Global Information Assurance Certification Paper

A Comparison of Directory Solutions for Windows NT /2000

1. Introduction

There have been many articles comparing the differences between Microsoft Active Directory and Novell's eDirectory. While most of these have focused on features sets and performance, very little has been done to compare the security aspects of the two major competing directories. The directory is a central repository of configuration and security information. Security of the contents of the directory is paramount since it contains all the relevant system information. The ease of use of the directory and its interface to the hardware and software controlled by the directory are also important. A successful hack of a directory would grant the hacker unlimited access to all network resources! The systems that protect the directory must be as robust as possible since it includes the user interface for the directory administrator. A bug ridden or poorly designed user interface for configuring the directory might introduce vulnerabilities or configuration errors.

2. History

Microsoft introduced Active Directory as part of the Windows 2000 system. Active Directory adds the ability to manage all users, computers, and security settings of Windows 2000 systems. Microsoft did not start development in a vacuum. Many of the features and functionality of AD is based largely on Novell's NDS and LDAP. Microsoft even copied the naming convention of NDS, which is installed on the SYS: Volume, or "Sysvol" in Novell parlance. This is also the name of the share on Windows 2000 for the directory. There are several key features that AD adds for managing servers, workstations, and users to enhance overall system security these are:

IPSEC
Group Policy
Trust relationships
Common interface for management
Digital Certificates and certificate management
Support for smart tokens
Key protection, exchange and recovery
File system encryption
Extensible database
Open standard support
Single Sign-on
Auditing

Novell's eDirectory started as the directory for all objects on a Novell Netware 4 network back in 1994. Novell's practice of coding in ANSI C facilitated the decision to port NDS to other platforms and eventually spin it off as a separate product dubbed

eDirectory. The new version of the directory no longer requires a Netware server to store the directory.

There is one fundamental difference in the implementation of the directory in security. Novell eDirectory runs as a service that stores all access and control data, and pushes them to the server and clients. This works best on native Netware, but does function on the supported platforms. Novell has planned a new, major release of their core operating system, Netware 6 that is scheduled to be out in mid October 2001. This release will include many new features, which I will include here if they are likely to have an impact on security.

3. Directory as an element of security.

Directories are important for network usefulness and security as proven by Banyan with their Street Talk for Vines. Since that now defunct product introduction, every major platform offers or has in development a directory and directory enabled applications. The goal is to simplify administration by placing all the resources of a network in one area. It also makes locating network services or resources easier for the connected devices since all the necessary lists of available services and connections are in one place. But what does this mean for our interconnected and Internet attached systems? If all of the network resources are listed in one place, we have given a potential hacker a single "keys to the kingdom" target.

Key questions:
Is the directory secure?
Can it be replicated securely?
Can the directory be configured to enhance security of the devices under its control?
Is the User Interface to the directory well enough designed to limit chances of human error?
Does the directory provide management of all necessary resources?

Both Novell and Microsoft have taken different approaches to the same goal with each company building on their non-directory enabled systems. From that foundation, the programmers of the directory software had to pick some basic rules of how the directory can control security. There are two basic models of directory security called static and dynamic inheritance mode. Inheritance defines how security is passed between one object in the directory and another. In a static model of inheritance, rights at each level in a directory tree must be explicitly defined, while in a dynamic model rights are designed to flow down the tree. Each model of inheritance of rights has validity for computer networks, but the differences do play a factor in how secure each would be on any particular network. Static inheritance tends to be better in large, decentralized networks where security is under the control of isolated, local administrators since security does not automatically move between organizational units. Dynamic inheritance directories would favor a more centralized network with administration coming from one group.

There are always exceptions to how each model could best apply, and both Microsoft and Novell programmers were cognizant of that. Each group has added

functionality to their respective models of inheritance from borrowed features of the other. In a static inheritance model, administrators may want to apply a change more universally than the model would easily allow. Microsoft included the powerful concept of "Group Policy" as a way to allow a directory change to be applied to more than one object at a time. Novell programmers faced the opposite problem of how to block changes from flowing down to objects in their directory tree. Their solution is "Inherited Rights Mask" which will block a change at a higher level in the tree from traversing all objects or branches below that point. It is clear that while the core design of each system is very different, the basic needs of the system administrators to manage their networks will define how a directory must be implemented.

