Global Information Assurance Certification Paper

A Plan for Migrating to Microsoft Windows 2000

SANS GIAC Securing Windows NT Practical Assignment
Deirdre Perkins-Moore November 2000

Table of Contents

Disclaimers

This document was written to fulfill requirements for the practical assignment portion of the GIAC-NT certification. It merely scratches the surface of all of the planning and analysis required for a successful Windows 2000 migration.

All efforts have been made to ensure the accuracy and completeness of the information contained in this document. This document is meant to serve only as a sample guide and is not a complete plan for migrating to Windows 2000. A thorough and complete analysis as well as courses on Group Policy is recommended.

All recommendations should be tested throughly before implementing them on production systems.

1 Before Getting Started

Before migrating to a Windows 2000 environment you will need to perform a proper analysis of your organization's environment. You may want to consider the following questions:

- Do you have network security plan or strategy?
- What kind of hardware platforms will be migrated?
- What resources are available including consultants?
- Do you have adequate budget and time?
- What area will be migrated first, servers or workstations?
- How can you migrate with the least amount of disruption?

1.1 Network Security Strategy

Upgrading from Windows NT 4.0 to Windows 2000 requires a great deal more planning and strategizing than upgrading from Windows 3.51 to Windows 4.0. Windows 2000 has basically the same Windows NT 4.0 architecture with some new security functionality. Because of these new components, it is important to carefully consider how the components will be used before implementation. How will these new security features fit into your security strategy?

Table 1 Comparison of NT and W2K Security Components (Schultz, Gene 2000)

Capability	**WNT4.0**	**Win2K**
Authentication	NTLM	NTLM, Kerberos, other
Security APIs	CryptoAPI, SSPI	CryptoAPI, SSPI
Object access control	NTFS permissions	NTFS permissions (NTFS5)
Encrypted network traffic	PPTP, SSL, Secure DCOM	PPTP, SSL, Secure DCOM, IPsec, L2TP
Administration	SAM database, Security Configuration Manager	Security Configuration Manager, Active Directory, smart cards
Auditing	Event Logger	Event Logger, Active Directory
File Encryption	None	Encrypted File System
Certificate/Key Management	Certificate Server, SSL	Certificate Server, SSL, Active Directory

.

1.2 Determine Network Logon and Authentication Method

Kerberos is Windows 2000 major method for authentication, but it can use NTLM for backward compatibility. You will need to decide on the type of network authentication method that is best for your organization. Windows 2000 supports NTLM logon (same as NT4), Kerberos logon, smart card logon, or certificate mapping such as LDAP. Keep in mind that NTLM is not available in Native mode. There is Kerberos support for other clients such as Win98, but this requires that you install the Directory Services client.

1.3 Strategies for Developing a Network Security Template

There are a lot of different security features in Windows 2000 and they require a lot of analysis and planning. Before you can create an network security template or strategy you will need to have an information security policy. If you do not already have one, the book Information Security Policies Made Easy is a good one. Next you will want to create your network security strategy and keep in mind the checklist in Figure 1 taken from *Configuring Windows 2000 Server Security*:

Figure 1 Checklist for the Network Security Plan (Shinder 1999)

Assignment	Comments
What universal groups are necessary?	
What global groups are necessary?	
How will we utilize the built-in local groups?	
What local groups are necessary?	
What filters are necessary for group policies?	
What policies are required for the Active Directory objects?	
What policies are required for the file system?	
What policies are required for registries?	
What policies are required for system?	
What policies are required for network accounts?	
What policies are required for local computers?	
What policies are required for Event Logs?	
What policies are required for restricted groups?	
How will we perform network logon and authentication?	
What approach do we take with smart cards?	
What approach do we take with certificate mapping?	
How do we implement PKI?	
How do we implement the Encrypting File system?	
How will we provide authentication for remote access users?	
What approach do we take with IPSec?	

What approach do we take with secure e-mail?	
How do we protect the Web site?	
How do we implement code signing?	

Regarding PKI, unless your organization is an all Microsoft shop, I would not use the Windows 2000 PKI solution.

