Global Information Assurance Certification Paper

GCWN Practical Assignment

Version 3.1

Option 1 – Design a Secure Windows 2000 Infrastructure

January 2003

Prepared by: John M. Shaw

Table of Contents

List of Figures

List of Tables

Introduction

This document describes a secure Microsoft Windows 2000 Active Directory network for GIAC Enterprises. GIAC is a business specializing in the sale Healthcare industry software.

GIAC Enterprises has a campus headquarters located in Overland Park Kansas and about twenty operational offices located worldwide. This document focuses on the design considerations for GIAC's internal network and is comprised of the following main elements:

Company Overview – A brief description of GIAC's History, it's various business units and departments, and their basic computing requirements.

Network Design and Diagram – This section details GIAC's internal network. Included are the physical/geographical layout of GIAC's business centers, location of key servers and basic network architecture.

Active Directory Design and Diagram – Active Directory logical designs are included with diagrams of both the Domain and OU hierarchy as well as the site structure A brief explanation of the role of each logical object is also included.

Group Policy and Security Design – This section outlines the suggested Group Policy Objects to be created and the policy settings associated with them. The emphasis of this Group Policy design is on security.

GIAC Enterprises Company Description

GIAC Enterprises started on a park bench in Kansas City, Missouri. Three friends in the software consulting industry were working for a large, structured, inflexible (in their opinion) company. They yearned for the flexibility of running their own company and the opportunity to provide products and services to clients quicker than a larger company. Since they were already in the field of healthcare services that was the vertical market they chose to pursue.

GIAC's first product was a system to keep track of the pharmaceutical orders, supply, and accounting. As the years went on they found themselves competing with products in similar areas. The products they sold against were specific to the service involved. After ten years the products were helping hospitals, medical offices and insurance companies in ordering, supply, payables and receivables. But these systems proved very costly and the overhead involved with combining each system into a single bill was becoming unbearable to clients. A client had to look at multiple systems to bill a patient for a stay in the hospital. Radiology had their own system, the pharmacy, Internal Medicine, not to mention the logistical arrangement for rooms and meals and services.

Inspired by a story of a long-time employee and her issues of seeing multiple doctors for the same thing, having to rehash her medical history until she was ready to explode, and the lack of communication she saw between doctors, nurses and hospitals, the three founders went out on a limb, invested millions into a 'product of the future' pushed the architecture of an electronic medical history, something that could be carried with a patient and would be given exactly the same to each nurse, doctor or hospital one saw.

The company is divided into several lines of business. The Corporate Operations includes Human Resources, Finances, Information Technology and the Vision Center. Product Engineering is concerned with development of new product, updating existing product and supporting client issues. The Sales and Marketing folks (while are spread out all over to cover the larger part of the United States with the idea of being only a couple of hours from any given client at any time. The Advanced Technologies Group is concerned with research and development. Within the healthcare industry the faster technology can be implemented in the community the more opportunities the professionals have to save or better patients lives.

As the company grows a natural tendency is to eliminate competition or speed up product development by acquiring competitors or subject matter expert companies. This has been a recent struggle for the Information Technology team on transitioning those offices into the corporate infrastructure and providing the correct level of security for support personnel in the field. The list of branch offices is located here:

Location Name	Abbreviation	Location Name	Abbreviation
Overland Park	KSOP	**Stamford**	CTSTM
Minneapolis	MNMIN	Cowles	NYCOW
Irvine RGR	CARGR	5 Penn Plaza	NY5P
Irvine ESB	CAESB	East 44th NY	NYE44
Emeryville	CAEMV	18th Street Manhattan	NY18
Denver	CODNV	Ft. Washington	PAFTW
Media PA	PAMED	Atlanta	GAALT
Detroit	MIDET	Clarksdale	MSCLK
Malibu	CAMLB	Houston	TXHOU
Indianapolis	ININD	Chicago 35E	IL35E
England	UKLON	Chicago 29N	IL29N
MID	CAMID	Chicago Wabash	ILWAB
Olathe	KSOLA		

Table 1 - Branch Offices

Network Design and Diagram

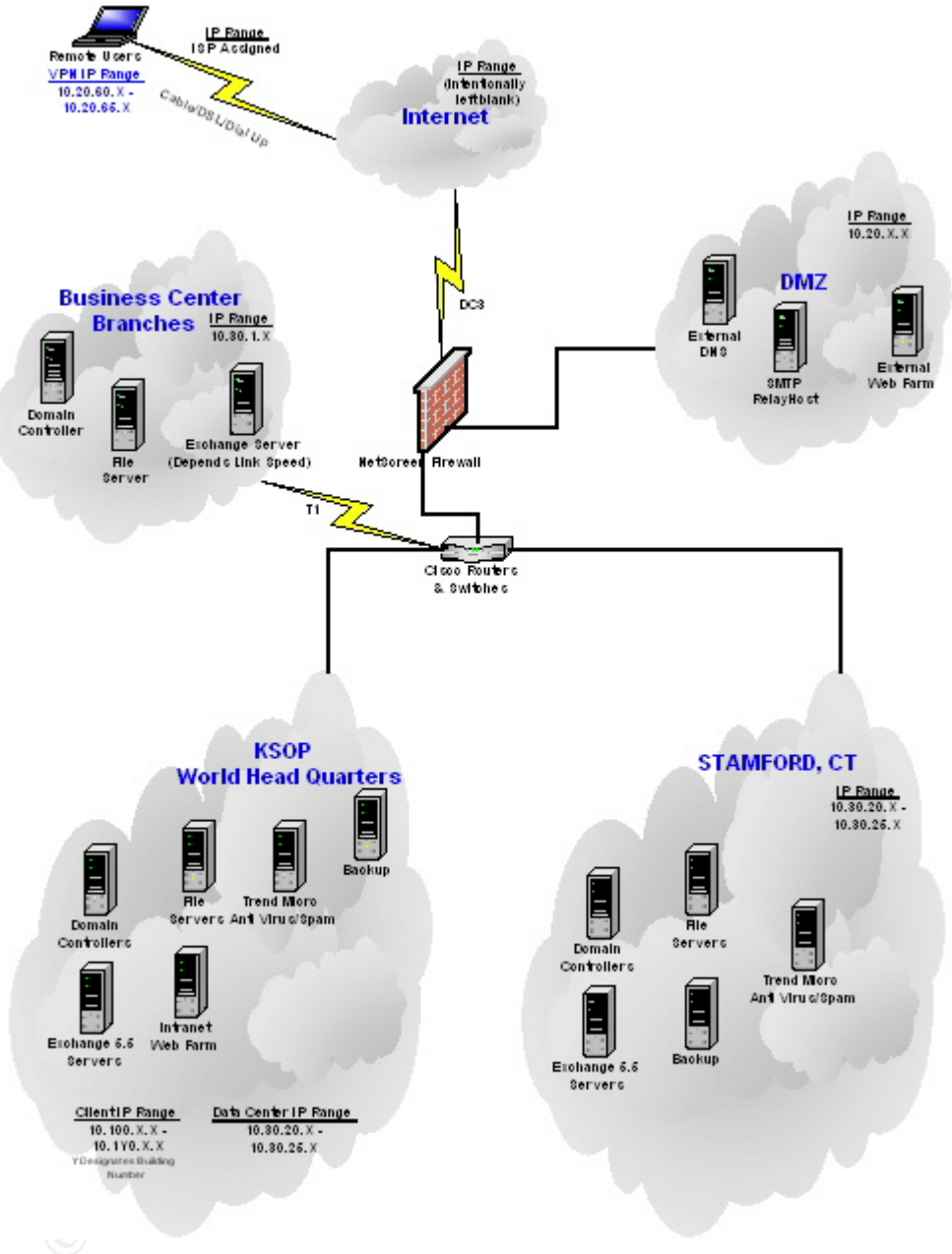


Figure 1 - Physical Network Diagram

Network Overview

GIAC's world head quarters hosts the company's external internet presence with a web farm located in the DMZ. The connection to the internet is a DC3 and serves as the only connection to the internet from any branch office in the company. There are also servers in the external DMZ for hosting our registered DNS domain name and a smart relay-host for sending and receiving internet email.

GIAC's network consists of a world head quarter's campus in Kansas, an alternate fail-over site in Stamford, Connecticut and additional business centers and branches. There are three classifications of branch offices. The first is Stamford which has some redundancy and hosts email servers for locations on the East Coast. There is a systems engineer on staff along with support technicians. The next designation is a branch with lower bandwidth to warrant having their email hosted locally. The last classification is the most common and maintains a domain controller and file server only. Each branch has a support technician, either an associate of GIAC or through a third party vendor.

