GIAC Certification
GCWN Practical Assignment
Version 3.2
Option 1

Merging between SANS Co. and GIAC Enterprise.
Consolidation of company's network infrastructure.

Prepared by: Diego Travaini

April 13, 2004

Introduction on the paper

This paper is a practical assignment for the SANS GIAC Certified Windows Security Administrator (GCWN) program. It's based on the specs of version 3.2, so a merging between two fictional companies is considered. Each of these two companies have an extensive Active Directory (AD hereafter) infrastructure, and this prerequisite ruled out the option of migrating one forest to the other.

Here is given a brief overview of the entire paper, which describes the different aspects of a secure deployment of a network infrastructure based on Microsoft technology.

The first chapter is descriptive and gives only a simple overview of the companies we are speaking about, describing their business and the reasons of the merging between them.

The second chapter is about the network design and the active directory structure adopted by each company. The design of a company's network and active directory is based on the GCWN practical of Jason Lamb (http://www.giac.org/practical/Jason_Lam_GCWN.pdf), used as a reference and adapted to my needs. The second design is a new one, created for this paper.

The third chapter is about the company's organization after the merging, and shows the strategy chosen to integrate the two networks and the new active directory structure adopted: the main goal of this section is to obtain a manageable system that simplify administration and reduces IT overhead.

The next chapter, the fourth, speaks about group policies and describes how the newly-merged systems are configured: it explains the parameters configured, their management through a multiple forest environment, and demonstrates the results of the group policies applied on a sample server.

The fifth chapter is about auditing and discusses the auditing method adopted by the IT staff of the merged company, including gathering and managing of event logs produced by every server and by IIS log: the whole configuration of the system is analyzed, and sample reports are shown.

The last part of the paper contains the appendix and shows the scripts and snapshots produced during the environment test of and its configuration.

Preface to the technical discussion

Background information on both the companies will be presented here.

Sans Co. (SANSCO hereafter) is an international company, founded in San Jose (CA) about ten years ago. Its main business is selling of a broad range of product regarding Uninterruptible Power Supplies (UPS) for the midrange and professional market. SANSCO develop internally every product: until now this company has based its whole business on professional family of product for the high availability market.
During the past years this company has grown a lot, starting from a little office built around the R&D department located in the States, becoming an international company, with headquarters all around the world.
Now SANSCO has a production facility located in Brazil, the main R&D department located in Israel and a European office located in Hamburg (Germany).
US office is the main headquarter, now its main purpose is to keep contact on the North America's market: the European office achieves the same goal in Europe. Each office has a support unit, meant to help customers, and a small R&D unit, which assists customers and implements little changes, like localization.
The purpose of the facility in South America is to build and test new models of UPS.
The main R&D unit is wholly located in Israel, and it's growing by acquiring new technologies by locale start-up companies: the main UPS software team is also located here.

Now this company is exploring a new business market: production of power supplies. The objective of this decision is being able to offer a complete solution about power needs of their customers, becoming their main referring in this field.

The second fictional company we consider in this paper is called Giac Enterprises (GIACENT from now) and its main business is the production of a broad range of power supplies for the IT market, spreading from middle-range servers to network appliances.
GIACENT started with a commercial office located in Taiwan, acting as a distributor of power supplies for the IT market. After a rapid growth, GIACENT became itself a developer of power supplies, focusing its core business on these products, and signing contract with other fast-growing Taiwanese companies.
For this reason GIACENT built a plant in China, whose task is research, develop and build its portfolio of products.

GIACENT is now a well know company in Asia, and has partnership with other Taiwanese companies. GIACENT consolidated its position in the power supplies market, and its main competitor is far behind it. Now it's willing is to expand the business: the next step may be offering a technologically rich product portfolio, which grants more revenues.

Starting from these assumptions, SANSCO e GIACENT realized that their needs may be met by joining their capabilities, to gain a competitive position in the power supply market.
So, a fusion between the two companies was decided: SG Enterprise was born (SGENT from now).
SANSCO can offer its know-how in production of UPS, and its distribution chain in America and Europe. GIACENT bring its client portfolio of VAR and integrators in Taiwan, not to mention its production facility in China, that offer a valuable and cost effective quality at low price.
After the merging GIACENT will be able to push UPS in the Asian market, using an aggressive pricing policy; the same product family will became more cost attractive in Europe and America.

On the other hand, SANSCO can increase its influence in Asia, and, at the same time, enlarge its product range with a complete family of power supplies at an interesting price, pushing them to its clients in Europe and America, trying to become the main reference concerning power source of the high end market.

We have exposed the surroundings of the merging between the two companies.
From a technical point of view, the interesting part is to arrange a reliable and effective solution permitting interoperability between the two different networks.

Overview of the two companies Network

In this chapter a brief overview of the two companies will be given, just to explain their organization before the merging. After a short introduction the network infrastructure and the active directory deployment chosen by each company will be described.

Description of SANS Co.

The growth of the company, due to its success on the market, required the planning and deployment of an extensive network infrastructure, able of supporting the needs of SANSCO.
The company started from a small office, but after few years three other offices opened abroad: this shows the need of a flexible network design, capable of supporting the growth of the company, without posing limitations on performance and manageability.
SANSCO internally produces and sells software bundled with their UPS: this software helps managing and reporting power failures. Its website has an extensive section regarding support and upgrades of this software, and also a trial section is present: a complete FAQ zone, used for reporting problems and for obtaining answers. It's also provided a dynamic website, with a backend database server that hosts a forum about software problems.

Here will be shown the final architectural design of both the network and the Active Directory deployment: the main goal of these two designs is to scale, simplifying future expansion.

Network Design

At the time of writing SANSCO network is made up of four different offices around the world.

United States office:
It's the originating building, where all started, now mainly dedicated to marketing and representation for the American market. There's also a small development group, mainly for personalization of the UPS software. A small IT department is responsible of managing the network and servers, and as helpdesk for the personnel workstations. The company's website is hosted here, administered by the local IT staff.

South American's office:
This is the production facility, located in Brazil. Only a minimal financial and human resource group is present. An IT group is also present for internal support.

European Office:
This office is SANSCO's bastion in Hamburg, mainly for commercial needs: its role is analogous to the United States office.
A small development group is responsible of internationalization of UPS software, manuals and brochures. IT is present only for internal support.

Middle East Office:
This is the research facility, located in Israel. Its purpose is research new products and to develop the main code of UPS software. IT is present for supporting and securing local servers.

Based in this structure, we can summarize staff duties at SANSCO:

	US Office	SA Office	EU Office	ME Office	Total
Develop	2	20	2	20	44
Financial	5	3	5	3	16
Human Resources	5	5	5	5	20
Sell	15	0	15	0	30
IT	6	4	4	5	19
Total	33	32	31	33	129

Table 1 - SANSCO employees distribution.

Each headquarter adopts a unique numbering structure, as shown in the following picture.
This arrangement allows a simple and clear identification of the source machine, and the creation of a new office isn't a problem.

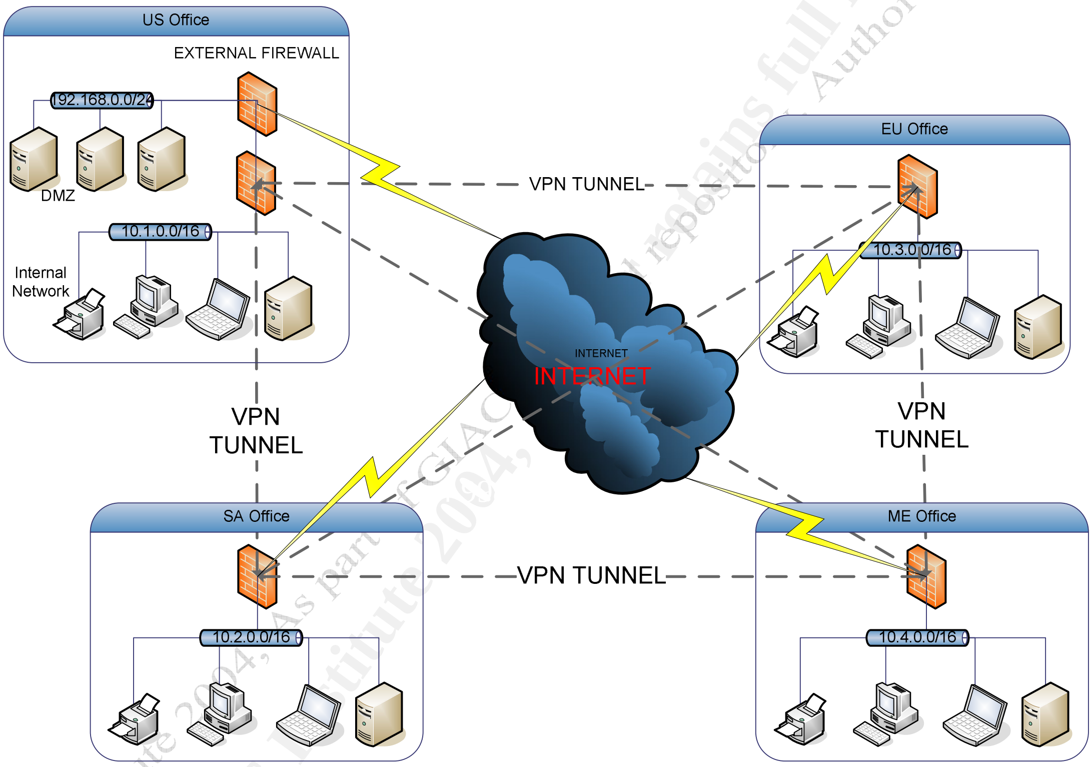


Figure 1 - Schematic design of SANSCO network.

The main office has a particular difference; two separate private networks are made here: 10.1.0.0/16 is used by internal servers and workstations, and 192.168.0.0/24 by the DMZ, whose servers are translated to the internal network in the range 10.0.0.0/16.
That's because the North American headquarter hosts the corporate web site: a DMZ allows a secure and manageable administration of these machines exposed on the web.

In general each office's internal network is protected from the internet by a firewall with strict policies about inbound and outbound traffic: only requests from internal network are allowed. Another goal of that firewall is to avoid internal addressing being showed to external network (egress filtering)[1]. These firewalls are responsible of linking each headquarter to the others using an IPSec VPN tunnel through the internet.

[1] Egress filtering for a healthier Internet

A second firewall is present at the North American office, due to the DMZ: a set of ACL rules allows only traffic due to DMZ server's administration from inside, internet traffic requested by internal network and IPSec tunnel generated by the innermost firewall.

The DMZ is made up of two web servers (based on IIS 5.0) in load balancing and two domain controllers used as local DNS: also a backend database (a SQL Server 2000) and a mail server are there.

The internal network consists of staff's workstations (both Windows 2000 Professional and Windows XP Professional) and internal servers: two domain controllers (used also for internal DNS), a fileserver, a mail server and development servers.

Active directory structure

To achieve better manageability of its resources, about two years ago SANSCO set up an internal active directory structure (based on Windows 2000 Server) made of four domains, one for each geographical region: North and South America, Europe and Middle East.

This deployment permits good manageability of resources in each of the headquarters, allowing different settings to be applied at each domain, accordingly to local preferences.

The internal root domain is named SANSCO.COM; the other three AD domains are named after the geographical location, in the following way:

- EU.SANSCO.COM
- SA.SANSCO.COM
- ME.SANSCO.COM

These four domains made up the internal forest; the external forest (SANS.COM) is built around the servers placed in the DMZ: this forest is under direct administration of the US office's IT group.
The naming schema adopted implies a parent/child relationship between the internal domains, due their DNS names: this relationship in not present and not wanted between the internal forest and the DMZ forest.
DNS in DMZ haven't references to internal domain, at opposite, internal domain references external domain DNS.

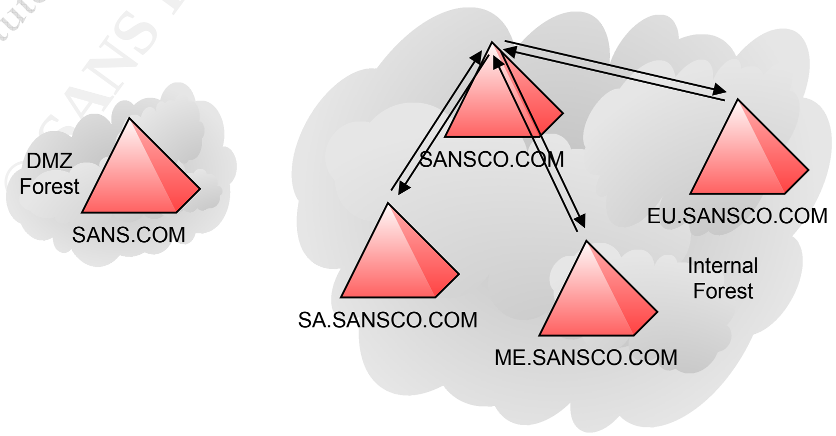


Figure 2 - SANSCO AD Network.

http://www.hackinglinuxexposed.com/articles/20030213.html

The previous picture depicts the two way trusts established between the four domains in the internal forest: no other trusts are configured between these domains, because only sporadic access to others domain's resources was needed, making creation of additional trusts an option.
No trust was established between the main forest and the DMZ forest: this would lead to weaker security. Administration of the external forest is in charge of the IT staff of the US office: each member responsible of the external forest has a separate account there. An internal company policy denies the same password to be used.

Each domain has two domain controllers (DC1 and DC2): this choice give a good level of fault tolerance, allowing redistributions of FSMO roles between the two servers. This design might seem over dimensioned at child domains, but SANSCO thinks that reliability is a key issue and using two domain controllers allow better fault handling.
The US headquarter has a different distribution of FSMO roles: it's the first domain of the forest, so its domain holds schema master and domain naming master roles, which are forest wide roles.
The same considerations apply to DMZ servers, which form another forest.

The following arrangement was setup, accordingly with Microsoft recommendation[2]:

	US domain and DMZ domain	Other domains
DC1	Schema Master Domain Naming Master Global Catalog	PDC Emulator RID Master Global Catalog
DC2	PDC Emulator RID Master Infrastructure Master	Infrastructure Master

Table 2 - FSMO roles distribution at SANSCO.

SANSCO, in order to take advantage of Active Directory planned a wide use of Organizational Units (OU)[3] allowing delegation of administration by means of Group Policy.
In general, the following OU structure is present in each domain:

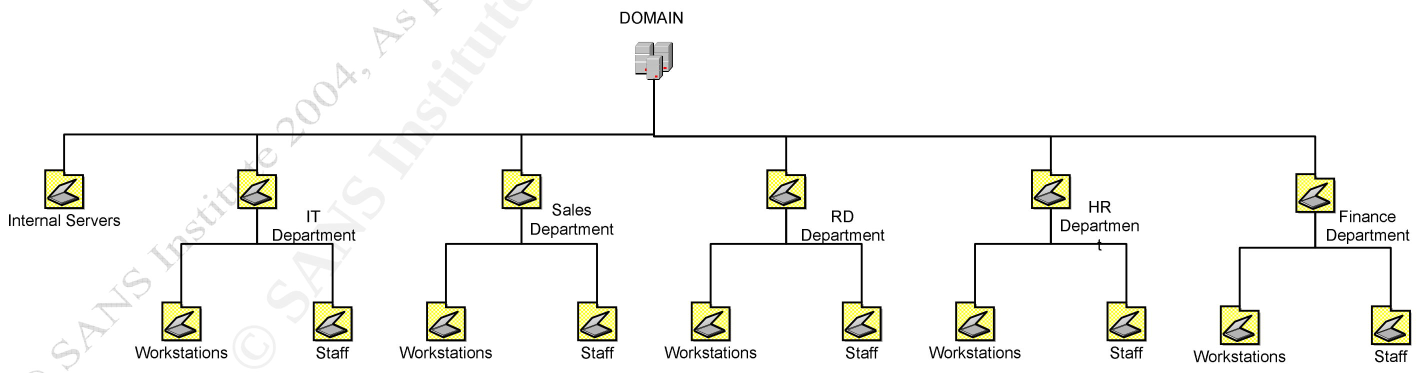


Figure 3 - OUs created in each domain at SANSCO.

[2] FSMO Placement and Optimization on Windows 2000 Domain Controllers (http://support.microsoft.com/default.aspx?scid=kb;en-us;223346)
[3] Organizational units (http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_ADintro_19.asp)

Each department OU holds user accounts and computer accounts OUs. Depending on the domain considered, OUs corresponding to departments which aren't characteristics of the headquarter are left empty.
DMZ forest has a slightly different OU structure, due to its nature: only separate OUs for servers and an OU for administrators are present.