1.4 Develop Network Security Migration Plan

Plan to transfer your NT4 security over to your WINDOWS 2000 security. Some steps that you may want to consider when migrating NT4 security to WINDOWS 2000 security are:

- Obtain a listing of current settings
- Set up an access framework, then translate NT4.0 groups to Windows 2000 groups
- Map Group policies to Systems policies and User Manager for Domain policies
- Check that all security related settings are enforced only by Group Policies
- Use the "least privilege" principle when migrating NT4.0 domain administrators to Windows 2000
- Use security templates to set initial security levels
- For each group, translate Windows NT4.0 permissions to Windows 2000 permissions

2 Budget Factors

2.1 Hardware Platforms

If your environment is anything like my organization's environment you probably have a wide assortment of computing platforms. You will need to ensure that Windows 2000 will run on the range of hardware platforms that you have. The RAM requirements for Windows 2000 servers increased to 128 MB minimum RAM, with a minimum 5.2GB of hard disk space and a 500mz minimum processor speed. Windows 2000 Pro clients hardware requirements start at a Pentium 133 MHz with at least 64MB of RAM and around 2GB of hard disk space.

2.2 Consultants and/or Migration Tools

For medium or larger networks, it is probably a good idea if you hire a consultant to aide in the creation of your migration plan. Remember If your organization is going to hire a consultant, make sure that the consultant is at least Windows 2000 Certified. Oh, and don't forget about the 5 million dollar or E/O clause in their contract.

Third party products may also be necessary to manage a smooth migration. BV-Migrate by Bindview is a tool that you may want to invest in.

3 Plan a Domain Structure

3.1 Setting DNS or name resolution process

Windows 2000 uses DNS as a naming convention. DNS is hierarchical and the first Windows 2000 domain that you create will be the root domain. Develop names for your domains and determine how these domains (if you have more than one) will fit together. Will you divide them geographically, by division or by function? You need to be really sure about naming conventions prior to deployment. Windows 2000 uses DNS type names and if you have a name and then change your mind, you will have to reinstall Active Directory to change the domain name.

3.2 What will the DNS infrastructure be?

If your company is like many companies, it uses some type of Unix DNS servers. If you're using a version of Bind that supports SRV records (RFC 2052), dynamic updates (RFC 2136), and supports machine names with underscores, then you can continue using your Unix DNS servers. If not then you either have to upgrade your DNS server to a version with RFC 2052, RFC 2136, and underscore support, or configure a Windows 2000 system as a DNS server.

If none of these options are available to you then you can 1) create a sub-domain (eg. W2k.acme.com), or 2) create an internal Windows 2000 DNS server that is not connected to the Internet.

Effectively utilizing Dynamic DNS (DDNS) will depend on what type of DHCP and DNS servers are used. Because Microsoft includes additional options in their RFC standard, some combinations work better than others. You could have Unix DHCP and DNS servers and the Windows 2000 servers will be okay. However you may run into problems if you have a Unix DHCP server and Windows 2000 DNS server. And, I haven't tried this, but theoretically a Windows 2000 DHCP server and Unix DNS server should work provided they follow the RFC standards.

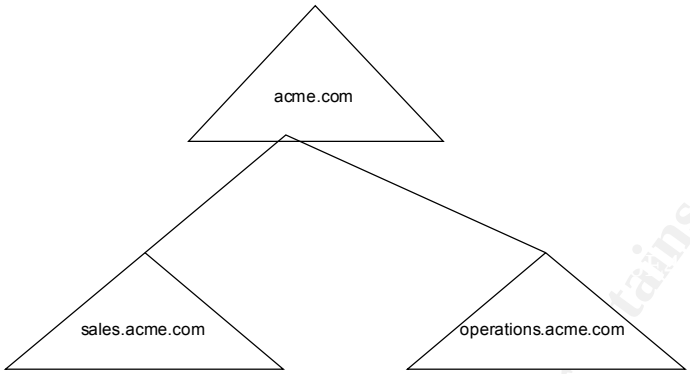
3.3 Collapse Multi Domain Structure

The transition from a Windows NT single domain model to Windows 2000 domain, is a lot simpler than the transition from a Windows NT multi domain model. Therefore, if it is at all possible, collapse your Windows NT multi domain into a single domain model before migrating to Windows 2000. Migrating the SAMs is simple enough, but permissions and shares are where you will spend the most labor.