4. How they compare

A. Moving to a Directory and Installation

Microsoft has drawn some criticism for making the migration from Domains to Active difficult since it cannot act as a drop in replacement for a Primary Domain Controller.[1] This migration from a Windows NT 4.0 domain architecture to an Active Directory system may be less secure since there are now more chances for a system administrator to make a mistake in migrating security. Active Directory is an application that runs tightly integrated to Windows 2000 and still has roots in the domain model. It requires servers to handle file and print functions, and access security to be controlled by the server file system. [2] Access to the file shares is still maintained by NT File System (NTFS) with Active Directory providing a Graphical User Interface (GUI) for the settings of NTFS.

Novell's migration path operates as a backward compatibility or direct replacement system. They have maintained this upgrade plan since very early in their product line, back at version 2.15. The migration utility allows for the existing server to be overwritten with the updated operating system and installs the directory. This type of upgrade is generally not a good path. In practice the server that stores the directory needs more space on the SYS: volume than would normally be set up, and needs more performance from the processor and memory. The better upgrade is a migration to a different server. The migration utility runs a new server install, creates the directory, and copies all the data from the old server. This allows for easy disaster recovery from a failed migration since the original server is basically intact and has the advantage of easily upgrading server hardware at the same time. There is a slight security advantage to eDirectory on the migration because it is a more mature utility with less chance of user error.

Both Microsoft and Novell offer utilities to help migrate from each other's platforms. From a practical standpoint, cross platform migrations are possible, but not recommended. What usually happens is that the directory winds up clogged with old users, confused security rights, mixed groups, and generally the worst from each of the platforms instead of granting the minimal rights to a user or group necessary to get the job done.

eDirectory and Active Directory can be managed in a centralized or decentralized fashion. eDirectory is better suited generally for centralized IT management. Since it is based primarily on the dynamic model, all changes administrators make to objects, automatically flow from that point down. This single location provides eDirectory with reduced risk of error. Active Directory is a bit better in a distributed management environment. To facilitate operations that must span domains or organizational units, Microsoft introduced Group Policy Objects. Unfortunately, even with the Group Policy Objects, security information must be stored on the individual servers along with the possible risks that dispersion could introduce. [3]

Planning is often overlooked when selecting a directory for a network. More often it is monetary, salesmanship, or even mental inertia that are used to select a directory to install. Yet, a good plan is the first step of any effective security system. Administrators given the task to make this selection should start with a large whiteboard and diagram how a directory should look based on corporate structure, physical location and departmental functions. They must decide who needs to see what and where, and use that plan as the pseudo directory first; then, investigate how to adapt the currently available directory solutions to the model developed.

B Directory authentication

Probably the most common use for a directory is users authentication to network resources. Authentication is typically done with a username and password, but security is only as good as the weakest user password. New authentication methods have been introduced, as security needs increase. Two examples of these methods are token based and biometrics authentication where an electronic key or characteristics of the user are used in place of or to augment usernames and passwords. Active Directory and eDirectory both support authentication services through their own unique set of APIs so neither has an advantage over the other in security.

Client authentication has changed dramatically between Windows NT and 2000. NT was limited by its use of the older LANMAN standards for its core and by concerted efforts of hackers. NT depends upon the SAM database on the Primary Domain Controller (PDC) so the loss of the PDC causes the administrator substantial efforts to promote a Backup Domain Controller to the PDC in order to have a fully functioning security system again. Windows 2000 has adopted the Kerberos authentication model developed by MIT. [4] Kerberos is a proven, reliable if somewhat bandwidth intensive authentication based on proving identity once only, then sending encrypted information between servers. This is ideal for a network that may have many servers and directory aware applications because all the authentication of the user to a server, after the first server, is done encrypted and behind the scenes from the viewpoint of the client. Because Kerberos is a published standard, Active Directory can theoretically support single sign-on to Microsoft and non-Microsoft servers. But, there have also been vocal critics, mostly in the Linux community that Microsoft did not follow the Kerberos authentication protocol accurately enough to interact with non-Microsoft servers which may cause the Single Sign-on to fail. Kerberos depends upon Public Key Infrastructure (PKI), and it is only as secure as the keys and digital certificates of the PKI system. It requires the system administrator to configure and maintain PKI to gain these security features.

