largest user base by applying the Group Policy to the Corporate Users OU. More restrictive policies, such as the restriction of use of the floppy drives, could then be applied lower down to our Contract Employees OU, thereby preventing the removal of data from the network on diskettes.

We could have a completely different set of standards to apply to our LAN Administration OU. (Some might argue for even tighter control over the systems since they have elevated privileges on the network, such as a 60-second password-protected screen saver. Others might recommend looser restrictions so that they could accomplish their required task, such as access to a computer's screen resolution). No matter which way we go, the settings applied to the general user population at the Corporate Users OU will not affect the LAN Administrators because of our Active Directory layout design.

Security Design Philosophy: Once again we use separate "branches" of the OU tree for new sets of policies: one set for out LAN Administration OU, another for Auditors and

[9] McIntosh, Robert. "Group Policy and Security." *Window 2000 Magazine.* July 24, 2000 http://www.win2000mag.com/Articles/Index.cfm?ArticleID=9169 (February 8, 2002)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

even another for Corporate Users. Secondly, we apply stricter policies as we move down the tree at the lower levels, as seen with our Contract Employees.

3. Software Rollout

One of the exciting new features of Active Directory is the ability to rollout software through Group Policies based on a Domain or Organization Unit structure. This feature falls more under the category of easy of administration instead of security. But we may have specific security software that we wish to roll out and manage centrally through Active Directory. Examples of security related software would be: antivirus, inventory controls or encryption software. These need to be considered in the design of the Active Directory.

A more detailed discussion on the mechanics of software rollouts from Microsoft can be found at:

- http://www.microsoft.com/windows2000/techinfo/planning/management/swinstall.asp [10]

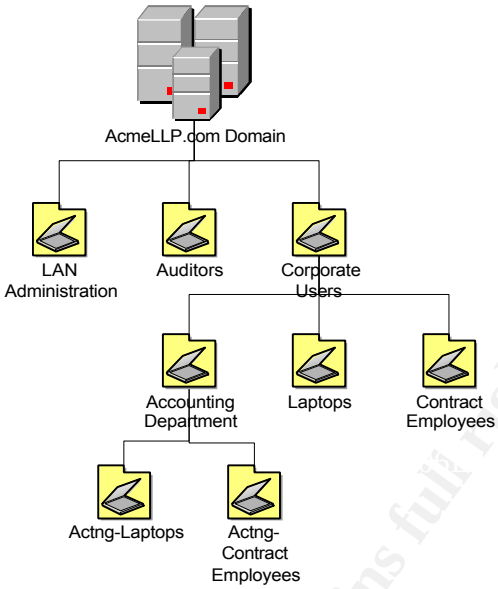
It is of interest to note that designing the Active Directory for software rollout may conflict with designing for security. The reason is that they often have competing needs. For example, we may wish to roll out software for both the Auditors and the Accounting department, but the groups in our example are spread out over two separate Organization Units, and in fact the Accounting Department does not have its own OU.

We can reconcile these needs by adding more layers to our design, as seen in *Illustration 4*.

Illustration 4: New Design with Just One New Department

[10] Microsoft. "Step-by-Step Guide to Software Installation and Maintenance," *Microsoft Step-by-Step Guide.* February 16, 2000 http://www.microsoft.com/windows2000/techinfo/planning/management/swinstall.asp (February 8, 2002)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



However, with this new design, we see how much more complex our plan becomes with just a single new department. While this will help our goal of serving both software rollouts and security, it adds much complexity to the design. And where there is complexity, there is the potential for misconfiguration and security lapses. This art of Active Directory design requires a delicate balance of simplicity and completeness. Competing needs of security and software rollouts makes the design process more challenging. While there can be various configurations that would work, some will be better plans than others.