Server Hardware Assumptions

All servers have Windows 2000 operating systems with Service Pack 3. A tool from Ecora called Patch Master is used to keep the servers up-to-date with patches and hotfixes. A maintenance window is scheduled for all servers and communicated to the groups using them when implementing those changes. All servers have their operating system physical drives with RAID0+1 and the file storage as RAID 5 for recoverability and fault tolerance. The RAID0+1 drive is divided into the c:\ partition for the os and the d:\ drive for program files. The RAID 5 volumes are for data storage. All file systems are formatted with NTFS. All systems are backed up regularly and a rotation schedule keeps weekly, monthly tapes offsite in a secure location.

DMZ - Web Farm

The web farm is a group of servers using a hardware load balancing (HLB) network appliance to balance the load between servers. The (HLB) allows for immediate reaction to security threats within the IIS product. Each server can be brought down, patched and brought up without affecting clients access to the site. Further security considerations include[1]:

- The IIS Admin site is not installed during setup
- Internet Printing is disabled
- The default web page is disabled
- All unnecessary services and subsystems are disabled
- NetBios binding are disabled
- SSL encryption is required on the Outlook Web Access site
- The Microsoft baseline.inf and IIS incremental.inf[2] are used during server build
- Lodckdown Tool is used after server builds.

DMZ - SMTP Relay Host & DNS

The SMTP relay host is running sendmail and using the anti-spam features of the Black Hole List to keep UCE (Unwanted commercial email) from users mailboxes.

---

[1] Fossen, Jason, Securing Internet Information Server 5.0, Sans Institute, 2002

[2] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/windows2000/staysecure/secops03.asp

The DNS servers are running a Primary and Secondary external presence for GIAC.com. The servers are configured not to accept dynamic updates. Log files are routinely checked for malicious activity. These servers are not a member of any domain and only one authorized account is given permission to make updates to DNS.

NetBios is disabled on these servers

Domain Controllers

Because GIAC is aggressively expanding and merging the decision was to use an empty forest root domain to allow for multiple forest and child domains with non-centralized control if the situation occurs. There are two servers of the empty forest root in the KSOP Data Center with an additional empty forest root server in Stamford. The child domain has three domain controllers located in Kansas, two in Stamford and one in each of the branch offices. One domain controller in each site is designated as a Global Catalog server.

The drive configuration differs from the assumptions in that domain controllers are configured with three RAID0+1 sets. The two additional mirrored drives are used to separate the Active Directory database, sysvol, and the transaction logs.

Each domain controller is installed with the minimum windows software packages as possible, IIS is not installed. Trend Micro Server Protect for NT scans for viruses.

File Servers

World head quarters has multiple file servers allowing users home directory space and groups to have department shares for collaboration. Each branch has its own file server with a storage quota third party tool to manage the storage space and Trend Micro Server Protect for NT is installed for virus protection.

Each file server is installed with the minimum windows software packages as possible and IIS is not installed.

Email Servers

The Microsoft Exchange 5.5 email system has the bulk of its resources at world headquarters but Stamford and Chicago have their own email servers because of bandwidth considerations and the proximity of several larger branches. Trend Micro Scanmail for Exchange scans email for all viruses.

The drive configuration differs from the assumptions in that the email servers are configured with three RAID0+1 sets. The two additional mirrored drives are used to separate the Exchange Server database, transaction logs, and archived SMTP email traffic.

Each email server is installed with the minimum windows software packages as possible and IIS is not installed.

Branch IP Address Scheme Template

Network ID: 10.30.X.Y (X = Designated Branch IP Number)
Subnet Mask: 255.255.255.0
Default Gateway: 10.30.Y.1
Networking Device: 10.30.Y.1 – 5
Server Addresses: 10.30.Y.5 – 10
Printers 10.30.Y.10 – 20
DHCP Scope 10.30.Y.25 – 225
*The exception is the Stamford location with it's own host of IP Ranges 10.30.20.X through 10.30.25.X.

Client Hardware

Clients' workstations have (as part of the Windows 2000 implementation) been upgraded and installed with Windows 2000 SP3. The workstations are new Dells with P3/1400 Mhz Processor and 512 MB RAM. The file server and domain controllers are Compaq/HP machines and are described below. These workstations security will be discussed further under the group policy section below.

Server Hardware

Last two or three digit designation
RDCn Domain controller in root domain = giac.com
DCn Domain controller in child domain = northamerica.giac.com
FSn File Server for storage and Printers (if at the Branches)
PR Printer Server
NSn DNS Server
RH SMTP Relay Host
IISn Web Server running Internet Information Services.
EXCHn Microsoft Exchange 5.5 Server
* n stands for the number of servers in use incremented as new servers come online.

Location – Overland Park (KS)
DL380 G2 - "KSOPDC1", "KSOPDC2", "KSOPDC3"
DL380 G2 - "KSORPDC1", "KSOPRDC2"
DL380 G2 - "KSOPPR".
DL380 G2 - "KSOPRH". - **DMZ**
DL380 G2 - "KSOPIIS1","KSOPIIS2","KSOPIIS3","KSOPIIS4". - **DMZ**
DL380 G2 - "KSOPNS1", "KSOPNS2". - **DMZ**
DL380 G2 with additional 4100 storage array - "KSOPFS1","KSOPFS2","KSOPFS3"
DL580 additional 4100 storage array - "KSOPEXCH1","KSOPEXCH2","KSOPEXCH3"

Location—Stamford
Stamford is to be the backup site for GIAC.
DL380 G2 - "CTSTMDC1"

DL380 G2 - “CTSTMDC2”
DL380 G2 – “CTSTMRDC”.
DL380 G2 - “CTSTMFS1”.
DL380 G2 - “CTSTMFS2”.
DL380 G2 with additional 4100 storage array - “CTSTMEXCH1”

Location—Atlanta
DL380 G2 - “GAALTDC”.
DL380 G2 - “GAALTFS”.

Location—San Jose (MID)
DL380 G2 - “CAMIDDC”.
DL380 G2 - “CAMIDFS1”.

Location—5 Penn Plaza
DL380 G2 - “NY5PDC”.
DL380 G2 - “NY5PFS1”.

Location—Cowles
DL380 G2 - “NYCOWDC”.
DL380 G2 - “NYCOWFS1”.

Location—E44th ST NY
DL380 G2 - “NYE44DC”.
DL380 G2 - “NYE44FS1”.

Location—Manhattan 18th St
DL380 G2 - “NY18DC”
DL380 G2 - “NY18FS1”..

Location—Clarksdale
DL380 G2 - “PNCLKDC”.
DL380 G2 - “PNCLKFS1”.

Location—Houston
DL380 G2 - “TXHOUDC”.
DL380 G2 - “TXHOUFS1”.

Location—Indianapolis
DL380 G2 - “IDINDDC”.
DL380 G2 - “IDINDFS1”.

Location—Ft. Washington
DL380 G2 - “PNFTWDC”.
DL380 G2 - “PNFTWFS1”.

Location—Media, PA
DL380 G2 - “PNMEDDC”.
DL380 G2 - “PNMEDFS1”.

Location—Chicago 29N
DL380 G2 - “IL29NDC”.
DL380 G2 - “IL29NFS1”.

Location—Chicago 35E
DL380 G2 - “IL35EDC”.
DL380 G2 - “IL35EFS1”.

Location—Chicago Wabash
DL380 G2 - “ILWABDC”.
DL380 G2 - “ILWABFS1”.
DL380 G2 with additional 4100 storage array - “ILWABEXCH1”

Location—Minneapolis
DL380 G2 - “MNMINDC”.
DL380 G2 - “MNMINFS1”.

Location—Detroit
DL380 G2 - “MIDETDC”.
DL380 G2 - “MIDETFS1”.

Location—Denver
DL380 G2 - “CODNVDC”.
DL380 G2 - “CODNVFS1”.

Location—Irvine RGR
DL380 G2 - “CARGRDC”.
DL380 G2 - “CARGRFS1”.

Location—Irvine ESB
DL380 G2 - “CAESBDC”.
DL380 G2 - “CAESBFS1”.

Location—Emeryville
DL380 G2 - “CAEMRDC”.
DL380 G2 - “CAEMRFS1”.
WINS lookup to replicate with Stamford.

Location—Malibu
DL380 G2 - “CAMLBDC”.
DL380 G2 - “CAMLBFS1”.

Location—England
DL380 G2 - “UKLONDC”.
DL380 G2 - “UKLONFS1”.