The standard eDirectory authentication is based on secure and well-understood encryption standards from RSA for a username and password. Novell recognized that only username and password authentication was inadequate and has since released Novell Modular Authentication Service version 2.0 (NMAS2). With NMAS2 installed, Novell supports authentication by: [5]

X.509 version 3 certificates compliant with PKCS#12 format of digital certificates.
Entrust implementation of X.509
Universal Smart Cards
RADIUS
LDAP (with iChain product installed)

eDirectory allows the administrator a choice in the source of the certificate authority: to use an internal implementation of digital certificates, or certificates from Entrust, Baltimore, and Verisign with little concern for interoperability.

Single Sign-on is a separate, optional product from Novell that differs from Active Directory's included Kerberos single sign-on system even though again they do much of the same authentication task. Novell's eDirectory implementation modifies the directory schema to include fields for application information, key storage, and Security Domain Infrastructure Key (SDIK). The SDIK is a key exchange protocol to establish secure communications between the servers supporting the applications for single sign-on. Novell can charge for their Single Sign-on because it has a much wider range of applications supported. The current list includes:

Internet Browsers
Windows Applications
Mainframe Terminal Emulators
Lotus Notes
Entrust
Microsoft Access
Peoplesoft 7
SQL Integrator
Vantive
Groupwise 5.5 Enhanced or Groupwise 6

Novell has a list of APIs and sample code to create "Connectors" so any application for which a company has the source code can add support for the Single Sign-on software package.

Novell has a potential problem with the current client based authentication method used. The Novell client requires null user sessions to authenticate to a Windows NT or Windows 2000 workstation from which the client is running. There have been several exploits of null user sessions to garner information about a workstation where null user sessions are allowed. Starting in Netware 6, due out mid October 2001, the workstations no longer need to have a monolithic client loaded to authenticate to the network and directory. Instead there is a web-based interface and a native file system

access support infrastructure. This interface bears some concern in the future since the Netware based file servers will have all of its existing security issues plus security concerns for CIFS and NFS as well as any other sharing technology that may be added later.

Microsoft does have an advantage in directory authentication because they support a strong, standard based authentication system out of the box. Novell has lagged behind in this, depending upon their proprietary client a little too long. This will need to be reviewed again after the release of Windows XP and Netware 6.

C. Directory Replication

For the directory to work on a network, changes made in one physical location may impact another server or office. Each copy of the directory must be able to receive and send changes to the other servers containing directory information. The Novell eDirectory replicates over an IPX or IP port, with IP the currently preferred method. It takes advantage of the dynamic inheritance simplicity of replicating only changes so it is very robust in that only any values changed in an object or group of objects are replicated across the network. This model could potentially be more "chatty" system when performing many directory operations like adding multiple users, but each replication request is fairly small and can easily flow through low bandwidth connections. There are no known problems with integrity of the directory during replication operations when changes are made from multiple locations because of the time synchronization protocol established between servers and because only the changed values are transmitted. eDirectory has the ability to control where portions of the directory reside, how it is synchronized and when. Any eDirectory tree can be subdivided based on organizational units called partitions, with each partition containing a master copy that resides on one server and as many replicas on remote servers as desired. The remote replicas may be read/write or read only types depending upon the need for administrators at the remote locations to make security changes to objects in the tree. At any time, a read/write replica may be converted to a master replica for load balancing or for replacing a replica on a failed server. In very large trees, it may be desirable to have one dedicated server to be a master for one or more partitions.

Active directory still has ties to the Domain Controller structure of Windows NT, and each domain controller promoted to Active Directory contains the entire directory. There are currently no provisions for subdividing Active Directory. A change to a single attribute of an AD object requires the entire object to be replicated to all servers. Near simultaneous changes to the same object has been demonstrated to cause problems with Active Directory. If two administrators on two different Domain Controllers modify the same object, even if it is different properties on the same object, only the administrator who finished last will have their changes in the Active Directory. One extension to Active Directory is the Global Catalog, which aids the browsing of multiple directory trees joined in a single forest. While this speeds the client's location of objects on a large network, it increases replication traffic and can slow the servers. Microsoft has tried to address this with Site Links. With these links, the administrators can define the frequency and direction that the directory changes are propagated between servers, even the protocol or communication may be specified.