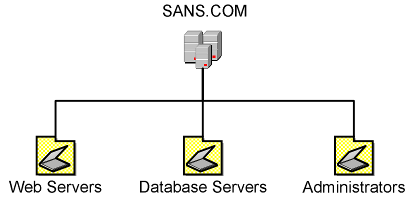


Figure 4 - SANSCO DMZ OUs.

This articulated design allows gaining advantage of some Active directory features, like delegation authority and group policy. Each OU in the internal forest delegates administration to a user in charge of that department (the manager), and group policy specifically meant for that OU can be applied.
SANSCO adopt the NSA security configuration guidance for both servers and workstations: no personalization was made during AD deployment.

Description of GIAC Enterprise

For the network design we'll consider the GCWN practical of Jason Lam. This practical depicted a complete network solution for the company, which fits the needing of this practical.
Here we'll present only a brief discussion of the structure of GIACENT, tailoring the design to my needs.

GIACENT is an aggressive company, whose plans are to grow a lot, so it built an active directory network infrastructure, ready for future enhancement.
GIACENT offers a dynamic website, but doesn't require a backend database for this purpose: it offers only datasheet and specifications of its broad range of product and nothing more. Support is offered only by email and only to customers. For load balancing and failsafe, a couple of IIS servers are arranged.

Network Design

GIACENT network is depicted in the next page: it's logically divided in two trunks, one for each building. At each facility a firewall protects the internal network.
At the main building two firewalls are present: the external one filters traffic for the DMZ servers, avoiding unwanted traffic from the outside. The only traffic permitted is due to DMZ server's management from inside, internet traffic requested by internal machines and IPSec tunnel generated by the innermost firewall.
The second firewall segment the different inner networks and does NAT, allowing communications between internal and DMZ hosts. This firewall is IPSec VPN capable, and creates the tunnel link with other's building firewall.
The firewall at the satellite building provides only segmentation of internal network, support of the IPSec VPN tunnel and filtering of the internet traffic generated by internal machines.
This design allows an easy expansion of the network, due to the birth of new buildings: it's necessary to provide a VPN tunnel between each headquarter.

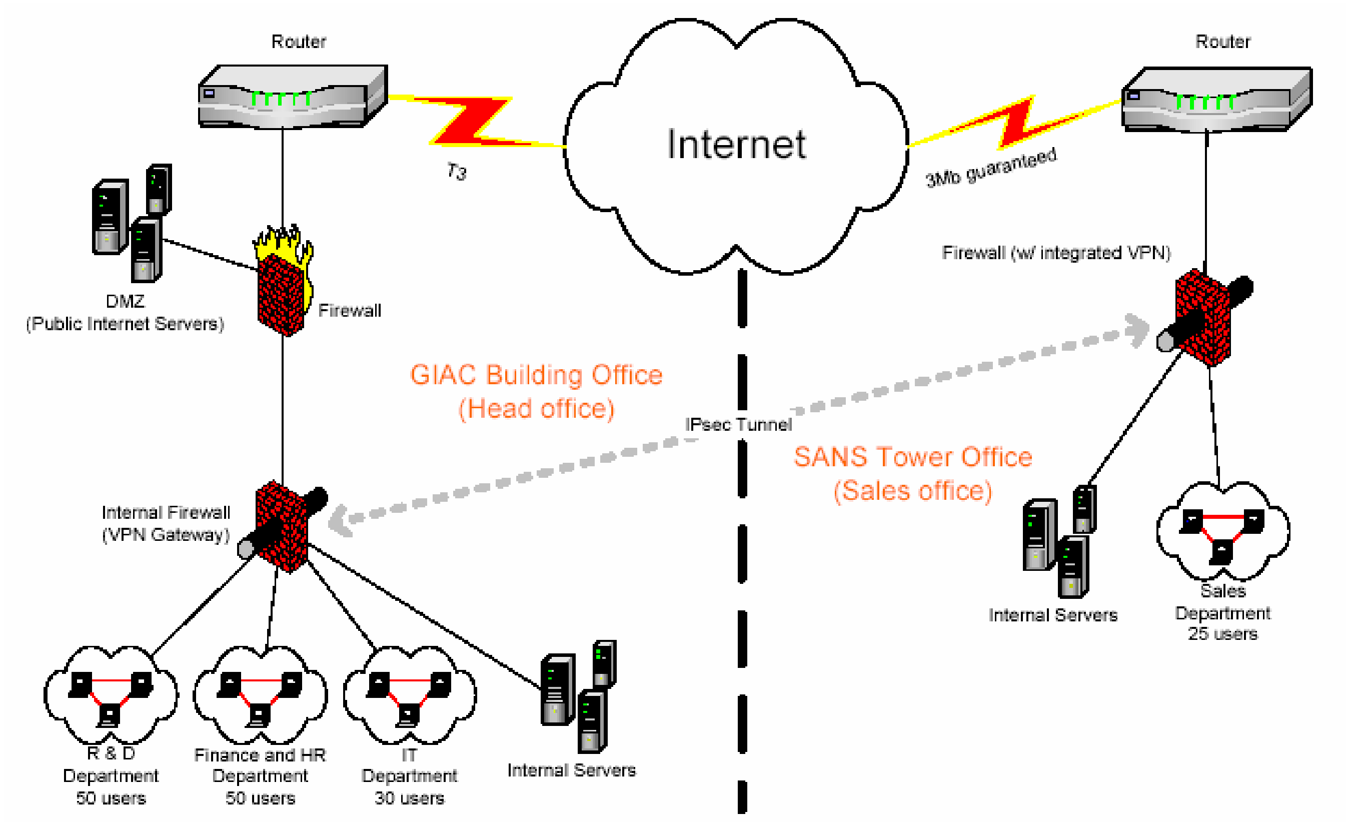


Figure 5 - GIACENT Network diagram.

Active directory structure

At the time of writing, GIACENT internal network is logically divided in two domains, one for each geographical location. These two AD domains are named GIACENT.COM and CN.GIACENT.COM, as stated in the following picture.

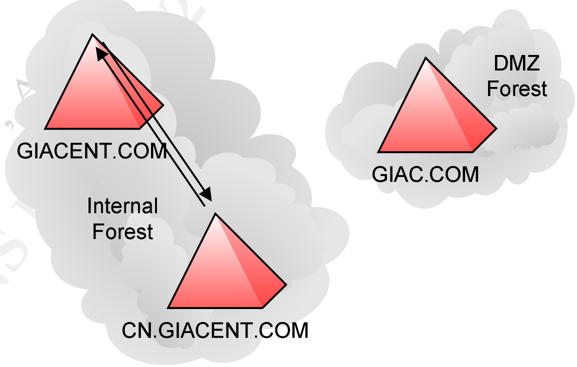


Figure 6 - GIACENT AD deployment.

A separate forest is created for the DMZ's servers (web servers, database server, DNS server and mail server): this subdivision logically isolates these servers from the internal network, tightening security.

The AD deployed at GIACENT takes advantage of Organizational Units: they permit a logical representation of the each department, allowing administration, delegation and enforcing security.

An organizational unit is created for:

- Internal servers
- IT department

- Sales Department
- R&D Department
- HR and Finance Department

Unlike the internal servers OU, which contain only servers, other OU's contain users and workstations specific for the department.

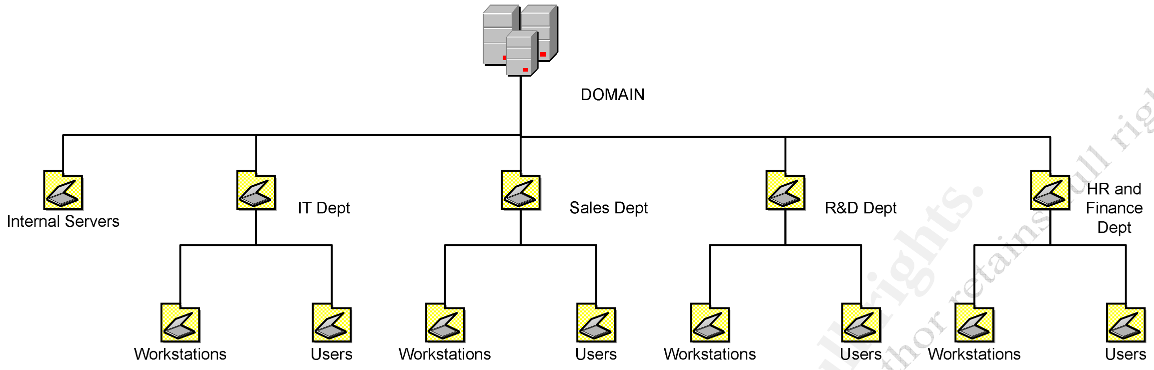


Figure 7 – GIACENT's internal domain OUs hierarchy.

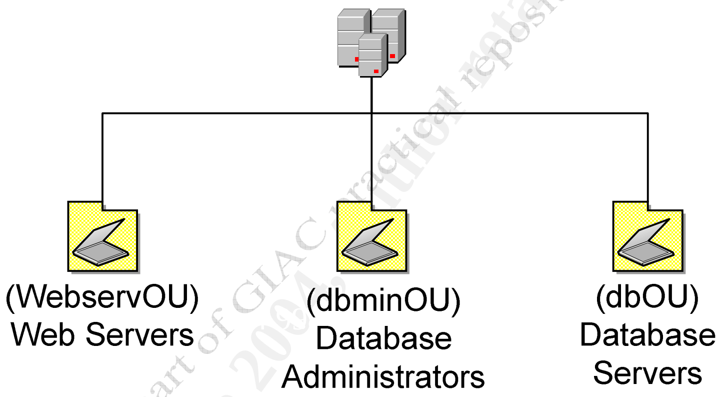


Figure 8 – GIACENT's DMZ domain OUs hierarchy.

GIACENT infrastructure relies on Group policies to enforce security: the group policies are based on NSA recommended configuration, slightly modified by the company's IT staff. Separate families of group policies are applied on servers and workstation, based on its forest's belongings.
A detailed description of these policies can be found on the GCWN mentioned at the beginning of this paper.

Merging between Sans Co. and Giac Enterprise

From the IT point of view, the fusion between the two companies must allow, and eventually enhance, the information flow between the parent networks, giving the best interoperability possible without reducing security.
Through this design I'll provide for SGENT a secure IT infrastructure, based on the assumption that each organization has arranged a security plan and has setup internal procedures in order to protect the information path between each geographical location and, internally, in each internal network.
This goal may become complex since we want to join two network infrastructures developed with different characteristics, where different choices was taken.
Starting from this assumption, we must develop a solution that must allow the best possible interoperability between SANSCO and GIACENT.
First the resultant design of the merged network will be shown and after the integration between the two Active Directories.
The next section is about Group policies applied to the resulting multiforest environment, with a analysis of the policies used for an internal web server.
Auditing is the topic of the last section of this paper.

Resultant Network Design

Each company's network was designed to allow communication through a secure channel between the different headquarters. This goal was achieved establishing an IPSec VPN channel between the firewall of each location. This deployment allows additional secure paths to be established when a new office is added, due to company's expansion.
Starting from this assumption, we can link the two networks establishing additional paths between each headquarter of SGENT, extending the original design by considering existing buildings as new offices added abroad.
This purpose is achieved configuring firewalls at each VPN tunnel's boundary. It's important to remember that each internal network has its numbering schema, and a NAT is still necessary. Luckily, SANSCO internal network didn't adopt the same numbering of GIACENT's: that simplifies the merging between them.

Next, it's mandatory to configure each DNS server to forward request to the other. It's a good choice setting conditional forwarding between SANSCO DNS and GIACENT's.

As stated in the introductory section, GIACENT has only a representative website, not designed for e-business. At the beginning of the fusion's process, the two DMZ are maintained and only minimal changes to web pages are made to reflect the merging: after this phase, the migration of GIACENT's website on SANSCO's web servers must be evaluated: this option allows a better manageability and reduces the global TCO of the DMZ.

The picture in the next page represents a schematic network design after the merging.

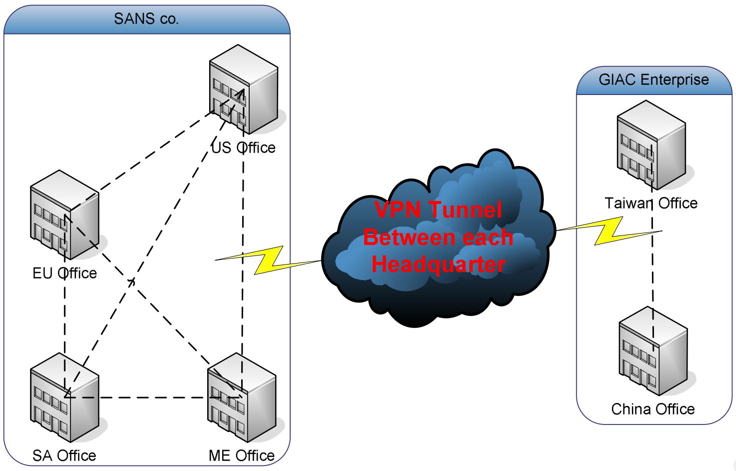


Figure 9 - Resultant network link after the merging.

Active Directory Trust

Each of the two original companies has an extensive AD infrastructure, based on two forests with multiple domains. Each company arranged a separate forest, which hosts the external IIS website and the backend database. This secondary forest is located in the DMZ and is populated only by servers and by accounts necessary to manage them.

Let's start considering the two internal forests: the same roles are present and also special resources that must be shared with adequate security.
For this reason a trust must be established between them: we must consider that the AD schema, global catalog and NC are different, so we have to allow interoperability avoiding synchronization between these forests[4].
The windows AD technology provides a variety of possible trusts[5], but only two of them might be suitable for our needs, and each one has a drawback to consider.
When the two forests were established Windows 2000 AD was used, so we start discussing the chances this technology provides.
Starting from this assumption, the best solution is establishing two external trusts between the two forest's root domains (called GENENT.COM and SANSCO.COM): external trust derives by the backward compatibility with Windows NT4 domains, and allows resource's sharing without synchronization between the two AD. The negative aspect comes from its non transitivity, so only the two root forest domains can share resources, not their children.
If we choose this technology, we must provide other external trusts between the child domains.
The other option is upgrading every domain in the forests to Windows 2003 server, to take advantage of a new feature of this operating system: forest trust[6]. With forest trust a transitive trust without synchronization can be established between the two forests. We must explicitly define the trust in both domains, in order to obtain a two way trust.

[4] When to create a forest trust
http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/x_c_whencreateforest.asp

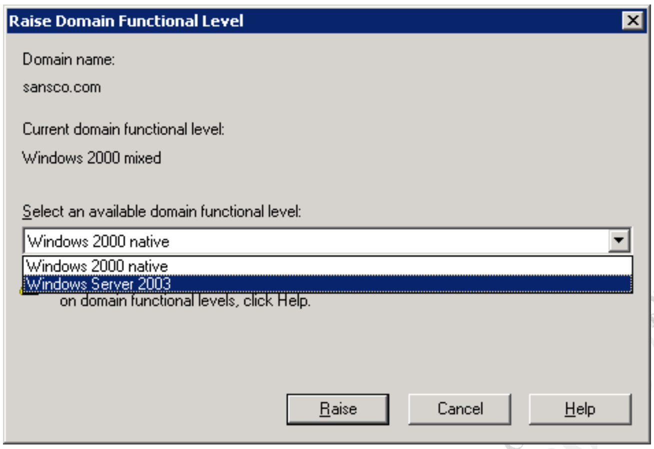
[5] Trust types
http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/domadmin_concepts_trusts.asp

[6] Forest trusts
http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/x_c_foresttrusts.asp

This solution also has a drawback: it requires the upgrade of every domain server (not the member servers) to Windows 2003 server and setting the forest functional level in both forests to Windows Server 2003[7].

This is an additional cost of the merging, taking into account at least two licenses must be paid in each domain: this lead to of 20 licenses only for the domain controllers, to which add licenses for additional servers, like the web servers.
The second one is the taken option for the merging: upgrading all domain controllers to Windows 2003 allows other features[8] of this operating system being used, like, for example, the improved IIS v. 6.0 and a better management of group policies through forests.

To raise domain functional level we must open "*Active Directory Domains and Trusts*", right-click the on the domain name node and then click "*Raise Domain Functional Level*"*:* picture 10 show the window that appear. Select *Windows Server 2003* and click *Raise* to apply the changes. Once the domain level has been set to Windows Server 2003, it cannot be changed back to Windows 2000.
To raise forest functional level select "*Active Directory Domains and Trusts*" node and click "*Raise Forest Functional Level*"*:* picture 11 show the window that open.


