Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Securing Windows and PowerShell Automation (Security 505)"
at http://www.giac.org/registration/gcwn

Implementing a Secure Microsoft Windows Server 2003 Terminal Services Infrastructure:

A Case Study for ACME Healthcare, Inc.

© SANS Institute 2004, Author retains full rights.

James Tarala
GCWN Practical
Version 3.2
December 2003

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, Author retains full rights.

Table of Contents

TABLE OF CONTENTS **3**
ABSTRACT **5**
CURRENT ORGANIZATIONAL ENVIRONMENT **6**
VISION AND SCOPE **7**
ASSUMPTIONS **8**
CONCEPTUAL NETWORK DESIGN **9**
TERMINAL SERVERS 10
DATA STORE 10
APPLICATION SERVERS 11
LICENSING SERVER 11
SESSION DIRECTORY SERVICES (TSSD) 12
USER WORKSTATIONS 13
INTERNET CONNECTION 13
HARDWARE SPECIFICATIONS **15**
HARDWARE CONFIGURATION & BUILD PROCESS **17**
CORE OPERATING SYSTEM CONFIGURATION & BUILD PROCESS **18**
CREATING THE UNATTENDED INSTALLATION SCRIPT 18
INSTALLING THE CORE OPERATING SYSTEM 30
CORE OPERATING SYSTEM CONFIGURATION 31
LOCAL ACCOUNTS 31
LOCAL GROUPS 32
APPLICATION INSTALLATION & CONFIGURATION **33**
CONFIGURING THE APPLICATIONS 33
PROFILE ACCOUNT CUSTOMIZATIONS 34
TERMINAL SERVICES CONFIGURATION **36**
WINDOWS SERVER 2003 TS FARM HARDENING PROCEDURES **43**
WINDOWS UPDATES / AUTOMATIC UPDATES 43
LOCAL SECURITY POLICY SETTINGS 44
LOCAL SERVICES SETTINGS 49
LIMITED APPLICATION ACCESS 52
NETWORK LOAD BALANCING INSTALLATION & CONFIGURATION **54**
SESSION DIRECTORY INSTALLATION & CONFIGURATION **60**
ADMINISTRATION & MAINTENANCE **63**
ADMINISTERING THE SERVER 63
REGULAR MAINTENANCE ACTIVITIES 64
MANAGING RISKS TO TERMINAL SERVICES **66**
CONCLUSION **71**
APPENDIX A – UNATTENDED INSTALLATION SCRIPT (TSFARM.TXT) **72**

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

APPENDIX B – AUTOMATIC UPDATE SCRIPT (AUTOUPDATETS.VBS)..... 73
REFERENCES..... 74

© SANS Institute 2004, Author retains full rights.

Abstract

In the current atmosphere of healthcare information technology there are two driving factors which influence most every organization across the US. These factors are cost and security. Not that either of these factors is new, or even unique to healthcare, but with the adoption of HIPAA regulations in 1996, the subsequent finalization of the data security regulations in 2003, and the nationwide financial crisis in healthcare, enterprises have sought to find increasingly new and creative ways to satisfy both of these requirements for information technology projects and initiatives.

One technology, which offers healthcare environments the opportunity to meet the increased demands for fiscal responsibility and tighter security controls, is Microsoft Windows Server 2003 terminal services. This technology allows organizations to leverage existing workstation hardware, limit decentralized end user support, and standardize the end user's computing environment, thus reducing costs. It also controls the distribution of potentially harmful applications, reduces the surface area for potential threats, and centralizes the management of end user computing environments, thus increasing the overall security of the enterprise.

This document describes the specific implementation of terminal services within ACME Healthcare, Inc. (ACME) and outlines specific instructions for installing and configuring a TS farm at a local site. This document has been written with a centralized view of the enterprise, however it focuses specifically on how to install and configure a TS farm at one location. The idea behind this document is that the methods described can be used to install a server farm with one or many terminal servers as a part of the farm. It provides a step-by-step guide to installing a secure TS farm so that anyone with a reasonable understanding of Windows Server 2003 should be able to use this guide to deploy a farm of their own. Finally the server configuration described has been designed securely in such a way as to allow these servers to be installed either internally, as a way to provide internal users with a centralized desktop, or externally, as a part of a demilitarized zone (DMZ) which remote users could access as a limited replacement for an enterprise virtual private network (VPN).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Current Organizational Environment

ACME is a geographically dispersed organization with hospital, health park, and nursing care facilities scattered throughout the Eastern United States and one centralized corporate administrative office. Traditionally the organization's IT structure has been distributed, with each local market maintaining and supporting the data networks individually with limited collaboration between systems. However in recent years the organization has realized the value of sharing information between systems in order to promote understanding and standardization between systems.

Currently within ACME there is a disjointed approach to thin clients in general and terminal services specifically, with each local system utilizing these services in a different manner. Currently the local systems have been divided between the use of Microsoft terminal services alone and terminal services combined with various third party add-on applications for implementing thin client and hosted solutions. However more and more systems have been investigating the use of terminal services due to its seamless integration with Active Directory Services and the lower total cost of ownership associated with the Microsoft product.

Currently the majority of local systems are using thin client solutions, and terminal services specifically, for application specific purposes. These solutions typically involve applications launched from one of these servers as a way to increase manageability and security for these applications. However with the increased need for workstation and network security and the increased need for desktop manageability, more and more local systems are considering the possibility of rolling out Microsoft terminal services as a way to meet these objectives.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Vision and Scope

Specifically Microsoft terminal services are being considered within ACME to meet the following business objectives:

1. Desktop Security – By implementing Microsoft terminal services administrators are able to better control the end user's environment and thus the security of the overall environment. By limiting the resources users have locally administrators can better mitigate against security risks which threaten the network.
2. Secure Wireless Networking – Terminal services allows for physicians and staff that require access to patient health information (PHI) to utilize wireless technologies along with tablet and PDA technologies in a secure fashion when used in conjunction with terminal services.
3. Desktop Manageability – By integrating this technology into a local system support staff have a lower burden for supporting user issues. This results in faster issue resolution times, more issues being resolved by helpdesk staff over the phone, and lowers the total cost of supporting applications within the enterprise.
4. Lower Total Cost of Ownership (TCO) – Most organizations implementing terminal services have found significant monetary savings due to the lower total cost of managing and securing user environments in a centralized setting.
5. Higher Customer Satisfaction – Help Desk response time to end user problems can often be decreased, allowing more issues to be resolved by a "first responder." User issues can thus be resolved in a timelier manner, resulting in a lower overall cost of ownership and a higher satisfaction level by the end users.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Assumptions

Throughout this document the following assumptions have been made regarding the rollout and configuration of terminal services within ACME:

1. The terminal servers will be installed with Microsoft Windows Server 2003 as the core operating system. Depending on the environment, some local systems may choose to use the Standard Edition of the OS, while others choose to use the Enterprise Edition of the OS, depending on the size of the site and the use of Session Directory.
2. The desktops interacting with terminal services will run an operating system which supports that latest version of the Remote Desktop Client in order to fully support Windows 2003 terminal services and the Remote Desktop Protocol (RDP) version 5.2.
3. Terminal services will be managed by local system staff and supported by others within the organization collaboratively to again move towards a unified ACME and a spirit of cooperation between local systems. Although at the same time terminal services by nature promotes the ability of remote users assisting with the management of the servers if necessary.
4. Any application that will be installed on a terminal server must first be tested and its functionality validated on an offline testing server before it will be installed on a production terminal server. As noted previously, many vendors will not support their application on terminal services and therefore local systems may be constrained where they will be able to utilize this technology.
5. Microsoft patches and service pack updates will be centrally managed through Software Update Services (SUS) and Windows Automatic Update Services. In those environments with Microsoft Systems Management Server (SMS) installed, the SUS Feature Pack will be used instead.
6. Each facility within ACME will follow the organizational anti-virus standard and install Network Associates (McAfee) NetShield anti-virus software on each of the servers on the network, including all terminal services servers, licensing servers, and data stores to protect against malicious code infecting these systems.

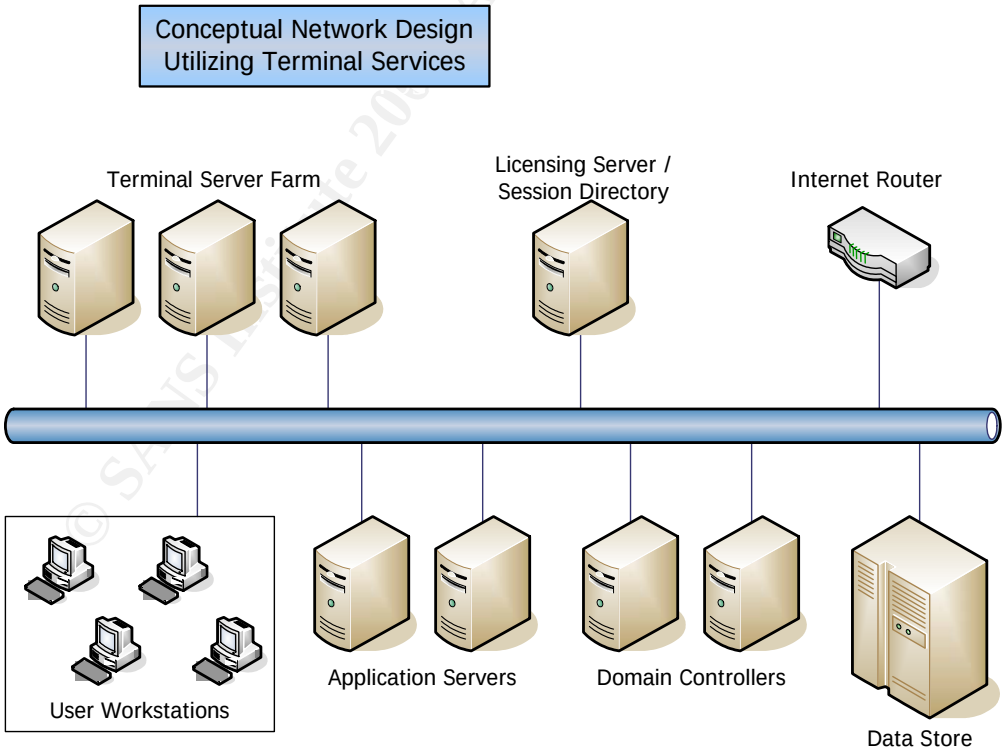
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Conceptual Network Design

The following design is a conceptual design intended to be implemented at a single site within the organization[1]. Local systems may find that they have multiple geographic sites and thus have multiple occurrences of this design repeated in different facilities. As mentioned earlier some of these implementations may be external, Internet facing farms while others will be strictly internal systems. The conceptual design for either of these designs is the same, and when properly secured should be configured with the same restrictive settings. The terminal services infrastructure will be broken into the following major categories in each environment:

1. Terminal Server Farm
2. Data Store
3. Application Servers
4. Licensing Server
5. Session Directory Server
6. User Workstations
7. Internet Connection

The following diagram summarizes the overall conceptual design of the terminal services Infrastructure:



[1] In fact, currently Microsoft's Network Load Balancing (NLB) tool only supports servers located in the same subnet.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The specific design of the TS farm will vary from facility to facility depending on its size, the number of users who will be utilizing terminal services, the type of applications that will be running on the terminal servers and the amount of data storage space required by that system. Also in some implementations certain services may be non-existent or combined into a single hardware device (such as the domain controllers, licensing server, session directory server, and the data store). However this design should provide a general architecture for the overall design of a farm within ACME.

Terminal Servers

These servers provide the backbone for the TS farm and provide the majority of the support for this architecture. The farm itself consists of Windows Server 2003 servers configured to run as terminal servers. These servers provide a centralized location for all of the organization's desktop environments where employees will conduct their day to day tasks. This is especially useful in the healthcare market where many PCs are implemented simply for task workers who use the machines as basic mechanisms for data entry and alerting.

Also these servers will be configured in a Network Load Balanced (NLB) configuration. While this is not a clustered environment it still provides system level redundancy and load balancing features which will increase the overall stability and availability of the farm. NLB, in brief, allows a user to connect to a virtual IP address which represents a series of servers configured as members of the farm. The servers then utilize an algorithm based on availability and present load statistics to direct the user to one server where a session can be established. Each of these servers is still a unique machine which can be connected to independently, yet functions as a part of the whole.

This is especially crucial given the nature of the TS farm being modeled in this document. Within ACME these servers will be solely responsible for providing a computing environment to enterprise employees. Rather than employees working from a decentralized workstation where all of their work is performed at the desktop, ACME employees utilizing one of the TS farms will instead be conducting all of their work on a centralized set of servers. Should the farm go offline users would lose their complete working environment, thus high levels of redundancy are mandated.

Data Store

The configuration of the data store for each local system will be unique based on the storage requirements for that particular system. Currently ACME employs a range of different storage solutions, from standard file and print servers to Storage Area Networks (SANs) utilizing both Microsoft and Novell file and print services to manage the data. With the standardization of all local systems on Microsoft Active Directory imminent, all systems will standardize on Microsoft File and Print Services. While the software configuration for data storage will be similar, the hardware platforms that will be used for this will vary on the needs of the system and the finances available.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Regardless of the system configuration, these data stores must be both highly available and highly redundant.

In relation to terminal services, these data stores will serve as the location for the following types of data:

1. Shared User Data
2. Application Data
3. Individual User Data
4. Individual User Profile Data

The overarching principle of the data store is that no unique data will be stored on any of the terminal services servers. These servers should have the potential of being re-imaged at any given point without any impact to the end users. This is a requirement for those server farms that will be utilizing Terminal Services Session Directory (TSSD). Since a user may connect to a different TS server each time he or she connects to the network, their user data and profile configuration must not be stored locally on a terminal server. Instead it must be offloaded to a separate data store where the data will be consistent regardless of the TS server being utilized at the time.