Both directories have good replication systems with Microsoft's the more versatile and Novell's the more robust and bandwidth efficient. This difference is primarily the result of the design constraints of the directories from each company. Still, Novell has a slight advantage in replication and continuity primarily because it does not have the risk, no matter how small or documented, that administrators could cancel changes they have made.

D. Directory Security and Integrity

No matter which Operating System (OS) is used, at some point the directory files must reside on a server somewhere on the network. Protecting the file system is critical to the protection of the directory. Microsoft places the directory on a system-controlled share to limit access to the directory. Novell places their directory on a hidden directory _Netware on a Netware server's SYS: volume and on restricted directories on the Unix variants. Microsoft adds encryption at the file system level to protect user files. However, the Active Directory cannot be stored on an encrypted file system because all types of clients need to access the share for authentication. Novell does not use an encrypted file system but does have a directory enabled data protection product called iFolder that will encrypt files before committing them to disk on all of their supported platforms. The iFolder option also adds support for accessing files remotely over HTTPS, for synchronizing folders, and for setting storage limits for the client.

Both Microsoft and Novell have counted on obscurity for security in their directories. Both are closed systems with available APIs and utilities for third party integration. Novell's eDirectory has stood the test of time and a dedicated hacking project called Pandora. [6] Pandora has only found six exploits in eDirectory/NDS, four of which require physical console access. Novell has also acted promptly to patch these holes in their security. Active Directory has remained secure to date, with hackers most often using many other security problems in Windows 2000 to gain administrator account access and hence Active Directory access. Windows 2000 systems installed with Active Directory and IIS are especially vulnerable due to all the security problems with IIS 5.0.

E. Directory User Interface and Scripting.

Both Novell and Microsoft allow changes to the directory through command line utilities. This makes scripting operations and support for multiple management platforms possible. Microsoft's utilities are compatible with their WIN32 platform operating systems. Novell has taken a more open approach with support for Windows NT/2000, Linux, Solaris, Tru 64 Unix, and they are adding more still. IT is possible to add scripts for the command line operations. Microsoft supports Vbscript, Jscript and DOS with the ability to add support for other scripting languages. Netware only supports Netbasic and Java on the Netware server and DOS from the clients. [7]

F. Backup, Recovery, and Repair of the Directory

Backup operations of a robust, distributed and replicated database, at first glance, seem to be a waste of time since the internal replication of the database assures that the failure of any one server will not significantly impact the performance of the directory. However, that reasoning does not take into account the wide spread disruptions that may come from natural disasters like fires, floods, or from poorly trained system administrators. Each directory vendor offers some type of backup and restore functionality out of the box. Normally, most directory vendors work closely with third party software developers to support the developer's enhanced backup package such as Verita's Backupexec, and CA's Arcserve. In practice, it is probably best to select one of these third party vendors' solutions, but here is a comparison of the included directory backup software.

Active Directory can be backed up with the Windows Backup Utility [8] but the restore process can only be done by specifically booting the domain controller into directory service recovery mode through selecting F8 at boot time. There are several settings in the Active Directory that will influence how old a backup can be used to restore the directory, specifically the "Tombstone Lifetime" entry that defaults to 60 days. Restore of older copies is possible, but it is a more complicated procedure. The trust relationships between servers can be lost during recovery operations and may require the administrator to redefine NTLM trust relationships. [9]

Novell created a basic infrastructure called Storage Management Services (SMS) which is for backup and recovery across their entire Netware product line. The SMS agents give seamless access to the eDirectory and file system without having to worry about the state of the directory during backup or restore operation. The Netware backup utility, SBCON, uses a primitive, C-Worthy text interface program instead of a GUI. While it is very good at backing up the eDirectory, it is not intuitive or easy for the administrators. A third party backup solution should be considered part of the cost of implementing a Netware based eDirectory installation. Novell has released two other SMS compliant command line packages for backup and recovery options on eDirectory. They are SMSENGN for Windows NT/2000 and ndsbackup for Linux, Solaris, or Tru64 Unix. Even though the interface is command line or text based, the restore operations are very flexible. It is possible to restore the whole tree or any part of the tree on down to a single leaf object.