Raise Domain Functional Level

Domain name:
sansco.com

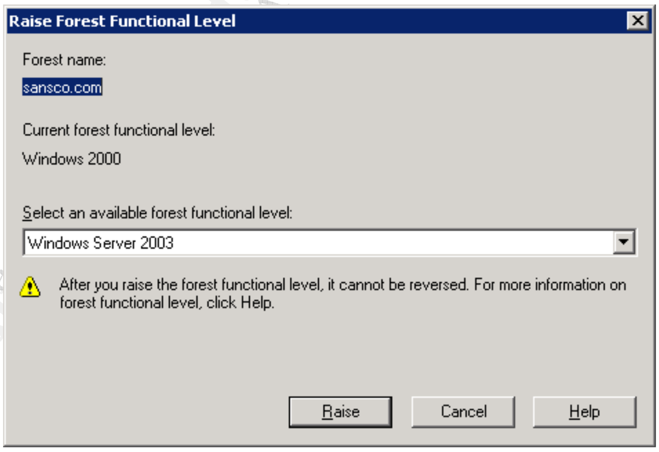
Current domain functional level:
Windows 2000 mixed

Select an available domain functional level:
Windows 2000 native

Windows 2000 native
Windows Server 2003

on domain functional levels, click Help.

Figure 10 - Raise domain functional level.


Raise Forest Functional Level

Forest name:
sansco.com

Current forest functional level:
Windows 2000

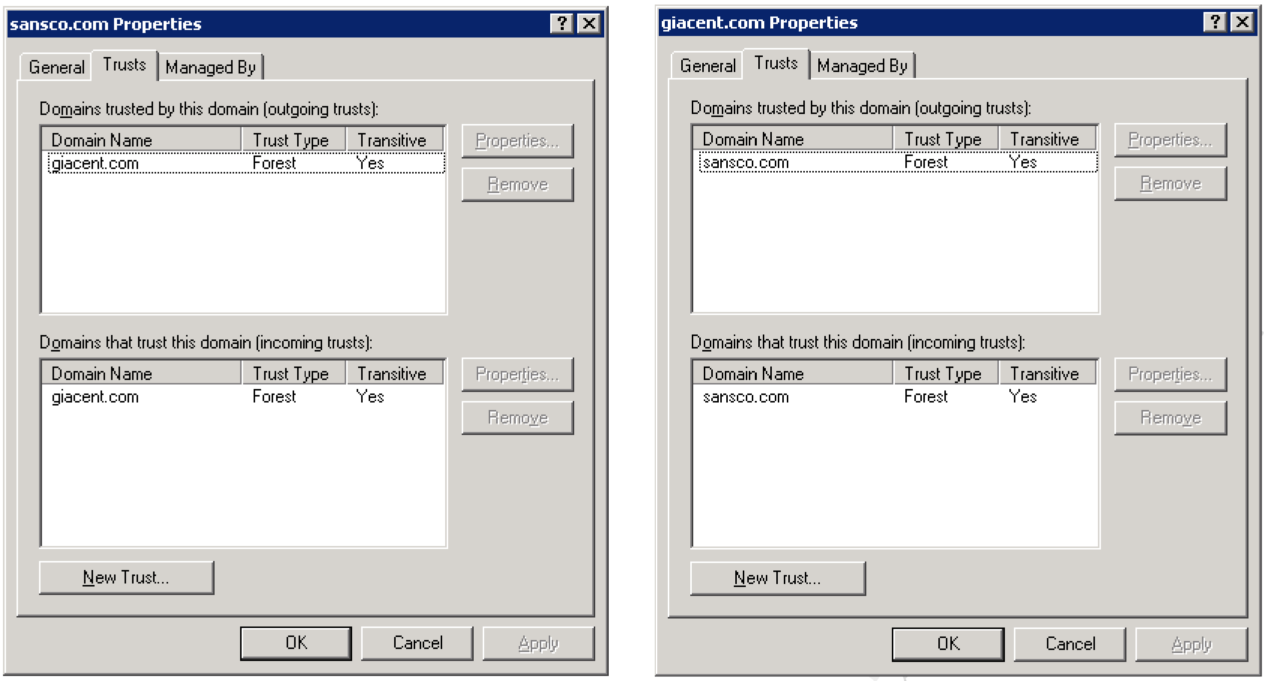
Select an available forest functional level:
Windows Server 2003

After you raise the forest functional level, it cannot be reversed. For more information on forest functional level, click Help.

Figure 11 - Raise forest functional level.

The next step is to configure the forest trust.
Using *Active Directory Domains and Trusts*" right-click on the domain name node and then click properties: on the *"Trust"* tab click on the *"New Trusts…"* button and follows the instruction prompted by the wizard. It's possible to establish a two way trust between the forests, using an account authorized to establish trust in the foreign forest when prompted.
At the end of the process the trust tab on both of the domains will appear like the two pictures in the next page.

[7] To raise the forest functional level
http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_changeforestlevel.asp
[8] Top 10 Benefits of Windows Server 2003
http://www.microsoft.com/windowsserver2003/evaluation/whyupgrade/top10best.mspx



sansco.com Properties

General | Trusts | Managed By

Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
giacent.com	Forest	Yes

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive
giacent.com	Forest	Yes

giacent.com Properties

General | Trusts | Managed By

Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
sansco.com	Forest	Yes

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive
sansco.com	Forest	Yes

Figure 12 – Resultant forest trust.

Using forest trust solves the interoperability issue, but we must not forget the trust is established only between the two root forest domains: this implies that the resource requests in the foreign domain must refer to a TGT issued by the root domain: this causes the growth of the trust path between child domains.

In these circumstances it's a good choice to setup shortcut trust[9]: creating shortcut trusts is useful when there is frequent access to resources in foreign domain and the number of domains in the trust path increases. Shortcut trusts can reduce the traffic through the root domain, optimizing the authentication process.
Creation of shortcut trusts[10] is done with the *"Active Directory Domains and Trusts"* MMC snap-in or, more easily, using the *netdom* command (part of the support tool) in the following manner:

netdom trust *TrustingDomainName* **/d:***TrustedDomainName* **/add /twoway**

Shortcut trusts are established between domains with equivalent tasks, but adding trust between each domain in the two forests doesn't seem to have any drawback on the performances of the network.
Starting from these assumptions, the definitive relationship between the two AD forests is depicted in the picture that follows.

[9] When to create a shortcut trust http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/domadmin_concepts_windowstrust.asp

[10] To create a shortcut trust http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/domadmin_createshorttrust.asp

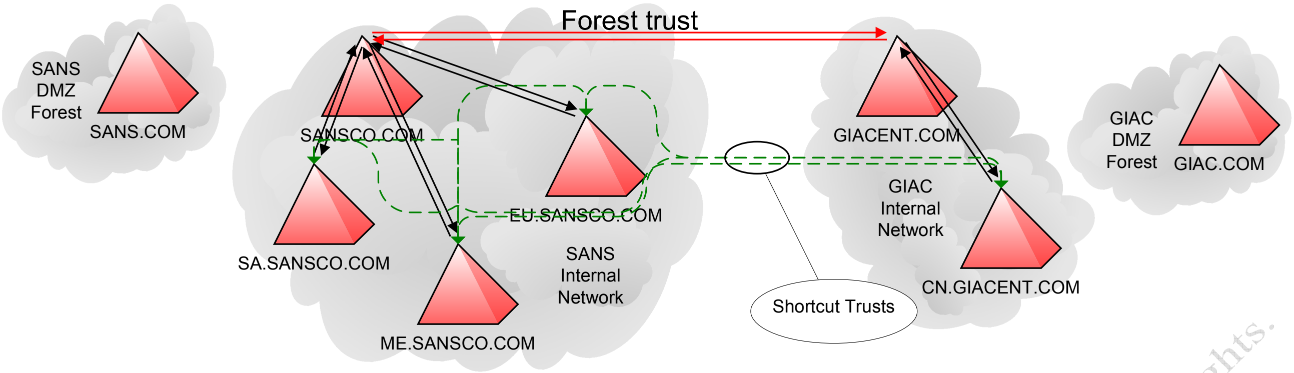


Figure 13 - Resultant trust between the two companies.

The two DMZ forests are left with no trust link with the other forests: this tighten security without complicating management. IT staff has an administrative account in these forests, and policies can be managed using Group Policy Management, a featured tool introduced with Windows 2003, discussed in the next section of this paper.
This easy management is the key reason to decide not altering the original design, at the first step of the merging

Deployment of a WebDAV server

Now is necessary to give a brief overview about this server, and why SGENT chooses to deploy this service.
The WebDAV[11] server offers a flexible resource accessible by each user of the domain, simple than a FTP service or a generic file server with shared folders: employees can access public and restricted folders, using their browser, from inside any Microsoft Office products or with third party software WebDAV compatible: this allows a better information handling, held in a centralized, well secured location and under regular backup. This solution avoids document dispersion over different file server or, in the worst case, on the personal workstation of the employee.

Every worker has a personal folder where he can backup all the documents he is working on: he has read and write permission on the resource, and he can also create subfolders in it.
Every department can setup as many folders as needed, reflecting every project it's working on: this task is delegated to the department's manager, which can also give the appropriate rights to every worker involved in the project.

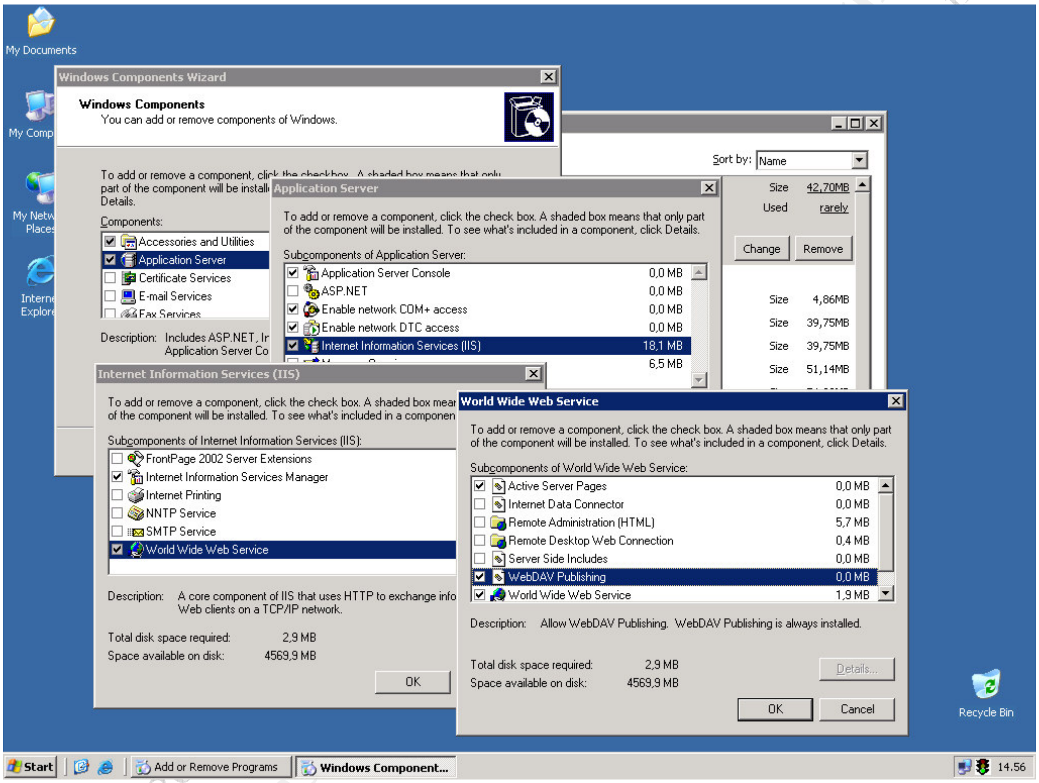
This service wasn't offered by SANSCO or by GIACENT: after the merging, the company's IT staff decides to deploy a dedicated IIS WebDAV server in each building. This reason arises because IIS v. 6.0 is considered more robust than the previous versions, which suffered for series of flaws related to this service[12].

The option of having only a centralized WebDAV server was ruled out: each building holds local information, some of them restricted, and mixing them, even if protected by NTFS permissions, wasn't considered safe. After this deployment, giving each working group a separate server will be considered.

[11] http://www.webdav.org
[12] The last reported flaw of IIS related to WebDAV is from 07 Mar 04 (http://www.kb.cert.org/vuls/id/117394). The following link (http://www.cert.org/current/archive/2004/02/27/archive.html) report W32/Welchia.D to benefit from a flaw in Microsoft implementation of WebDAV in IIS 5.0

Starting from this assumption, we consider a new IIS server hosted in the internal domain of US headquarter. The setup follows the recommended guidelines about dimensioning and partitioning for an IIS server[13]: briefly was chosen a partitioning schema that separates data from the system partition, and also a partition for the swap file was set.
We'll assume that every employee has a personal directory for storing his files, on which it exercises full control: these folders are contained in a department folder, which also hosts restricted folders, accessible only from few employees. This directory tree reproduces the OU's hierarchical structure adopted.

Windows 2003 comes with a reduced number of services active by default compared to the previous version: IIS and WebDAV aren't two of them, so a manual installation is necessary. The following picture reassumes the steps necessary for having IIS and WebDAV running.



Windows Components Wizard

Windows Components
You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be install… Details.

Components:

☑ Accessories and Utilities
☑ Application Server
□ Certificate Services
□ E-mail Services
□ Fax Services

Description: Includes ASP.NET, Ir… Application Server Co…

Application Server

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Application Server:

☑ Application Server Console 0,0 MB
□ ASP.NET 0,0 MB
☑ Enable network COM+ access 0,0 MB
☑ Enable network DTC access 0,0 MB
☑ Internet Information Services (IIS) 18,1 MB
6,5 MB

Internet Information Services (IIS)

To add or remove a component, click the check box. A shaded box mear… of the component will be installed. To see what's included in a componen…

Subcomponents of Internet Information Services (IIS):

□ FrontPage 2002 Server Extensions
☑ Internet Information Services Manager
□ Internet Printing
□ NNTP Service
□ SMTP Service
☑ World Wide Web Service

Description: A core component of IIS that uses HTTP to exchange info… Web clients on a TCP/IP network.

Total disk space required: 2,9 MB
Space available on disk: 4569,9 MB

OK

World Wide Web Service

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of World Wide Web Service:

☑ Active Server Pages 0,0 MB
□ Internet Data Connector 0,0 MB
□ Remote Administration (HTML) 5,7 MB
□ Remote Desktop Web Connection 0,4 MB
□ Server Side Includes 0,0 MB
☑ WebDAV Publishing 0,0 MB
☑ World Wide Web Service 1,9 MB

Description: Allow WebDAV Publishing. WebDAV Publishing is always installed.

Total disk space required: 2,9 MB
Space available on disk: 4569,9 MB

Details...
OK Cancel

Figure 14 - WebDAV installation.

After having setup the service, is necessary to prepare the directory structure needed, and to configure IIS to use these directories as virtual folders.
The directory tree's structure follows the OU organization of the domain: a folder for each department and subdirectories for each user in that OU.
This simplifies a lot the management of this feature: in fact IT staff wrote a script, scheduled on the WebDAV server, which creates the directories in the file system, if they where missing, and force the group policy being updated. In appendix B this script is shown.
Due to this characteristic, the WebDAV server is kept updated every time the script is run: IT staff needs only to add the users and inserting them at the group representing the department, and this task is achieved through the *"Active Directory Users and Computers"* console. Next the

[13] Deploying Internet Information Services (IIS) 6.0 http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/all/deployguide/en-us/iisDG60_overview.asp

administrator must choose access rights, through the WebDAV policy, to set the wanted permissions on the file system of the server.
The script scheduled on the server causes the directory being created and force the creation using the *gpupdate /FORCE* command on the WebDAV server, causing the policy being fully applied.

The next section of this paper drafts the policies chosen for this service.