3.4 Windows 2000 OUs Domains Trees and Forests

In Windows 2000 a domain is a group of servers or workstations that are part of one unit of management. Each domain has its own security policy settings. Many of the reasons for creating a multi domain model with Windows NT4 do not exist for Windows 2000. The political concerns that caused people to use the multi domain model can be resolved by creating sub-domains. These sub-domains can be organizational units (OU) or domains. OUs can be used to divide domains. These OUs can correspond with

geographical (e.g. east.acme.com or west.acme.com) or organizational (e.g. sales.acme.com or (operations.acme.com) boundaries depending upon your structure.



Domains in Windows 2000 are primarily an issue of controlling replication, not security and administration. A simpler approach would be to use OUs instead of domains, but if your corporate policy or business model dictates that subdomains are domains, then you can create a tree. A tree is a two or more domain in a hierarchical domain structure where one of the domains serves as the root or parent domain. The naming convention will look the same as the single domain with OUs but you'll have to be aware of trusts relationships.

A forest is two or more domains where one domain is not a DNS subdomain of the other, but they still trust each other.

3.5 Organizational Units

Determine what needs to be an OU and what needs to be a Domain. Sometimes a domain may be an administrative burden and you may need to create subdomains or organizational units. OUs can contain users, resources, groups, shared folders and other OUs from the domain. Keep in mind that the purpose for putting these entities into OUs is to assign group policy objects, delegation of authority and for making searches more efficient.

4 Group Policy Strategy and Design

4.1 Security Group Design

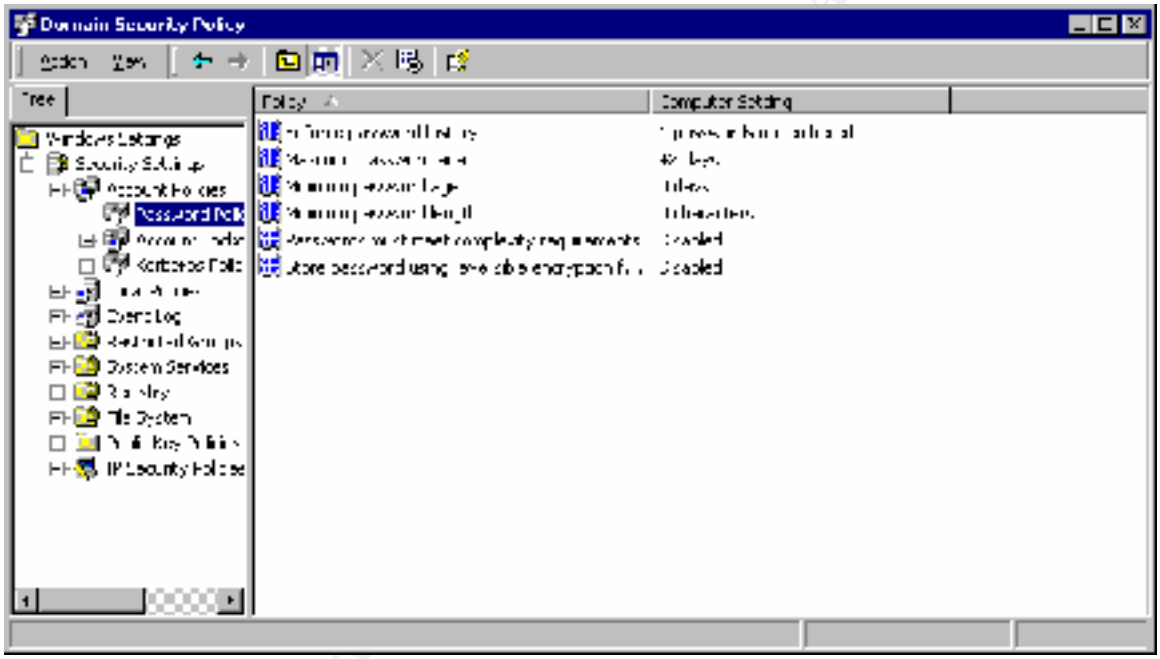
There are three types of groups in Windows 2000, universal, global, and local. Universal groups are a new type of group. Since Windows NT4 does not recognize Universal Groups, it can only be used in Native-Mode Active Directory. Universal groups can contain users and groups from every domain within any forest. Global groups