Diagnosing a directory error is an important part of deciding what might need to be restored from tape. In some cases, repairing the database is a better option than restoring from a backup. eDirectory includes the utilities DSTRACE and DSREPAIR, which are very good at finding errors in the directory database and diagnosing communication errors between replications. The eDirectory utilities can be run with the network online. DSRepair will lock the eDirectory files during parts of the diagnosis and repair process. Any user that tries to authenticate during the locked period of the repair is placed in I/O wait. This is a much simpler system than required for repairing Active Directory. The Active Directory is robust enough that repair operations are possible and may be preferable to a restore operation. [10] Most of the repair options for AD require at least one reboot of the Domain Controller where the directory resides. Novell definitely has the advantage here in uptime during directory repair and diagnosis that could help avoid the need to restore from tape.

5. Directory enabled applications to enhance security

Because the directory is essentially a replicated and distributed database, it provides a fantastic framework for building any application where centralized storage of data is required. All widely used directories provide for extensions through schema. Schema is a user definable added field or record type for the directory's database and can be used to enhance the functions of the directory or can allow the directory to function almost as a database engine for user coded applications. It is not recommended to use the directory as an application database since the amount of data created in most applications would overwhelm distribution and replication channels of just about any directory!

A. Desktop Control

Both Active directory and eDirectory have a mechanism for setting preferences on desktop systems from the directory. Microsoft uses their existing infrastructure of the Windows 2000 platform to control the desktop deployment. There is also a Windows Active Directory client for the older Microsoft operating systems that adds some of the functionality. Microsoft then uses the scripting capabilities of VBScript or Jscript along with the command line utilities to control all options of Windows 2000 and XP client workstations. Novell has developed a whole toolkit for desktop control called ZENWorks (shortened from Zero Effort Networking.) This package is an additional cost in using the NDS for desktop control but there is also added value. ZENWorks does not share the limitation of functioning on one platform or full functionality on only one operating system. ZENWorks can run a scripting language and also control an application scripting language, Network Application Launcher (NAL). This enables very fine desktop control that can even replace roaming profiles in NT and 2000 systems. The application control scripts of NAL are also not operating system dependent, One script will work on several families of platforms. The NAL also will manage application installs through snapshots for each supported operating system and tools for creating snapshots and scripts.

B. Web Server

A directory is not an obvious choice for managing web servers. As server farms grow and load balancing is used in more environments, it makes more sense to control the web server functions centrally. Windows 2000 is a good application platform supported by many developers so it is no surprise that it is commonly used on the Internet as a web server. In light of the recent spate of worms that affect IIS, the Gartner Group has recommended users of IIS investigate other web server platforms. [13] Active Directory does not directly control IIS but the Microsoft Management Console interface is similar for the user and Group Policies can be used to push IPSEC settings to the web servers. Novell does bundle WebSphere as a web server with their core Netware 5.1 product that gets much of its configuration information from the directory. Novell has even provided

sample code on how to access the eDirectory from the browser using HTML or IIS active server pages. [11]

C. Name Services and IP address assignments

DNS and DHCP are another set of standard network applications that are perfect candidate for moving to the directory. The table of IP addresses and MAC addresses are easily stored in a directory and can be distributed among many servers yet still controlled from one console. Microsoft's implementation of DNS, called Dynamic DNS is tightly coupled with Active Directory, which depends upon the extensions to DNS for proper operation of the replication and other services. This makes it much more difficult to use DNS with Windows 2000 in a mixed environment. Novell treats DNS and DHCP as separate modules that can be used or ignored as desired. NetWare's faster directory replication allows DHCP to be distributed among many servers for greater redundancy and speed.