Additional configuration of the servers

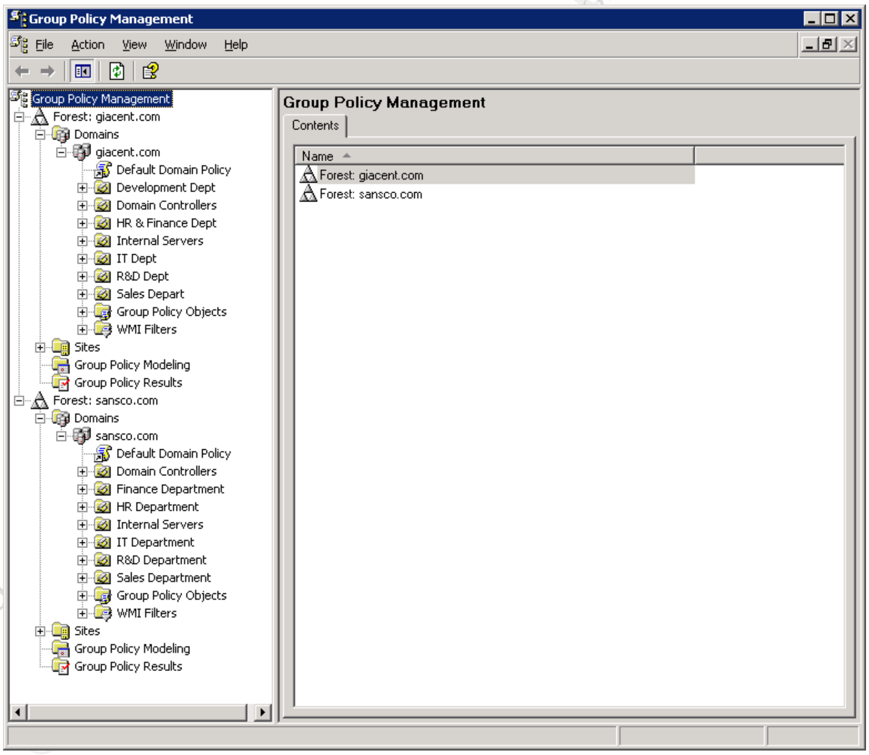
To improve log handling and auditing capabilities an additional service was deployed to each server of SGENT, a syslog service, to store and analyze in a centralized manner all the event that are logged locally. In the auditing section will be given more details on the software chosen and on the configuration adopted.
The auditing system requires two additional machines being prepared: the current implementation is based on a couple of windows machines. The operating system chosen is Windows XP Professional but also Windows 2000 Professional can be used.

Group Policy and Security

In this section, the proposed design of group policy for the merged AD network will be discussed. The main goal of this section is to create an organic and coherent directory environment, born from two AD deployment that have different behavior.

A key point to analyze is the distribution of group policies across a multi forest environment: when each AD was deployed Windows 2000 technology was available and administrators must provide by hand or with scripting to distribute policies between the forests.
Now, a new tool of Microsoft, Group Policy Management console[14], can be used: that make simpler replicating group policies across forests and backing them up and is also useful for managing DMZ forest's policies with a single interface, simplifying the whole Group Policy management of SGENT.
This tool can be used directly from the console of a domain controller, because every DC of SGENT was upgraded to windows 2003: this eases a lot administration of the whole AD environment: without the upgrade, administration must be carried out by a Windows XP console: the usefulness of this tool will be reduced.

A screenshot of that tool is shown below:



```
Group Policy Management
  Forest: giacent.com
    Domains
      giacent.com
        Default Domain Policy
        Development Dept
        Domain Controllers
        HR & Finance Dept
        Internal Servers
        IT Dept
        R&D Dept
        Sales Depart
        Group Policy Objects
        WMI Filters
    Sites
    Group Policy Modeling
    Group Policy Results
  Forest: sansco.com
    Domains
      sansco.com
        Default Domain Policy
        Domain Controllers
        Finance Department
        HR Department
        Internal Servers
        IT Department
        R&D Department
        Sales Department
        Group Policy Objects
        WMI Filters
    Sites
    Group Policy Modeling
    Group Policy Results
```

Forest: giacent.com
Forest: sansco.com

Figure 15 - Group policy management console configured for the two AD internal forests.

Policies are set at domain level and at OU level, so SGENT uses an incremental policies design.
Policies for the domain, domain controllers, IIS server and the new WebDAV server are shown here.

[14] Group Policy Management Console with Service Pack 1 runs only on Windows XP and Windows 2003, but can also manage Windows 2000 AD domains.
http://www.microsoft.com/downloads/details.aspx?familyid=c355b04f-50ce-42c7-a401-30be1ef647ea&displaylang=en

In the next pages I'll assume that the guidelines of *"Windows Server 2003 Security Guide"* release v1.3 of January 22, 2004[15] are adopted for each server of SGENT network: these templates are tailored for a particular functional server, and make distinction between "Member Server Baseline", "Domain Controller" and other specialized server like "Infrastructure Server", "File Server" and so on.
It's important to emphasize that passwords policies and account lockout policies are set up in a separate template, named *"Enterprise Client - Domain.inf"* or *"High Security - Domain.inf"*: so an incremental policy must be arranged for every server or workstation of the company.

For the employee's workstations, the NSA security configuration guidance for Windows 2000 and XP will be adopted.

Domain wide policies

SGENT adopts policies based on Microsoft templates: an incremental policy is built, accordingly with the checklist contained in the document mentioned above.
Different setting where applied by the IT staff on internal servers and DMZ servers, reflecting their different usage and the different threat they are potentially exposed: this lead to a slight change in the template proposed by Microsoft.
These changes were made using *"Domain Security Policy"* MMC snap-in.
In the followings paragraphs will be shown the choices taken for the whole domain.

Password Policies

The following table reassumes and compares suggested policies and the stricter one chosen for the internal domains and for the DMZ:

Policy	Microsoft's defaults	SGENT Setting (Internal Forest)	SGRNT Setting (DMZ Forest)
Enforce password history	24 password remembered	24 password remembered	24 password remembered
Maximum password age	42 days	30 days	15 days
Minimum password age	2 days	2 days	2 days
Minimum password length	12 characters	12 characters	12 characters
Passwords must meet complexity requirements	Enabled	Enabled	Enabled
Store password using reversible encryption for all users in the domain	Disabled	Disabled	Disabled

Table 3 - Comparison between Microsoft's and SGENT's password settings.

The minimum password length of twelve characters is suggested by Microsoft by default, allowing passwords to better resist against brute force attacks: for every SGENT domain this setting is used, because a minimum of 14 characters is allowed, and raising the limit by two characters doesn't make the difference.
Using so much characters is preferred, because the policy statement *"Password must meet complexity requirements"* forces the use of non alphanumeric characters inside passwords: so, may

[15] Windows Server 2003 Security Guide. http://www.microsoft.com/downloads/details.aspx?familyid=8A2643C1-0685-4D89-B655-521EA6C7B4DB&displaylang=en

be easier to adopt a relative simple phrase with non alphanumeric character than remembering a cryptic word only eight characters long.
A frequent change of password is required for DC at SGENT: password history's setting is kept, because 24 is the maximum allowed.

Account Lockout policies

Account lockout policy suggested by Microsoft, shown below, is considered not adequate for SGENT, and a strict policy is adopted:

Policy	Microsoft's defaults	SGENT Setting (Internal Forest)	SGENT Setting (DMZ Forest)
Account lockout duration	15 minutes	30 minutes	60 minutes
Account lockout threshold	10 invalid logon attempts	5 invalid logon attempts	5 invalid logon attempts
Reset account lockout counter after	15 minutes	30 minutes	60 minutes

Table 4 - Microsoft suggested lockout policy.

These three combined settings offers good response to brute force attacks against accounts.
IT staff has decided to increase *"Account lockout duration"* and *"Reset account lockout counter"*, to be less affected by hackers guessing passwords. For the same reason *"Account lockout threshold"* is reduced, to disable the account after a fewer number of wrong password entered.

I'd like to emphasize that without an adequate auditing of unsuccessful logons this policy became useless, because IT staff can't block an intruder if they don't know he's here!
The combination of these parameters could lead to a kind of denial of service: hackers guessing passwords can lead to a voluntary account lockout, avoiding legitimate users to utilize the system.
An adequate auditing system, like the one shown in the next chapter, can minimize that threat by reporting the attack to the administrators, making useless the hacker's work.

Kerberos Policy

Microsoft doesn't suggest a template about Kerberos policies, but the default settings of a Windows 2003 DC seems adequate for SGENT.

Policy	Windows 2003 default
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Table 5 - Windows 2003's default Kerberos settings.

Domain controller's policies

The last setting defined in the *"High Security - Domain.inf"* template is related to account lockout policies: the *"High Security - Domain Controller.inf"* template is required to set the following parameters, necessary to complete the domain controller's configuration through group policy.
The next settings aren't domain wide, and must be configured also on internal servers.
These settings where applied using the *"Domain Controller Security Policy"* MMC snap-in.

Audit policy

SGENT adheres to Microsoft template, shown below, only for few settings.

Policy	Microsoft Template	SGENT Template
Audit account logon events	Success, Failure	Success, Failure
Audit account management	Success, Failure	Success, Failure
Audit directory service access	Success, Failure	Success, Failure
Audit logon events	Success, Failure	Success, Failure
Audit object access	Success, Failure	Failure
Audit policy change	Success	Success, Failure
Audit privilege use	Success, Failure	Success, Failure
Audit process tracking	No auditing	No auditing
Audit system events	Success	Success, Failure

Table 6 - Auditing policies adopted at SG.

I'd like to emphasize that the setting about *"object access"* is potentially dangerous because can cause a great amount of data being logged, depending on ACL set on the file system: auditing only failures might be sufficient.

User rights assignment

The High security template proposed by Microsoft is modified only in the fields shown below, where everyone is removed from *"Bypass traverse checking"*:

Policy	SGENT Setting
Bypass traverse checking	Administrators, Authenticated Users

Removing *"Authenticated Users"* from *"Access this computer from the network"* causes the group policies not being applied, as stated in Microsoft Knowledge Base Article 262958.

Security options

Microsoft's high security template fits well SGENT's needing, and only interactive logon events are left unmodified, removing the personalized message proposed.

Event Log

Microsoft's suggested template is maintained only for internal few parameters, and shown below for thoroughness, but for SGENT's DC a slightly different one is chosen.
The log size parameter is a critical setting, together with the retention mechanism chosen. Microsoft suggests a relative small size and allows overwriting the event log if needed. This second choice is potentially dangerous because could lead to the loose of important events: a hacker could write in each event log, flooding it with garbage data.

Policy	Microsoft Template	SGENT Settings
Maximum application log size	16384 kilobytes	4194240 kilobytes
Maximum security log size	81920 kilobytes	4194240 kilobytes
Maximum system log size	16384 kilobytes	4194240 kilobytes
Restrict guest access to application log	Enabled	Enabled
Restrict guest access to security log	Enabled	Enabled
Restrict guest access to system log	Enabled	Enabled
Retain application log	Not Defined	Not Defined
Retain security log	Not Defined	Not Defined
Retain system log	Not Defined	Not Defined
Retention method for application log	As Needed	As Needed
Retention method for security log	As Needed	As Needed
Retention method for system log	As Needed	As Needed

Table 7 - Log related policies adopted for SGENT's domain controllers.

These setting where modified by SGENT IT staff: all the logs have their maximum size increased to 4GB, if more logging is needed, events will be written discarding the old one. This setting doesn't force the allocation of 12GB, but raise the maximum allowed size of the file: all the servers, however, have a boot partition great enough to hold these files.

With these settings, the risk of overwriting old events is rare, however IT staff scheduled a per day backup strategy that keep all the information collected.

Apart from these backup, the auditing system proposed in the next chapter keep track of critic events reported locally by each server, this ensure an additional copy of the events, stored on another server.

System Services

Microsoft leaves some unnecessary services active in automatic or manual startup on domain controllers[16], even after its template being applied.

Here's the list of additional services disabled by SGENT policy.

SGENT Setting	
Automatic Updates	Network Location Awareness (NLA)
Computer Browser	Remote Registry
Cryptographic Services	Removable Storage
DHCP Client	Volume Shadow Copy
Intersite Messaging	Microsoft Software Shadow Copy Provider

Table 8 - Other disabled services for DC.

These choices come out from the assumption that:

- Automatic Updates: updates will be deployed by hand.
- Computer Browser: is provided only for backwards compatibility with client computers that are running earlier versions of Windows. At SGENT is unnecessary.
- Cryptographic Services: currently no certificates related services are active or established.
- DHCP Client: all the domain controllers have their IP set by hand.

[16] System Services for the Windows Server 2003 Family and Windows XP Operating Systems http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/management/svrxpser_7.mspx

- Intersite Messaging: no sites are configured.
- Microsoft Software Shadow Copy Provider: no shadow copy is needed.
- Network Location Awareness (NLA): computers mustn't move between different networks.
- Remote Registry: no remote management of registry is wanted.
- Removable Storage: a catalog of identifying information for removable media is unnecessary.
- Volume Shadow Copy: no shadow copy is needed.

For using Group Policies Modeling wizard is necessary to leave on automatic startup *"Resultant Set of Policies Provider"*, that the template set on Disabled.
Additionally, must be explicitly set on Automatic the service named NTsyslog, a syslog service used to send logs to a central repository. In the auditing section, more information on this service and to its behavior will be given.

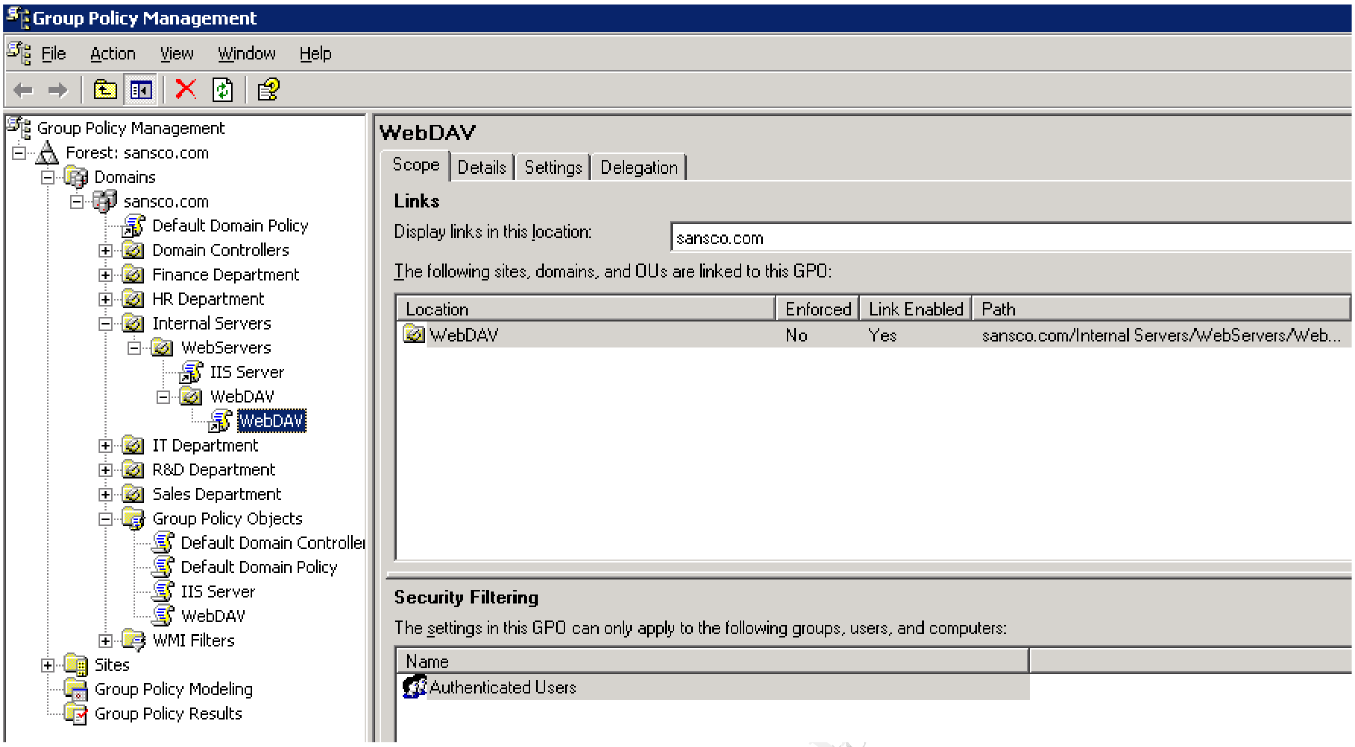
Workstation's policies

As state in the introductory part of this chapter, SGENT adopts NSA security configuration guidance for Windows 2000 and XP. No further actions are taken about employees workstations.

Auditing will be discussed in another section.

