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.

Basic Security Issues of Active Directory

The old cliche the "network is the system" becomes a reality with Microsoft's Windows 2000 Distributed Services. A single login provides access to applications and resources spread throughout your Windows 2000 network. At first, this might appear to be a security management nightmare, but if Windows 2000 is properly deployed it provides a centralized security platform with many enhanced security features. Kerberos and the Public Key Infrastructure provide networking security opportunities The Microsoft Management Conso...

Copyright SANS Institute
Author Retains Full Rights

AD

Basic Security Issues of Active Directory
Johnny L, Waddell Version 1

Introduction

The old cliché the "network is the system" becomes a reality with Microsoft's Windows 2000 Distributed Services. A single login provides access to applications and resources spread throughout your Windows 2000 network.

At first, this might appear to be a security management nightmare, but if Windows 2000 is properly deployed it provides a centralized security platform with many enhanced security features. Kerberos and the Public Key Infrastructure provide networking security opportunities The Microsoft Management Console (MMC) and enhancements to the Group Policy simplify management while providing flexible control over system and application access.

If you currently have an NT4.0 environment with a large number of servers and domains, then upgrading to a Windows 2000 platform will require careful planning and implementing.

Forest and Domains

A directory service located within the core of Windows 2000's security subsystem, called Active Directory, provides the structure and functions for managing network resources. The Active Directory database contains information about network objects. Objects include network sites, domains, servers, workstations, printers, groups, and users. These objects are placed in domains, which are relevant to a specific group of users. The domains become administrative and security boundaries for the objects. Administrative privileges do not extend into other domains, and each domain has security policies for objects within it. Each domain also has security polices for relationships to other domains.

The domains are arranged in a hierarchical structure called a forest. This structure starts with a domain called the forest root domain. The domain then is arranged in format similar to a family tree, with children domains, parent domains, grandparent domains, and so on. A forest can contain one or more trees.

Any child domain by default has a two-way trust with its parent, which is extended to all other domains in the forest. This is called a transitive trust. When one domain's authentication authority authenticates a user or application, then all other domains accept the authentication because of this two-way trust. Access to resources within the trusting domains is limited to the access controls of each domain. A domain is basically a security boundary.

A trust relationship can exist between a Windows 2000 domain and a UNIX MIT-based realm to provide network access to resources within the domain. A Windows 2000

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

domain controller can authenticate a client in a UNIX MIT-based realm to provide network resources.

Trust relationships can be established between domains comprised of Compaq VMS systems using Advance Server. A Compaq VMS system using Advance Server can also be a member server of Active Directory in a native state.

When Active Directory is installed, the first domain created will be the forest root domain. Careful consideration should be given to given to choosing a name for the forest domain, because once named it cannot be changed. Additionally, in the event of a catastrophic loss of all the domain controllers in the forest root domain, you can only restore the forest root domain from a backup. It is impossible to recover a forest root domain by reinstalling it. Reinstalling it would mean the whole forest would have to cleared and recreated.

The Enterprise Admins and Schema Admins groups only exist in the forest root domain. These are the core administrative and security groups for the forest and have unlimited power. Once the forest is established, access should be limited.

Backing up the Active Directory also includes backing up system state data files.

System state data files includes:

- Active Directory
- Certificate services database (if a certificate server)
- Class registration (database of information about the component services)
- Cluster service (if installed)
- Performance counter configuration
- Registry
- Sysvol (shared folder that contains group policy templates, and login scripts)
- System startup files.

System state data backups can be performed with regular backups. Note that Active Directory does not currently support incremental backups. A restore is only possible from a full backup. You cannot perform a restore from a backup over 60 days old, as this is known as the tombstone lifetime. 60 days is the length of time a domain controller keeps track of deleted objects.

There are two types of restores, nonauthoritative and authoritative. Nonauthoritative is a restore of Active Directory to the state at the time of the backup. After the restore, Active Directory performs a consistency check and maintenance. Then replication from other domain controllers updates Active Directory and the file replication service (FRS).

After a nonauthoritative restore has occurred, an authoritative restore may be performed. Multiple domain controllers in a domain allow an authoritative restore of specific information in the database which has been marked to be updated. Each object

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

in the database is marked with a version number and the domain controller with the highest version number will update the database. These allow Active Directory to be restored to a known state.