D. Digital Certificates, Digital Signatures, and PKI

Public Key Infrastructure (PKI) and digital certificates and their management is a fairly new application for the directory and has been driven by the need to improve security through verifying identities of users or computers in information exchange. PKI and digital certificates are difficult concepts to understand which has slowed their acceptance and use. They are very important to security and all major software vendors are trying to find some way to implement PKI services and there are even a few companies dedicated to helping business deploy and manage PKI and certificates. The core of PKI are the public and private keys that allow users or computers to securely authenticate their identity and establish secured communications over a public network. The practical implication of this is you must always have the keys and certificates available or your users cannot authenticate and communications between systems may be unavailable. By moving PKI management to the directory, there is a much greater chance that the important storage and retrieval of keys will be available even if a single server or communications link fails since the directory will replicate the PKI information at the same time it replicates and distributes itself. Since PKI is a standard the ability to differentiate features is somewhat limited in scope, with most of the differences in initial configuration, key storage, and maintenance for the system administrator. A few of the differences between eDirectory and Active Directory of PKI may affect security. Active Directory on Windows 2000 has a more feature rich implementation of PKI that adds certificate revocation, Netscape certificate requests, certificate hierarchies, user choice of databases for certificate storage, SET compliance, and LDAP certificate storage. [12] Certificate revocation is important to invalidate certificates that may have been fraudulently created, or expired. Certificate hierarchies are important in the Windows 2000 implementations of PKI. The key storage under Windows 2000 resides on a single server. The system administrator can generate the root certificate with a very long expiration period and install it on an old computer and use it to generate child certificates with shorter expiration periods. The root certificate server may be taken offline and

physically secured, protecting the root key and passwords. Novell's eDirectory uses a completely different approach by storing the certificate information and keys as properties of the directory object, which have been issued the certificate. The advantage to security in this model is that the certificates are effectively backed up to any server and available from any server without the administrative tasks of building a hierarchy. The certificates are also protected by the same robust encryption used by the directory. Overall, the flexibility of the Microsoft PKI implementation is better than what is currently offered by Novell. The imminent release of Netware 6 is likely to require re-evaluating this

E. Secure communication

Microsoft's use of IPSEC is commendable and is presently not matched by Novell except in specialized cases of some network interface cards. Windows 2000 has the IPSEC functionality built into the operating system protocol stack where Active Directory Group Policies can then easily control it. NDS also can script changes to Windows IPSEC but with more effort on the part of the network administrator. Neither directory has an advantage when deploying IPSEC to any older versions of Windows. In the older versions, IPSEC is usually implemented in the NICS hardware and driver.

Novell uses their own client to connect to the native Netware servers with the workstation. There is an option for encryption on both the server and client and a negotiation system for determining the encryption levels. This system has been compromised by the Pandora Project on all but the highest security setting on the client and server. Novell responded to this threat with a free add on to Netware 5 called, Novell International Cryptographic Infrastructure (NICI) to implement 56 bit DES encryption and 1024 bit RSA key management.

6. Auditing

No matter how secure a system may appear to be, there is always a chance some hacker will find an exploit or use social engineering to gain access to the systems or directory on the network. A good audit trail is essential to confirm suspicious activity as a security breach and to maintain evidence for prosecution. Ideally, the audit and network administration duties should be separated so no one person controls the network and has access to the audit logs. The financial services industry has separation of these duties as a requirement for FDIC insurance. Audit can be internal to the directory or operating system or it could be a third party application running on a separate system. The "perfect" auditing system would be configurable on what is audited and on how long the audit history is kept. It should support multiple levels of audit security so more than one auditor could view the history, but only the senior auditor can make changes. And the history would track all those changes. Auditing requires the network administrator to strike a balance and that balance is not static. Whenever there is any significant change in the network topology or services, or if there is even a hint of suspicious activity, the audit settings may need adjustment.

Like designing a directory, the auditing parameters should be done before auditing is activated on the system. As a rule of thumb, NT and Windows 2000 servers and domain controllers should have some level of auditing active. On the Netware platforms, servers with any outside access or servers with a replica of the eDirectory or NDS are good candidates to have auditing enabled. Decide how long the logs should be retained online and offline. Start with a written policy on auditing. If your company has a record retention policy and a new employee handbook, start with these since they will define what has to be kept, how long it must be kept, and who has restrictions on the activities they may perform on the job. A well thought out and written policy will help generate the procedures to audit the network and guide you in applying those procedures to the audit settings of your directory.

The Microsoft audit is based on a domain and file system model with separate auditing settings for each one possible. File system auditing is done at the folder level and will work on both NT and 2000 servers with small differences. Auditing of the Active Directory is done at the domain level. To activate auditing, the administrator must go to the properties of the domain and navigate to the Group Policy and from there down to the Audit Policy. Select the object and define in the object properties whether you want to log success, failure, or both for that item. Turning on the auditing of Active Directory is a little convoluted, but reviewing the logs is much simpler. The security logs are readable in Event Viewer and can be exported from there to other programs with some third party tools. Exporting to a database or spread sheet is desirable because it make searching through the log files for specific items much faster and less taxing on the network administrators who are normally very busy to begin with.