IIS server's policies

These policies must be carefully planned, in order to raise security level without compromising functionality.
The SGENT IT staff prepared a set of distinct group policy for the web servers in the internal forest and for DMZ's web servers.
All those policies can be easily administered through the group policy management console, due to the administration account draw up in advance in the DMZ forest: so, only one interface is needed for managing all the domains of SGENT.
These group policies are designed to act in an incremental manner: there is a generic IIS policy, which fit for a generic server, configuring parameters common to each IIS deployment, like service startup, and NTFS permission on system files. This is achieved due the common configuration adopted during the server deployment.
An additional policy, specific for every kind of server, take into account the different tasks to which it's assigned: an incremental policy for internal web servers, external web servers, and the internal WebDAV server is prepared: the next picture is a snapshot of group policy management console, and represents the policies being applied.



Links

Display links in this location: sansco.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
WebDAV	No	Yes	sansco.com/Internal Servers/WebServers/Web...

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users

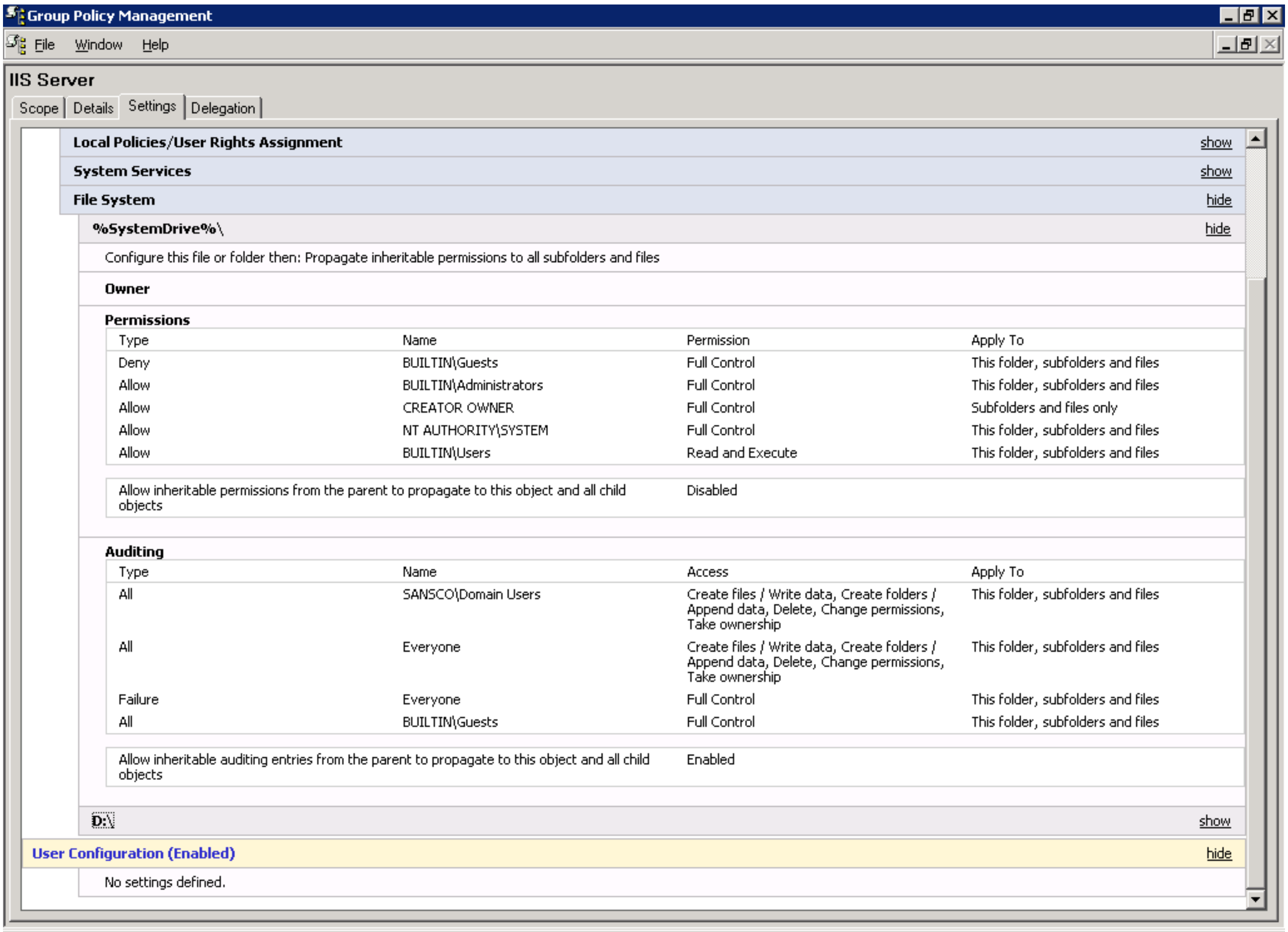
Figure 16 - Group policies being applied on the WebDAV server.

Here will be discussed first the generic IIS policy, and then the WebDAV policy adopted by IT staff in the US office.

Generic IIS policy

This policy is based on the High security web server template *"High Security - IIS Server.inf"* proposed by Microsoft in its security guide: IT staff configured more settings out from Microsoft one, enforcing security more than a standard IIS 6 installation.
The IIS policy configures the audit settings and event log setting like the domain controller's policy, because Microsoft's template leave these parameters undefined.

The next picture shows the file system settings chosen for %systemdrive% and the virtual folder's volume.



IIS Server

Local Policies/User Rights Assignment

System Services

File System

%SystemDrive%\

Configure this file or folder then: Propagate inheritable permissions to all subfolders and files

Owner

Permissions

Type	Name	Permission	Apply To
Deny	BUILTIN\Guests	Full Control	This folder, subfolders and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders and files
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders and files
Allow	BUILTIN\Users	Read and Execute	This folder, subfolders and files

Allow inheritable permissions from the parent to propagate to this object and all child objects: Disabled

Auditing

Type	Name	Access	Apply To
All	SANSCO\Domain Users	Create files / Write data, Create folders / Append data, Delete, Change permissions, Take ownership	This folder, subfolders and files
All	Everyone	Create files / Write data, Create folders / Append data, Delete, Change permissions, Take ownership	This folder, subfolders and files
Failure	Everyone	Full Control	This folder, subfolders and files
All	BUILTIN\Guests	Full Control	This folder, subfolders and files

Allow inheritable auditing entries from the parent to propagate to this object and all child objects: Enabled

D:\

User Configuration (Enabled)

No settings defined.

Figure 17 - File system setting for the IIS policy.

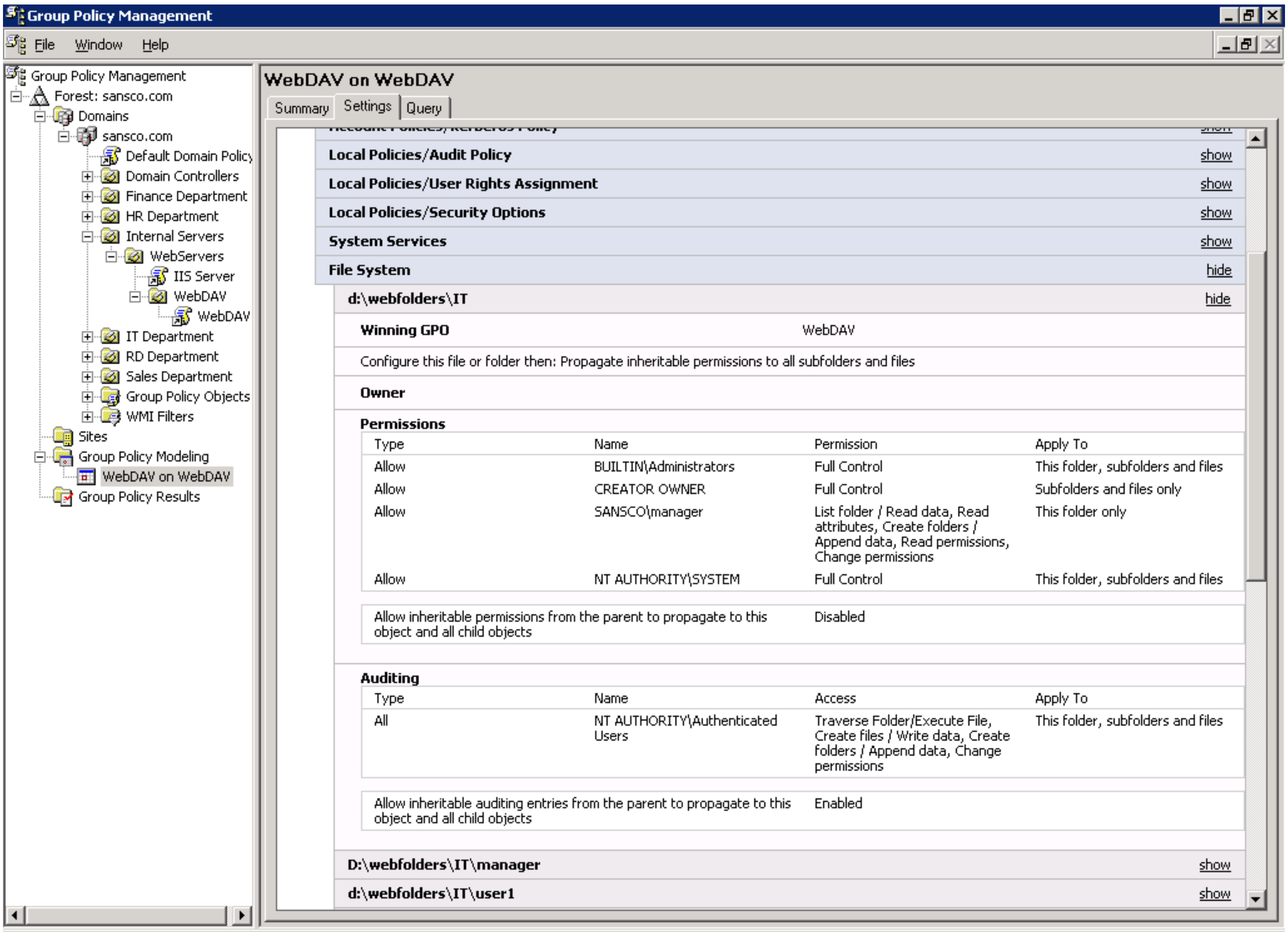
Windows 2003 come out with a reduced set of services active that give a strict access to resource than the previous version, but some of them are unnecessary for SGENT needing. When group policy will be evaluated, a snapshot of disabled services will be shown.

The incremental policy adopted start from this policy and build up a specialized policy due to the server's task.

WebDAV server policy

The WebDAV policy defined here defines only the permission and auditing assigned to the folders created for this service, so only the file system tab is configured. Other settings are inherited by the IIS policy.

The next picture shows the ownership and auditing setting for the main folder of a department: it's taken as an example d:\webolfers\IT. It's clearly visible that the manager of the IT department has particular rights on that folder, that aren't inherited by subfolders: this implies that the user's folders aren't accessible for him.



WebDAV on WebDAV

Local Policies/Audit Policy	show
Local Policies/User Rights Assignment	show
Local Policies/Security Options	show
System Services	show
File System	hide
d:\webfolders\IT	hide

Winning GPO	WebDAV

Configure this file or folder then: Propagate inheritable permissions to all subfolders and files

Owner

Permissions

Type	Name	Permission	Apply To
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders and files
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	SANSCO\manager	List folder / Read data, Read attributes, Create folders / Append data, Read permissions, Change permissions	This folder only
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders and files

Allow inheritable permissions from the parent to propagate to this object and all child objects	Disabled

Auditing

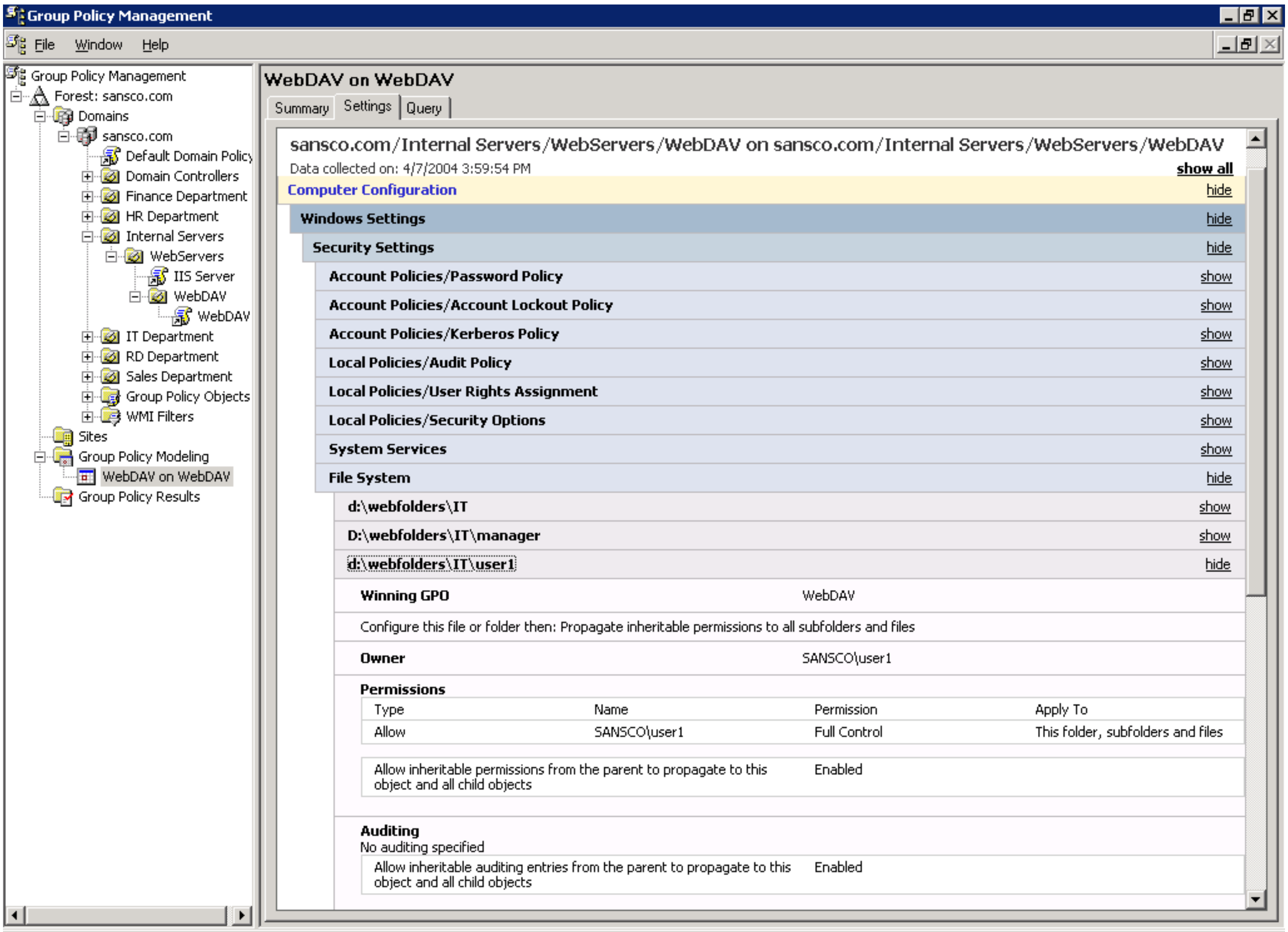
Type	Name	Access	Apply To
All	NT AUTHORITY\Authenticated Users	Traverse Folder/Execute File, Create files / Write data, Create folders / Append data, Change permissions	This folder, subfolders and files

Allow inheritable auditing entries from the parent to propagate to this object and all child objects	Enabled

D:\webfolders\IT\manager	show
d:\webfolders\IT\user1	show

A similar policy is configured for each department's folder, because the script shown in appendix A creates four others folders named HR, Finance, Sales, RD: each folder has a policy like the one shown in the picture, that assign to the manager of the department folder creations rights.