Application Servers

These servers represent the various applications installed at any given local system. These are the servers that users will access in order to run applications that are necessary for the functioning of their role. Examples of such servers would be lab servers, radiology information systems servers, pharmacy servers, etc. They are shown in the above diagram to represent the servers that must be accessed from the terminal servers for the user to complete their day to day responsibilities. The hardware and software configuration for these servers will be unique to each vendor's product, and are many times even managed by the vendors themselves.

Licensing Server

Each Local system must also install and configure at least one terminal services licensing server per each TS farm. Currently there are three licensing models supported by Microsoft for terminal services:

1. Per Device Licensing
2. Per User Licensing
3. External Connector Licensing (unlimited)

Since the terminal services servers in this configuration are to be used primarily by internal ACME employees the third option, the external connector license, will be unavailable. This license only supports individuals from outside of the organization (business partners, customers, etc) who need to access terminal services. Therefore the choice in licensing becomes either licensing per device or per user connection. Each local

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

system will need to decide which licensing model makes more sense for their market. If there are more users accessing the system than devices being utilized, then the Per Device model should be chosen. If there are more client devices accessing the system than users, then the Per Client model would be the right choice.

It should be noted that the per device and per user licenses are not concurrent licenses. Each user or device that connects to a terminal server will reserve one of the licenses for their connection and hold onto it for 90 days, at which time it can be renewed. It should also be noted that the previous licensing model under Windows 2000 Server, where any client whose OS was Windows 2000 or later had a built-in connection, is no longer applicable with Windows Server 2003 terminal services.

As noted earlier, each facility with a TS farm must have a licensing server installed at that location in order to support the servers. Depending on the size of the environment one of two options are available as to where the licensing service may be installed. For smaller facilities the licensing server should be installed and configured on one of the servers that are a part of the data store. This service utilizes very few resources and can easily be installed on a server providing file and print services to the network. For larger facilities a dedicated server should be established to house the licensing service. This server could then also host the facility's TSSD service on the same machine. In either case both the TSSD service and the licensing service should co-exist on the same machine for ease of maintenance and for fiscal responsibility. In no case should either of these services be installed on one of the terminal servers in the TS farm since each of these machines should be identical clones of each other in order to properly support NLB.

Session Directory Services (TSSD)

The TSSD server provides a consistent way of managing user initiated sessions throughout the TS farm. Unfortunately during the course of a terminal services session a user may become disconnected with the server that he or she was working on without closing the session that was originally opened. If that user were to try to reconnect to the TS farm the NLB service could possibly connect that user to any server in the TS farm, not knowing that a previous session had already been opened on one of the servers. That's where the Terminal Services Session Directory (TSSD) service comes in. Before NLB connects a user to a server in the TS farm it checks with the TSSD service to see if that user already has an open session on one of the servers in the farm. If that user does not have a current session open, the user is directed to any available server in the farm. If the user previously had a session open in the farm that was still open, he or she would be redirected to that server where the session could be reestablished. Thus the user re-enters their environment just as they left it, with all applications and windows open.

This allows for the following vision in a healthcare environment. Imagine a physician working in an emergency room environment. One of his or her most basic needs is the ability to be able to quickly diagnose and treat patients coming into the facility. In order to accomplish this in the timeliest manner possible the physician needs access to

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

information as quickly as possible and from wherever possible. The physician using a TS farm enabled with TSSD could begin a shift working at one PC, but then be called into a patient room to consult. He or she would have the option of disconnecting from the current TS session (with the click of one button), and then logging into the PC in the patient's room, without losing any data, and having the same user environment (windows, applications, and all) immediately available. Thus information becomes more readily available and patient care and service can increase exponentially.

User Workstations

Workstation hardware and software specifications will also vary from local system to local system. Most likely within each individual local system there will be varying models of workstations that will be used to access these terminal servers, from desktops, laptops, PDAs, and even Tablet PCs. One of the benefits of utilizing terminal services is that the processing for a user's computing session is being performed on a server, not at the client's workstation. Therefore regardless of the computing power of the user's workstation the user will be able to access resources and process requests at the same speed and efficiency an older legacy machine as with the latest and greatest desktop hardware. This lends itself to a longer desktop lifecycle and ultimately lower costs at the desktop.

However, one common denominator for these systems is that they should attempt to use an OS that allows the user to utilize version 5.2 of Microsoft's Remote Desktop Protocol (RDP). Clients with other OSs that do not support the RDP 5.2 client should not be permitted to access the terminal servers. However while only Microsoft Windows XP, service pack 1 or later natively supports this version of the protocol, the following operating systems currently support version 5.2 after a free client has been installed on the machine[2]:

1. Microsoft Windows 95
2. Microsoft Windows 98 (and SE)
3. Microsoft Windows ME
4. Microsoft Windows NT
5. Microsoft Windows 2000
6. Microsoft Windows XP (pre-SP1)
7. Mac OS X[3]

Internet Connection

Facilities within ACME will have the option of configuring these TS farms as internally accessible only farms, externally accessible only farms, or a combination of the two. One of the benefits of this architecture is that users have the opportunity to access the same

[2] http://www.microsoft.com/windowsxp/pro/downloads/rdclientdl.asp
[3] http://www.microsoft.com/mac/downloads.aspx?pid=download&location=/mac/DOWNLOAD/MISC/RDC.xml&secid=80&ssid=9&flgnosysreq=True

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

workstation environment whether they are in the office, traveling for business, or simply working from their home. With the reality of the mobile workplace and within ACME the constant need for individuals to travel between local facilities, terminal services provides a mechanism for users to experience the same computing environment regardless of their location, without compromising security.

Terminal services, and more specifically the RDP protocol, works through the use of one primary TCP port, port 3389. If a facility desired to make their terminal services farm available to employees while they were outside of their facility, they could easily do so through the use of the Internet simply by opening one port in the organization's firewall. While there are always risks associated with allowing remote access to a system, in this case the risks are minimal, especially when they are compared against the gains in functionality. This potentially eliminates the needs for many workers to even utilize VPN software in order to connect to the facility's network, which is costly in both employee management resources and financial resources. A full discussion of the risks involved in this model, are discussed later in the document.

It should also be noted that in this conceptual network design, none of these servers is noted as being a web server dedicated to hosting the Terminal Services Web Client (TSWeb) ActiveX control. Since there are documented vulnerabilities with the TSWeb client and since simply installing Internet Information Systems (IIS) on a server opens a whole world of risks to the system which must be managed, this service should not be installed as a part of a ACME TS farm. This service is used to allow for easy access to a TS farm, and most often to give system administrators an easy way of remotely accessing a system. However, as will be noted later, there are other ways of accessing these servers without threatening the overall security of the design.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Hardware Specifications

Each TS farm will consist of similar servers configured using Microsoft Windows Server 2003's built in NLB service and where appropriate, TSSD service. Each of the servers in the farm, for the sake of NLB and for the sake of consistency and standardization, should have an identical hardware configuration. Recognizing that cost effective specifications change on a monthly basis, the following configuration has been chosen at the time of this writing in order to balance the need for performance with the need for cost-effectiveness:

Hardware Vendor	HP / Compaq
Model	DL 360 G3
Form Factor	1U Rack Mountable
Processor	Dual 2.8 Ghz Xeon
Memory	4 GB
Drive Array	2 Mirrored 36.4 GB SCSI Drives
Remote Management	Integrated Lights Out Advanced (RILO)
Warranty	24x7 4 hour Response

This configuration has been based off of studies performed by both Microsoft and HP/Compaq, as well as by Avanade, on the average hardware requirements in order to support users in varying configurations. For the sake of this study the servers noted above will be assumed to be able to support 50 concurrent users on one server. This number is a balance between the numbers provided by HP/Compaq on their Smart Answers website (110-410), the numbers provided by Microsoft in their Terminal Services Scaling document (200-440), and the actual number of users being supported per server by Avanade in their Windows Server 2003 terminal services configuration (30)[4].

The point of this discussion is to establish a baseline number of concurrent users on a terminal server, not to determine the validity of test scripts or the actual number of users supported by a particular server. The number of concurrent users is a slightly subjective balance between lab studies and live utilization figures. However, more information can be found on each of these studies at:

HP/Compaq Active Answers Study:

http://activeanswers.compaq.com/aa_downloads/6/100/225/1/72358.pdf

[4] It should be noted that while HP/Compaq and Microsoft both based their numbers on similar, if not identical, hardware configurations, Avanade's terminal services environment utilizes slightly older servers with dual 1.4 Ghz Xeon processors and only 2 GB of RAM.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Microsoft Terminal Services Scaling Whitepaper:

http://www.microsoft.com/windowsserver2003/docs/TSscaling.doc

Avanade Case Study:

http://www.microsoft.com/resources/casestudies/casestudy.asp?casestudyid=13212

© SANS Institute 2004, Author retains full rights.

Hardware Configuration & Build Process

Since each individual facility will have different configurations for rack space, rack rail types, UPS specifications, etc, actually mounting the server into the environment is beyond the scope of this document. This document also assumes that either the hardware described in this document will come pre-assembled, or that it will be assembled by knowledgeable individuals with an understanding of server hardware. So for the most part, this document will not discuss the process for assembling and mounting the server into a datacenter.

The one requirement that must be common, in order to facilitate some of the scripts which are noted later in this document, is that the two hard drives in the system be configured in a mirrored array before the operating system gets installed. The hardware specified in this document has a built in HP Smart Array 5i RAID controller. During the boot-up process the administrator can press <F8> to enter the initial configuration for this array. The defaults are to configure the array as a RAID 1 configuration, so the administrator can simply choose to save the defaults and the array will be mirrored. The administrator must then use the boot disk to create a partition on the drive and format that partition to allow the script to automatically install the OS on the server.

Another configuration choice that can be done to help make the server more efficient is during the initial boot-up process to press <F9> to enter the Rom-Based Setup Process. In this menu the administrator tells the server which operating system will be installed on the server. For performance gains the server should select Windows 2000/2003 Server. Once this choice has been saved the server will need to reboot.

However there is one aspect of the hardware of the server mentioned above which is vital, and must be mentioned for security reasons, though specific settings are beyond the scope of this discussion, and that is the Remote Integrated Lights-Out (RILO) board that comes built into the hardware specifications described earlier. The RILO board on HP/Compaq systems can be used to remotely manage a server in a “lights-out” computing environment, thus enabling an administrator to manage every aspect of the server without physically touching the machine at all. Because this board is integrated into the hardware specifications previously mentioned, and because it allows a user to fully control the server, its secure configuration is vital.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Core Operating System Configuration & Build Process

The core build for each of the servers in the TS farm should be based off of a similar image or installation process. In order for these servers to function properly with NLB, each of the servers in the farm should utilize identical hardware and software configurations. In order to accomplish this each server should be initially installed utilizing an unattended installation process where only unique fields should be allowed to be changed as a part of the installation. For disaster recovery purposes a syspreped image should also be taken of the core OS build in order to facilitate the quick recovery of one of the servers in the event of a downed system. There are many imaging software packages available, Symantec and Altiris being two companies which support such products. Each system should find one that they find most comfortable using.

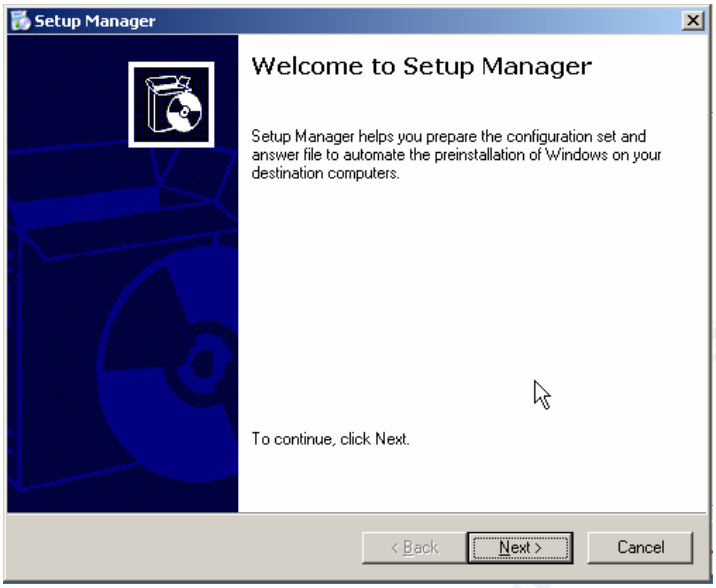
Creating the Unattended Installation Script

In order to install the core operating system on a new terminal server the installation process should be completed using an unattended setup file. This file can be generated within the Windows Server 2003 environment using the Setup Manager utility (accessible after installing the support tools from the Windows Server 2003 CD). Once the initial unattended installation script has been generated that script can then be used to install all of the servers in the TS farm.

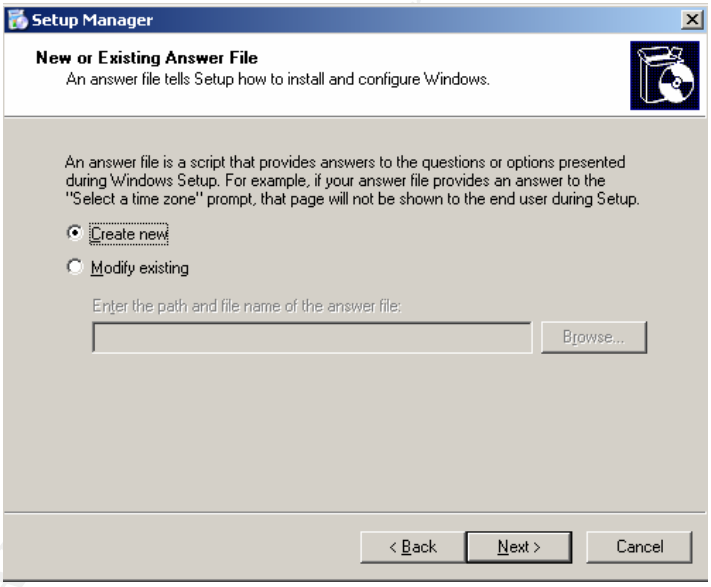
Within ACME a common unattended installation script has already been generated to facilitate commonality and standardization in the operating system setup process (see Appendix A). However, to illustrate the process of creating this script the following screen shots demonstrate the choices selected when running the Setup Manager to create the script:

1. Start the Setup Manager after extracting the file from the Deploy.cab file located on the Windows Server 2003 CD in the /support/tools directory.