Active Directory (AD) Design and Diagram

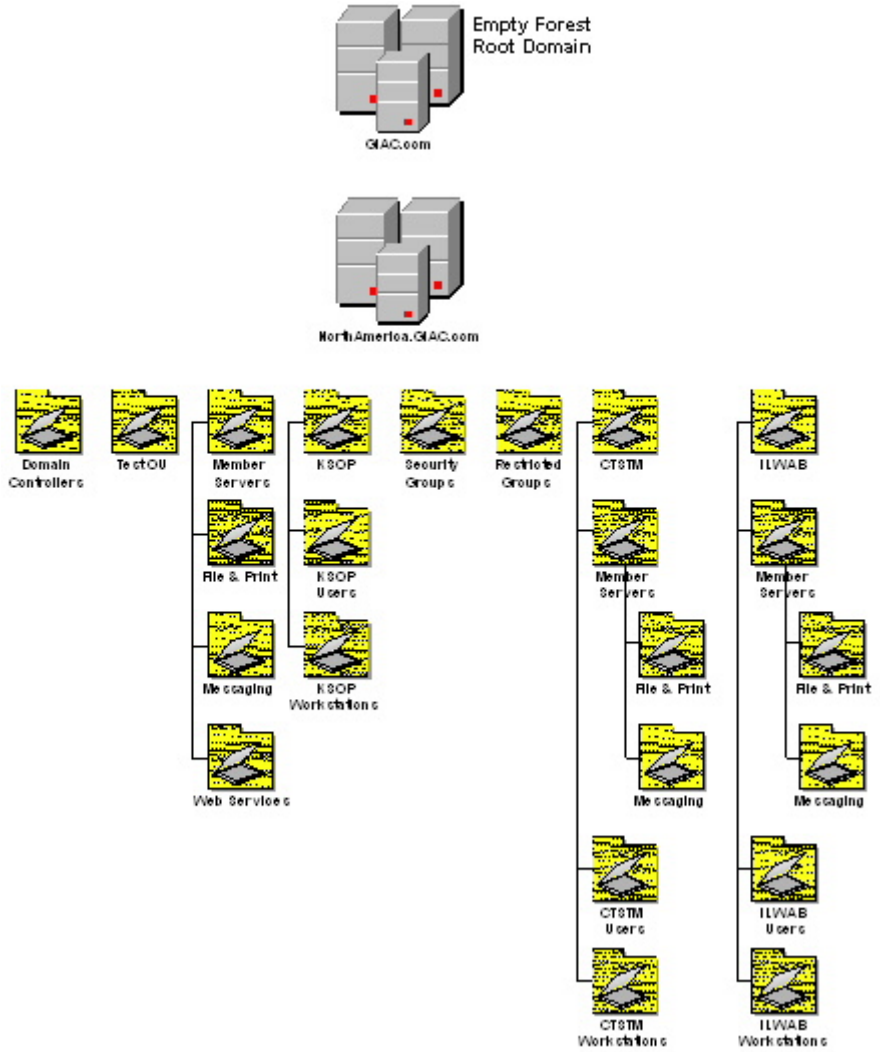


Figure 2 - Active Directory Domains and Containers

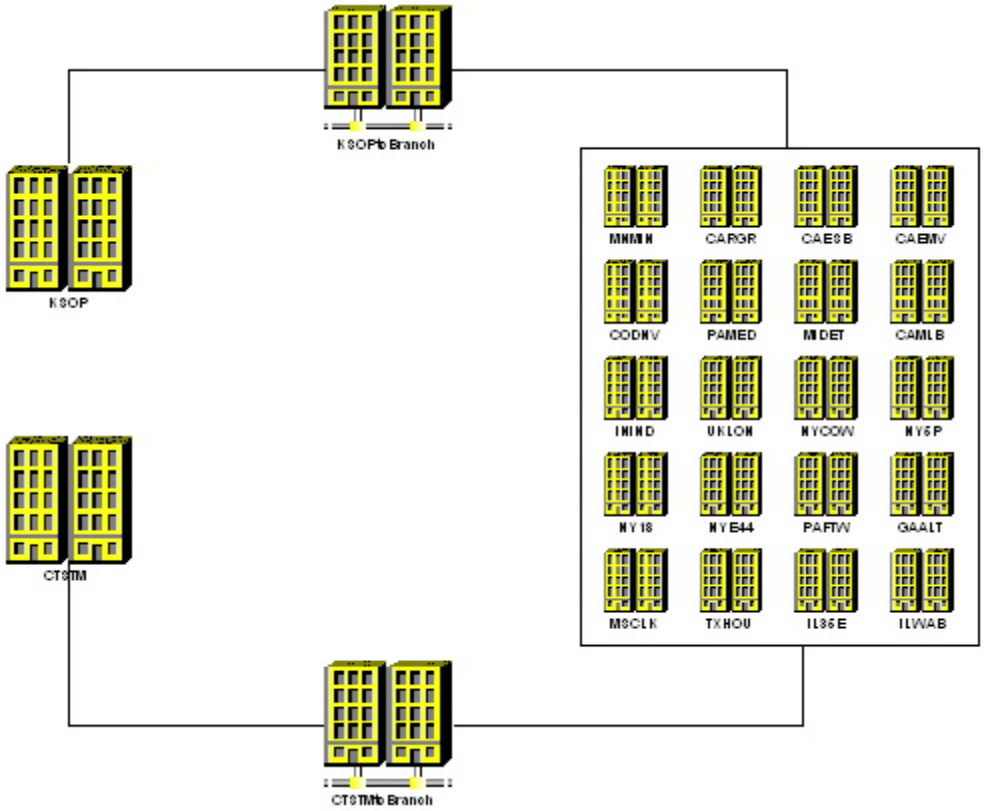


Figure 3 - Active Directory Sites and Site Links

Active Directory Design

Overview

Active Directory (AD) acts as the central authority for network security, letting the operating system readily verify a user's identity and control his or her access to network resources. Use of Active Directory reduces the costs associated with managing users, passwords, software installations, and security permissions. This section outlines the components of Active Directory and discusses the Active Directory approach implemented.

Active Directory Infrastructure

The four basic components that make up an Active Directory structure are forests, domains, organizational units, and sites. The performance and manageability of the enterprise will rely heavily on all four of these components.

Forests

A forest is a collection of Active Directory domains. Forests serve two main purposes: to simplify user interaction with the directory, and to simplify the management of multiple domains. The following are characteristics of a forest:

- **Single Schema** – The Active Directory schema defines the types of objects that can be created and utilized in the Active Directory. A single schema will dictate that all domains have consistent objects and attributes enterprise wide.
- **Complete Trust** – within a forest, each domain has a two-way transitive trust between itself and the other member domains. This allows for easy manageability of users that need resources from multiple domains.
- **Single Global Catalog** – The global catalog contains a copy of every object from every domain in the forest but only a select set of the attributes from each object. The global catalog enables fast, efficient searches that span the entire forest. The global catalog makes directory structures within a forest transparent to end-users.

Forest Determination

The number of forests to create relies on the amount of centralized management that will take place, the needs of the company, the amount of replication required, schema design and the number of global catalogs. The determination of the number of forests to create depends on the above listed items. The following outlines the above criteria: Centralized Management – a forest can be managed from a single point. All network resources and security will spawn from a single point in a single forest domain. The result of this can cause undesired results across an entire organization if a strict change management plan is not enforced. A multiple forest design will allow an organization to divide the responsibility of managing the resources and security within their scope of responsibility. In a single forest, design the network must contain one entity that makes all decisions that will affect all network resources within that forest. An organization that has diverse needs within its informational systems technology could be adversely affected by a single forest.

- **Replication** – Within a single forest design all servers within that forest must be able to contact a global catalog. The global catalog then must be able to replicate with other global catalogs in order to keep the distributed database current and provide fault tolerance for the Active Directory. The replication must be provided by secure, stable, and sufficient wide area links in order to successfully update the Active Directory with current information. A minimum of 256/kbs is recommended for links between global catalogs. A multiple forest environment will not necessarily require the expensive costs of the WAN links needed by a single forest design. A link between multiple forests is only necessary when users from one forest need access to resources in an adjacent forest. GIAC currently has a WAN in place that can successfully handle the replication traffic generated by Active Directory replication. GIAC will utilize these links to implement a replication design that will support a single forest design.
- **Schema Design** – The schema within a forest will be consistent throughout all domains that are members of that forest. This limitation can cause potential difficulties within a network that utilizes a diverse selection of software. Software applications are becoming more and more Active Directory aware and will need to make changes to the Active Directory schema. This causes possible incompatibilities with schema changes from different software vendors.

- **Global Catalogs** – The location of global catalogs within a forest must be carefully planned. A global catalog must be available when a user authenticates to the Active Directory. The location of global catalogs within a forest will eliminate users traversing the WAN to authenticate and locate network resources located in the Active Directory. A single forest design would increase the numbers of global catalogs and the amount of traffic generated between those global catalogs within an organization. The multiple forest design does not require the global catalogs of each forest to communicate with global catalogs of other forests. This will eliminate the need for purchasing and providing bandwidth between physical locations within an organization.