In the next picture are shown the rights and auditing settings assigned on an IT department employee called user1. The policy allows inherit from the parent folder for user rights and for auditing: this implies that setting these parameters on the department folder is sufficient to configure the employee's folders.



sansco.com/Internal Servers/WebServers/WebDAV on sansco.com/Internal Servers/WebServers/WebDAV

Data collected on: 4/7/2004 3:59:54 PM — show all

Computer Configuration — hide

Windows Settings — hide

Security Settings — hide

Account Policies/Password Policy — show

Account Policies/Account Lockout Policy — show

Account Policies/Kerberos Policy — show

Local Policies/Audit Policy — show

Local Policies/User Rights Assignment — show

Local Policies/Security Options — show

System Services — show

File System — hide

d:\webfolders\IT — show

D:\webfolders\IT\manager — show

d:\webfolders\IT\user1 — hide

Winning GPO	WebDAV
Configure this file or folder then: Propagate inheritable permissions to all subfolders and files	
Owner	SANSCO\user1

Permissions

Type	Name	Permission	Apply To
Allow	SANSCO\user1	Full Control	This folder, subfolders and files

Allow inheritable permissions from the parent to propagate to this object and all child objects	Enabled

Auditing

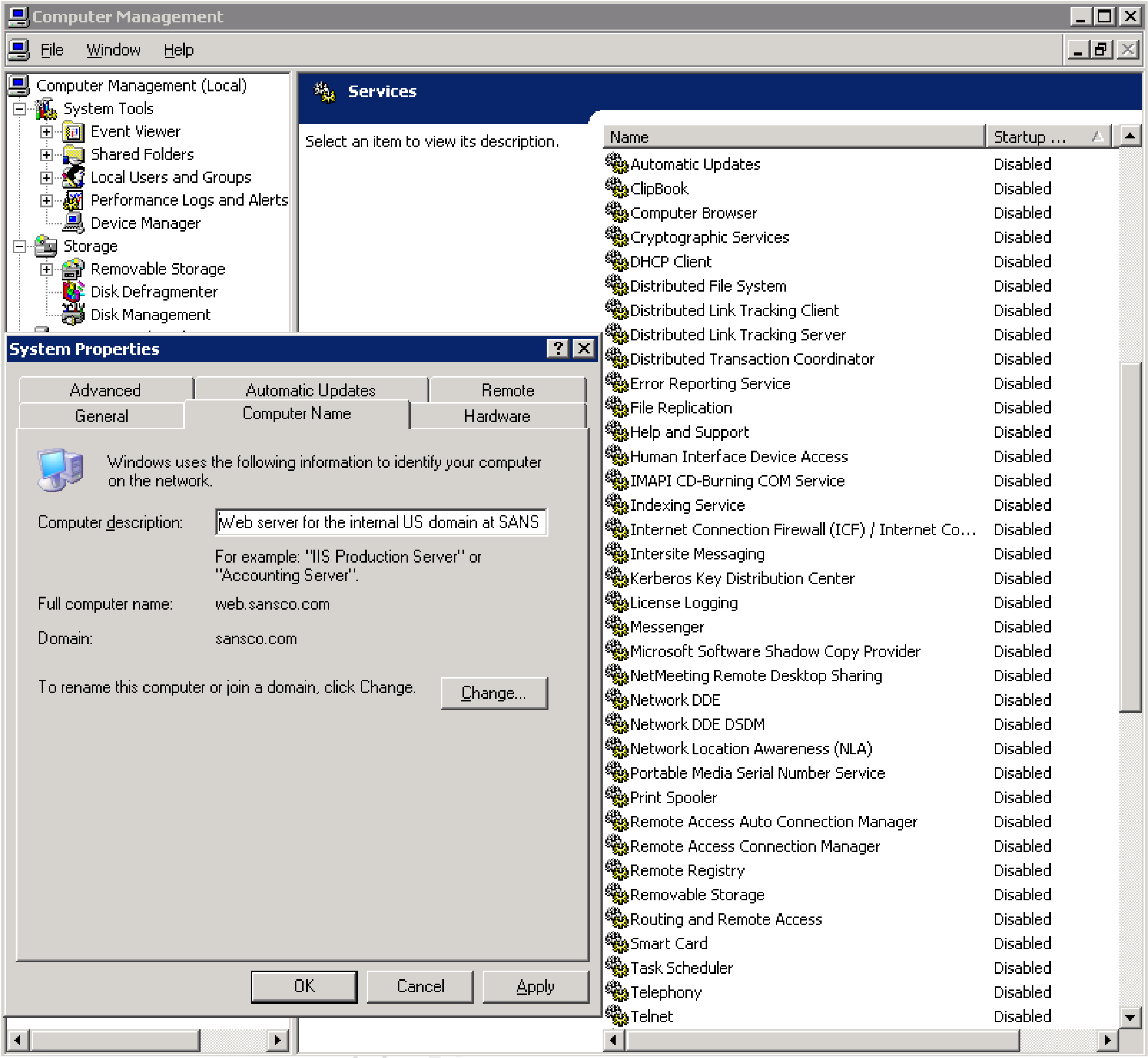
No auditing specified

Allow inheritable auditing entries from the parent to propagate to this object and all child objects	Enabled

Evaluating group policy behavior

The simplest test that can be carried on the WebDAV server is to check if all the required services are up and running, and if the unneeded where disabled.

The next picture shows the disabled services after the policy is applied.



Windows uses the following information to identify your computer on the network.

Computer description: Web server for the internal US domain at SANS

For example: "IIS Production Server" or "Accounting Server".

Full computer name: web.sansco.com

Domain: sansco.com

To rename this computer or join a domain, click Change.

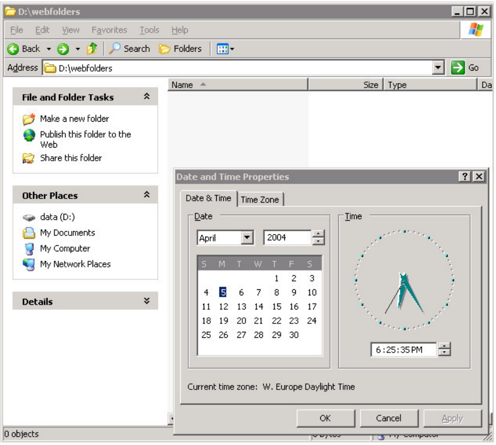
Name	Startup ...
Automatic Updates	Disabled
ClipBook	Disabled
Computer Browser	Disabled
Cryptographic Services	Disabled
DHCP Client	Disabled
Distributed File System	Disabled
Distributed Link Tracking Client	Disabled
Distributed Link Tracking Server	Disabled
Distributed Transaction Coordinator	Disabled
Error Reporting Service	Disabled
File Replication	Disabled
Help and Support	Disabled
Human Interface Device Access	Disabled
IMAPI CD-Burning COM Service	Disabled
Indexing Service	Disabled
Internet Connection Firewall (ICF) / Internet Co...	Disabled
Intersite Messaging	Disabled
Kerberos Key Distribution Center	Disabled
License Logging	Disabled
Messenger	Disabled
Microsoft Software Shadow Copy Provider	Disabled
NetMeeting Remote Desktop Sharing	Disabled
Network DDE	Disabled
Network DDE DSDM	Disabled
Network Location Awareness (NLA)	Disabled
Portable Media Serial Number Service	Disabled
Print Spooler	Disabled
Remote Access Auto Connection Manager	Disabled
Remote Access Connection Manager	Disabled
Remote Registry	Disabled
Removable Storage	Disabled
Routing and Remote Access	Disabled
Smart Card	Disabled
Task Scheduler	Disabled
Telephony	Disabled
Telnet	Disabled

Figure 18 - Snapshot of disabled services on a web server of the internal forest.

The policy is working as expected: these settings are inherited by the IIS policy.

A more interesting test is to check if the required directory tree has been created in and if the corresponding rights where assigned.

The three next pictures show the directory tree on the WebDAV subfolder and the rights assigned.



D:\webfolders

Address D:\webfolders

Date and Time Properties

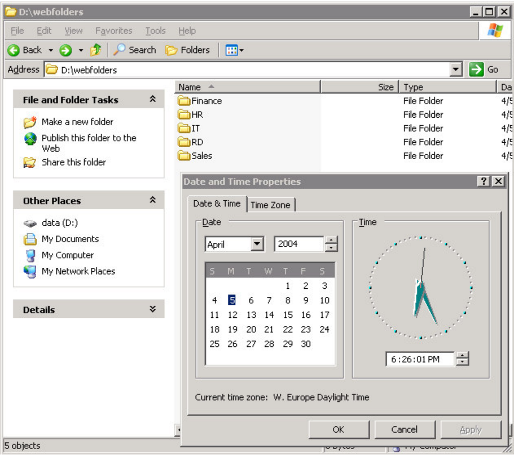
April 2004

6:25:35 PM

Current time zone: W. Europe Daylight Time

0 objects

Figure 19 - No subfolders in the WebFolders directory.



D:\webfolders

Address D:\webfolders

Name	Size	Type
Finance		File Folder
HR		File Folder
IT		File Folder
RD		File Folder
Sales		File Folder

Date and Time Properties

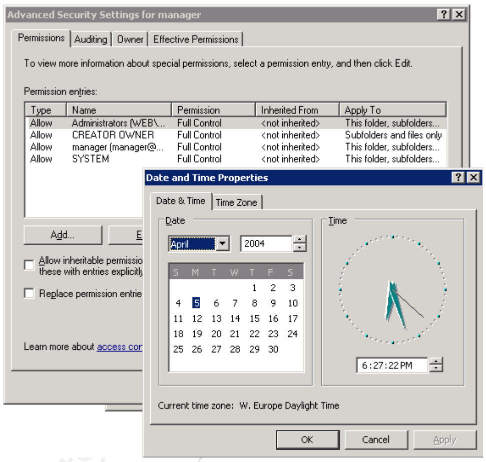
April 2004

6:26:01 PM

Current time zone: W. Europe Daylight Time

5 objects

Figure 20 - The subfolders are created by the scheduled script.



Advanced Security Settings for manager

To view more information about special permissions, select a permission entry, and then click Edit.

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Administrators (WEB\...	Full Control	<not inherited>	This folder, subfolders...
Allow	CREATOR OWNER	Full Control	<not inherited>	Subfolders and files only
Allow	manager (manager@...	Full Control	<not inherited>	This folder, subfolders...
Allow	SYSTEM	Full Control	<not inherited>	This folder, subfolders...

□ Allow inheritable permissio these with entries explicitly

□ Replace permission entrie

Learn more about access cor

Date and Time Properties

April 2004

6:27:22 PM

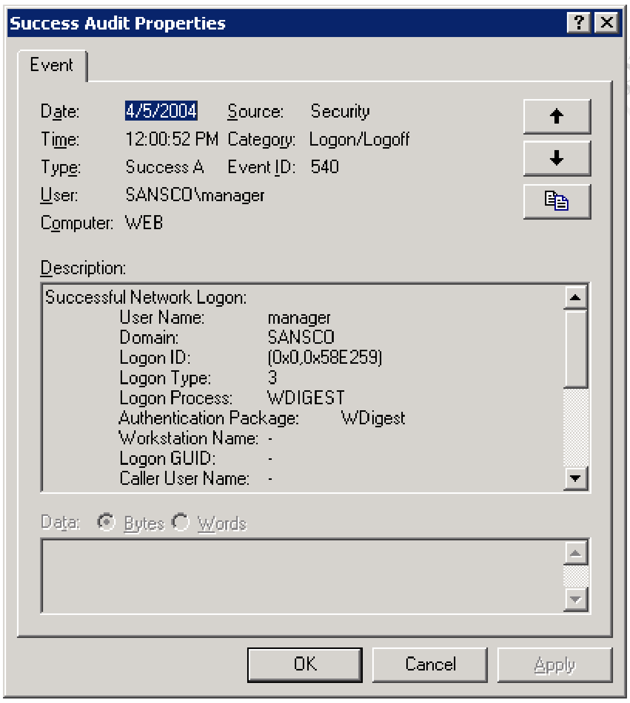
Current time zone: W. Europe Daylight Time

Figure 21 - The permissions are set.

The directory "webfolders" is empty, after the script has run the subfolders appears and then we can verify that the desired permissions and auditing parameters are set. The second picture shows the subfolders created by the scheduled script.

After these preliminary checks, a usability test can be carried on, cross checking with the event viewer to see if a prohibited access is reported.

The following picture is related to this test, and shows the two events logged by the system.



Success Audit Properties

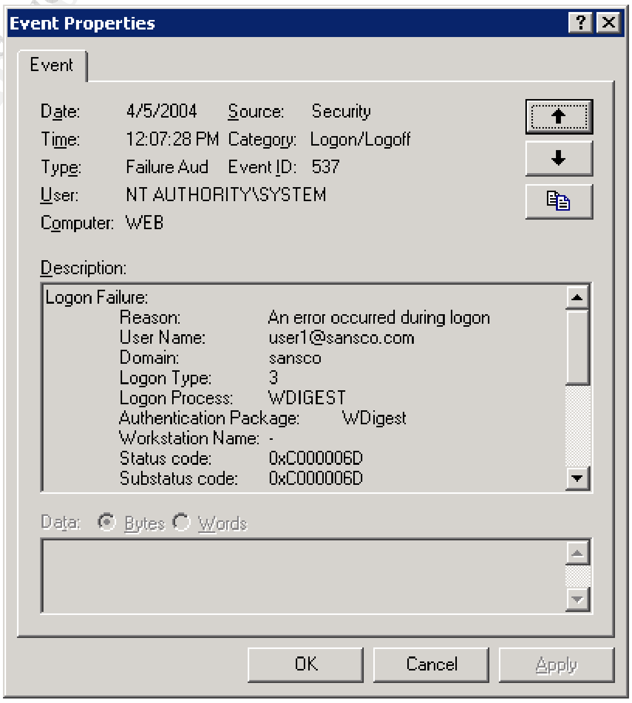
Date: 4/5/2004 Source: Security
Time: 12:00:52 PM Category: Logon/Logoff
Type: Success A Event ID: 540
User: SANSCO\manager
Computer: WEB

Description:

```
Successful Network Logon:
        User Name:              manager
        Domain:                 SANSCO
        Logon ID:               (0x0,0x58E259)
        Logon Type:             3
        Logon Process:          WDIGEST
        Authentication Package:         WDigest
        Workstation Name:       -
        Logon GUID:             -
        Caller User Name:       -
```

Data: ● Bytes ○ Words

Figure 22 - Successful logon.



Event Properties

Date: 4/5/2004 Source: Security
Time: 12:07:28 PM Category: Logon/Logoff
Type: Failure Aud Event ID: 537
User: NT AUTHORITY\SYSTEM
Computer: WEB

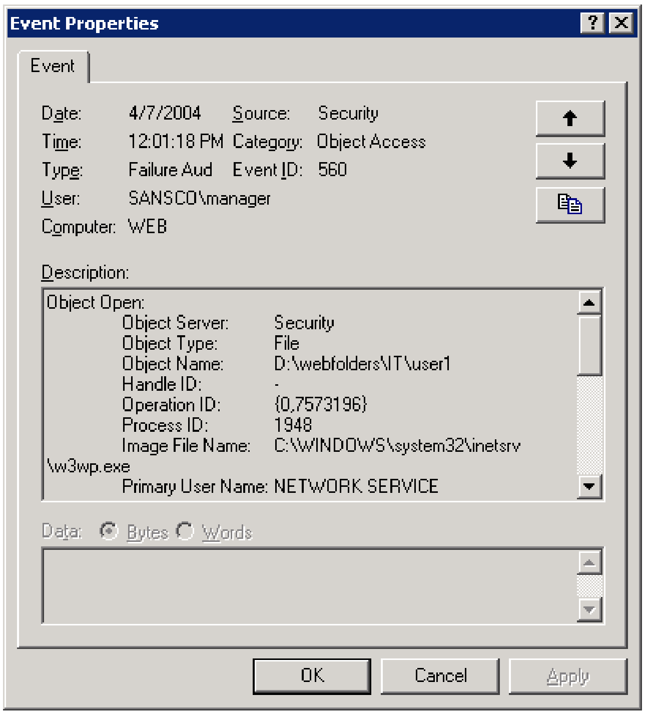
Description:

```
Logon Failure:
        Reason:                 An error occurred during logon
        User Name:              user1@sansco.com
        Domain:                 sansco
        Logon Type:             3
        Logon Process:          WDIGEST
        Authentication Package:         WDigest
        Workstation Name:       -
        Status code:            0xC000006D
        Substatus code:         0xC000006D
```

Data: ● Bytes ○ Words

Figure 23 - Unsuccessful logon.

The next two pictures show the event viewer event produced accessing to the directory \IT\manager by an unauthorized user, and the access of the legitimate owner.