© SANS Institute 2004, Author retains full rights.

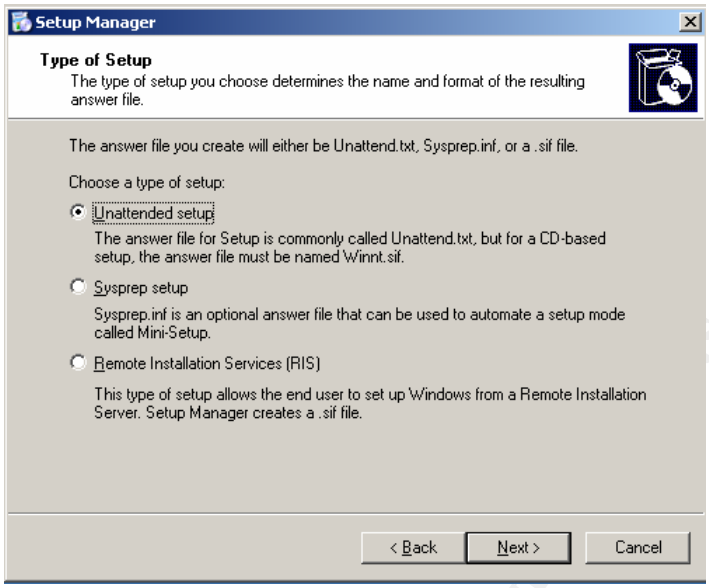


2. Create a new installation file. This file that's created will be the unattended installation script that will be used to automate the operating system installation.

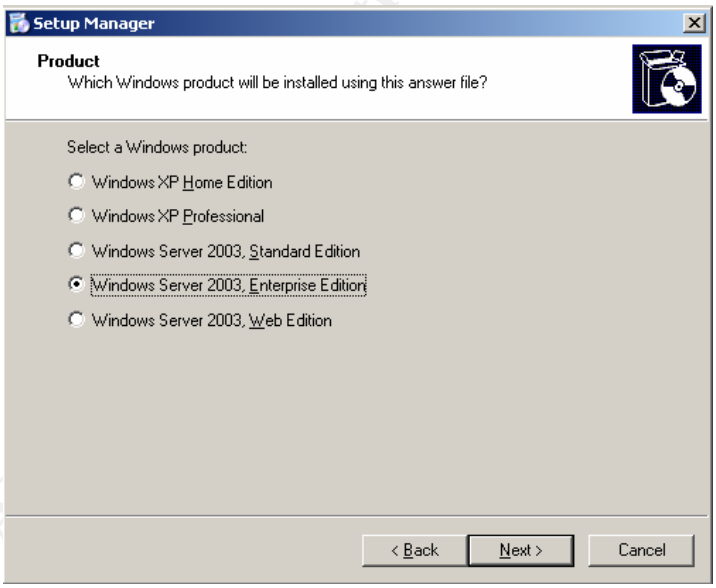


3. Choose to create an unattended installation script. Although a syspreped image could be created here, since this document describes the first terminal server in a farm to be created, sysprep images will be unavailable. Also, since ACME has a limited installation of Microsoft Active Directory which is currently being rolled out to all of the local systems, the Remote Installation Services (RIS) script will not be chosen (since it requires Active Directory to utilize).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

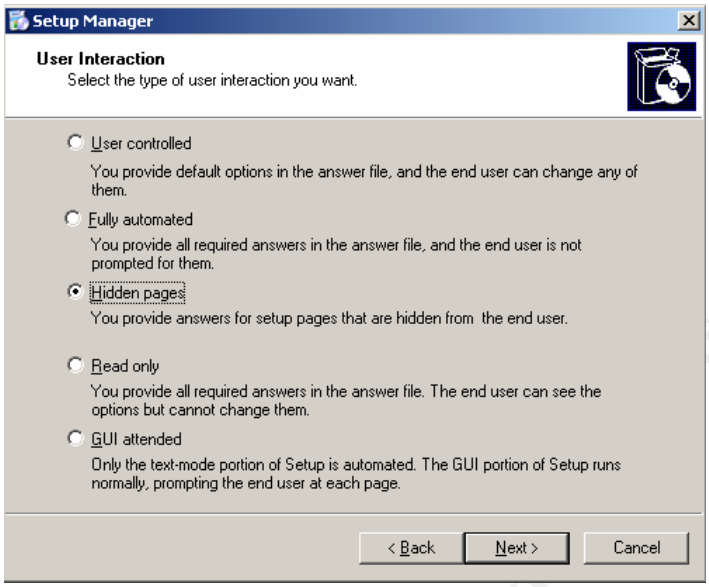


4. Windows Server 2003 Enterprise Edition will be the operating system installed for each of the terminal servers in the TS farm. Since in order to utilize the TSSD service a terminal server must be running Enterprise Edition, all of the servers should be installed with that edition of the OS.

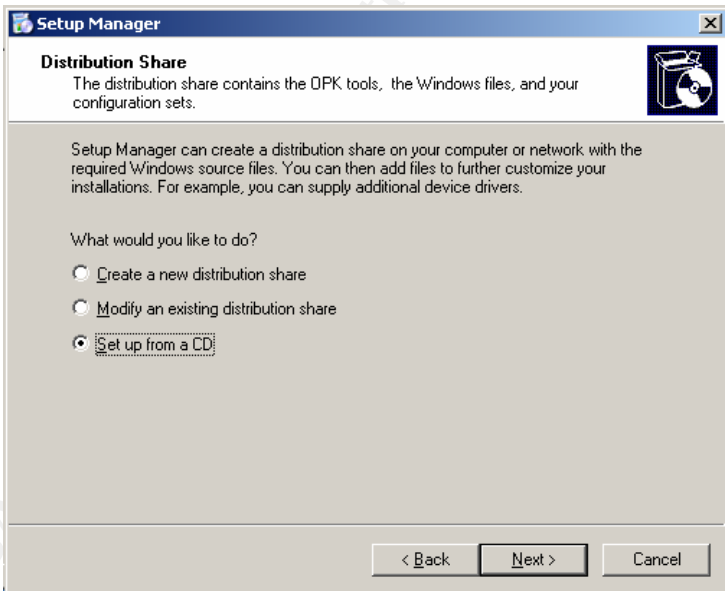


5. User interaction will utilize the “hidden pages” option in order to limit and hide the installation options from the people who install the core operating system.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

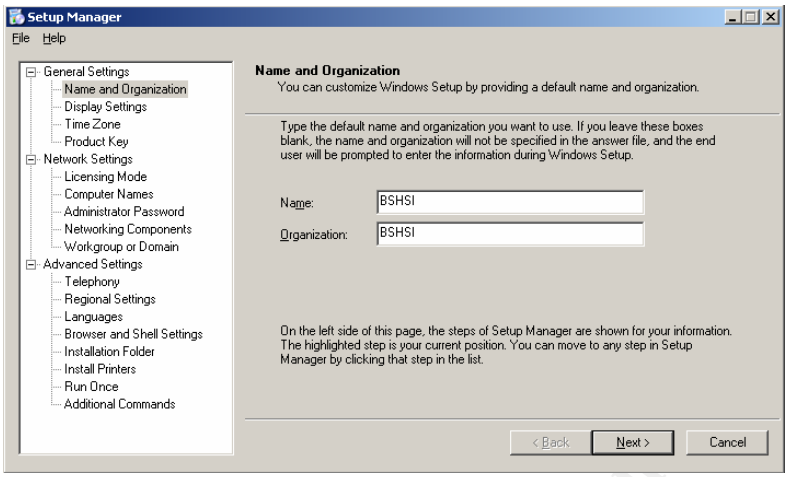


6. The follow choice indicates where the installation media for the terminal server installation will be located. Since these servers will be distributed at multiple facilities within the organization and since network bandwidth is limited, all installations will be via CD.

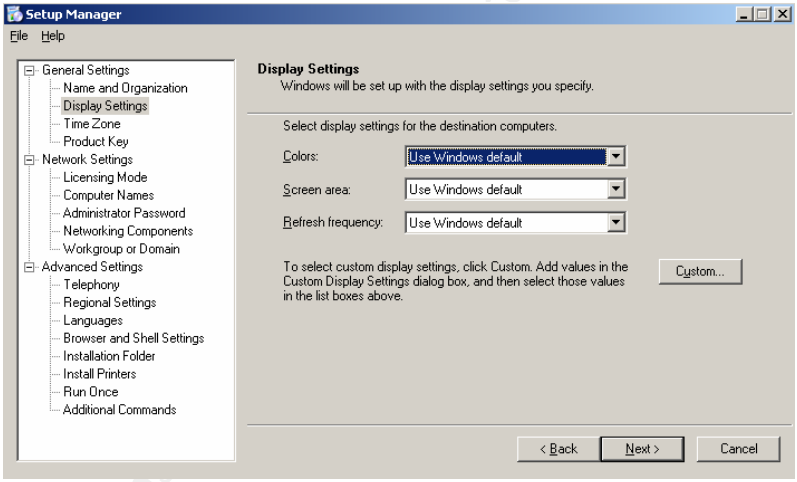


7. This now begins the section of the Setup Manager which starts to answer the questions prompted to a user during the Operating System's installation. The first question simply indicates the name and organization where the server will be installed, in this case ACME.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

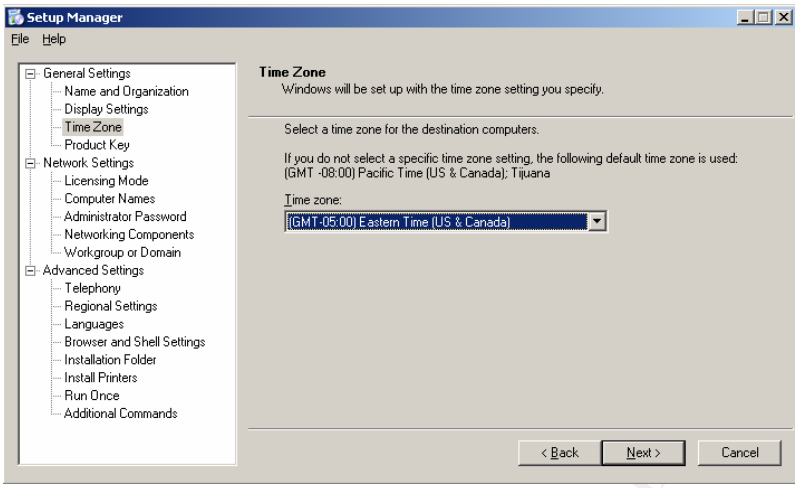


8. The next choice prompts for what monitor colors, screen area, and refresh frequency will be user for the server being installed. Since these servers will all be rack-mounted servers, utilizing different monitors, the Windows default settings should be chosen.

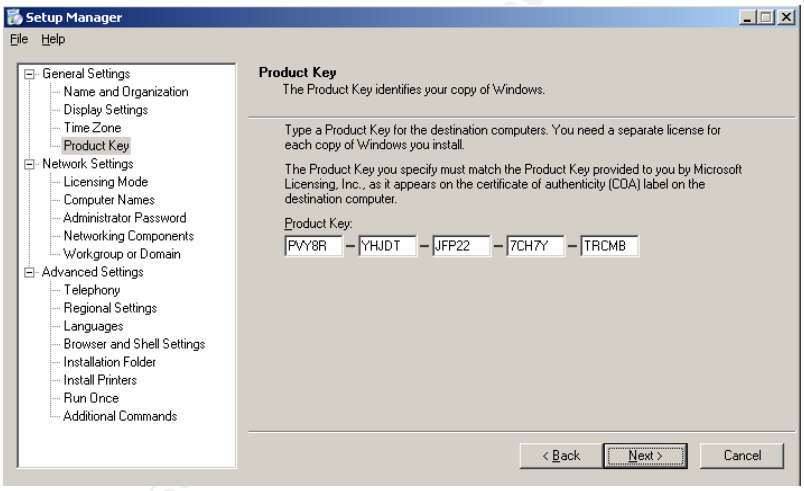


9. Since all of the ACME facilities are located in the Eastern United States, the Eastern Time zone has been chosen.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

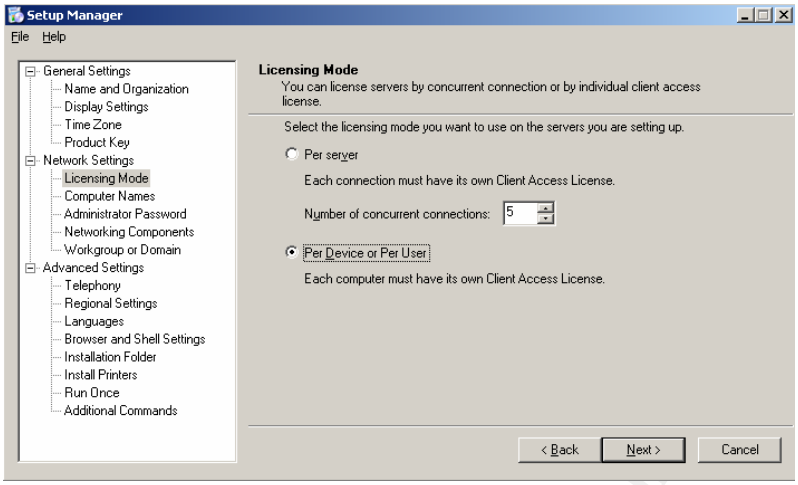


10. The following indicates the product key that should be used to install the operating system. Since all of ACME subscribes to the same Microsoft Select license, the following key can be shared between facilities and used to install the operating system.