Novell implements their auditing through the "Full Service Directory Model" where user logins, open files, modification of files, and user object changes are all recorded in the log files. The DSTrace provides much of the useful directory audit history, but only as a text file. In a Netware based directory implementation, the included AUDITCON utility will turn on server auditing on almost any supported version of Netware. AUDITCON is extremely thorough in recording events, and it requires separate passwords and user accounts for auditors to enforce the separation of duties. The only reason for not using Netware's auditing is the amount of storage and processor power required. Novell recommends that eDirectory customers on non-Netware platforms use one of several third party audit tools. The recommended list from the eDirectory manual includes Bindview, Blue Lance, and Netpro.

Novell definitely has a superior auditing solution for the directory and for the Network Operating System. In any work environment where auditing is a criticial business function, like financial services, it is better to run eDirectory on Netware. If auditing is not as important, then eDirectory on another platform with one of the third party tools is almost as good and has a similar cost. As Active Directory is a new product, the auditing functions should be re-examined with the release of Windows XP.

7. Directory Management Console

A directory can get large quickly since there is potentially an object for every printer, user, server, workstation, application, public key, and email account. The

directory management console has to allow the network administrator to effectively view and edit all of these objects. The interface must be intuitive for the majority of people managing the systems.

Active Directory management is a plug in for the Microsoft Management Console. The advantage to this type of configuration is that the network administrator has one tool to control the directory, the servers, and common system wide applications like disk defragmenting and virus scanning. The down side is that the commonality of the core Microsoft Management Console menus and screen layout might limit some of the choices the interface designer has.

Novell started with a Windows application, NWAdmin for managing the directory and has continuously improved the tool up through release 5 of Netware. A new administration tool was added for the launch of the eDirectory since it no longer needs to be installed on a Netware server and the DLL set used for NWAdmin just will not run on many of the platforms supported by eDirectory. The solution from Novell was to extend the work done for NWAdmin and port the administration console to Java for its "write once run anywhere" feature. The result is called, "Console One" and it does have a clean, efficient interface for directory management but one that has been plagued by performance issues. Performance has improved with release of Console One 1.2 code and improvements of the Java Virtual Machine that it runs on. Console One like Microsoft Management Console, is extensible through snap in code.

Both consoles do the basic administration jobs required to maintain the directories. Novell's is the older of the two and it shows in the layout and efficiency of the user interface. Navigation to objects and modifying properties of objects is much easier than the Microsoft Management Console which requires more navigation and combinations of right and left clicks to manage objects. Console One also has an advantage of running on multiple platforms while Microsoft Management Console only runs on Windows 2000 stations.

Some may prefer to use third party management utilities for directories instead of the ones shipped with them. [14] Some examples of these that have received positive reviews in the press are:

Patchlink for Web Interface for both directories
Directory Resource Administrator from NetIQ for MS Active Directory
BvControl reporting tool for AD, eDirectory, and Unix

These could be especially useful in a mixed environment where there are Windows 2000, Novell, and /or Unix servers.

8. Conclusions

I started this paper with the goal of recommending either eDirectory or Active Directory as the more secure to use in a typical enterprise. After this item by item comparison, it is evident that there is no single best solution. On the positive, both products are mature enough with enough features to enhance security that there is no reason to delay migrating to a directory-based infrastructure. The ability to centrally

control network resources and user controls is very good as a cost justification in reduced load on network administrators.

The first recommendation I can make is to plan right up front what the directory should look like. Start with the corporate structure as a broad framework for creating the directory. Modify that diagram with geography so you do not have authentication traffic traveling over low speed or high latency links. Consider what groups in the company share information and try to move them closer together in the tree map. Consider creating separate Organization Units for types of objects. In a very large tree some containers will have so many leaf objects that it becomes difficult to see what is in that container. (This works better in eDirectory than Active Directory.) Once you have the directory mapped out, keep it and update it. Diagnosing any problem with the directory is much harder if you do not have a good understanding of what is in place.