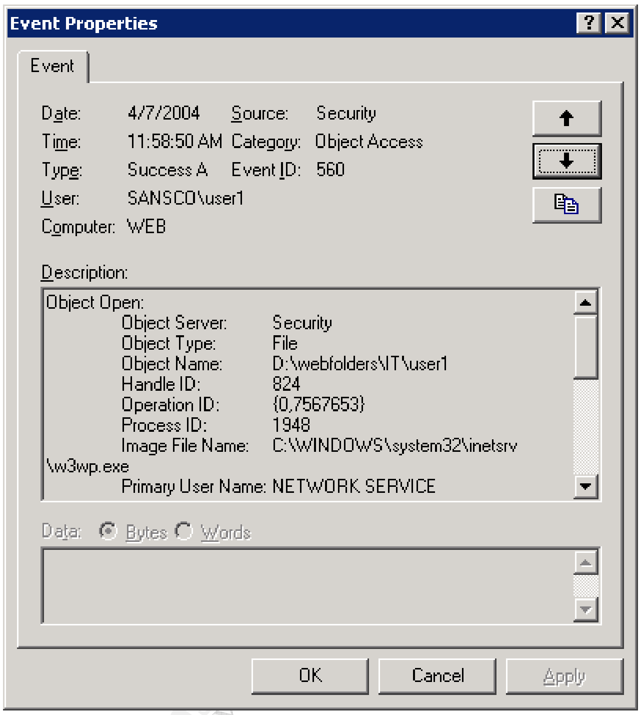


Date: 4/7/2004 Source: Security
Time: 12:01:18 PM Category: Object Access
Type: Failure Aud Event ID: 560
User: SANSCO\manager
Computer: WEB

Description:

```
Object Open:
          Object Server:       Security
          Object Type:         File
          Object Name:         D:\webfolders\IT\user1
          Handle ID:           -
          Operation ID:        {0,7573196}
          Process ID:          1948
          Image File Name:     C:\WINDOWS\system32\inetsrv
\w3wp.exe
          Primary User Name: NETWORK SERVICE
```

Figure 24 - Audit of prohibited access to a user folder.



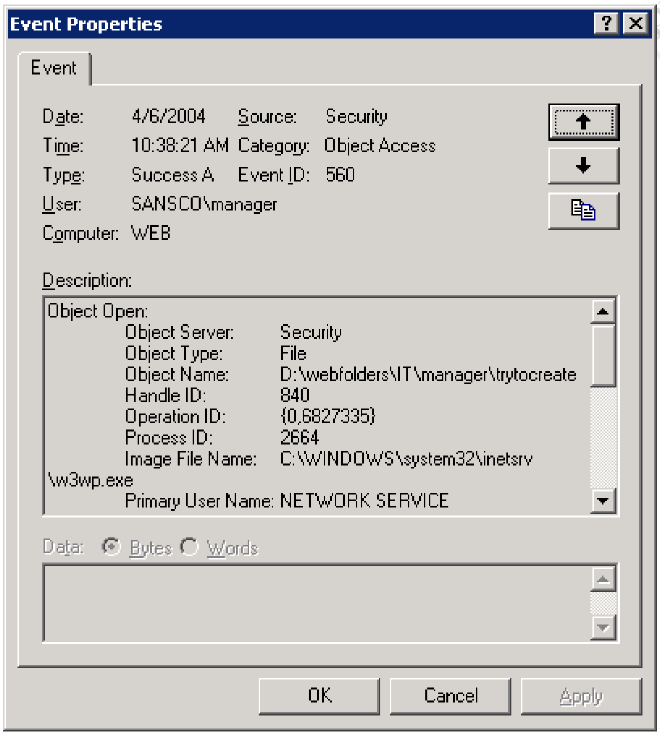
Date: 4/7/2004 Source: Security
Time: 11:58:50 AM Category: Object Access
Type: Success A Event ID: 560
User: SANSCO\user1
Computer: WEB

Description:

```
Object Open:
          Object Server:       Security
          Object Type:         File
          Object Name:         D:\webfolders\IT\user1
          Handle ID:           824
          Operation ID:        {0,7567653}
          Process ID:          1948
          Image File Name:     C:\WINDOWS\system32\inetsrv
\w3wp.exe
          Primary User Name: NETWORK SERVICE
```

Figure 25 - Audit of legal access to a user folder.

The next picture shows the event produced by the creation of a new folder by the IT department's manager in its folder and in the department's folder: the last snapshot is due to the creation of a new project's folder. The event viewer shows clearly that the event audited has been completed.

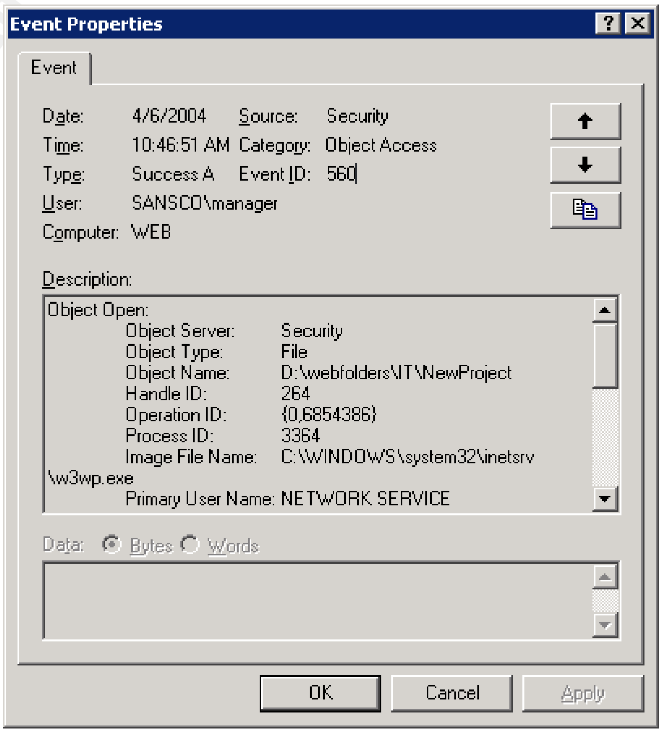


Date: 4/6/2004 Source: Security
Time: 10:38:21 AM Category: Object Access
Type: Success A Event ID: 560
User: SANSCO\manager
Computer: WEB

Description:

```
Object Open:
          Object Server:       Security
          Object Type:         File
          Object Name:         D:\webfolders\IT\manager\trytocreate
          Handle ID:           840
          Operation ID:        {0,6827335}
          Process ID:          2664
          Image File Name:     C:\WINDOWS\system32\inetsrv
\w3wp.exe
          Primary User Name: NETWORK SERVICE
```

Figure 26 - A user create a subfolder in his folder.



Date: 4/6/2004 Source: Security
Time: 10:46:51 AM Category: Object Access
Type: Success A Event ID: 560
User: SANSCO\manager
Computer: WEB

Description:

```
Object Open:
          Object Server:       Security
          Object Type:         File
          Object Name:         D:\webfolders\IT\NewProject
          Handle ID:           264
          Operation ID:        {0,6854386}
          Process ID:          3364
          Image File Name:     C:\WINDOWS\system32\inetsrv
\w3wp.exe
          Primary User Name: NETWORK SERVICE
```

Figure 27 - The manager create a project's folder.

After these test we can argue that the group policy was applied successfully, and the system is accessible by allowed users. Also, the manager of the department is able to create and manage new project's folders, setting permission on them but without accessing or modifying others user's folders.

The policy designed doesn't refer to a particular server's parameter and can easily been applied on other WebDAV servers in the others domain, stating that every machine must be installed with the same directory tree. This eases a lot administration of the service by the IT staff.

Auditing

Administrators must make efforts to plan an efficient auditing method. This is a mandatory task, which must be achieved with maximum attention.
In the previous section where shown the group policies about auditing adopted at SGENT: these policies are studied to give an acceptable level of information to the IT staff, without exceeding in messages and alert, not to mention false alarms. The DMZ policy, due to the critic nature of these servers, reports more events than the internal one.
Choosing what to audit is the first step of the whole auditing process: now in this section will be analyzed the second, but not less important, dowel.

It's important to remember, however, that auditing is not a preventive task: in fact auditing is though to inform IT staff of trouble reported by server and other networks appliance being monitored. But auditing can be the first step to realize a IDS, because the auditing system may became the Host based intrusion detection block of the IDS.

Strictly speaking auditing should be extended to every network element capable of generating reports: this allow a better control on what's happening. This would lead to an increased amount of data collected by the central repository system. In the current implementation of the audit system, the software architecture deployed is meant for monitoring SGENT servers.

It's important to develop an accurate auditing mechanism, to reduce the time interval between the alarm and the response to the threat, in order to undertake the necessary actions. For this reason an auditing system must provide various alarm methods, like by email, SMS and so on. The audit system implemented at SGENT is able of sending emails and SMS.

Another aspect that mustn't forget is that the auditing system must be reliable, and IT staff must be able to check if the system is working properly, so a redundant architecture must be prepared, allowing two or more servers to cross check each others.

Speaking about Microsoft systems, Windows supplies an exhausting reporting ability after a careful configuration, but lacks a centralized storing and an easily manageable monitoring. Event logs and IIS logs are stored locally by defaults on each server, and additional work must be carried out using third party tools or by developing custom scripts.
The first option might seem the simpler one and the most effective, but we mustn't forget that writing our own script give better flexibility to adapt on the needing of our company.

SGENT planned an auditing system internally developed and maintained. IT staff is responsible of the installation and of the configuration of the auditing system and to keep it up to date.
This auditing system's goal is collect event logs and IIS logs in a centralized store, using a RDBMS to archive that information and to retrieve relevant data.
This system can also be used for forensic capture and later analysis: in fact the local log on the attacked server could be altered or removed by the intruder before the threat is discovered, analyzed and documented.
The auditing system proposed is focused on keeping IT staff aware of possible threats reported by the servers on the network, but doesn't consider employees' workstations not network appliances.
This is a limit of the actual deployment, which can be extended to include hardware different from servers, because the proposed architecture is flexible enough to allow this enhancement, but the hardware required must be evaluated carefully.

System requirements

The auditing architecture implemented required two servers for each headquarter: they receive and store locally the events sent by servers' domain. Each log server monitors the other: this increase the fault tolerance of the auditing system.
The two servers must have enough disk space to store the collected logs from the servers: the amount of the stored data can be partially controlled acting on the configuration file of the software adopted, but about 50GB must be reserved for this task.
Two Windows Machines are used in the current implementation of the auditing system, but the software chosen can also run on Linux machines, this give to the whole architecture a better flexibility: changing will require rewriting management scripts in a language suitable for that platform, and found alternative tools that substitute the one that haven't a Linux port.

IT staff must dispose a backup strategy for the data collected on the servers, coordinated with a log rotation handling, which keep old logs on tapes, reducing the size of the stored file on the disk.

Software chosen for the current auditing system

At SGENT was chosen a set of open source tool, to collect a selected number of events on the two auditing servers. These tools offers a good manageability but rely, after the log is written on the central server, on data processing procedures to query the local copy of the logs and report the possible security threat to the IT staff, if needed.
These scripts can run from every machine, also the workstation of and administrator, but a system DSN must be created to connect to the central log server.
This is a useful feature that was used at SGENT, due to the need of sending SMS. Later on this paper the reason will be explained.

Currently SGENT auditing architecture is made up by these tools:

Tool Name	Tool Goal	Version	Web Resource
NTSyslog	Windows NT syslog service.	1.13	http://ntsyslog.sourceforge.net/
SysLog2ODBC	Writes logs received to an ODBC DSN.	0.4 Beta	http://sourceforge.net/projects/syslog2odbc/
ODBCConnector	ODBC driver for MySQL.	3.51.06	http://www.mysql.com/
MySQL	The DBMS chosen to record locally remote logs.	4.0.18	http://www.mysql.com/
Microsoft SMS Sender	Send SMS through a cell phone connected to the server.	1.0	http://www.microsoft.com/downloads/details.aspx?FamilyID=06a4f997-7f69-4891-8929-37b9041924a2&DisplayLang=en
Blat for windows	Sends emails from a script.	1.9.4	http://www.interlog.com/~tcharron/blat.html

Table 9 - Software chosen to implement the auditing architecture.

This architecture was chosen evaluating different aspect: first of all, the majority of software is open source so it can be freely used without license problems. The second argument is that this architecture is based on simple tools, which ease management and troubleshooting of the possible problems.

The last, but not less important argument, come out from the management of IIS log in a centralized manner, through the ODBC logging feature[17]. This would require an alternative method for querying IIS logs.
There are arguments of strong discussion due to the possible overhead of writing logs to a SQL server[18], as stated by Microsoft in the document referenced on note 18:"T*he impact of logging Internet Information Server (IIS) activity to disk is minimal compared to logging it to a SQL Server database. The performance impact of logging to SQL Server is greater and depends on the SQL Server implementation and the hardware you use."*
However, this paper was written when IIS 4 was available, and takes into account a Microsoft SQL Server database system: these assumptions are far away from the current architecture, and the IT staff must evaluate the performance impact of this choice, and eventually, switch to the traditional file logging on IIS.

Setting a MySQL database on an internal server was the critic factor of the whole deployment, from a security point of view, but a lot of resources are available for deploy in a secure way MySQL[19].
This DBMS can be easily managed through command line or using other tools: I suggest MySQL control centre.

Configuring the tools

A little manual configuration is needed for every tool, which can be automated later on with scripting once the common settings where established.

We assume that IIS is already configured to use ODBC logging: the resource on note 17 clearly shows how to enable this feature. Microsoft supplies SQL code that is used to automate table creation: this script (named logtemp.sql) can be found on the %windir%\system32\inetsrv directory after IIS installation.
A SQL script (shown in appendix B) was prepared to automate the creation of each table on the DBMS: this code uses logtemp.sql to set the required database and table for IIS logs.

Here will be shown only a schematic list of the configuring steps needed:

- NTSyslog: install on every server, configure the server to which forward logs to, and choose what event to send (syslog refers to a "facility" and "severity").
- SysLog2ODBC: installed as a service on the log collector servers, configure the SQL query to store logs into a table using a system DSN.
- ODBCConnector: used to create two systems DSN on the log collector servers: one for writing and one for writing.
- MySQL: create a database for the logs collected; create a user with insertion right and a user with select right.

The first three steps are the simplest to configure, because only few parameters must be set: in appendix C SysLog2ODBC configuration file is shown.
Configuration of the syslog service must be planned carefully, choosing what to forward to the central repository. SGENT IT staff chooses to do extensive logging on every server; this behavior is easily controlled by group policy: syslog demon configuration must be planned carefully, to filter

[17] HOW TO: Configure Web Site Logging in Windows Server 2003
http://support.microsoft.com/default.aspx?scid=kb;en-us;324279
[18] Internet Information Server Performance Logging to Disk vs. ODBC
http://support.microsoft.com/default.aspx?scid=kb;en-us;142557
[19] A brief introduction on how to secure a MySQL database comes from its documentation, available on the following page http://www.mysql.com/doc/en/Security.html

and limit the data extracted from the event log and sent on the network. This choice doesn't affect the amount of data logged locally but only the subset of the log chosen to be centrally managed.

The syslog service used allows forwarding logs to two servers: this feature is used by SGENT IT staff, to improve reliability and fault tolerance.

The syslog demon uses the standard UDP port number 514 for sending the logs across the network: as we want to control the DMZ servers, a rule must be set on the firewall to allow traffic from the DMZ to the log servers in the internal network: this rule must declare the source and destination IP address for the syslog traffic. Also the external firewall must block this traffic.

Next, it's necessary to configure MySQL: different database's types can be chosen, with different features and performances. The current implementation uses the standard myISAM storage engine, but InnoDB storage engine could be used, benefiting from its particular feature: tablespace can be created from several files.
The current file limit depends only by the file system used by the operating system: NTFS limit is 16 terabytes[20], so the volume size is the real limit.
This is a problem to focus on: volume size must be carefully planned. The database must be put in a large capacity volume, as stated in the previous section; it can grow fast and fill a bad dimensioned partition, especially in a large network with a lot of event generating machines.
For sending email a free tool, blat, is used and not the CDO object. It requires to be copied in a directory in the path, and a after a simple configuration it can send also attachments.

The auditing system allows sending SMS for alerting the administrators of a problem[21]. Due to the nature of the SMS (only 160 characters) only a short advice is sent.
IT staff use a free downloadable tool called *"Microsoft SMS Sender"*[22] that allows sending SMS using a GSM phone connected to a PC (runs on Windows Server 2003 and Windows XP) using some command line parameters. Due to the flexibility of this tool an old GSM phone can be recycled for sending alerts, but its mandatory to install it as a modem over an interface such as Infrared (IrDA), Serial Cable, Bluetooth, PCCard etc.
If IT staff wants to migrate to Linux architecture a replacement tool must be found. Luckily a lot of software is available to meet this needing.