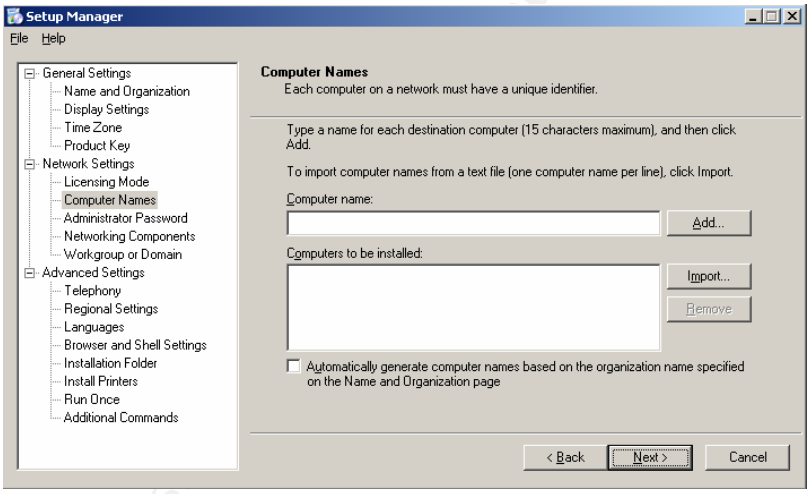


11. Per device licensing is the licensing model that has been chosen throughout ACME for all of their server systems. Therefore that licensing model should be chosen for this installation as well.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

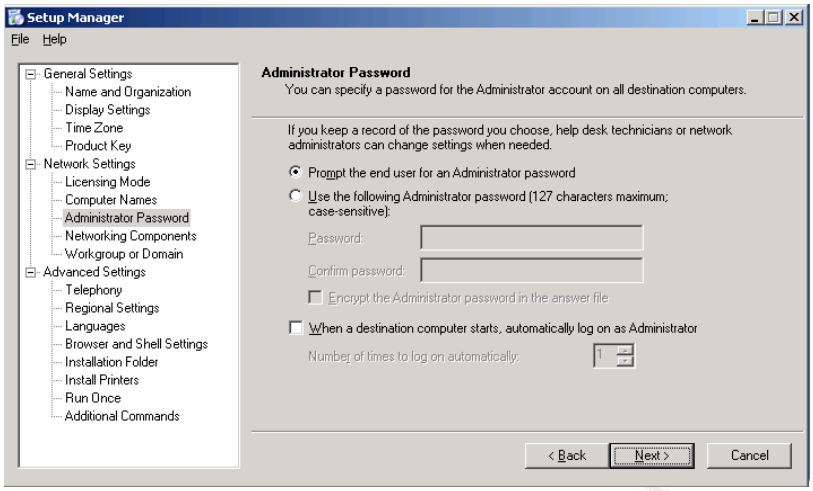


12. Since there will be an unknown number of installations of terminal servers throughout the enterprise, this field will be left blank to allow the administrator of the local facility to enter their own name for the server.

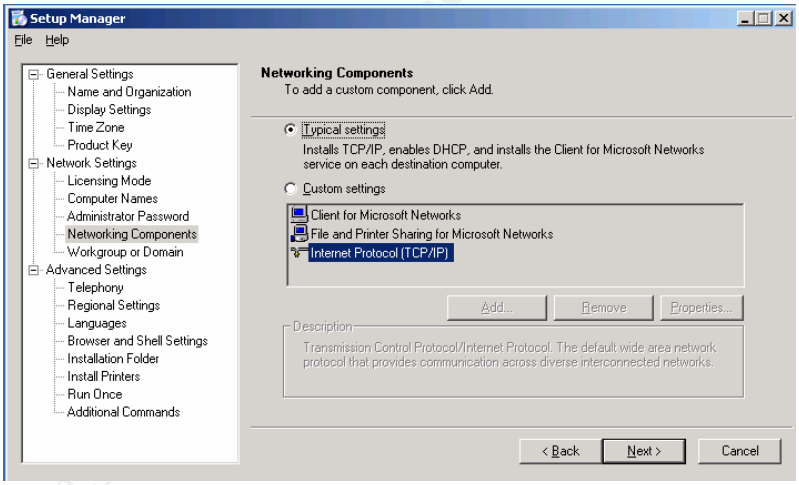


13. For the sake of system security, the local server's administrator password should not be entered as a part of this unattended installation process. Instead that should be entered during the actual installation of the server with a password known only to the local administrators of the server. Often local systems seek to use a common local administrator password that can then be changed on a regular basis. This password should of course conform to standard strong password creation policies and be at least six characters long, using a combination of upper/lower case alpha, numeric, and special characters.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

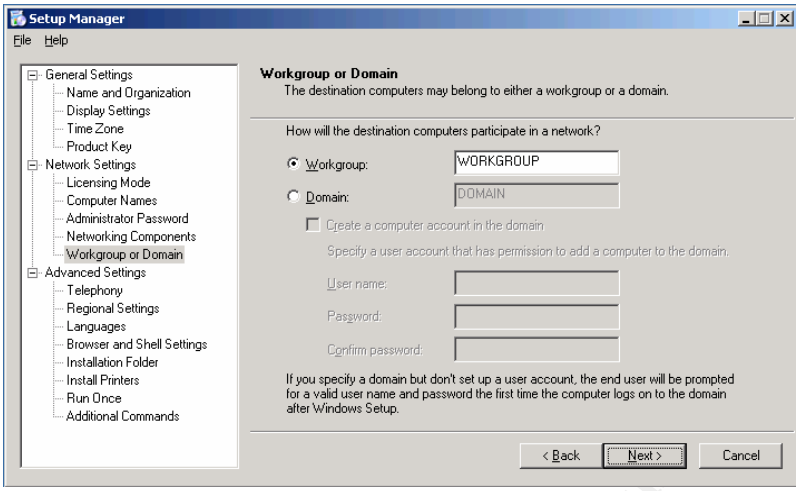


14. The typical network settings have been chosen as a part of the unattended installation process. Although the typical settings will not permanently be used for this server, they do allow the server to access the network immediately after installation (using DHCP to obtain an address). Once the installation is complete, one of the post-install tasks will be to change the IP address and network settings to a static address which also uses local facility network settings.

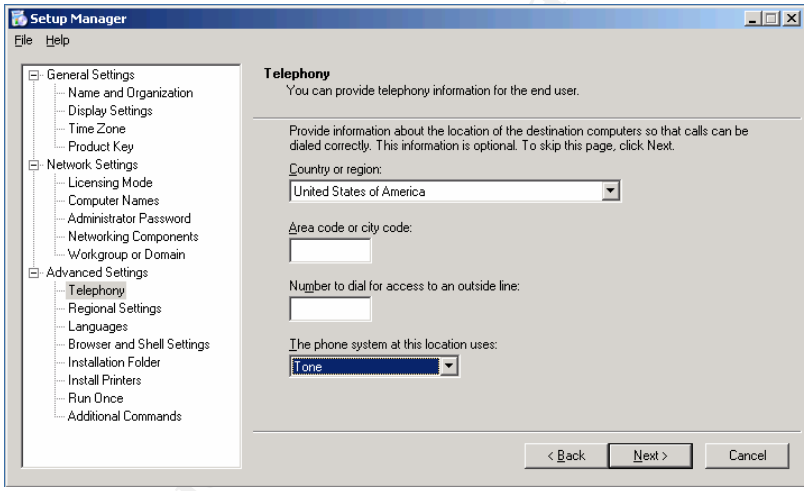


15. As with network settings, the domain membership of the server should be configured post-installation. Since the goal of this script is to provide cross-facility interoperability, and since there are currently a number of Windows NT domains across the enterprise, this must be configured post-installation and joined to the local domain available at that facility. Once ACME has finished its migration to Active Directory all of these servers will be able to join the ACME domain.

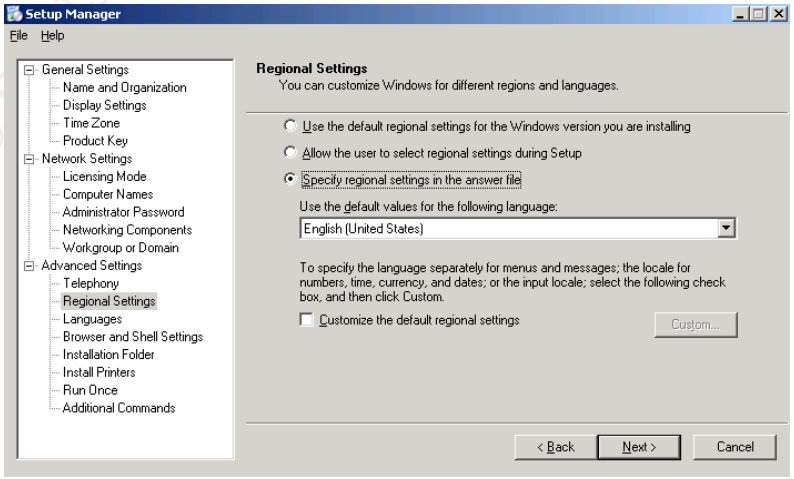
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



16. Again due to differences between facilities the telephone settings will vary from system to system.

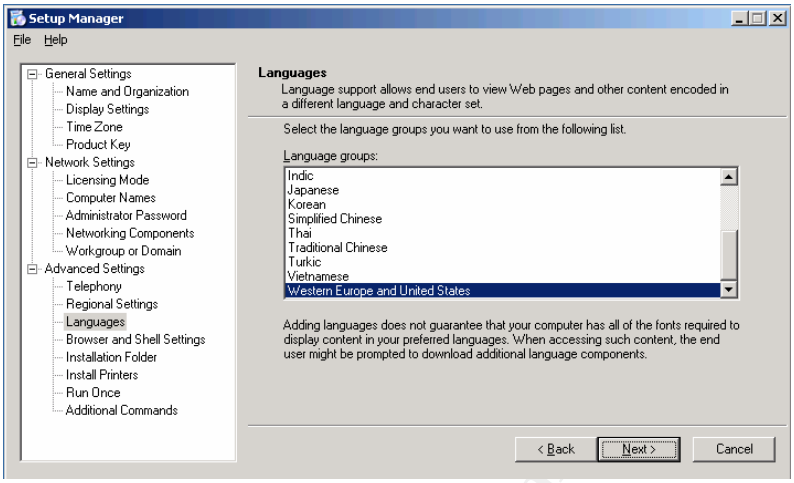


17. All facilities are located in the United States and use English as their primary language. Therefore English (United States) regional settings have been chosen.

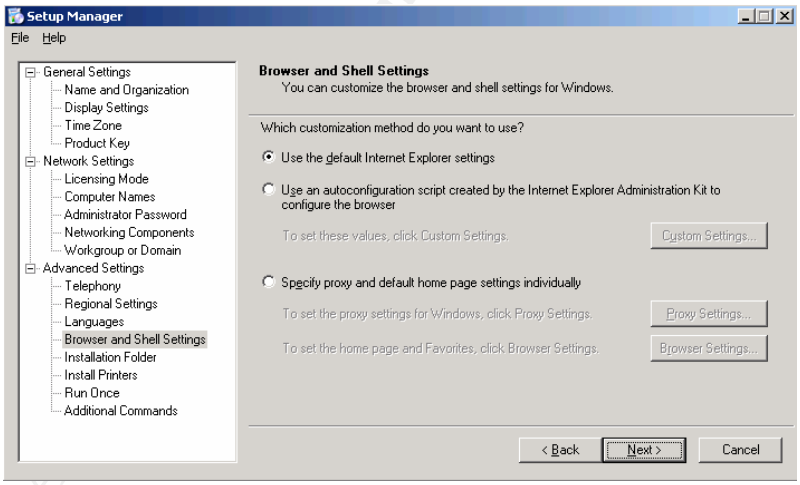


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

18. As mentioned earlier, English is the common language spoken between facilities, and should thus be chosen as the only language pack installed.

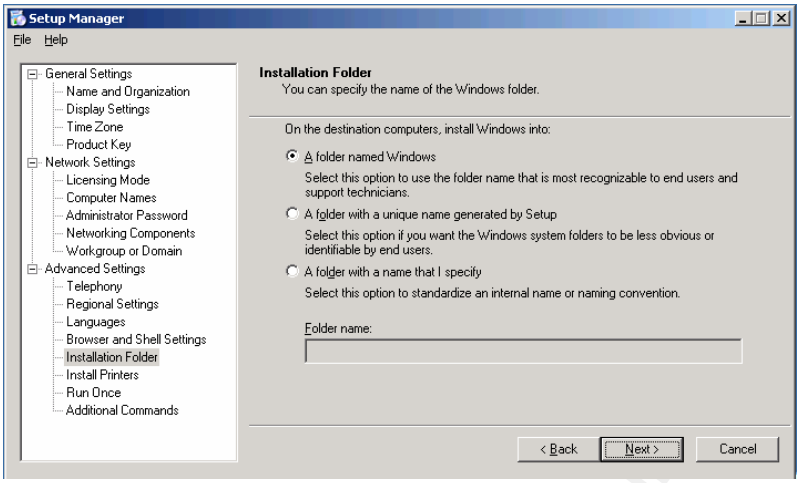


19. Currently there is no ACME standard as to how internet access is controlled. Some facilities utilize proxy servers, while others simply rely on the default gateway to provide internet access. Therefore this section has been left at default to allow administrators the freedom to customize this post-installation.

