Windows 2000 Active Directory Security Overview
Michael Gnau
September 13, 2000

Active Directory Overview

Active Directory consists of trees and forests. The tree contains multiple domains and network objects while domains contain network objects. The forest is a collection of trees joined together. In Windows NT the domain was a separate entity requiring the security to be applied to each separate domain. Active Directory allows the security to be managed from the top down allowing for a consistent security policy through out the organization.

Authentication

The administrator has several options for user authentication within AD. The default authentication method is Kerberos. This method provides better security, efficiency and interoperability than Windows NT authentication. AD also provides for authentication by Public Key Infrastructure (PKI), smart cards and the older Windows NT standard NTLM. All of the available authentication methods can be used at the same time, by using policies in AD you can specify which type of login that is required for individual users or groups of users according to your security needs.

Kerberos

This is an industry standard authentication scheme developed at MIT and is used on many Unix systems. This authentication method not only verifies the clients right to access the network it authenticates the server to the client. When a client PC requests authentication to a server the request goes to the Key Distribution Server (KDC), the KDC responds to the client with the requested servers key, the client sends this key along with its request to the intended server, the server then authenticates the user. All of this communication is encrypted for use over an unprotected network.

PKI

PKI authentication is normally done to authenticate external users. The external user must have a certificate, this can be from a trusted certificate authority or can be issued from the certificate server that comes with Windows 2000. The certificate of the external user is mapped to a user account setup for external users, AD uses these mappings to allow access to resources that the user is entitled to use.

NTLM

NTLM is used to authenticate users that are using PC's that don't have Windows 2000 installed on them. This authentication method is also used when computers outside of a domain, attempt to access the domain. NTLM requires a separate authentication for each resource on the network that the user attempts to access, where as with the Kerberos authentication the AD uses single sign-on.

Trusts

To allow users the use of single sign-on domains have to trust each other. In Windows NT these trusts were one way non-transitive trusts. This created the need to create trusts manually between domains. This was relatively easy as long as the number of domains remained small. The number of trusts increased exponentially as domains were added. AD uses a transitive trust relationship, which is established by default within a tree. These trusts are two way implicit trusts between the parent domain and all of the child domains. The child domains trust each other based on the fact that the parent domains trust the other domains. Transitive trusts between trees in the forest can also be established, but they must be established manually. AD also supports one way non-transitive trusts to allow the use of Windows NT servers within the tree.

Security Policies

When a user logs into AD an access token is created, these tokens consist of an individual Security Identifier (SID), a group SID for each group the user belongs to and user rights. When the user tries to access any AD object this token is compared to an Access Control List (ACL) to verify the user has authority to access the object.

Security is set in AD using group policies. This allows the administrator to set a uniform security policy across the domain. These policies can be set at the highest level of the organization and pushed down to all users. Some of the types of policies that can be set are password policies and audit policies. It is also possible to set a base security policy for the corporation and give domain administrators the right to alter only portions of the policy.

Delegation of Authority

AD is designed for large spread out organizations. This could create administration problems if they maintained the Windows NT style of domains. When maintaining a large network with Windows NT each domain was administer separately, maybe from one workstation but still separately. With AD all domains within a tree can be administered as a single entity, while still having the ability to delegate control of a container object to a user or group. An example of this would be, if your company had its headquarters in Chicago and remote offices in New York and Los Angeles. The tree would be located in Chicago with each sub office having a domain connected by a WAN. You as the enterprise administrator have the ability to administer the complete tree but you only want the sub offices to be able to administer there own users. You would set a group policy for each office giving them the required rights. It is also possible to set group policies that only give users permission for specific operations such as adding new users or adding new computers to the domain.

Encryption

While not a true part of AD Internet Protocol Security (IPSec) is an important part of Windows 2000 security. IPSec provides integrity, authentication, confidentiality, and nonrepudiation for IP packets, you can define IPSec within security policies. These policies can be configured to use IPSec only, use IPSec if available or don’t use. This can be used to secure communications through out the network. For example, communications across the network from Payroll to the server can be required to use IPSec to encrypt the communications to prevent ease dropping. AD also provides transparent encryption down to the file level. This encryption can be used with any application since the O/S is doing the work.

Conclusion

Active Directory is a very complicated set of services that allow complete control of a Windows 2000 network. It has some shortcomings such as Microsoft’s lack of clients for other operating systems plus the fact that it is still new and few people really understand AD. It is still a giant step forward for corporations that have standardized on Microsoft’s network.

"IT Introduction to Windows 2000 Security", January 5, 2000, Microsoft Corporation
url: http://www.microsoft.com/WINDOWS2000/guide/server/features/secintro.asp

Smith, Randy F, "Windows 2000 Security Gains", Winter 1999, Windows 2000 Magazine, url:
http://www.ntmag.com/Articles/Index.cfm?ArticleID=7434

Proctor, Paul E, "Security and Windows 2000 Active Directory", March 1999, Windows NT Systems
url:http://windows2000.about.com/compute/windows2000/gi/dynamic/offsite.htm?site=http%3A%2F%2Fwww.ntsystems.com%2Fdb_area%2Farchive%2F1999%2F9903%2F303c3.shtml

"Windows 2000 Security Technical Overview" August 17, 2000, Microsoft Corporation
url: http://www.microsoft.com/windows2000/library/howitworks/security/sectech.asp

"Active Directory Architecture" October 12, 1999, Microsoft Corporation url:
http://www.microsoft.com/windows2000/library/howitworks/activedirectory/adarch.asp