Single Forest Environment

A single forest is easy to create and maintain. Users are unaware of the directory structure because they will use a single global catalog. Trusts do not have to be created between domains within a single forest. This environment requires a centralized governing body that can make decisions for all domains within the enterprise. Any change to the forest will directly affect all domains within that forest. The domains within a forest will most likely be used and utilized by users of other domains. Because forests have shared elements, such as schema, it is necessary for all the participants in a forest to agree on the content and administration of those shared elements.

The single forest environment (GIAC.com) will allow the network administration to be streamlined and centralized. The single forest will allow all users ease of access to all resources within GIAC. A single forest environment will reduce cost by eliminating the need for the users to understand the directory structure and reducing the time it takes for basic administration of one user. The single forest environment also allows for future use of forest trusts if they become necessary. This design requires a root domain controller in KSOP and one in CTSTM with domain controllers at each site for the NorthAmerica child domain that must replicate with all other sites. Replication traffic has to be carefully monitored and controlled as to not overload the WAN link.

Domains

The domain within an Active Directory forest is used to divide the Active Directory database into more manageable pieces. The Active Directory is a distributed database that can reside on more than on computer. Therefore by breaking the database into smaller units and placing that data in proximity to the users that utilize the data we can utilize the database more efficiently. The domain object also is used as a unit of authentication and a boundary for administration and group policy.

Domain Determination

A single domain model (northamerica.GIAC.com) will be created and administered at GIAC. The single domain model will allow central administration of all users and resources from one centralized point. A domain controller will be located at each site

and will allow for local authentication. Group Policies will allow for a single point of administration of desktops and user configurable settings within the domain. A single domain model will provide the following benefits:

- **Increased security** – A single domain model will reduce the number of domain admin accounts as compared to a multiple domain environment
- **Reduce Hardware Costs** – Each domain that exists requires at least one domain controller. A single domain model only requires a single domain controller, which reduces the required amount of hardware necessary.
- **Reduced point of failure** – Within a single domain a user can authenticate and access all network resources if there is at least one domain controller available. The multiple domain model presents a single point of failure between domains.

Organizational Unit (OU) Design

Organizational Units (OU's) are containers that enable AD designers to logically group objects such as users and computers. OU's are used as a scope for applying Group Policy and delegating administration of AD objects.

Sites

An Active Directory site topology is a logical representation of a physical network. Active Directory clients and servers use the site topology of a forest to route query and replication traffic efficiently. A site topology also helps you decide where to place domain controllers on your network. A site is defined as a set of IP subnets connected by fast, reliable connectivity. As a rule of thumb, networks with LAN speed or better are considered fast networks. Site links are used to model the amount of available bandwidth between two sites. Users will utilize the sites in such a way that each user will attempt to connect to a domain controller in its own site before traversing the WAN to locate a domain controller.

The Knowledge Consistency Checker uses the site topology to generate replication connections. These connections are used to replicate the Active Directory changes and updates. Replication consists of inter-site replication and intra-site replication. Intra-site replication is tuned to minimize the latency caused by Active Directory's distributed database structure and inter-site replication is tuned to minimize bandwidth usage across WAN links.

The following table shows the differences between inter-site and intra-site replication:

Intra-site replication	Inter-site replication
Replication traffic is not compressed to save processor time.	Replication traffic is compressed to save bandwidth.
Replication partners notify each other when changes need to be replicated, to reduce replication latency.	Replication partners do not notify each other when changes need to be replicated, to save bandwidth.
Replication partners poll each other for	Replication partners poll each other for

changes on a periodic basis.	changes on a specified polling interval, during scheduled periods only.
Replication uses the remote procedure call (RPC) transport.	Replication uses the TCP/IP or SMTP transport.
Replication connections can be created between any two domain controllers located in the same site. The KCC creates connections with multiple domain controllers to reduce replication latency.	Replication connections are only created between bridgehead servers. One domain controller from each domain in a site is designated by the KCC as a bridgehead server. The bridgehead server handles all inter-site replication for that domain. The KCC creates connections between bridgehead servers using the lowest cost route, according to site link cost. The KCC will only create connections over a higher cost route if all of the domain controllers in lower cost routes are unreachable.

Table 2 - Intersite and Intrasite Replication Traffic

Site topology is separate and unrelated to domain hierarchy. A site can contain many domains, and a domain can appear in many sites.

GIAC will design the site topology parallel to the network physical topology. A site and a subnet will be created at each physical location (KSOP and CTSTM will have multiple subnets). Site links will be created according to the Figure 3. This design will optimize the performance of replication across the WAN links.

Active Directory Implementation

Domain Controllers and AD (FSMO) Roles

Microsoft describes the Active Directory domain controller roles as the following[3]:

> *Certain domain and enterprise-wide operations not well suited to multi-master placement reside on a single domain controller in the domain or forest. The advantage of single-master operation is to prevent the introduction of conflicts while an operation master is offline, rather than introducing potential conflicts and having to resolve them later. Having a single-operation master means, however, that the FSMO role owner must be available when dependent activities in the domain or enterprise take place, or to make directory changes associated with that role.*

3 http://support.microsoft.com/default.aspx?scid=kb;en-us;223346

> *The Active Directory defines five FSMO roles: schema master, domain master, RID master, PDC emulator, and infrastructure. The schema master and domain naming master are per-forest roles. The remaining three, RID master, PDC emulator, and infrastructure master, are per-domain roles.*

Following the Microsoft Best Practices the forest roles have been split between two servers. The forest domain roles will not exist in the child NorthAmerica domain but will be configured as shown below.

CTSTMRDC1 (GIAC.com)
- Domain Naming Master
- Infrastructure Master

KSOPRDC2 (GIAC.com)
- Schema Master
- PDC Emulator
- RID Master
- Global Catalog

KSOPDC1 (NorthAmerica.GIAC.com)
- PDC Emulator Master
- Infrastructure Master

KSOPDC2
- RID Master
- Global Catalog Server

All other Domain Controllers
- Global Catalog Server

First Level Containers

Table 3 shows the default Active Directory containers, which should not be confused with Administrative OU's, as they cannot be used for the application of specific Group Policy Objects (GPO's) they can inherit from the domain policy, but have no ability to override that policy as the administrator decides. They do, however, allow for the delegation of administrative control and so may be useful for containing unmanaged objects. One exception to this rule is the Domain Controllers group, which does allow for GPO's.

It is recommended that no production-related AD objects be created in these containers. The "Computers" container is suitable for NT/W2K "admin" workstation machine accounts if these systems do not need to be managed through Group Policy but GIAC will create a separate OU Structure to locate workstations.

Container	Contains
Users	Default User Accounts
Computers	Default Workstation or Server (Non-Domain Controllers) Machine Accounts
Built-in	Contains built-in groups Also contains special access groups such as "Pre-Windows 2000 Compatible Access" which in turn contains the Everyone group
ForeignSecurityPrincipals	Used by Active Directory
LostAndFound	Used by Active Directory during upgrades from Windows NT
System	Used by Active Directory
Domain Controller	Default Domain Controller Machine Accounts

Table 3 - Default Active Directory Containers

Organizational Unit Hierarchy

GIAC's OU hierarchy is shallow, simple and stable. The OU hierarchy can be kept very shallow (a single level) and simple (only one-half dozen OUs) given the limited variety of AD objects in use.

First-Level OU Design

NorthAmerica.GIAC.com is the domain object with default active directory containers underneath along with administrative OU's. Here is the logical design which is built from Figure 2 including all branch offices.

- Builtin
- CAEMV
- CAESB
- CAMID
- CAMLB
- CARGR
- CODNV
- Computers
- CTSTM
- Domain Controllers
- ForeignSecurityPrinciples
- GAALT
- IL29N
- IL35E
- ILWAB
- ININD

- KSOLA
- KSOP
- LostAndFound
- Member Servers
- MIDET
- MNMIN
- MSCLK
- NY18
- NY5P
- NYCOW
- NYE44
- PAFTW
- PAMED
- Restricted Groups
- Security Groups
- System
- Test OU
- TXHOU
- UKLON
- Users

Second-Level OU Design

Each Location OU's contain second level OU's for administrative and security purposes. Those second level OU's break down into Users, Workstations, and Member Servers. All servers are placed into the Member Servers OU, while user accounts and Workstations are placed in their respective OU's.

The three common OU's at each site are Users, Workstations, Member Servers with additional third level OU's within the Member Servers OU. This OU design was architected to facilitate the application security and administration for the helpdesk, second tier technicians and the third level systems engineers. Each helpdesk person assigned to a specific branch will be in that branch's sitename-Helpdesk Windows 2000 security group. That group has been delegated permissions to the Branch first and second level OUs, while being explicitly denied access to the Member Server second level OU.

OU Descriptions and Members

Table 4 outlines how the OUs should be configured to allow for the delegation of authority and GPO management for OU objects to appropriate security principals defined in the domain.