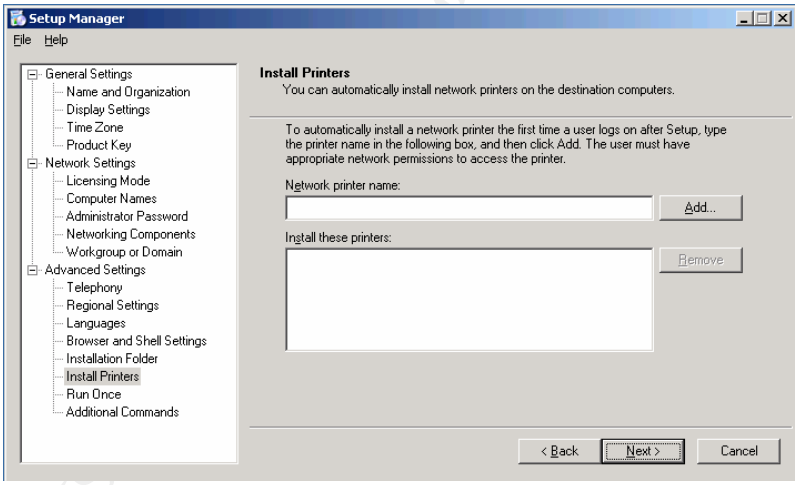


20. For the sake of this installation of Windows Server 2003, there is no need to obfuscate the location of the system directory. In fact this would only cause confusion in the distributed administrative model that ACME has.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

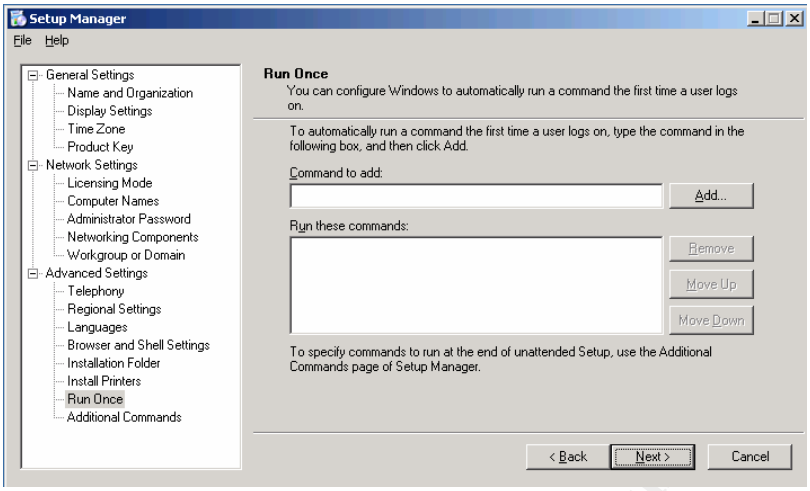


21. Again, do to the disparity between facilities this choice has been left at the default, blank settings. Also since these servers will be a part of a TS farm, printers will be configured on the local workstations and then redirected to the particular server in the farm the user is attempting to connect to. Especially since a user may connect to a different server each time they connect to the farm, there is no reason to install a printer by default on the server.

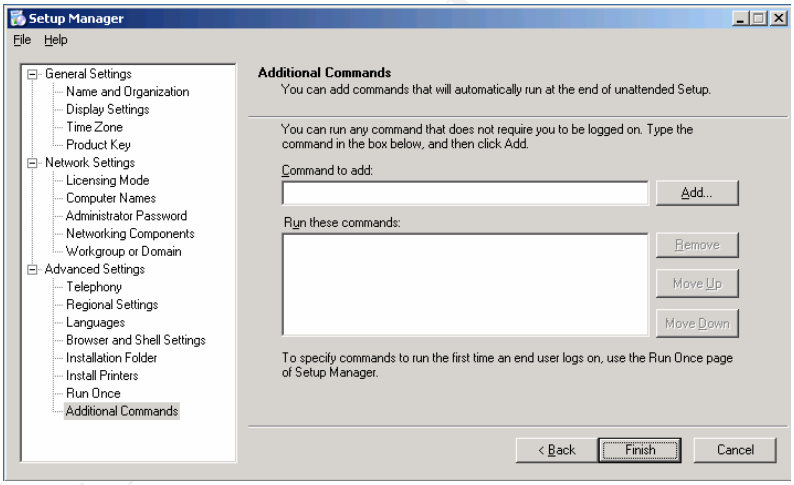


22. Although there are post-installation activities and scripts that must occur in order to complete the configuration of this server, those tasks will be performed manually through the following checklist, or as a part of the Local Security Settings on the server.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

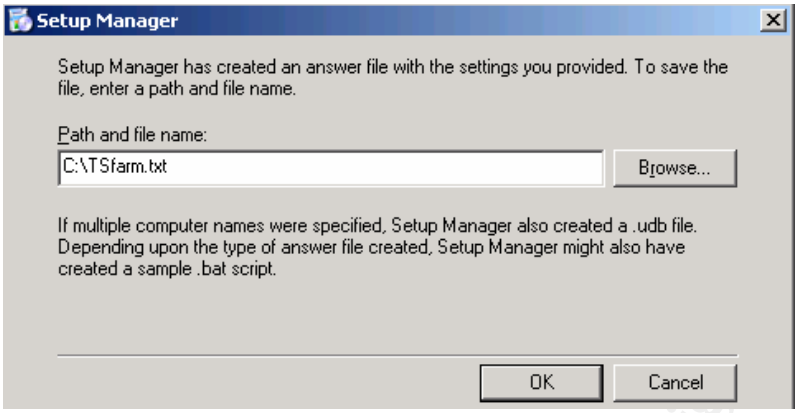


23. Again, although there are post-installation activities and scripts that must occur in order to complete the configuration of this server, those tasks will be performed manually through the following checklist, or as a part of the Local Security Settings on the server.

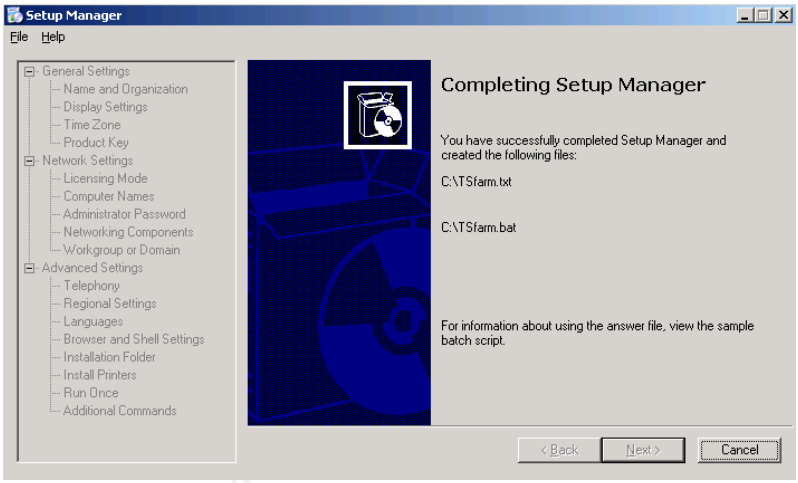


24. Once all of the above configurations have been specified the unattended installation script must be saved to the hard drive to be used later during an actual Windows Server installation.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



25. This completes the unattended installation script setup process using the Setup Manager utility that comes with Windows Server 2003.



Installing the Core Operating System

Once the setup script has been generated, the system administrator can begin installing the terminal server that is to become a part of the new TS farm. Different environments may choose to use different versions of Windows Server 2003 as the core operating system for their TS farm. Terminal services are currently supported on either the Standard or Enterprise editions of the OS. While there are many differences between the versions, the major difference to consider when choosing which version to install is concerning the issue of TSSD. In order for a terminal server to be a part of a TS farm that utilizes the TSSD services the terminal server must be installed with the Enterprise version of the OS. Since the configuration being described in this document assumes the use of the TSSD service in the TS farm, all installations will be performed using the Enterprise edition of the OS. To begin the installation the administrator will issue the following command on the server from a DOS prompt:

```
E:\i386\winnt.exe /u:tsfarm.txt /s:e:\i386
```

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

This command assumes you will be booting with a Windows 98 boot disk with CD-Rom support and will launch the installation of the Windows Server 2003 environment, using the TSfarm.txt file, also copied onto the Windows 98 boot disk, as an unattended installation answer file. This installation will require minimal input on the part of the administrator performing the installation. Once the installation process has completed, the server will reboot and wait for the administrator to login to the server in order to complete the configuration of the new terminal server. All additional operating system configurations will need to be performed after the installation has completed and the server has rebooted.

Core Operating System Configuration

Once the core Windows Server 2003 operating system has been installed on the server hardware using the unattended installation process described above, the operating system should be configured and customized for its purpose as a part of the TS farm. Again as noted before, each of the following steps should be taken on the original server that is installed in the farm, with subsequent servers being created from a syspreped image. The following steps should be taken to customize the operating system once it's been installed:

1. Confirm Date and Time Setting in the Bios
2. Install the terminal services service (through Control Panel – Add/Remove Programs – Windows Components)[5]
3. Add Notepad shortcut to Administrator's Send To menu

Local Accounts

One local account should be created on each of the terminal servers. This account will be used later to configure the default profile for each user that logs into the server farm. This account will only be used to configure the default profile, and will later be deleted from the system. In order to configure the default local profile for a user, first the administrator will need to create the following local user account:

Account Name:	Profile
Full Name:	Default Desktop Account
Description:	Used to create Default User Profile
Password:	<Complex password>
User must change password at next logon:	Not checked
User cannot change	Checked

[5] While the terminal services service should be installed at this point on the server, the terminal services Licensing service should not be installed, but instead will be installed on a different server in the TS farm later in this process.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

password:	
Password never expires:	Checked
Account is disabled:	Not Checked
Member of following Groups	Remote Desktop Users Users

Local Groups

In order for users to be able to logon to the terminal server, their account needs to be a part of the local terminal server's Remote Desktop Users group. This will enable the user to logon interactively through a remote login session. In order to properly scale the membership of this group a Windows domain account should be created to manage the list of users[6]. A domain local or global group (depending on the group's scope) should be created in the local domain and should be called something along the line of *TSUsers*. This new group should then be added to the terminal server's local Remote Desktop User's group. This enables support staff to simply add new users of the TS farm to one group at the domain level and grant them access to login to each of the servers in the farm. Thus all security controls and access can be granted from a central group that will then automatically manage who has the authority to login to the TS farm.

© SANS Institute 2004, Author retains full rights.

[6] This approach requires a Windows domain of some sort, NT or Active Directory, in order to centrally manage this list of users. Without a Windows domain present users will be required to login locally to each machine in the farm and user accounts will have to synchronized manually between machines.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Application Installation & Configuration

Configuring the Applications

Once the terminal server hardware and then the core operating system has been installed and configured, the facility administrator must install various third party applications to secure and customize the server. These applications will be used to secure the server further and allow the administrator to more easily manage the server. First the administrator should install the following applications on the TS server:

1. HP Hardware Support Pack (includes all required HP drivers)
2. Check for latest bios version and install latest HP/Compaq bios version
3. Network Associates (McAfee) NetShield Anti-Virus
4. Compaq Insight Agents
5. Support Tools – located in the deploy.cab file on the support directory on the Windows 2003 Server CD. This includes tools such as setup manager and sysprep.
6. Windows Server 2003 Adminpak
7. Windows Server 2003 Recovery Console
8. Veritas Backup Exec Remote Agent

When installing these applications the administrator must remember that special care must be exercised before installing new applications on a terminal server. There are two primary ways of prepping a terminal server before installing new applications. The best practice for this process is to:

1. Connect to the console of the terminal server (either remotely or at the physical console, more information is provided on how to do this later in this paper. Although some applications do have trouble still when they are installed via the remote console).
2. Place the server into installation mode by entering the following command into a command window – `change user /install`
3. Open the Control Panel – Add/Remove Programs and choose to install a new application through this window.
4. Close the Add/Remove Programs dialog windows that open after the installation process is complete. Reboot the server if necessary.

Once the above core applications have been installed on the terminal server, the administrator must determine the specific business purpose of the TS farm. During this process a list of all applications should be compiled and agreed upon by each of the facility administrators. Applications such as this should not be installed without proper testing and verification to see if the application functions properly on a terminal server or without verification that it is proper to install this application on the server. Some of the applications that administrators may consider installing are:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. MS Office XP Professional [7]
2. Rumba or other terminal emulation software
3. Adobe Acrobat Reader
4. Other Applications as Required by the Local Facility

It should be remembered that applications must be installed on each of the servers in the TS farm. Since users may connect to any of the servers in the farm on a given day, ACME must ensure consistency on each of the servers in the farm. Therefore an application should either be installed on all of the servers in the farm, or none of them at all. Strict change control procedures should be followed when modifying TS farm software or when installing new applications. Where possible Group Policies or Systems Management Server (SMS) 2003 should be used to install software to these servers once Active Directory services is available.

Also it should be remembered that when installing an application on a Windows Server 2003 terminal server the application needs to be installed either through Control Panel-Add/Remove Programs or by issuing the "change user /install" command and then running the setup program for the application. Both of these methods will ensure that the application is properly installed and configured for a mulit-user, terminal services environment.

Profile Account Customizations

Once all of the applications have been installed and configured as the local system administrator, they will then need to be configured for use by the default user of the server. In order to do this the administrator will need to login as the local user, "Profile," created earlier in this process, with the password specified for this account. In order to customize the default user profile the logged in user will then need to walk through the following steps in order to customize the default user's environment:

1. Configure Taskbar – Right Click Taskbar-Properties-Taskbar Tab
2. Clear Show Quick Launch
3. Check Show Clock
4. Start Menu Tab
5. Classic Start menu | Customize
6. Remove | Delete Remote Assistance icon and Outlook Express
7. Remove accessories folder
8. Select Clear button to clear recently accessed documents
9. Remove My Computer icon from Desktop
10. Sort Icons in Start bar - Start | Programs – right click on Application pane and select Sort by Name
11. Hide Volume icon in taskbar
12. Empty Recycle Bin

[7] Although Microsoft Office 2003 is available at the time of this writing, and Office 2003 has been reported as having enhancements specifically for terminal services, ACME's current licensing model supports only up to Microsoft Office XP, and is thus used on the terminal servers in this farm.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

13. Logoff Profile Account

Once all of the above configuration steps are complete, the administrator needs to log off as the local user “Profile” and re-login with the local system administrator account. Once logged in as the local administrator again, the user needs to copy the contents of the “c:\Documents and Settings\Profile” directory into the hidden “c:\Documents and Settings\Default User” directory. This will overwrite the profile settings for each new user that logs onto the server, and thus reduce the administrative time it will take to configure each new user’s profile that logs onto the system. Note, this will not eliminate the need for new user profiles to be configured the first time they log into the TS farm, but it will cut down on the time it takes to perform the tasks common to customizing each user profile.