are somewhat equivalent to global groups in Windows NT. Local groups can contain users or groups from any domain that is trusted.

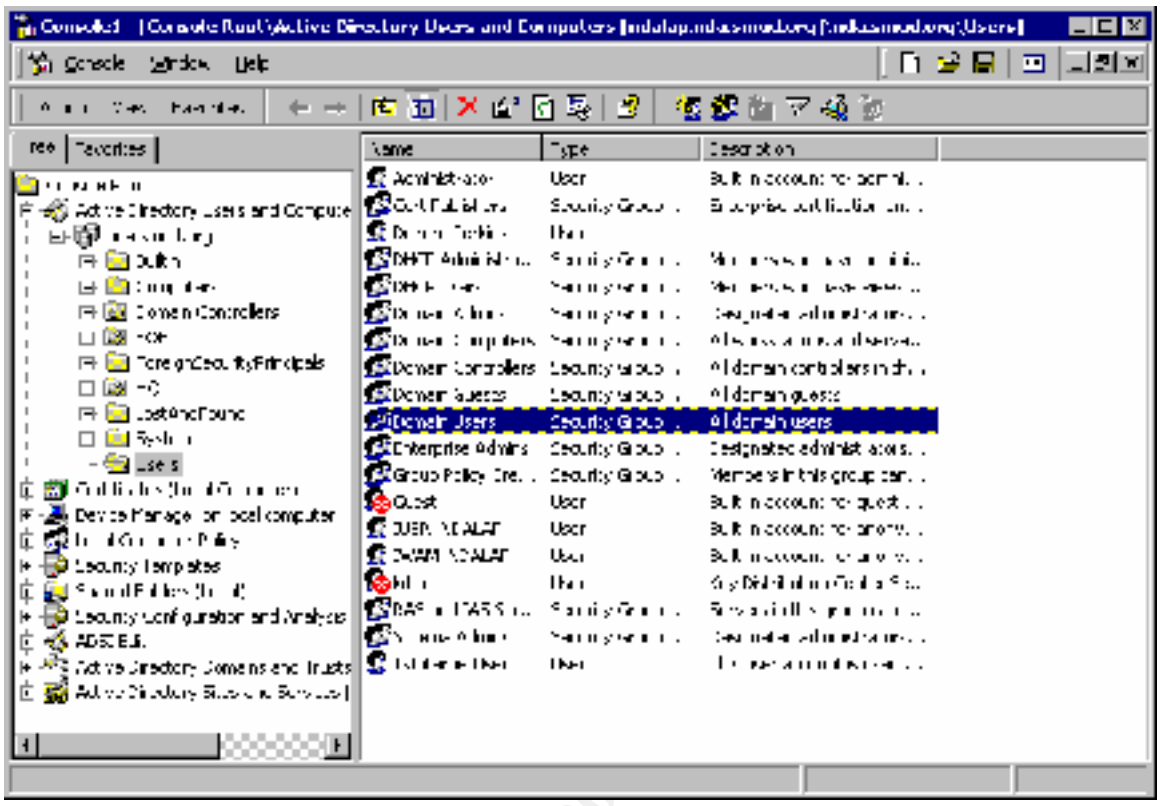
Your security group design should detail how you will use existing groups as well as any new groups to be created. One grouping method may be to make a top layer group for organizational units (OUs) and then a second layer might be functions within a department. You could also create a group for functions that span OUs.

4.2 Develop Group Policy Strategy

Group Policy can be used to change the configuration of computers and user preferences automatically.