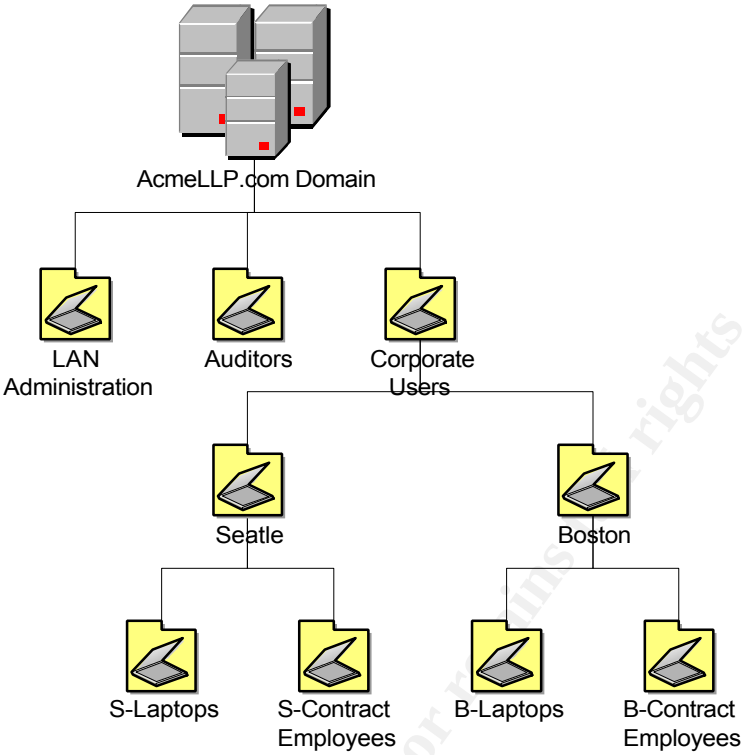
Sites: *The Forgotten Active Directory Object*

At this point we have spent little time discussing the use of Active Directory Sites. A Site is a collection of computers that belong to the same set of IP subnets. It is a way of designating computers that can communicate quickly over a relatively high speed LAN. This tool is used to control replication traffic between domain controllers. While this is an important object and can be used for delegation and group policies, we recommend that Sites be used strictly for controlling communication within an Active Directory forest.

Instead, we suggest that you use location based Organization Units where applicable. For example if you have networks in both Seattle and Boston, you add them in as Organization Units. See *Illustration 5* as an example.

Illustration 5: Sites Turned into Organization Objects

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



Now we can assign full or partial network administrative duties to the employees responsible for each city. The old NT model requires the extremes of either including regional administrators in the ever-powerful Domain Admins group or the creation of new NT domains, complete with trust relationships. Both solutions often violate the rules of granting only enough privileges to accomplish the management needs. Using the new geographical based OUs, we can give each city's remote administrators the power over only the computers in their city that they need to manage.

With this design, we have moved the Active Directory Sites, which are traditionally not seen in the logical design, into our security mapping. This is a cleaner and more manageable arrangement to have all the rules and security settings tied to one logical structure as opposed to spreading it over both logical and physical settings of our network.

Security Objects vs. AD Elements: *Confusion Cleared Up*

All of these new objects introduce confusion on where and when to use each new tool. Let's clarify the differences between a "container" and a "security group."

Container Objects are used to: 1) organize objects in the active directory, 2) provide a target for group policies and delegation of management. These include: Domains, Sites and Organization Units. As we have seen throughout this paper, Organization Units provide the most detailed level of control.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Security Objects (which Microsoft call "Object Class"): Users, Computers and Groups. In Windows 2000 you assign permissions and rights to users, computers or groups. You cannot assign permissions or rights to container objects![11]

What that means is that you cannot delegate the management of organization units to another organization unit. You delegate the management to only a user, group or computer[12].

Conversely you **cannot** delegate the control over an individual user or group. You can only grant powers to manage Domains, Sites or Organization Units, which in turn hold users and groups.

Furthermore, the rollout of Group Policies can only be applied to containers, not security objects. (The irony of the "Group Policies" name is that it is NOT applied to groups, only to Domains, Sites and Organization Units.).

With this clarification, we now understand why we need to create separate "Help Desk" and "Network Admin" groups. The delegation of management was granted over an Organization Unit container and was given to a specific group. A common mistake is to make additional Organization Units when only a group is needed.

As always, we could grant rights and delegation powers to users, but the use of groups is a cleaner approach. It is easer to change membership of a group, then to remove and reapply security to individual users, such as when an LAN administrator retires or leaves.