Running the Auditing system

After the software is configured and the services are running, it's necessary to schedule a task that queries the tables searching for error messages: the script then send an email to alert the administrators, reassuming the fault found.
The script first check if the other log server is up and running and report an error if the server doesn't reply.
The script is scheduled on a five minutes interval: this period is used for searching in the database for events newer than 5 minutes, avoiding duplicated alarms being generated. A SQL query is used for this task, and can be easily changed to search for new records.

In appendix D is shown the whole code written.

[20] How Big MySQL Tables Can Be
http://www.mysql.com/doc/en/Table_size.html
[21] This feature wasn't tested, because I wasn't able to find out a GSM phone to connect to a PC.
[22] Microsoft SMS Sender
http://www.microsoft.com/downloads/details.aspx?FamilyID=06a4f997-7f69-4891-8929-37b9041924a2&DisplayLang=en

Sample of the reporting feature of the Auditing system

Here is shown the output produced by the script, running different queries.

The following output was generated by the script, searching the IIS table for event number 500:

```
ClientHost:     10.1.0.155
Username:       manager
Logtime:        4/5/2004 12:33:13 PM
serverip:       10.1.0.153
target:         /it/manager/2Kboot.bin
machine:        WEB
service:        W3SVC1
operation:      PUT
```

The following example is the result of searching in the IIS table for the command *delete* issued to the WebDAV server:

```
ClientHost:     10.1.0.155
Username:       manager
Logtime:        4/5/2004 12:29:01 PM
serverip:       10.1.0.153
target:         /it/manager/newfolder
machine:        WEB
service:        W3SVC1
operation:      DELETE

ClientHost:     10.1.0.155
Username:       manager
Logtime:        4/6/2004 10:46:38 AM
serverip:       10.1.0.153
target:         /it/NewProject/allow
machine:        WEB
service:        W3SVC1
operation:      DELETE

ClientHost:     10.1.0.155
Username:       manager
Logtime:        4/6/2004 10:46:42 AM
serverip:       10.1.0.153
target:         /it/NewProject
machine:        WEB
service:        W3SVC1
operation:      DELETE

ClientHost:     10.1.0.155
Username:       user2
Logtime:        4/6/2004 11:02:14 AM
serverip:       10.1.0.153
target:         /it/user2/try
machine:        WEB
service:        W3SVC1
operation:      DELETE
```

The next example shows the searching of logon failures:

```
Msg:       Apr   8  15:08:28  security[failure]  534  NT  AUTHORITY\SYSTEM   Logon
Failure:  Reason:The user has not been granted the requested  logon type at this
machine   User Name:user1   Domain:SANSCO   Logon Type:10   Logon Process:User32
```

```
Authentication Package:Negotiate   Workstation Name:DC1   Caller User Name:DC1$
Caller  Domain:SANSCO    Caller  Logon  ID:(0x0,0x3E7)    Caller  Process  ID:864
Transited Services:-  Source Network Address: 10.1.0.155  Source Port:2134
SenderIP:       10.1.0.171
ReceivedAt:     2004-04-08 15:14:11

Msg:       Apr   8  15:08:36  security[failure]  534  NT  AUTHORITY\SYSTEM   Logon
Failure:  Reason:The user has not been granted the requested  logon type at this
machine   User Name:manager   Domain:SANSCO   Logon Type:10   Logon Process:User32
Authentication Package:Negotiate   Workstation Name:DC1   Caller User Name:DC1$
Caller  Domain:SANSCO    Caller  Logon  ID:(0x0,0x3E7)    Caller  Process  ID:864
Transited Services:-  Source Network Address: 10.1.0.155  Source Port:2134
SenderIP:       10.1.0.171
ReceivedAt:     2004-04-08 15:14:12
```

Appendix Section

Appendix A: Script for creating the directory tree on the WebDAV server and apply the policies.

This script is scheduled on the WebDAV server.

```
OUs = array("IT Department","HR Department","Sales Department","Finance
Department","RD Department")

SET FSO = CreateObject("Scripting.FileSystemObject")

FOR EACH OU in OUs
      SET objGroup = GetObject ("LDAP://cn="& OU &",ou="& OU
&",dc=sansco,dc=com")
      Subfolder = split(OU," ")
      ParentFolder = "d:\webfolders\"& Subfolder(0) &"\"
      IF NOT FSO.FolderExists(ParentFolder) THEN
            FSO.CreateFolder(ParentFolder)
      END IF
      FOR EACH objMember in objGroup.Members
            Name = split (objMember.Name, "=")
            IF NOT FSO.FolderExists(ParentFolder&"\"&Name(1)&"\") THEN
                  FSO.CreateFolder(ParentFolder&"\"&Name(1)&"\")
            END IF
      NEXT
      SET objGroup = NOTHING
NEXT

SET FSO = NOTHING

ScriptEXEC = "gpupdate /force"
SET oShell = WScript.CreateObject("WSCript.shell")
oShell.run ScriptEXEC,0,true
SET oShell = NOTHING
```

Appendix B: SQL commands to configure MySQL.

Here are shown the SQL commands needed to create the database, tables and users needed to collect all the logs generated on remote servers.

A database is created, that contains all the tables needed. The names used must be set into the system DSN used by SysLogODBC and IIS.

Two users are added: user **`logcollector`** can do only an *insert* and user **`logreader`** can do only a *select:* this user is used in two additional DSN, used by the script in appendix D.
These two users have granted these privileges on every table created.

Any additional IIS server requires the creation of a new table. In this example only a single IIS server is considered, but adapting this code to many IIS server is a simple task.

```
CREATE DATABASE eventcollector;

USE eventcollector;

CREATE TABLE SysLogData (
Msg text, SenderIP varchar(20),
SenderPort_S varchar(6), SenderPort_I int(6), Priority int(3),
Severity int(3), SeverityDesc varchar(255), Facility int(3),
FacilityDesc varchar(255), RawMsg text, ReceivedAt varchar(255));

GRANT INSERT ON eventcollector.SysLogData TO 'logcollector'@'localhost'
IDENTIFIED BY 'password to insert into this database';

GRANT SELECT ON eventcollector.SysLogData TO 'logreader'@'localhost' IDENTIFIED
BY 'password to select into this database';

FLUSH privileges;

CREATE TABLE inetlog (
ClientHost varchar(255), username varchar(255),
LogTime datetime, service varchar(255), machine varchar(255),
serverip varchar(50), processingtime int, bytesrecvd int,
bytessent int, servicestatus int, win32status int,
operation varchar(255), target varchar(255), parameters varchar(255));

GRANT INSERT ON logcollector.inetlog TO 'logcollector'@'localhost' IDENTIFIED BY
'password to insert into this database';

GRANT SELECT ON logcollector.inetlog TO 'logreader'@'localhost' IDENTIFIED BY
'password to select into this database';

FLUSH privileges;
```

Appendix C: Syslog2ODBC configuration file.

Here are the parameters used for configuring Syslog2ODBC. IT staff choose to log all the possible information received by the syslog service, the data post processing is in charge of the additional scripts.

```
[Server]
BindToIP=10.1.0.153
Port=514

[ODBC]
ConnectionString=DSN=SysLog2ODBC
SQLStatement=INSERT INTO SysLogData( Msg, SenderIP, SenderPort_S, SenderPort_I,
Priority, Severity, SeverityDesc, Facility, FacilityDesc, RawMsg, ReceivedAt )
VALUES ( ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, NOW() )
Param1=MSG
Param2=SENDERDEVICE_IP
Param3=SENDERDEVICE_PORT_S
Param4=SENDERDEVICE_PORT_I
Param5=PRIORITY
Param6=SEVERITY
Param7=SEVERITYDESC
Param8=FACILITY
Param9=FACILITYDESC
Param10=RAWMSG
WaitOnError=15
MaxRetryCount=4

[ParamDefault]
Severity=4
Facility=0
```

Appendix D: Sample script to query MySQL tables.

```
'
' Variables section.
'
' Set the required variables for the connection.
CONST adOpenStatic = 3
CONST adLockOptimistic = 3
CONST adUseClient = 3
' Computer from which WMI is used.
CONST strComputer = "."
' Other log server......this server is logserver1.sansco.com
CONST Logserver = "logserver2.sansco.com"
' These are the constants that represent the report of the query logged to a
file.
CONST IISReport = "d:\IISReport.txt"
CONST EventReport = "d:\EventReport.txt"
' This variable is set to 1 on the master logserver, on the slave is set to 0.
' It's used to choose if sending mail and SMS.
CONST master = 1
'
' Code section.
'
' This is a preset for this variable: I set this variable to 1 if the other log
server is down.
NotReachable = 0
' This variable store the number of record found that satisfy the SQL query.
Found = 0
' This is the time interval for checking into the log.
CONST interval = 5
'
' This piece of code prepare the date string to search into the database.
'
' I split the date returned by the date function
result=split (date,"/")
' if the month and the day are only one character, I add a leading 0.
if result(1)<10 then
      result(1)="0"&result(1)
end if
if result(1)<10 then
      result(0)="0"&result(0)
end if
' I create the string for the minute to start searching for.
min=minute(time)-interval
' And I save the hour
h=hour(time)
' If the minute is negative.
if min<0 then
      min = 60+min
      h=h-1
' Else I add a trailing 0.
else if min<10 then
      min = "0"&min
      end if
end if
' Then the string to search for is ready.
sqlstring = "%"&result(2)&"-"&result(0)&"-"&result(1)&" "&h&":"&min&"%"

SET oShell = WScript.CreateObject("WSCript.shell")
' First we chech if the other server that collect logs is up.
' We use a WMI class that implement the ping service...requires at least
WindowsXP.
SET objWMIServicePri = GetObject("winmgmts:{impersonationLevel=impersonate}!\\"
& strComputer & "\root\cimv2")
SET colPingedComputers = objWMIServicePri.ExecQuery ("Select StatusCode FROM
Win32_PingStatus Where Address = '" & Logserver & "'")
FOR EACH objPingedComputer IN colPingedComputers
      IF objPingedComputer.StatusCode <> 0 THEN
            ' The server is down, trigger an alarm.
            ScriptEXEC = "blat -subject 'Other log server unreachable' -t
auditing@sansco.com -q"
            oShell.run ScriptEXEC,0,true
            NotReachable = 1
SET oShell = NOTHING

      END IF
NEXT
SET colPingedComputers = NOTHING
'
' Now I analyze the syslog table
'
' Connect to the DSN specified for IIS.
SET objConnection = CreateObject("ADODB.Connection")
objConnection.Open "DSN=HTTPLOG-Read;"
SET objRecordset = CreateObject("ADODB.Recordset")
objRecordset.CursorLocation = adUseClient
objRecordset.Open "SELECT ClientHost,Username,Logtime,serverip,target FROM
inetlog WHERE Logtime LIKE '"&sqlstring&"'", objConnection, adOpenStatic,
adLockOptimistic
' I save the number of record returned.
Found = objRecordset.RecordCount
' Now I create a new file.
SET FSO = CreateObject("Scripting.FileSystemObject")
SET LogReport = FSO.CreateTextFile (IISReport,true)

DO WHILE NOT objRecordset.EOF
      LogReport.WriteLine "ClientHost: "& vbTab & objRecordset("ClientHost")
      LogReport.WriteLine "Username: "& vbTab & objRecordset("Username")
      LogReport.WriteLine "Logtime: "& vbTab & objRecordset("Logtime")
      LogReport.WriteLine "ServerIP: "& vbTab & objRecordset("serverip")
      LogReport.WriteLine "Target: "& vbTab & objRecordset("target")
      LogReport.WriteLine
      objRecordset.MoveNext
LOOP
' This server send an email and SMS only if the other one is unreachable or if
' it's the master log server and the query return something.
IF ((NotReachable = 1 OR Master = 1) AND (Found >0)) THEN
      ' Send an email
      ScriptEXEC = "blat "& IISReport &" -subject 'Error reported on IIS logs' -
t auditing@sansco.com -q"
      oShell.run ScriptEXEC,0,true
      ' Send an SMS
      ScriptEXEC2 = "smssender.exe /i +393482222222 /p:1 /m:'Error reported on
IIS logs'"
      'oShell.run ScriptEXEC2,0,true
END IF
objRecordset.Close
objConnection.Close
LogReport.Close
SET objRecordset = NOTHING
SET objConnection = NOTHING
'
```

```
' Now I analyze the syslog table
'
' Connect to the DSN specified for syslog.
SET objConnection = CreateObject("ADODB.Connection")
SET objRecordset = CreateObject("ADODB.Recordset")
objConnection.Open "DSN=Syslog2ODBC-Read;"
objRecordset.CursorLocation = adUseClient
objRecordset.Open "SELECT Msg,SenderIP,ReceivedAt FROM SysLogData WHERE
ReceivedAt LIKE'"&sqlstring&"'", objConnection, adOpenStatic, adLockOptimistic
' I save the number of record returned.
Found = objRecordset.RecordCount
' Now I create a new file.
SET FSO = CreateObject("Scripting.FileSystemObject")
SET LogReport = FSO.CreateTextFile (EventReport, true)
DO WHILE NOT objRecordset.EOF
      LogReport.WriteLine "Msg: "& vbTab & objRecordset("Msg")
      LogReport.WriteLine "SenderIP: "& vbTab & objRecordset("SenderIP")
      LogReport.WriteLine "ReceivedAt: "& vbTab & objRecordset("ReceivedAt")
      LogReport.WriteLine
      objRecordset.MoveNext
LOOP
' This server send an email and SMS only if the other one is unreachable or if
' it's the master log server and the query return something.
IF ((NotReachable = 1 OR Master = 1) AND (Found >0)) THEN
      ' Send an email
      'ScriptEXEC = "blat "& EventReport &" -subject 'Error reported on Event
logs' -t auditing@sansco.com -q"
      oShell.run ScriptEXEC,0,true
      ' Send an SMS
      ScriptEXEC2 = "smssender.exe /i +393482222222 /p:1 /m:'Error reported on
Event logs'"
      oShell.run ScriptEXEC2,0,true
END IF
' Closes the object for the connection.
objRecordset.Close
objConnection.Close
' closes the file.
LogReport.Close

SET oShell = NOTHING
SET FSO = NOTHING
```

References

1. Egress filtering for a healthier Internet
http://www.hackinglinuxexposed.com/articles/20030213.html

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

3. Organizational units
http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_ADintro_19.asp

4. When to create a forest trust
http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/x_c_whencreateforest.asp

5. Trust types
http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/domadmin_concepts_trusts.asp

6. Forest trusts
http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/x_c_foresttrusts.asp

7. To raise the forest functional level
http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_changeforestlevel.asp

8. Top 10 Benefits of Windows Server 2003
http://www.microsoft.com/windowsserver2003/evaluation/whyupgrade/top10best.mspx

9. When to create a shortcut trust
http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/domadmin_concepts_windowstrust.asp

10. To create a shortcut trust
http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/domadmin_createshorttrust.asp

11. WebDAV site
http://www.webdav.org

12. The last reported flaw of IIS related to WebDAV is from 07 Mar 04 http://www.kb.cert.org/vuls/id/117394.

13. The following link http://www.cert.org/current/archive/2004/02/27/archive.html report W32/Welchia.D to benefit from a flaw in Microsoft implementation of WebDAV in IIS 5.0

14. Deploying Internet Information Services (IIS) 6.0 http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/all/deployguide/en-us/iisDG60_overview.asp

15. Group Policy Management Console with Service Pack 1 runs only on Windows XP and Windows 2003, but can also manage Windows 2000 AD domains. http://www.microsoft.com/downloads/details.aspx?familyid=c355b04f-50ce-42c7-a401-30be1ef647ea&displaylang=en

16. Windows Server 2003 Security Guide. http://www.microsoft.com/downloads/details.aspx?familyid=8A2643C1-0685-4D89-B655-521EA6C7B4DB&displaylang=en

17. System Services for the Windows Server 2003 Family and Windows XP Operating Systems http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/management/svrxpser_7.mspx

18. HOW TO: Configure Web Site Logging in Windows Server 2003 http://support.microsoft.com/default.aspx?scid=kb;en-us;324279

19. Internet Information Server Performance Logging to Disk vs. ODBC http://support.microsoft.com/default.aspx?scid=kb;en-us;142557

20. A brief introduction on how to secure a MySQL database comes from its documentation, available on the following page http://www.mysql.com/doc/en/Security.html

21. How Big MySQL Tables Can Be http://www.mysql.com/doc/en/Table_size.html

22. Microsoft SMS Sender http://www.microsoft.com/downloads/details.aspx?FamilyID=06a4f997-7f69-4891-8929-37b9041924a2&DisplayLang=en