The Windows 2000 Security Configuration Tool Set is an easy to use program that will allow configuration of domain, OU and local security. The Tool Set allows the administrator to get a handle on the configuration and management of the Windows 2000 security scheme. The administrator can group the Tool Set components together into a single Microsoft Management Console (MMC) and mandate security for the entire enterprise from a central location.



Limit policies because they must be downloaded to each computer during startup and to each user profile during logon. Windows 2000 comes with a number of pre-defined templates that can be modified. For a detailed explanation of all Group Policy options, see the Group Policy documentation that accompanies the Windows 2000 Resource Kit.

The group policy feature is a very powerful and complex tool. My suggestion would be to take a class on Group Policy and then create your strategy.

5 Plan for time synchronizing

Once you set up the root domain, you will need to establish an authoritative timeserver there fairly soon. Next you should remove the Windows NT master timeserver's status as master timeserver. Include net time in Windows NT logon scripts for hosts that have not yet been upgraded to obtain the correct time.

6 Getting Started

6.1 Testing

Once you have a team of folks who are knowledgeable about Windows 2000, you should start to plan your migration. We've stressed that Active Directory will require a complete network design overhaul, but this is not the only component of the planning process

6.2 Backup

Test your plan in a test lab if at all possible. And as with any major change or migration, make sure that you have adequate backups before you get started. Also make sure that you have a back out plan.

6.3 Client Migration

Start your migration slowly in phases over several months. What will you migrate first, clients or servers? If you are doing a phased in approach, I would recommend targeting the migration of clients to Windows 2000 Pro first. If your plan is to do a full-scale migration all at once, then I would not recommend this approach unless you have a small network of 50 node or less. Remember, you can also use Terminal Servers to emulate Windows 2000 Pro if the client operating systems cannot feasibly be upgraded.

6.4 Server Migration

After your clients have been migrated to Windows 2000 Pro, now it's time to migrate your domain controllers. Migrate your PDC first and then migrate the BDCs. So that you can have some type of load balancing, I would recommend migrating one domain at a time and every server within the domain all at once. This will cause the least disruption. . If you have several BDCs and application servers that will all be set up in similar fashion, you might want to get the Windows 2000 Server Resource Kit. The kit has a utility called the Setup Manager that lets administrators create a list of answers to all of Windows 2000's setup questions.

When all these machines are running Windows 2000, you're ready to move into Native Windows 2000 mode. After you upgrade the domain controllers, you can start implementing the items in your security plan such as group policies.

Conclusion

Your Windows 2000 migration should be gradual. But the final step of moving to a native Windows 2000 environment only affects DC servers. Windows 2000 will default to a mixed-mode environment whenever it performs an upgrade from a Windows NT PDC. It won't stop the show but it would be a good idea to establish your DNS server prior to running DCPROMO on your PDC

Even though Windows 2000 is very different from Windows NT, investing in proper training and testing is probably the most important step towards a successful migration to Windows 2000.

References

Shinder T., Shinder D., White L., *Configuring Windows 2000 Server Security,* Syngress Media 2000

Schultz G., *Security in Windows 2000* (Sunday, October 15, 2000). The SANS Institute GIAC Training 2000

Fossen J., *Windows 2000 Active Directory and Group Policy* (Sunday, October 22, 2000). The SANS Institute GIAC Training 2000

Minasi M, Anderson C., Smith B. Toombs D., *Windows 2000 Server, Second Edition*, Sybex 1999.

Wood C., *Information Security Policies Made Easy, version 7*, Baseline Software, 1999.

http://www.bindview.com/products/bv-admin/ntmig.html

Rist, Oliver, Windows 2000: A Six-Step Migration Plan, http://www.internetwk.com/lead/lead012600.htm

Yegulap, Serdar and Finnie, Scot; The Essential Guide to Installing Windows 2000 http://www.winmag.com/windows/guides/win2000/

Last Updated: May 23rd, 2017

Upcoming Training

SANS Cyber Defence Canberra 2017	**Canberra, Australia**	**Jun 26, 2017 - Jul 08, 2017**	**Live Event**
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 06, 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 OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**