Security Design Philosophy: To understand how to design a secure Active Directory, it is important to know that: *Container Objects* are used for the management of computers and users. *Security Objects* are used to be given permission and security rights. Security Objects can manage Container Objects. Container Objects can apply policies to Security Objects.

Subtle Side Note on Groups: If you delegate management over an Organization Unit which includes a group. The power is only on the group membership list, not over the users in the group.

To clarify this point, let's reexamine *Illustration 2*. The user Bugs is in the "Management Organization Unit" and is also a member of the "Road Group." The "Road Group" is listed under "Sales Organization Unit." Should we delegate full management of "Sales Organization Unit" to user Wilie, he has the ability to control who is in the "Road Group" group membership list but does not have management over the Bugs user object, even though Bugs is in the group of "Road Group."

[11] Container Objects do have Access Control Lists (ACLs), but once again, the security permissions to work with these objects are assigned to security objects (Users, Groups and Computers).

[12] Assigning rights to a computer brings up new security issue. While it is intriguing that we could put a computer in a physically secure room and only perform LAN management from that PC, it also means that we would have to restrict who logs on to the powerful PC.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Conclusion

Microsoft has given us a true enterprise networking operating system with Windows 2000 and Active Directory. The capability of separation of powers plus organizing our network logically gives us the ability to build a more manageable network where security naturally flows with the structure.

To accomplish this, we must design the domain to meet each networks specific security goals. Through the use of Organization Units, we will be able to create a subset of users and computers that we can delegate management to our day-to-day administrators. Through the combination of full delegation over parts of the network and the use of partial administration powers, we can protect the network by restricting membership in the various Windows 2000 Administrators groups.

While the Active Directory is a complex tool that has no single solution, it can creatively be built to meet each organization's security requirements.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References [This is a comprehensive list. Some of these references were listed in footnotes]

Barrett, James. "Windows 2000 Active Directory Design Restricting the Enterprise Administrators Group." Lucent Technology White Paper. June 1, 2001. http://researchcenter.zdnet.com/data/detail?id=992286116_292&type=RES&x=2083250870 (February 8, 2002

Bekker, Scott. "Active Directory: Microsoft Buttressing Best Practices Docs." ENTNews from 101Communications. December 12, 2001. http://www.entmag.com/news/article.asp?EditorialsID=5120 (February 8, 2002)

Dulaney, Emmett; Sankar, Vijay; Sankar, Sharon E. Active Directory: An Overview http://www.windowsitlibrary.com/Content/155/07/1.html (February 8, 2002)

McIntosh, Robert. "Group Policy and Security." Window 2000 Magazine. July 24, 2000 http://www.win2000mag.com/Articles/Index.cfm?ArticleID=9169 (February 8, 2002)

Microsoft. "Step-by-Step Guide to Software Installation and Maintenance," Microsoft Step-by-Step Guide. February 16, 2000 http://www.microsoft.com/windows2000/techinfo/planning/management/swinstall.asp (February 8, 2002)

Microsoft Training Material. Course 1561. "Designing a Microsoft Windows 2000 Directory Services Infrastructure"

Microsoft Training Material. Course 2150. "Designing a Secure Microsoft Windows 2000 Network"

Microsoft Training Material. Course 2154. "Implementing and Administering Microsoft Windows 2000 Directory Service"

Sharick, Paula. "The Active Directory Delegation of Control Wizard." Windows 2000 Magazine. September 2000. http://www.win2000mag.com/Articles/Index.cfm?ArticleID=9646&pg=2 (February 8, 2002)

Smith, Randy Franklin. "Delegating Password Reset Control in Windows 2000." Windows 2000 Magazine. May 10, 2000. http://www.secadministrator.com/Articles/Index.cfm?ArticleID=9190 (February 8, 2002)

Spivak, Wayne. "Has Microsoft Ever Read the History Books? Windows 2000 Server--a repeat of Novell 4.x?" VARBusiness. July 13, 2001. http://guide.sbanetweb.com/press/varbiz07116001.html (February 8, 2002)

Waddell, Johnny L. "Basic Security Issues of Active Directory" SANS Reading Room. June 11, 2001 http://rr.sans.org/win2000/active_dir.php (February 8, 2002)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**