1st Level OUs	2nd Level OUs	Description
Member Servers	Web Services File and Print Messaging	• Contains all member server machine accounts • Allows Group Policy Objects (GPO) to be

		applied to all servers
Security Groups	None	• Domain Admins group is located in this container for secured membership control • Modifications to objects in this OU can only be conducted by the Active Directory Enterprise Admins
Restricted Groups	None	• Contains accounts used by services for authentication • Modifications in this object is restricted to the systems administrators to reduce security risks from the helpdesk
CAEMR CAESB CAMLB CARGR CODNV CTSTM GAATL IL29N IL35E ILWAB ININD KSOLA KSOP MIDET MNMIN MSCLK NY18 NY5P NYCOW NYE44 PAFTW PAMED TXHOU UKLON	Member Servers Users Workstations	• (Level 1 OUs) Act only as a namespace • (Level 2 OU) Contains all user and machine accounts by branch and OU • Allows all Users and computers at a location to be managed by a GPO • Allows for Software packages to be installed on computers by location via GPO • Allows all Users and computers to be managed by a single GPO • Users reside where the computer account exists • Site-specific groups reside on the location root (these are rare)

Table 4 - Organizational Layout and Descriptions

OU Permissions Details

Table 5 outlines how the OUs should be delegated with respect to the appropriate security principals defined in the domain.

1st Level OUs	2nd Level OUs	Management Delegation
NorthAmerica.GIAC.com	None	• Administrators (Default) • Authenticated Users (Read) • Domain Admins (Default) • Enterprise Admins (Full) • Enterprise Domain Controllers (Default) • Pre-Windows2000 Compatibility Access (Default) • System (Full)
Builtin	None	• (No Inherited permissions) • Domain Admins (Default) • Enterprise Admins (Full)

		• Enterprise Domain Controllers (Default) • Pre-Windows2000 Compatibility Access (Default) • System (Default)
Computers	None	• Current plans do not call for the use of this OU • Authenticated Users (Read and Add) • Authenticated users have the right to add computer account information
CAEMR CAESB CAMLB CARGR CODNV CTSTM GAATL IL29N IL35E ILWAB ININD KSOLA KSOP MIDET MNMIN MSCLK NY18 NY5P NYCOW NYE44 PAFTW PAMED TXHOU UKLON	Member Servers Users Workstations	**1st level OU permissions;** • Administrators (Default) • Authenticated Users (Read) • Domain Admins (Full) • Enterprise Admins (Full) • %site%-Helpdesk (all account management permissions) *Example:* CAEMR-Helpdesk is delegated to the CAEMR OU • KSOP-Helpdesk (Specific account management permissions) • Pre-Windows2000 Compatibility Access (Default) • System (Full) **2nd level OU permissions;** • Administrators (Default) • Authenticated Users (Read) • Domain Admins (Full) • Enterprise Admins (Full) • KSOP-Helpdesk (Specific account management permissions) • Pre-Windows2000 Compatibility Access (Default) • System (Full)
Domain Controllers	None	• Administrators (Default) • Authenticated Users (Read) • Domain Admins (Default) • Enterprise Admins (Full) • Pre-Windows2000 Compatibility Access (Default) • System (Full)
Restricted Groups	None	• (No Inherited permissions) • Domain Admins (Full) • Enterprise Admins (Full)
Security Groups	None	• (No Inherited permissions) • Enterprise Admins (Full)
Foreign Security Principles	None	• All permissions are left configured as default
Lost and Found	None	• All permissions are left configured as default
Servers	None	• Administrators (Default) • Domain Admins (Default) • Enterprise Admins (Full) • Pre-Windows2000 Compatibility Access (Default) • Print Operators (Default)

		• System (Full)
System	Folders Only	• Administrators (Default) • Domain Admins (Full) • Enterprise Admins (Full) • Pre-Windows2000 Compatibility Access (Default) • System (Full)
Users		• Administrators (Default) • Domain Admins (Full) • Enterprise Admins (Full) • Pre-Windows2000 Compatibility Access (Default) • System (Full) • KSOP-Helpdesk (all account management permissions) *Note: this is for legacy account management*

Table 5 - Organization Unit Delegations Layout

Monitoring the Active Directory Infrastructure

Microsoft released an official branch deployment guide to help companies design their Active Directory implementation. From chapter nine page seven we read[4]:

> *This Active Directory branch office guide includes a set of quality assurance scripts that can be used to perform a daily quality assurance check on your branch office environment. These scripts should be scheduled to run daily on your domain controllers—both the branch office domain controllers and your bridgehead servers in the hub site.*

GIAC scheduled these scripts to run each morning on every domain controller in the empty root domain as well as the NorthAmerica.GIAC.com child domain. The scripts run diagnostic utilities and create the log files shown in Table 6.

File	Contents
Dcdiag.txt	Output of running Dcdiag.exe to perform domain controller diagnostic checks.
Netdiag.txt	Output of running Netdiag.exe to check the network configuration and health of the domain controller. When running Netdiag.exe, the Lightweight Directory Access Protocol (LDAP) tests are skipped as they can place a large load on the network when there is a large number of domain controllers.
GPOstat.txt	Output of running Gpostat.vbs to verify that each Group Policy object is in sync.
Ntfrs_ds.txt	Output of running Ntfrsutl.exe ds to list the FRS view of the DS.

[4] http://www.microsoft.com/windows2000/techinfo/planning/activedirectory/branchoffice/dply09.asp

Ntfrs_sets.txt	Output of running Ntfrsutl.exe sets to list the active replica sets.
Ntfrs_inlog.txt	Output of running Ntfrsutl.exe inlog to enumerate the FRS inlog.
Ntfrs_outlog.txt	Output of running Ntfrsutl.exe outlog to enumerate the FRS outlog.
Ntfrs_version.txt	Output of running Ntfrsutl.exe version to list the application programming interface (API) and service versions.
Ntfrs_reg.txt	Output of running Regdmp.exe to output the contents of the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NtFrs\Parameters registry key.
Ntfrs_sysvol.txt	Output of running Dir %*Systemroot*%\sysvol /s to store a list of the contents of the SYSVOL folder.
Frsconstat.txt	Output of running Connstat.cmd to summarize the FRS connection state. For more details on what this script does, see "Monitoring FRS Replication with Connstat.cmd" later in this chapter.
Ntfrs_errscan.txt	Output of running Findstr to search the %*windir*%\debug\ntfrs_*.log files for "error", "invalid", "fail", "abort", and "warn".
Ntfrs_parse.txt	Output of running Findstr to search %*windir*%\debug\ntfrs_0005.log for "error", "invalid", "fail", "abort", and "warn".
Ntfrs_parse2.txt	Output of running Findstr to search %windir%\debug\ntfrs_0005.log for "ERROR - EXCEPTION (000006ba): WStatus: RPC_S_SERVER_UNAVAILABLE", "ERROR - STAGING AREA FULL", "ERROR - DISK_FULL", "ERROR_DISK_FULL", "ERROR - EXCEPTION EPT_S_NOT_REGISTERED", "has no inbound server", "has no outbound server", "DS: Multiple connections from", "WARNING: Setting FrsVsn - Current system Time has moved backwards from value in config record", and "JRNL_WRAP_ERROR".
Ds_showreps.txt	Output of running Repadmin /showreps to list the replication partners for the domain controller.
Ds_showconn.txt	Output of running Repadmin /showconn to list the connection objects for the domain controller.
Services.txt	Output of running Net Start to list the services that are running on the domain controller.