Finally, once the default user profile has been customized the local account, “Profile” should be removed from the system. By leaving this account active on the system the administrator leaves the door open for one more point of entry through a generic system account. Typically accounts such as this are poorly maintained, and since it will be on each server in the TS farm that’s created, this can open a sizable security risk to the organization. Thus the administrator must make sure this account is removed before moving on to the next phase in the system’s configuration.

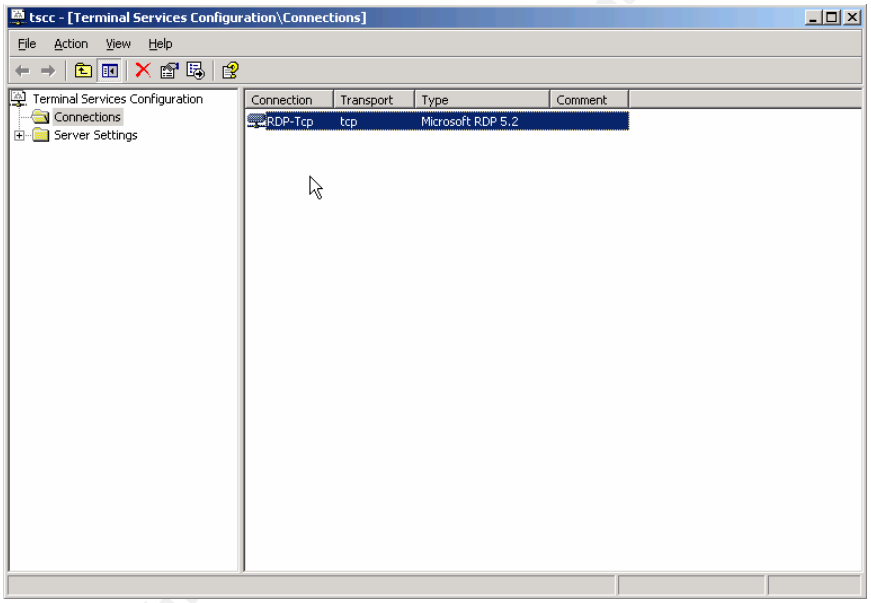
© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Terminal Services Configuration

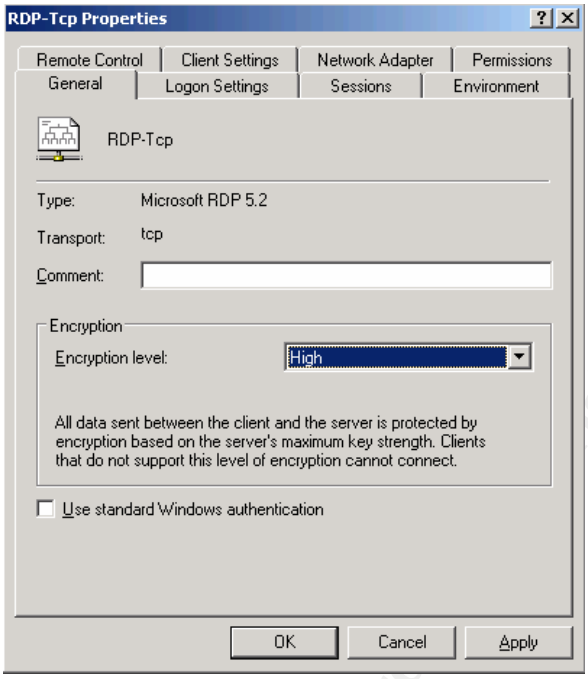
As a part of the core operating system configuration, described earlier, Microsoft terminal services has already been installed on the server being configured. As the next step in this process, the RDP settings for this server must be configured appropriately. In order to accomplish this, the administrator should open the Terminal Services Configuration on the server (located at Start-Programs-Administrative Tools-Terminal Services Configuration) and configure the settings to match the descriptions that follow.

1. The first Windows that is displayed shows the various options for terminal services, specifically the protocols installed and listening for available connections. This Windows specifically shows the default remote desktop protocol (RDP) 5.2 that's created by default during installation.

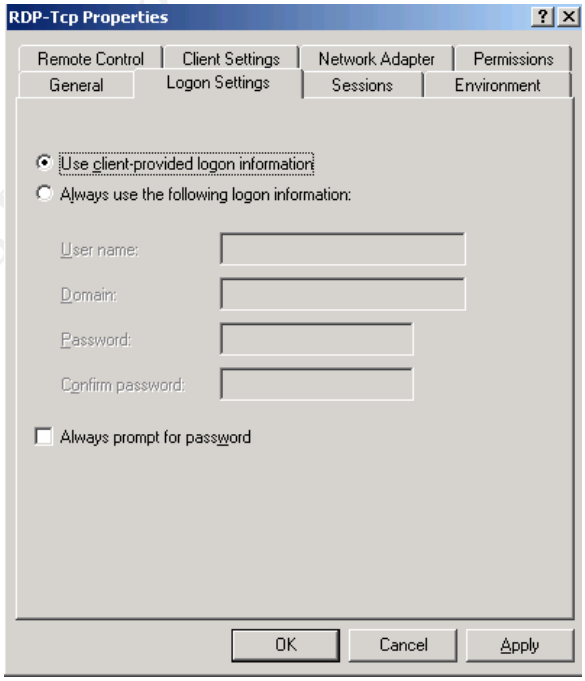


2. The General tab most importantly allows you to set the encryption level that will be used on the server. While there are four choices give for Windows Server 2003, since the clients who will be connecting to the farm will be capable of supporting the RDP 5.2 protocol, this setting will be set to use High Encryption. Should a facility need to allow down-level clients to connect to the TS farm, that don't support RDP 5.2, this setting should be lowered.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

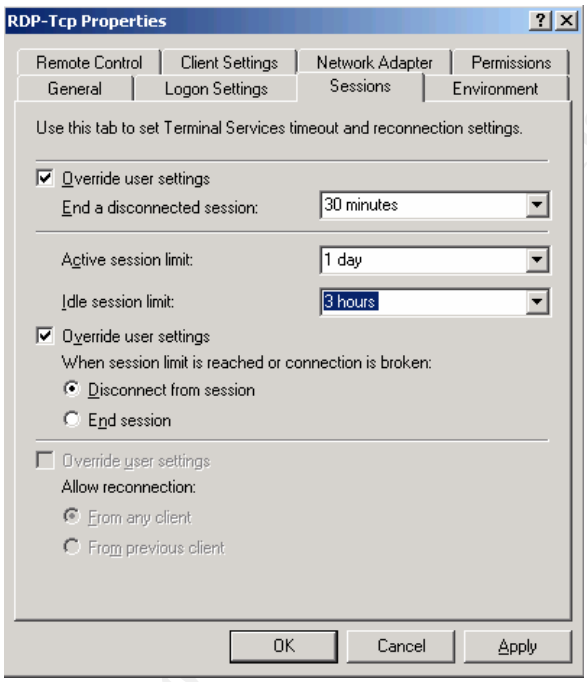


3. The “Logon Settings” tab allows the administrator to set default user credentials that will be used by anyone connecting to the TS servers, thus bypassing the need for authentication to the server. This should not be enabled, and the settings should be as noted below with the option to “use client-provided logon information” which will require the user to enter their own authentication information in order to connect. No servers in the TS farm should allow users to connect without providing valid credentials to the system.



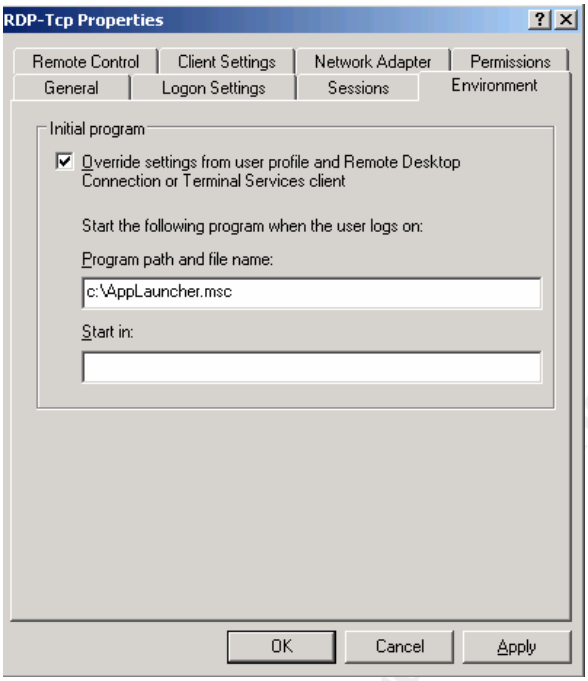
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4. The next tab, the “Sessions” tab, indicates the settings specific to the duration of sessions on the server and how to respond in the event of idle or disconnected sessions. The following settings are good best practices for these times; however they may be modified according to the needs of the facility. Again all of the servers within the farm must have the same settings for all of these connections. Also, the settings on the server should always override the settings from the client to better manage and secure these connections.

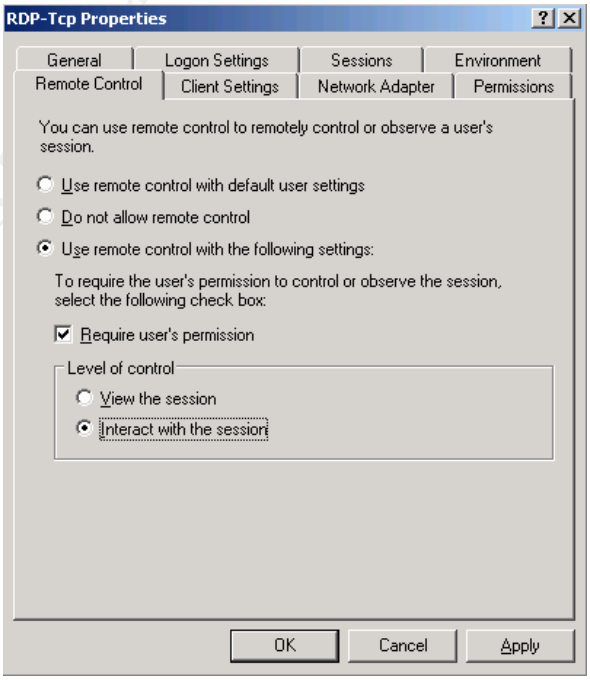


5. The “Environment” tab allows the administrator to specify an application to run once the connection to the TS farm is made. If the user closes this application, the entire terminal services connection is broken; the application is not simply closed. In this case a Microsoft Management Console, “applauncher.msc,” has been chosen to launch once a user connects to the farm. This MMC console is simply a collection of various applications that the user can initiate from this farm. This allows for a custom shell to be created which restricts the user’s environment to only the applications provided by the MMC console. More information on the specific use of this application will follow, but again note that the server settings should overwrite the client settings for the session.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

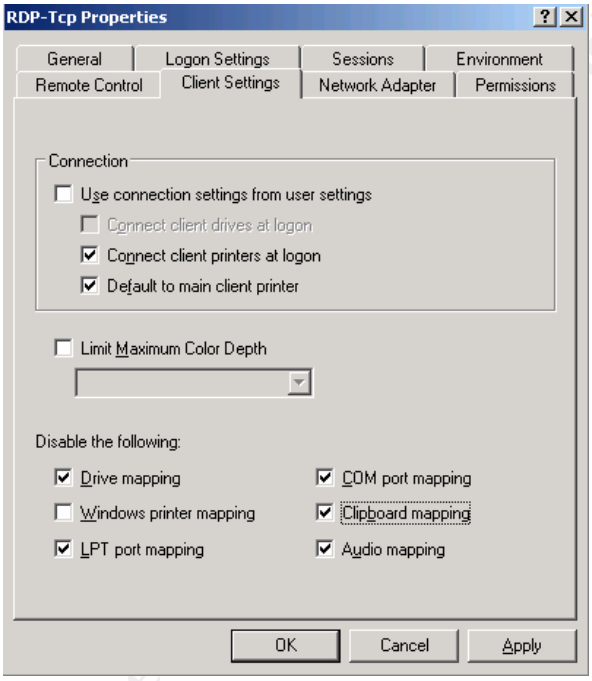


6. The “Remote Control” tab sets guidelines for whether or not an administrator can remote control a user’s session. This can be helpful when an administrator or the help desk needs to configure an application or troubleshoot a client problem. These settings should always be set to allow for remote control, but the setting for “Require user’s permission” must be checked. A system administrator should never control a user’s session without the explicit permission of that user. For support reasons the level of control should be set for “Interact with Session” to allow remote support staff to work with the user, not simply to view what actions they’re taking.



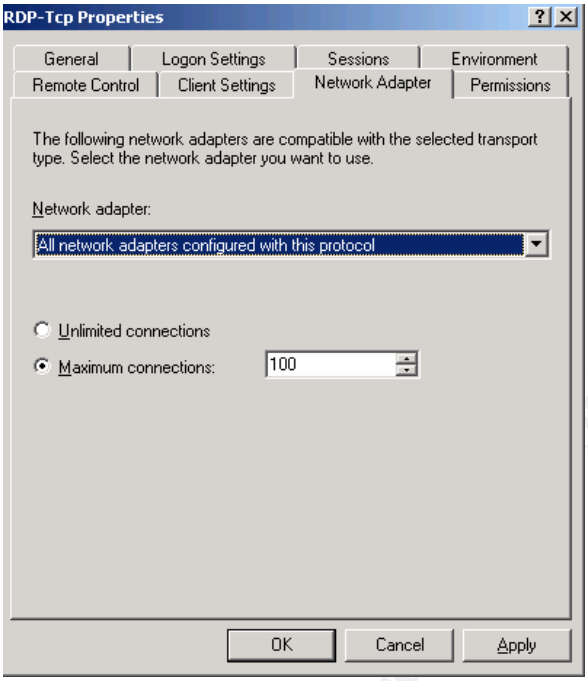
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

7. The next tab, the “Client Settings” tab is vital in defining what portions of the client’s desktop environment are transferred to the server. Users of ACME TS farms should be allowed to have their printers re-direct to the server, enabling them to print to whichever printer has been configured on their local workstation. However no other element of their local PC should be redirected. Drive mappings, LPT port mappings, COM port mappings, Clipboard mappings, and Audio mappings should all be disabled for security and bandwidth reasons. Again, the server’s settings should always override the client settings.