Domain controllers can contain copies of users' secret keys, which are used for domain authentication. Syskey can be used to recreate secret keys after a restore of the domain controller. Syskey is a Microsoft encryption tool that uses a 128-bit random key, and is provided to encrypt all secret keys. This key can be stored in a domain controller's registry or on a floppy disk. Microsoft recommends for maximum security to store the key on a floppy.

Native Mode

When you install Active Directory and create the first domain, Active Directory runs in the default mixed mode. This allows support of domain controllers running either NT4.0 or Windows 2000. This allows you to upgrade domain controllers to Windows 2000 as your schedule permits.

When running in the mixed mode, Active Directory is limited to the restraints of the NT 4.0 Security Accounts Manager (SAM). When running in the native mode, millions of objects are available.

When all domain controllers in the forest are running Windows 2000, you can switch to the native mode. Member servers can be at NT4.0, and workstations can be at 98, ME, or NT4.0. Native mode allows for group nesting and universal security groups. However, once you switch to native mode there is no switching back to mixed mode.

Schema

Active Directory's database of all the objects and their attributes, is called the schema.

If the default characteristics of the schema do not meet your organizational requirements, then you can create objects to meet your needs. The Active Directory schema design also defines which objects and attributes will be indexed and what will be published in the Active Directory's Global Catalog.

Objects are organized into groups called containers. A container can be nested within another container.

The schema is distributed among all the domain controllers within the forest. This allows information in the schema about objects and properties to be dynamically available to user applications. It is also dynamically updated when changes or new objects occur. A domain controller, called the schema master, will be assigned to control all the updates within the forest. Only one domain controller serving as the schema master can exist in a forest.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Organizational Units (OU)

Objects can be placed into logical groupings for administrative purposes. An Organizational Unit (OU) is a container object which organizes objects, such as groups, user accounts, computers, printers, and other OUs.

When creating a forest, administrators of existing NT4.0 domains can still perform administrative tasks on their environment while being restricted from the rest of the forest. This is accomplished by delegating administrative control over objects within an OU.

An OU can be assigned to a server or a workstation. This aids in securing a high risk or exposed machine.

Global Catalog

The global catalog is a warehouse of information that contains a subset of frequently queried information about all objects in Active Directory. An example is a user's logon ID, first name, and last name. Exchange 2000 would be utilizing the global catalog for distribution lists, mail addresses and so on.

The catalog resides on a domain server called the global catalog server. The first domain controller created in Active Directory is a global catalog server by default. Other domain servers can also be designated as global catalog servers to balance network traffic. One, or more, domain controllers in the forest root domain will always be a global catalog server. The availability of a global catalog server is crucial to the operation of Active Directory.

Lightweight Directory Access Protocol (LDAP)

Lightweight Directory Access Protocol (LDAP) is a directory service protocol that is used to query and update Active Directory. Each object with Active Directory has a name based upon the LDAP distinguished naming convention. LDAP provides unique naming paths for each object in Active Directory.

Active Directory is an enterprise-wide directory service that is used by both Windows 2000 and Exchange 2000. Therefore, Exchange 2000 uses LDAP to query the closest global catalog server for address searches and message routing. LDAP is not encrypted and is viewable with any network sniffing utility. This is an important security consideration when deploying global catalog servers.

Domain Controllers and Replication

A Windows 2000 network only has 2 types of servers, domain controllers and member servers. If a domain controller fails, the other domain controllers continue to provide network services and information because all domain controllers contain a replica of

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Active Directory. This is accomplished by the use of the multimaster replication component within Active Directory. The domain controllers replicate between themselves. Each server tracks the updates it receives from other servers, and can intelligently request only necessary updates to minimize network traffic.
Member servers can be promoted to domain controllers, and domain controllers demoted to members servers. This was not true under NT 4.0, which forced reinstallation of the server. This aspect is useful for balancing network traffic, or in the event of the loss of a domain controller.

At this time with Windows 2000, a situation exists where security group information could be lost or overwritten if several system administrators are working on different domain controllers simultaneously. This is due to replication latency between domain controllers throughout the network, in particular with remote domain controllers.