Table 6 - Branch Office Deployment Guide Script Output Files

An additional utility is then run to parse the log files generated and report any errors into a consolidated log file. The contents of the reported log file are then emailed to the Active Directory systems administrators for review every morning. This helps prevent errors and keeps the Active Directory Infrastructure stable and in-synch. The output of the consolidated log file is similar to the following:

```
Created on 1/25/2003 at 5:00:47 AM
QA_Parse.vbs Version 0.52

**************************************************
IP Configuration - from netdiag.exe
**************************************************
    IP Address . . . . . : 10.191.16.19
    Subnet Mask. . . . . : 255.255.255.0
    Default Gateway. . . . . : 10.191.16.1
    DNS Servers: 10.191.16.19 10.160.12.70
```

If any errors are reported in this section examine the C:\ADResults\netdiag.txt file on Domain Controller:CTSTMDC1

```
************************************************
DC Diagnostics tests - from dcdiag.exe
************************************************
```

If any errors are reported in this section examine the C:\ADResults\dcdiag.txt and C:\ADResults\dcdiagerr.txt files on Domain Controller:CTSTMDC1

```
        ..... CTSTMDC1 passed test Connectivity
        ..... CTSTMDC1 passed test Replications
        ..... CTSTMDC1 passed test NCSecDesc
        ..... CTSTMDC1 passed test NetLogons
        ..... CTSTMDC1 passed test Advertising
        ..... CTSTMDC1 passed test KnowsOfRoleHolders
        ..... CTSTMDC1 passed test RidManager
        ..... CTSTMDC1 passed test MachineAccount
        ..... CTSTMDC1 passed test Services
        ..... CTSTMDC1 passed test ObjectsReplicated
        ..... CTSTMDC1 passed test frssysvol
        ..... CTSTMDC1 passed test kccevent
        ..... CTSTMDC1 passed test systemlog
        ..... GIAC.com passed test Intersite

************************************************
FRS tests - from ntfrsutl.exe
************************************************
```

If any errors are reported in this section examine the C:\ADResults\ntfrs_*.txt file on Domain Controller:CTSTMDC1

```
************************************************
Active Directory Replication Connection Objects
from repadmin.exe /showconn
************************************************

************************************************
Active Directory Replication Tests
from repadmin.exe /showreps
************************************************
```

If any errors are reported in this section examine the C:\ADResults\ds_showreps.txt and C:\ADResults\ds_showconn.txt files on Domain Controller:CTSTMDC1

```
==== INBOUND NEIGHBORS ======================================
DC=northamerica,DC=GIAC,DC=com
====================

CN=Schema,CN=Configuration,DC=GIAC,DC=com
====================

CN=Configuration,DC=GIAC,DC=com
====================

DC=GIAC,DC=com
====================

************************************************
Group Policy Objects - from gpostat.vbs
************************************************
```

If any errors are reported in this section examine the C:\ADResults\gpostat.txt file on Domain Controller:CTSTMDC1

```
Found 11 Group Policies on Domain Controllers: CTSTMDC1
GPO information excluded for brevity

************************************************
Verify Running Services - from net start
************************************************
```

If any errors are reported in this section examine the C:\ADResults\services.txt file on Domain Controller:CTSTMDC1

Group Policy and Security

Group Policies will be used at GIAC Enterprises to govern user access rights, software package distribution, and desktop settings. Group Policy Objects (GPO's) refer to group policies as they exist in the Active Directory. GPO's allow for features such as roaming applications, roaming documents, desktop restrictions, and security settings. They get applied at system startup, user logon, and over time intervals which can be specified.

Two areas of focus are used within Group Policy creation, the user and the computer. The policies are divided into those two sections and depending on which section is used the gpo will be applied. When making changes to the Computer Configuration, the workstation itself is affected and it's interaction on the network. The User Configuration area is applied as a user logs on.

General Group Policies

There are two default GPO objects to be modified in every Active Directory Implementation, they will be the highest level of configuration and will generally be inherited by all objects in the directory (excluding those blocking inheritance). The first of these is the Default Domain Controller policy, and the second is the Default Domain Policy. We will look at the Default Domain policy first.

Default Domain Policy

The Default Domain policy is configured out of the box, but the security is lacking and the customizations are warranted. GIAC has modified several areas within the Default Domain Policy and they are listed in the following tables.

Windows Settings à **Account Policies** à **Password Policy**

The password policy at GIAC is straight forward and follows industry best practices[5]. A user is required to change their password every 60 days with a minimum length of eight characters. The password must remain in force for and entire day and the user cannot just choose the same password, but must have ten unique passwords before one can be reused. Perhaps the most change with the most impact will be the complexity requirements. Users will need to have a combination of Capital letters, numbers, and special characters. Table 7 shows the changes to the default policy.

Policy	GIAC Configuration	Original
Enforce password history	10 passwords remembered	1 passwords remembered
Maximum password age	60 days	42 days
Minimum password age	1 days	0 days

[5] Ferraiolo, D., Lynch, N., Toth, P. (1993). Minimum Security Requirements for Multi-User Operating Systems (NISTIR 5153). National Institute of Standards and Technology.

Minimum password length	8 characters	0 characters
Passwords must meet complexity requirements	Enabled	Disabled
Store password using reversible encryption for all users in the domain	Disabled	Disabled

Table 7 - Account Policies - Password Policy

Windows Settings à **Account Policies** à **Account Lockout Policy**
Working hand-in-hand with the password policy is the account lockout policy. This policy guards against brute force attacks (password guessing) on network accounts. The lockout duration is set to 15 minutes and with education the user will know to wait 15 minutes and try again. The good thing is that the counter is reset after 15 minutes also.

Policy	GIAC Configuration	Original
Account lockout duration	15 minutes	30 minutes
Account lockout threshold	3 invalid attempts	0 invalid attempts
Reset account lockout counter after	15 minutes	30 minutes

Table 8 - Account Policies - Account Lockout Policy

Windows Settings à **Local Policies** à **Audit Policy**
The audit policy determines the type of events on the network to flag and make that information available to administrators. Careful planning of auditing is necessary because the settings can affect the performance of the servers. GIAC is using a third-party security product which requires the following audit policies enforced on the network. This data is being mined and will be available through a database. Additionally configured but not shown in a table is the size of the Application, Security, and System logs. At GIAC each log is 50MB large with events being overwritten every 7 days. Access to view these logs is also restricted to systems engineers.

There is a concern that the log files are large, but the price of storage and the fact that each domain controller has a 30 GB for storage eliminates this as a concern.

Policy	GIAC Configuration	Original
Audit account logon events	Success, Failure	No auditing
Audit account management	Success, Failure	No auditing
Audit directory service access	Success, Failure	No auditing
Audit logon events	Success, Failure	No auditing
Audit policy change	Success, Failure	No auditing
Audit privilege use	Failure	No auditing
Audit system events	Success, Failure	No auditing

Table 9 - Local Policies - Audit Policy

Windows Settings à **Local Policies** à **User Rights Assignment**
Only authenticated users should have access to computers on the network. Some Administrative tasks including, back up and restore, taking ownership of files, and changing the system time are only granted to domain administrators. With some of the functionality given to the Support Technicians (device driver permissions and adding computer accounts). The Product Engineering and ATG groups will be allowed to debug programs, as they are software developers and it is vital to their job functions. GIAC will also disable the feature that allows users to gain access to files by knowing their complete path name and typing it in for retrieval. This security hole is fixed in Windows 2000 group policy.

Policy	GIAC Configuration
Access this computer from the network	Authenticated Users
Add workstations to domain	Domain Admins, Support Technicians
Back up files and directories	Domain Admins
Bypass traverse checking	Domain Admins
Change the system time	Administrators, Domain Admisn
Debug programs	Domain Admins, Product Engineering, ATG
Load and unload device drivers	Domain Admins, Support Technicians
Manage auditing and security log	Domain Admins
Shut down the system	Domain Admins, Administrators

Table 10 - Local Policies - User Rights Assignment

Windows Settings à **Local Policies** à **Security Options**
These additional security settings are available and are described below. The nature of the type of policy and the description make it difficult to sum up in paragraph form so they are given in bold with their explanations following Also see Table 11.

Additional restrictions for anonymous connections
This setting removes the "Everyone" and "Network" from the anonymous users token requiring that "Anonymous" be given explicit access to any required resources.

Clear virtual memory pagefile when system shuts down
This policy will clear the system pagefile on shutdown this will eliminated access to possibly critical data retained in memory.

LAN Manager Authentication Level
Since only Windows 2000 servers and workstations are on the GIAC network this setting tells Windows to use the updated NTLMv2 protocol for logon authentication.

Message text for users attempting to log on
This message will be used for a legal disclaimer for anyone accessing the network through a GIAC device.

Message title for users attempting to log on
The name of the message box of the above policy.

Rename administrator and guest account
Renaming the administrator and guest accounts will eliminate many hackers' attempts to get on your network. If a hacker already knows the name of a user account half the battle is over. GIAC will rename the administrator account to sysadmin and create a dummy Administrator account that is disabled and has no network access. This small configuration setting could be the difference between someone hacking you or not. If it is really hard most hackers would move on. The guest account is renamed and disabled.

Policy	GIAC Configuration
Additional restrictions for anonymous connections	Do not allow enumeration of SAM accounts and shares
Clear virtual memory pagefile when system shuts down	Disabled
Do not display last user name in logon screen	Enabled
Message text for users attempting to log on	This workstation is property of GIAC, unauthorized use is strictly forbidden
Message title for users attempting to log on	Logon Warning
Rename administrator account	sysadmin
Rename guest account	gv1245
Additional restrictions for anonymous connections	Do not allow enumeration of SAM accounts and shares
Clear virtual memory pagefile when system shuts down	Disabled

Table 11 - Local Policies - Security Options

User Configuration à **Administrative Templates** à **Start Menu & Taskbar**
Enable - Add Logoff to the Start Menu
This will help the casual system administrator not to accidentally shutdown the server when all they wanted to do was logoff.