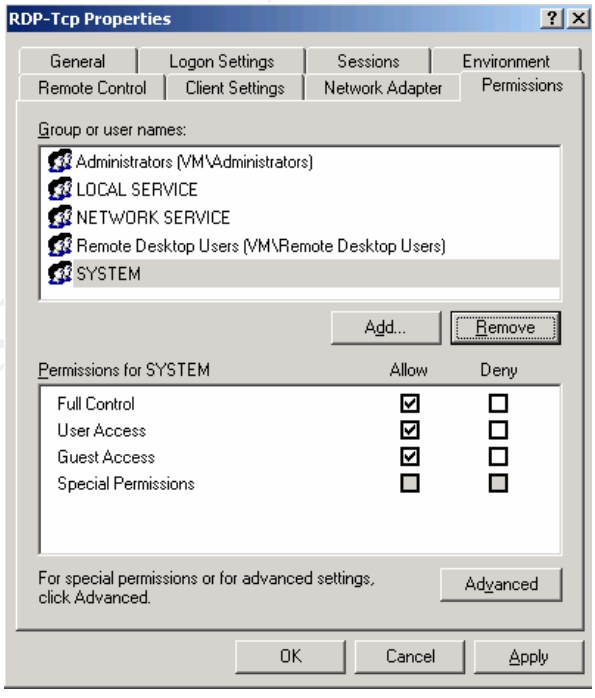


8. On the “Network Adapter” tab the administrator may select which network cards will listen for terminal services connections. In this scenario since many facilities have enabled adapter teaming and redundant LAN switches, the servers should listen on each of the NICs for incoming connections. It should also be noted that on this tab the number of allowed connections has been limited to 100, thus falling in line with performance numbers described earlier in this document. This will ensure that no more than 100 sessions are created at any given time on this server, thus protecting the first 100 sessions from additional connections which might slow the performance of the machine.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



9. Finally on the "Permissions" tab the administrator is able to customize which users or groups have Full control to the RDP protocol, user access, guest access, or any special permission. Due to the user and local group settings specified earlier, the default settings, as seen below, are sufficient.



After configuring these settings, the administrator can apply them and they will take effect immediately on the server. At this point the server itself has been fully configured for functionality and basic connectivity tests can be performed to ensure that the server

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

is responding as expected and that test users are able to perform basic tasks. However, before this machine can be syspreped and imaged onto other machines the server must be secured. The next section describes the steps necessary to harden and secure the server which will later be added to the TS farm.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Windows Server 2003 TS Farm Hardening Procedures

One of the most important aspects of configuring and setting up the servers in the TS farm is to secure and harden the system against possible compromise. There is always a delicate balance to walk between system functionality and system security. Microsoft traditionally has taken the approach of turning on system features, considering functionality more important than system security. With Windows Server 2003 Microsoft has begun to take the approach of "Secure by design, secure by default," thus locking down the system much more than ever before. Although Microsoft has taken more steps to secure Windows Server 2003 than other products in the past, there are still settings which should be altered to further secure the system. Securing these servers falls into four major categories:

1. Windows Updates / Automatic Updates
2. Local Security Policy Settings
3. Local Services Settings
4. Application Launcher MMC Console

Each of these sections should be addressed individually before imaging the server and distributing it to other machines. It should be stressed that these settings should only be applied to new servers being configured as a part of a TS farm. Applying these settings to production servers could easily break the functionality of the server.

Windows Updates / Automatic Updates

One of the key areas to securing this configuration is update and patch management. Specifically Windows service packs and hotfixes need to be kept up to date on each of the servers in the TS farm in order to protect the servers from malware that targets vulnerabilities in the operating system. The year 2003 has already illustrated the importance of keeping systems updates with service packs and hotfixes with worms such as MS Blaster and Nachi/Welchia running rampant infecting enterprises across the globe.

The first piece to updating the servers in the TS farm is to make sure that the original server image is up to date with all of the current service packs and hotfixes. At the time of this writing Microsoft has not released any service packs for Windows Server 2003 and don't plan to release one even into beta until 2004. However there are a fair number of hotfixes which must be updated on the server before it can go into production. The simplest way to accomplish this on the original server is to run Windows Update on the server immediately after installation. There are other options, such as deploying the patches through SMS, through software installation Group Policies, or even slipstreaming the hotfixes into the original installation media. However in this case the simplest method to update the original server is through Windows Update online.

Once the server has been initially updated a process needs to be put into place to keep the patch level current on the servers. For this there are many commercial tools

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

available, including Microsoft's Systems Management Server (SMS) 2003, GFI's LanGuard, Shavlik's HFNetChk Pro, and many others. For the sake of this configuration, Microsoft's free server service, Software Update Services (SUS) 1.0, will be used to manage all hotfix updates. While describing the exact configuration of this server is beyond the scope of this paper, there are many other documents and white papers available which describe this setup in detail.

Once the SUS server has been installed and configured, each of the servers in the TS farm, the data store, the session directory server, the licensing server, or any other server in the configuration, need to be configured to automatically get their updates from this server. In order to accomplish this either a template can be added to the group policy configuration to allow the administrator to specify which internal server to pull updates from, or a script can be run on the each of the servers which will modify a series of registry keys on the machines to point them to the internal server to get updates from. In order to add the template to configure these choices in Active Directory the "au.inf" administrative template should be added to the list of built-in administrative templates in the GPO. Also, a sample script which will configure this for each machine is included in Appendix B.

Local Security Policy Settings

One of the most important considerations when hardening the TS farm is to take advantage of the security settings provided through Group Policy. While most effective when used along side Microsoft's Active Directory services, these policies can also be used to secure individual computers. This tool allows the user to configure settings previously only configurable through directly editing the registry. Also, although many of these settings are available through Windows 2000 Group Policies, this configuration is based off of a Windows Server 2003 configuration, and many of these settings will not be found in the older version.

If the configuration of group policies is setup in an AD domain environment an Organization Unit (OU) should be created within the domain that is reserved only for the servers in the TS farm. Once the servers in the farm have been added to the AD domain, those computer accounts should be moved from the default "Computers" container, into the newly created OU for the TS farm. Once the servers are in their proper position within the domain structure a Group Policy Object (GPO) can be created and linked to this OU that will affect each of the servers in the OU consistently with the following settings. This is definitely the preferred method, as it allows for quick and consistent changes to be made to each of the servers in the farm. If the servers are not a part of an AD domain, then the following settings should be configured on a server by server basis through local security policy settings using the GPedit.msc policy editing tool.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Computer Configuration		
Windows Settings		
Location	**Default Setting**	**Secured Setting**
Security Settings – Local Policies - Audit Policy – Audit Account Logon Events	Success, Failure	Success, Failure
Security Settings – Local Policies - Audit Policy – Audit Logon Events	Success, Failure	Success, Failure
Security Settings – Local Policies – User Rights Assignments – Allow Logon Through Terminal Services	Administrators, Remote Desktop Users	Administrators, Remote Desktop Users, <Domain TS Group>
Security Settings – Local Policies – User Rights Assignments – Deny Logon Through Terminal Services	Blank	Administrator, <Domain Administrator>
Security Policies – Local Policies – Security Options – Accounts: Rename administrator account	Administrator	#LocalAdmin
Security Policies – Local Policies – Security Options – Devices: Restrict CD-ROM access to locally logged-on user only	Disabled	Enabled
Security Policies – Local Policies – Security Options – Devices: Restrict floppy access to locally logged-on user only	Disabled	Enabled
Security Policies – Local Policies – Security Options – Interactive logon: Do not display last user name	Enabled	Enabled
Security Policies – Local Policies – Security Options – Shutdown: Clear virtual memory pagefile	Disabled	Enabled
Administrative Templates		
Location	**Default Setting**	**Secured Setting**
Windows Components – Internet Information Services – Prevent IIS Installation	Not Configured	Enabled
Windows Components – Terminal Services – Client/server data redirection – Do not allow clipboard redirection	Not Configured	Enabled
Windows Components – Terminal Services – Client/server data redirection – Do not allow COM port redirection	Not Configured	Enabled
Windows Components – Terminal Services – Client/server data redirection – Do not allow drive redirection	Not Configured	Enabled
Windows Components – Terminal Services – Encryption and Security – Always prompt client for password upon connection	Not Configured	Enabled
Windows Components – Terminal Services – Encryption and Security – Set client connection encryption level	Not Configured	Enabled: High
Windows Components – Terminal Services – Temporary Folders – Do not delete temp folder upon exit	Not Configured	Disabled
Windows Components – Terminal Services – Session	Not Configured	Enabled

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Directory – Join Session Directory		
Windows Components – Terminal Services – Session Directory – Session Directory Server	Not Configured	Enabled: <Server Name>
Windows Components – Terminal Services – Restrict Terminal Services users to a single remote session	Not Configured	Enabled
Windows Components – Terminal Services – Remove Disconnect option from Shut Down dialog box	Not Configured	Enabled
Windows Components – Terminal Services – Set rules for remote control of Terminal Services user sessions	Not Configured	Enabled: Full control with user's permission
Windows Components – Windows Installer – Disable Windows Installer	Not Configured	Enabled: Always
Windows Components – Windows Update – Configure Automatic Updates	Not Configured	Enabled: Auto download and schedule the install, Every Day, 01:00
Windows Components – Windows Update – Specify intranet Microsoft update service location	Not Configured	Enabled: <server name>
Windows Components – Windows Update – Reschedule Automatic Updates scheduled installations	Not Configured	Enabled: 10 min.
Windows Components – Windows Update – No auto-restart for scheduled Automatic Updates installations	Not Configured	Enabled
System – Group Policy – User Group Policy loopback processing mode	Not Configured	Enabled
System – Do not display Manage Your Server page at logon	Not Configured	Enabled

© SANS Institute 2004, Author retains full rights.

User Configuration		
Administrative Templates		
Location	**Default Setting**	**Secured Setting**
Windows Components – Internet Explorer – Disable Find Files via F3 within the browser	Not Configured	Enabled
Windows Components – Internet Explorer – Do not allow AutoComplete to save passwords	Not Configured	Enabled
Windows Components – Internet Explorer – Browser Menus – Disable Context menu	Not Configured	Enabled
Windows Components – Application Compatibility – Prevent access to 16-bit applications	Not Configured	Enabled
Windows Components – Windows Explorer – Remove the Folder Options menu item from the Tools menu	Not Configured	Enabled
Windows Components – Windows Explorer – Remove File menu from Windows Explorer	Not Configured	Enabled
Windows Components – Windows Explorer – Remove Search button from Windows Explorer	Not Configured	Enabled
Windows Components – Windows Explorer – Remove Security Tab	Not Configured	Enabled
Windows Components – Windows Explorer – Remove Windows Explorer's default context menu	Not Configured	Enabled
Windows Components – Windows Explorer – Hides the Manage item on the Windows Explorer shortcut menu	Not Configured	Enabled
Windows Components – Windows Explorer – Hide these specified drives in My Computer	Not Configured	Enabled – Restrict A, B, C, and D drives only
Windows Components – Windows Explorer – Prevent access to drives from My Computer	Not Configured	Enabled – A, B, C, and D drives only
Windows Components – Windows Explorer – Remove Hardware tab	Not Configured	Enabled
Windows Components – Windows Explorer – Remove Order Prints from Picture Tasks	Not Configured	Enabled
Windows Components – Windows Explorer – Remove Publish to Web from File and Folders Tasks	Not Configured	Enabled
Windows Components – Windows Explorer – No "Computers Near Me" in My Network Places	Not Configured	Enabled
Windows Components – Windows Explorer – Turn off Windows + X hotkeys	Not Configured	Enabled
Windows Components – Windows Explorer – Turn on Classic Shell	Not Configured	Enabled
Windows Components – Windows Explorer – Common Open File Dialog – Hide the common dialog places bar	Not Configured	Enabled
Windows Components – Task Scheduler – Hide Property Pages	Not Configured	Enabled
Windows Components – Task Scheduler – Prohibit Task Deletion	Not Configured	Enabled
Windows Components – Task Scheduler – Prevent Task Run or End	Not Configured	Enabled
Windows Components – Task Scheduler – Prohibit New	Not Configured	Enabled

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Task Creation		
Windows Components – Windows Messenger – Do not allow Windows Messenger to be run	Not Configured	Enabled
Start Menu & Taskbar – Remove links and access to Windows Update	Not Configured	Enabled
Start Menu & Taskbar – Remove programs on Settings menu	Not Configured	Enabled
Start Menu & Taskbar – Remove Network Connections from Start Menu	Not Configured	Enabled
Start Menu & Taskbar – Remove the Search Menu from Start Menu	Not Configured	Enabled
Start Menu & Taskbar – Remove Drag-and-Drop shortcut menus on Start Menu	Not Configured	Enabled
Start Menu & Taskbar – Remove Favorites menu from Start Menu	Not Configured	Enabled
Start Menu & Taskbar – Remove Help menu from Start Menu	Not Configured	Enabled
Start Menu & Taskbar – Remove Run from Start Menu	Not Configured	Enabled
Start Menu & Taskbar – Remove My Network Place icon from Start Menu	Not Configured	Enabled
Start Menu & Taskbar – Add Logoff to Start Menu	Not Configured	Enabled
Start Menu & Taskbar – Remove and prevent access to Shut Down command	Not Configured	Enabled
Start Menu & Taskbar – Prevent changes to Taskbar and Start Menu settings	Not Configured	Enabled
Start Menu & Taskbar – Remove access to the shortcut menus for the taskbar	Not Configured	Enabled
Start Menu & Taskbar – Force Classic Start Menu	Not Configured	Enabled
Desktop – Remove Properties from My Documents shortcut menu	Not Configured	Enabled
Desktop – Remove Properties from My Computer shortcut menu	Not Configured	Enabled
Desktop – Remove Properties from Recycle Bin shortcut menu	Not Configured	Enabled
Desktop – Prohibit user from changing My Documents path	Not Configured	Enabled
Desktop – Remove My Documents icon from the Desktop	Not Configured	Enabled
Desktop – Don't save settings at exit	Not Configured	Enabled
Control Panel – Prohibit access to the Control Panel	Not Configured	Enabled
Control Panel – Display – Hide Desktop tab	Not Configured	Enabled
Control Panel – Display – Hide Appearance and Themes tab	Not Configured	Enabled
Control Panel – Display – Hide Settings tab	Not Configured	Enabled
Control Panel – Display – Hide Screen Saver tab	Not Configured	Enabled