If a centralized management is utilized, as recommended in Microsoft's guidelines, this is not an issue. The next version of Windows 2000, known as Windows 2002, resolves this scenario.

Domain Name System (DNS)

The integration of Domain Name System (DNS) and Active Directory is an important feature of Windows 2000. Active Directory uses the DNS naming standard for it's hierarchical naming structure for domains and computers.

DNS and Active Directory namespaces use the same hierarchical naming structure for computers and domains. Thus, the same hierarchical naming structure can represent both DNS nodes and Active Directory objects.

Therefore two rules for DNS naming convention, which should be followed in the creation of Active Directory domains:

- Two children domains of the same parent cannot have the same name
- A child domain can only have one parent domain.

If your organization has a presence on the Internet, the name of your forest root domain should be registered. An example would be the SANS Institute, which would use sans.com as a DNS namespace for the Internet, and sans.com would be the namespace for their Active Directory forest root domain

Active Directory requires that DNS servers support SRV (Service Resource Records). SRV records map domain controllers to network services. When a domain server boots up, it registers information about the services it provides to the DNS servers.

Windows 2000 uses SRV records to locate:

- A domain controller in a specified domain or forest.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- A domain controller at the same site as the client.
- Global catalog servers.
- Service providers of LDAP.
- Kerberos V5 services.
- A shared printer or folder.

Clients need at least one DNS server to locate a domain server for the log on procedure. The client would contact all domain servers returned by the DNS server and logon with the first domain controller that responds to the log request.

Beyond Windows 2000

Active Directory 's capabilities extended beyond just managing a Windows 2000 environment. ADSI (Active Directory Service Interfaces), previously known as OLE Directory Services, provide management of multi-platform products. ADSI 2.5 incorporates providers for Novell NetWare Directory Services (NDS), NetWare 3 bindery (NWCOMPAT), and LDAP. LDAP opens up the door for a common management platform for network vendors to utilize.

Compaq's Advanced Server/Pathworks V7.4 plans Windows 2000 interoperability, including Active Directory Integration.

Conclusion

Active Directory is a flexible and scalable management platform for distributive network resources and applications. Careful planning can provide a structured security environment that is transparent to your users. Poor planning and implementation can lead to a disaster.

© SANS Institute 2003, Author retains full rights

McIntosh, Robert. "AD's Operations Master Roles." 21 August 2000.
URL: http://www.win2000mag.com/Articles/Index.cfm?ArticleID=9782

Williams, Robert. "The alleged Active Directory Security Flaw." 13 April 2001. URL: http://www.windows2000advantage.com/tech_edge/04-16-01_alleged_flaw.asp

Microsoft. "Windows 2000 Advanced Server Documentation." Microsoft TechNet. 23 April 2001
URL: http://www.microsoft.com/windows2000/en/advanced/help/

Microsoft. "TechNet Active Directory." Microsoft TechNet. 17 January 2000
URL: http://www.microsoft.com/technet/win2000/intro11.asp

Microsoft. "Active Directory Service Interfaces Overview." Technical Resources. 22 March 2001 URL:
http://www.microsoft.com/windows2000/techinfo/howitworks/activedirectory/adsilinks.asp

Posey, Brien M. "Backing Up and restoring Active Directory." Active Directory "How to" Articles. 23 June 2000. URL:
http://networking.earthweb.com/netsysm/nettroub/article/0,,12474_623561,00.html

Compaq. "OpenVMS Version 7.3 New Features and Documentation Overview." OpenVMS Documentation. 30 March 2001.
URL: http://www.openvms.compaq.com/doc/73final/6620/6620pro_008.html

Compaq. "PATHWORKS/Advanced Server Interoperability With Windows 2000." Solutions and Applications. 1 September 2000
URL: http://www.openvms.compaq.com/pathworks/pw_win2000_stat.html

Internet Security Systems, Microsoft Windows 2000 Security Technical Reference. Redmond: Microsoft Press, 2000

Microsoft Corporation, MCSE Training Kit: Microsoft Windows 2000 Active Directory Services. Redmond: Microsoft Press, 2000

© SANS Institute 2003, 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**