User Configuration à **Administrative Templates** à **Control Panel** à **Display**
Enable Password protect the screen saver
Enable Screen Saver timeout - 5 minutes
This will eliminate the loss of data, downtime, and possible harassment areas by forcing an inactive, logged on user's machine to force a password logon event to gain access to the desktop. Additionally the Product Engineering and ATG groups within GIAC are very particular to people accessing their devices. Software developers could lose hours and days if a person knowingly or unknowingly closes a program, deletes some data etc.

The finance department and HR departments have sensitive and confidential data open at given times as well. It is important to the integrity of GIAC to have this information and data protected.

Domain Controller Policy

Many of the security configuration changes for the domain controllers are already in place with the default domain policy. The following will provide where changes are necessary.

Windows Settings à **Account Policies** à **Password Policy**
Will remain the same as the Default Domain policy

Windows Settings à **Account Policies** à **Account Lockout Policy**
The account lockout duration will be set to zero. This will force someone with permissions to unlock the password when failing to log into the domain controller.

Windows Settings à **Local Policies** à **Audit Policy**
Will remain the same as the Default Domain policy

Windows Settings à **Local Policies** à **User Rights Assignment**
Will remain the same as the Default Domain policy

Windows Settings à **Local Policies** à **Security Options**
Will remain the same as the Default Domain policy

Additional Group Policy

Desktop Configuration Policies

Desktop standards and policies are a necessity in providing a reliable and secure environment for the end user. By implementing desktop standards and policies, GIAC will forecast and proactively resolve issues as they relate to the end user and the desktop. This will increase end user performance and return on investment. The desktop standards and policies are designed not to inhibit the ability of the end user to effectively perform their job duties.

Group policy takes these requirements and streamlines them throughout the company reducing petty helpdesk calls and focusing the support team on doing real needed support.

The Desktop environment employed by GIAC will have the following key features:

- All printing will be provided via network printers located within the work area. Network Printers will be available by searching the directory or the usual UNC path name. Network print drivers will be configured automatically upon the selection of a printer.

- The Internet explorer default home page will initially be set to Intranet.GIAC.com and can be changed.
- Only Windows 2000 default screen savers will be available.
- All Computers will receive the default set of applications:
  - Microsoft Office 2000 (Word, Excel, PowerPoint)
  - Microsoft Outlook 2000
  - WinZip
  - Adobe Acrobat Reader
  - Trend Micro Antivirus (during the workstation build)
- The My Documents folder will be redirected to each user's home directory on the network. This will insure that all user data is secure and is copied to offline storage for emergency retrieval.

Software Installation

- All approved software will be preinstalled and available via the Add/Remove Software icon located in the control panel. Any software that is not available via the Add/Remove Software will need to get written permission for tracking software licenses and proper billing to the department.
- All other software will be delivered to the desktop based on user criteria. This will involve a written request endorsed by a team lead. That request is filtered into the helpdesk where the user is placed into the group that is assigned to have access to the particular piece of software.

GPO's linked to OUs

Each first level branch OU is configured with a Group Policy Object. The name of this gpo is <branch> local settings. The gpo contains specific configurations to point software installations and desktop redirection settings to a server local to the workstation or user receiving the gpo. For example If I authenticated in the ILWAB branch (and my user account and machine account were in the ILWAB OU). My My Documents folder would be redirected to the \\ILWABFS1\HomeDir\<myusername> folder and automatically synchronize the data between the two. If I were to then receive proper access to a new software installation, I would access my Control panel → Add or Remove Programs. I should see the title of the new software by clicking on the Add New Programs Icon. Because I am in ILWAB the gpo redirects my machine to the - \\ILWABFS1\Applications share and install the software.

Each first and second level Member Server OU is assigned the software packages for the Adminpak, Windows 2000 support tools and the Windows 2000 Resource Kit. Systems Administrators will be pleased that the next time they try and troubleshoot a server they won't need to spend half and hour searching for the correct tools. This however is blocked on the Web Servers OU. If a web server is compromised it's a bad idea to have useful command-line tools available to use.

1st Level OUs	Computer-based Software Installation Group Policy Objects	
CAEMR	**1st level Software GPO**	**Each local branch gpo varies pointing**

CAESB CAMLB CARGR CODNV CTSTM GAATL IL29N IL35E ILWAB ININD KSOLA KSOP MIDET MNMIN MSCLK NY18 NY5P NYCOW NYE44 PAFTW PAMED TXHOU UKLON	**objects to local resources** • Office 2000 (computer-based) o Assigned application o Slow-link detection • Outlook (computer-based) o Assigned application o Slow-link detection • WinZip (computer-based) o Assigned application o Slow-link detection • Acrobat Reader (user-based) o Assigned application o Slow-link detection • Visio (user-based) o Published application o Slow-link detection • Project (user-based) o Published application o Slow-link detection • Access (user-based) o Published application o Slow-link detection • FrontPage (user-based) o Published application o Slow-link detection • Visual Studio (user-based) o Published application o Slow-link detection • ACT 2000 (user-based) - Sales application o Published application o Installed with Elevated Privileges o Slow-link detection **1st level Desktop Configuration GPOs** • Folder Redirection-settings (user-based) o Published application o Redirects users My Documents to local file share o Slow-link detection • Login Script-settings (user-based) o Published application o Locally based for differing branch settings o Slow-link detection
Member Servers Domain Controllers	**1st level Software GPO** • Adminpak (computer-based) o Assigned application • Windows 2000 Support Tools (computer-based) o Assigned application • Windows 2000 Resource Kit (computer-based) o Assigned application

Table 12 - Group Policy - Software Installation

Additional Security

Helpdesk Administrative MMC Console

To help reduce the risk of inadvertent, and malicious access to Active Directory a management console was created to give the helpdesk access to specific resources without having them clicking around where damage could be done. This taskpad was created so that the helpdesk only has access to what is granted on the taskpad view. In this example the helpdesk person can pull up the contents of the KSOP OU and view the users and workstations associated with that OU. Access is granted to read the file share permissions on all file servers to determine what group to put a caller in when assigning new privilege or access. Also a knowledge base internal to the GIAC company can be launched from the taskpad view. Finally the helpdesk person can log into the helpdesk call center to work on tickets.

In the future as the need arises a vbscript will be used to automate common tasks. A monthly task force meets to discuss these needs and to offset administrative burden and increase helpdesk efficiency those scripts will be added to the taskpad.