Once the directory is planned out, examine what you may have in place for hardware. Administrators planning out new networks have the greatest range of choices. Both Microsoft and Novell offer small business solutions as complete kits to build a directory enabled network complete with shared Internet and email services. Novell's solution differs from the full version because it uses a slightly older version of the directory, NDS 8 and has a simplified administration console geared for the limited number of objects supported on a small business network. Microsoft offers Small Business Server for up to 50 computers. Both solutions are perfectly suited for a small business launch. This example highlights one of the fundamental differences between Active Directory and eDirectory.

The Microsoft solution will effectively manage all resources on the network as long as all the systems are Windows 2000 based. The Group Policy Objects and Active Directory settings will not easily apply to any non-Windows 2000 systems. Novell's Small Business Server takes a more open view of the network and will support everything from DOS clients through Windows 2000 Professional workstations equally well. Microsoft's directory implementation favors a homogeneous network while Novell eDirectory favors a heterogeneous network. As soon as an Active Directory network must support systems other than Windows 2000 (or Windows XP when released), compromises on features must be made. In a mixed NT and 2000 environment, Active Directory must run in compatibility mode and some features that aid security are lost or at least limited to only the Windows 2000 computers.

Novell eDirectory would than appear to be the perfect solution since it can run natively on a Windows 2000 or NT server. While it can run on a majority of workstations, some of the security features that may be deployed to the workstation require the purchase of additional software. To have a secure eDirectory implementation that spans the network, licenses for Novell Single Sign-on, ZENWorks, and a tape backup software package must be added. There is a great deal of functionality here, even greater than what Active Directory supports in a Windows 2000 only network, but those software licenses add cost and the initial setup requires much more time than needed in the Windows 2000 only network.

Network resources must be available during the business day and with the advent of the Internet, business might be 24 hours a day. Based on the directory monitoring, repair, backup and restore operations, eDirectory should be the first choice for 24 by 7 businesses. The Novell only solution might not work in an Internet based business

environment because many applications are written only for Microsoft IIS which means Windows NT or 2000 web servers. The eDirectory can manage the Windows based web servers, but not as well as Active Directory can.

The final result is that neither directory nor network operating system can be all things to all networks, or network administrators. The knowledge of the administrator must also be factored into the decision of which directory to implement. A long time MCSE with years of domain management will find adapting to Active Directory easier than eDirectory. A long time Netware 3 or 4 administrator will find the migration to eDirectory much easier to understand as well.

Both directories are secure with only a few exploits found after many years of running eDirectory or NDS. Active Directory has also held up much better than most Microsoft products with very few security problems. Running a network with both directories may seem wasteful of administrator time and server resources but might help security through the concept of defense in depth. One example is an Internet business running a web site and a back end network that might each have their own directory trees. If somehow the Active Directory on the web server farm is compromised, the switch to a Netware based eDirectory on the internal network might present an insurmountable barrier to the hacker who is not likely to know both systems in great depth. The best security will always come from administrators planning first than selecting the best tool for the task at hand, even if it means using more than one tool.

Sited Sources

1. http://www.zdnet.com/zdnn/stories/comment/0,5859,2715213,00.html
2. http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2433130,00.html
3.http://www.extremetech.com/article/0,3396,s%253D1034%2526a%253D1559%2526app%253D2%252ap%253D3,00.asp)
4. http://www.isi.edu/~brian/security/kerberos.html
5. http://www.nwconnection.com/2001_02/pdf/whats.pdf
6. http://www.nmrc.org/pandora.htm The Nomad Mobile Research Center has temporarily shut down after September 11th
7. http://www.novell.com/products/nds/details.html#requirements
8. http://support.microsoft.com/support/kb/articles/q216/9/93.asp
9. http://support.microsoft.com/support/kb/articles/Q216/2/43.asp
10. http://www.microsoft.com/windows2000/techinfo/reskit/samplechapters/dsbi/dsbi_add_zgsr.asp
11. http://developer.novell.com/research/appnotes/2001/september/07/a010907.htm
12. http://www.novell.com/competitive/netware/overview.html
13. http://www3.gartner.com/DisplayDocument?doc_cd=101034
14. www.nwfusion.com/reviews/2000/0813bg2.html

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 13, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**