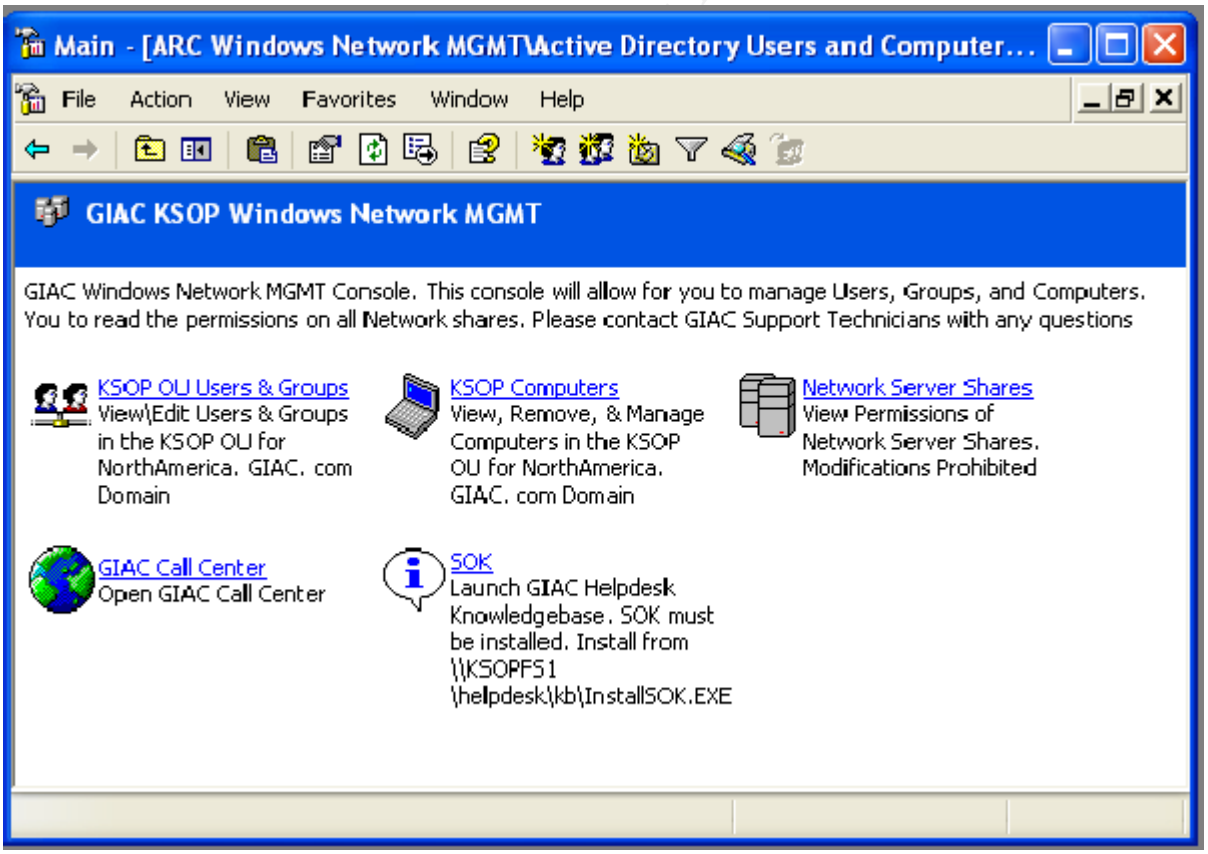


Figure 4 - Helpdesk Administrative MMC

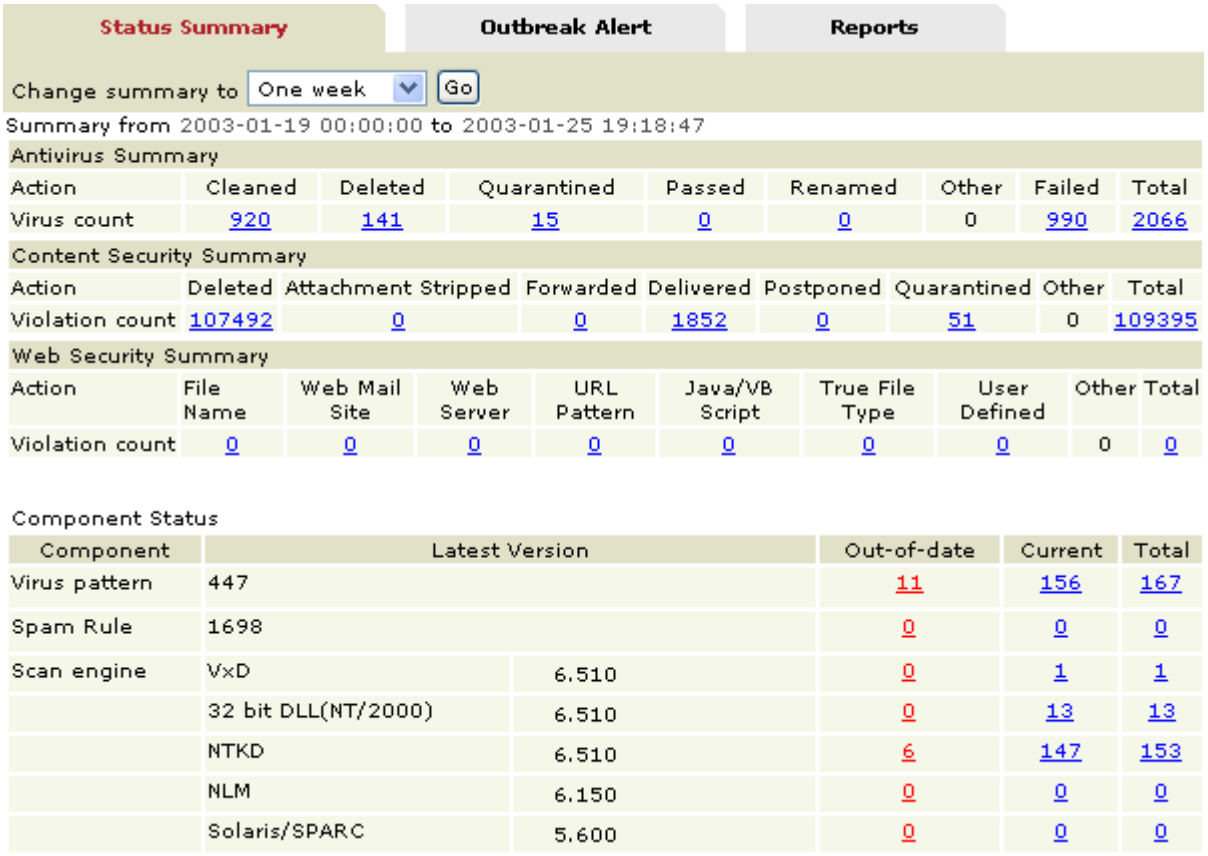
AntiVirus \ AntiSpam

GIAC has chosen Trend Micro as its antivirus software and anti-spam and content filter for email messages. GIAC is using the following Trend Micro Products:

- Scanmail for Exchange Server 5.5 v 3.8
- InternetScan Messaging Security Suite v 5.12
- Server Protect for NT v 5.35
- OfficeScan Corporate Edition v 3.54
- Trend Micro Control Manager v 2.5

Scanmail watches email for viruses, while ServerProtect and OfficesScan do the same for servers and workstations respectively. The InternetScan Messaging and Security suite does a little more. Not only is it watching email for viruses, but also is evaluating the content of messages flowing into and out of GIAC for content, pornography, profanity, etc… This allows us to keep a cleaner corporate image without losing face in certain situations. Also the product keeps spam out of our user's mailboxes. The spam rule is updated every twelve hours and averages blocking 300,000 email out of a total of 2 million a week.

The advantage to owning all these products from the same vendor is the use of the control manager management console. I can log into this portal and view at-a-glance the status of my virus pattern, scan engine, anit-spam pattern and see if clients and servers are behind. As shown in Figure 5 below:



Status Summary | Outbreak Alert | Reports

Change summary to One week Go

Summary from 2003-01-19 00:00:00 to 2003-01-25 19:18:47

Antivirus Summary

Action	Cleaned	Deleted	Quarantined	Passed	Renamed	Other	Failed	Total
Virus count	920	141	15	0	0	0	990	2066

Content Security Summary

Action	Deleted	Attachment Stripped	Forwarded	Delivered	Postponed	Quarantined	Other	Total
Violation count	107492	0	0	1852	0	51	0	109395

Web Security Summary

Action	File Name	Web Mail Site	Web Server	URL Pattern	Java/VB Script	True File Type	User Defined	Other	Total
Violation count	0	0	0	0	0	0	0	0	0

Component Status

Component	Latest Version		Out-of-date	Current	Total
Virus pattern	447		11	156	167
Spam Rule	1698		0	0	0
Scan engine	VxD	6.510	0	1	1
	32 bit DLL(NT/2000)	6.510	0	13	13
	NTKD	6.510	6	147	153
	NLM	6.150	0	0	0
	Solaris/SPARC	5.600	0	0	0

Figure 5 - Trend Micro Control Manager

In addition to the virus patter administrators can easily drill down to see the content being blocked and viruses being eliminated.

Hotfix and Patch Management

The ecora product patch manager is used to scan servers for potential hotfixes and can determine application level patches as well. SQL, Exchange, down to the OS can be scanned. This is incorporated into the maintenance window (mentioned previously) for each server. As the maintenance window comes up the vulnerabilities or upgrades are installed in a controlled environment.

Security Education

To better enable our systems administrators, and support technicians understanding of NT and networking security subscriptions to many of the major security mailing lists are archived in our Exchange Server Public Folders. This list available is:

- Bug Traq
- Cert Advisory
- Firewall Wizards
- Incidents
- NT Bug Traq
- SANS NewsBites

- SANS NT Security Newsletter
- Security Alert Consensus

Additionally our systems administration team is encouraged to attend local chapters of network security groups. The local ISSA chapter meets every third Thursday in a building on our KSOP campus.

Physical Access to the Data Center

The main data center located at the KSOP site has recently been reconfigured. Prior to the new design the practice was to just let anyone in that said they wanted to gain access. Now the process is much more difficult. First you must show your ID to the Team Lead on duty and sign in with a signature, purpose and duration. On exiting you must sign out. In addition to that process if a vendor is on sight a designated team member must be with them at all times while they have access to the new data center. To further increase our security, Compaq racks are being purchase that have locking mechanisms and can be controlled through the web.

References

Microsoft ; FSMO Placement and Optimization on Windows 2000 Domain Controllers
http://support.microsoft.com/default.aspx?scid=kb;en-us;223346

Microsoft ; Active Directory Branch Office Deployment Guide
http://www.microsoft.com/windows2000/techinfo/planning/activedirectory/branchoffice/dply09.asp

Fossen, Jason ; Securing Internet Information Server 5.0, Sans Institute, 2002

Ferraiolo, D., Lynch, N., Toth, P. Minimum Security Requirements for Multi-User Operating Systems (NISTIR 5153). National Institute of Standards and Technology, 1993

Security Operations Guide for Windows 2000 Server
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/windows2000/staysecure/secops03.asp

Last Updated: July 25th, 2017

Upcoming Training

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