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Control Panel – Display – Password protect the screen saved	Not Configured	Enabled
Control Panel – Display – Screen Saver timeout	Not Configured	Enabled; 900 seconds
Control Panel – Display – Themes – Remove theme option	Not Configured	Enabled
Add or Remove Programs – Remove Add or Remove Programs	Not Configured	Enabled
System – Prevent access to the command prompt	Not Configured	Enabled
System – Prevent access to registry editing tools	Not Configured	Enabled
System – Run only allowed Windows applications	Not Configured	Enabled – Define allowable applications here (although this could also be done with AppSec.exe)
System – CTRL+ALT+DEL Options – Remove Task Manager	Not Configured	Enabled
System – CTRL+ALT+DEL Options – Remove Lock Computer	Not Configured	Enable
System – Scripts – Run legacy logon scripts hidden	Not Configured	Enabled

There are many other security policies which should be configured in order to secure the enterprise's overall domain. Settings such as password policies, IPSEC policies, and others have not been specifically addressed here, but should be enabled at the ADS domain level in order to provide additional security. The settings described here are focused on those settings which should be configured for the servers in the TS farm, not the domain as a whole. Again, these settings should never be applied to production servers without first testing them thoroughly in a test environment, as these settings may stop production systems from functioning properly.

Local Services Settings

Automatic update settings and local security policy settings are two ways to help lockdown the servers in a TS farm. Another method for securing these servers is to ensure that only appropriate services are installed and allowed to run on the server. The following table lists the built-in Windows Server 2003 services which are installed in the configuration described earlier in this assignment. Along with the name of the service, the default and the secure settings are listed. Disabled services should not just be stopped, but disabled from running at startup. Again it should be remembered that this configuration should only be applied to systems as described in this document or after thorough testing has been performed. These settings should not be applied to production systems, terminal services or otherwise, without thoroughly testing these settings first.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Service Name	Default Setting	Secured Setting
Alerter	Disabled	Disabled
Application Layer Gateway Service	Manual	Manual
Application Management	Manual	Manual
Automatic Updates	Automatic	Automatic
Background Intelligent Transfer Service	Manual	Manual
Clipbook	Disabled	Disabled
COM+ Event System	Manual	Manual
COM+ System Application	Manual	Manual
Computer Browser	Automatic	Automatic
Cryptographic Services	Automatic	Automatic
DHCP Client	Automatic	Disabled
Distributed File System	Automatic	Disabled
Distributed Link Tracking Client	Manual	Disabled
Distributed Link Tracking Server	Disabled	Disabled
Distributed Transaction Coordinator	Automatic	Automatic
DNS Client	Automatic	Automatic
DNS Server	Automatic	Disabled
Error Reporting Service	Automatic	Automatic
Event Log	Automatic	Automatic
File Replication Service	Automatic	Automatic
Help and Support	Automatic	Disabled
HTTP SSL	Manual	Disabled
Human Interface Device Access	Disabled	Disabled
IIS Admin Service	Automatic	Disabled
IMAPI CD-Burning COM Service	Disabled	Disabled
Indexing Service	Disabled	Disabled
Internet Connection Firewall / Internet Connection Sharing	Disabled	Disabled
Intersite Messaging	Automatic	Automatic
IPSEC Services	Automatic	Automatic
Kerberos Key Distribution Center	Automatic	Disabled
License Logging	Disabled	Disabled
Logical Disk Manager	Automatic	Automatic
Logical Disk Manager Administrative Service	Manual	Manual
Messenger	Disabled	Disabled
Microsoft Software Shadow Copy Provider	Manual	Disabled
Net Logon	Automatic	Automatic
NetMeeting Remote Desktop Sharing	Disabled	Disabled
Network Connections	Manual	Manual
Network DDE	Disabled	Disabled
Network DDE DSDM	Disabled	Disabled
Network Location Awareness (NLA)	Manual	Manual
NT LM Security Support Provider	Manual	Manual
Performance Logs and Alerts	Manual	Manual
Plug and Play	Automatic	Disabled (after installation)
Portable Media Serial Number	Manual	Disabled

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Service		
Print Spooler	Automatic	Automatic
Protected Storage	Automatic	Automatic
Remote Access Auto Connection Manager	Manual	Manual
Remote Access Connection Manager	Manual	Manual
Remote Desktop Help Session Manager	Manual	Manual
Remote Procedure Call (RPC)	Automatic	Automatic
Remote Procedure Call (RPC) Locator	Manual	Manual
Remote Registry	Automatic	Disabled
Removable Storage	Manual	Disabled
Resultant Set of Policy Provider	Manual	Manual
Routing and Remote Access	Disabled	Disabled
Secondary Logon	Automatic	Automatic
Security Accounts Manager	Automatic	Automatic
Server	Automatic	Automatic
Shell Hardware Detection	Automatic	Automatic
Smart Card	Manual	Manual
Special Administration Console Helper	Manual	Manual
System Event Notification	Automatic	Automatic
Task Scheduler	Automatic	Automatic
TCP/IP NetBIOS Helper	Automatic	Automatic
Telephony	Manual	Disabled
Telnet	Disabled	Disabled
Terminal Services	Manual	Manual
Terminal Services Session Directory	Disabled	Disabled
Themes	Disabled	Disabled
Uninterruptible Power Supply	Manual	Disabled
Upload Manager	Manual	Manual
Volume Shadow Service	Manual	Disabled
WebClient	Disabled	Disabled
Windows Audio	Automatic	Disabled
Windows Image Acquisition (WIA)	Disabled	Disabled
Windows Installer	Manual	Manual
Windows Management Instrumentation	Automatic	Automatic
Windows Management Instrumentation Drive Extensions	Manual	Manual
Windows Time	Automatic	Automatic
WinHTTP Web Proxy Auto-Discovery Service	Manual	Disabled
Wireless Configuration	Automatic	Disabled
WMI Performance Adapter	Manual	Manual
Workstation	Automatic	Automatic
World Wide Web Publishing Service	Automatic	Disabled

While these service settings can be applied through manually editing the services' startup properties, it's better to configure these settings either through the local security policy of the server or through group policies if Active Directory is available. However,

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

since at this point Active Directory Services has not been deployed throughout ACME, local security policies should be applied. Through configuring these settings there they will be automatically re-applied each time the system restarts. Should an administrator change on of these settings, this policy will be refreshed and the administrator's changes will be reversed thus raising the system's level of security.

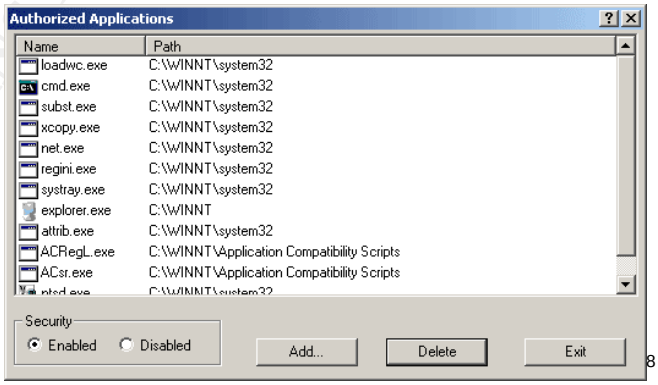
Limited Application Access

Another option for securing the server is to limit the applications that logged on users has access to. When legitimate users have too many rights on the system to execute applications, there is always the chance that one of those users will abuse those rights to cause damage to the environment. A user could use legitimate access rights to legitimate applications to violate the confidentiality, integrity, or availability of this or another system. One of the ways to protect the TS farm is to limit the applications that users have access to once their logged onto system.

One of the most effective ways to lock down which applications are accessible to a user is through the AppSec utility. Located on the Windows Server 2000 Resource Kit, the system administrator can install the "instappsec.exe" program which will install the "appsec.exe" utility along with the appropriate DLLs. Once installed the administrator has but to run this program and choose which applications regular users should have access to once they log onto the system.

There are only two contexts this program functions under, administrative and user. If someone with administrator credentials logs onto the system, that user will have full rights to execute any application on the system. However if a user without administrator access logs onto the system, that user will only have rights to the applications specified through the AppSec utility. Unfortunately there are no ranges of access with this tool or exceptions. The user is either an administrator or not, and thus either has rights to all applications on the server, or only those specified by the administrator.

The following screen capture shows an example of a configuration using the AppSec utility:



[8]

[8] Screenshot has been taken from a TechRepublic review of the AppSec utility at http://techrepublic.com.com/5100-6268-1054829.html.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Another comparable option that exists in Windows Server 2003 is Software Restriction Policies. This group policy setting allows an administrator to define which applications may not be run from the server. This can be used to define which applications are restricted from running on the server. One of the nice features of running these restrictions through Group Policies is that it can be applied at the local server level, or at a higher level within Active Directory to affect whole sets of workstations or servers, depending on the needs of the administrator. These policies can be configured by entering the appropriate level of group policy, and accessing Computer Configuration – Windows Settings – Security Settings – Software Restriction Policies.

Whichever of these methods are considered for locking down the server, the administrator must perform very thorough testing before applying them to the server. These policies perform very literal restrictions on the applications chosen and could easily break other applications if it is not configured properly. These settings should never be applied to a production system without being tested first.

Finally, either of these settings should be configured along with other group policies, at the local or AD level, which will restrict a user's ability to even see the applications that are restricted. Some methods of doing this are to remove Start Menu icons, disable desktop icons, and restrict the Run and CMD commands, basically turning the server into a kiosk.

This can also be done by creating a custom MMC console which provides the user a list of icons which represent the applications available to the user. This is similar to the way Novell's ZenWorks provides a Daily Work Group or Network Application Launcher (NAL) interface for users to run their most common programs. If the MMC console is chosen, this application should be launched via the RDP settings on the server and become the only application available through the server. It can become the gateway for which applications the user can access. However, if this method is chosen it will affect all users not connecting directly to the console of the terminal server.

At this point the server is ready to be syspreped and imaged with a tool such as Altiris or Symantec's Ghost and then distributed to the various members of the TS farm. Each of the initial member servers in the TS farm should be configured with all of the previously noted configuration options before moving to the next section. Once sysprep has been run, the image distributed, and the servers rebooted and given custom IP addresses, names, etc, the administrator may begin the next phase of actually configuring the farm using NLB and the TSSD service.

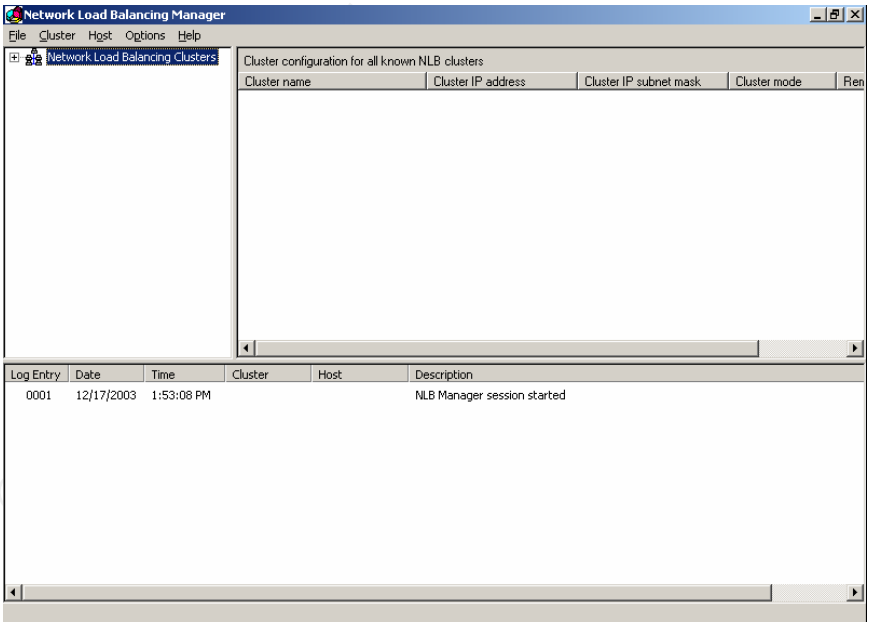
© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Network Load Balancing Installation & Configuration

Beyond simply ensuring the TS farm's confidentiality and integrity, one of the key components to securing the system is to ensure the farm's availability. One of the best ways to accomplish this availability is through the transparent redundancy provided by redundant hardware, configured with Microsoft's Network Load Balancing (NLB). NLB allows one virtual IP address to serve as the contact point for an entire farm of servers, in this case terminal servers. The users of the TS farm will all use one address to connect to the farm; however that address will direct them to another IP address of another server in the farm, based on a metric of the server's availability. This ensures that sessions are not only load balanced across a series of servers, but that should one of the servers fail, the users should not notice any downtime. While NLB has been available since the release of Windows 2000 Advanced Server, it really hasn't been a popular option for production use until its release with Windows Server 2003 (in both standard and enterprise editions).

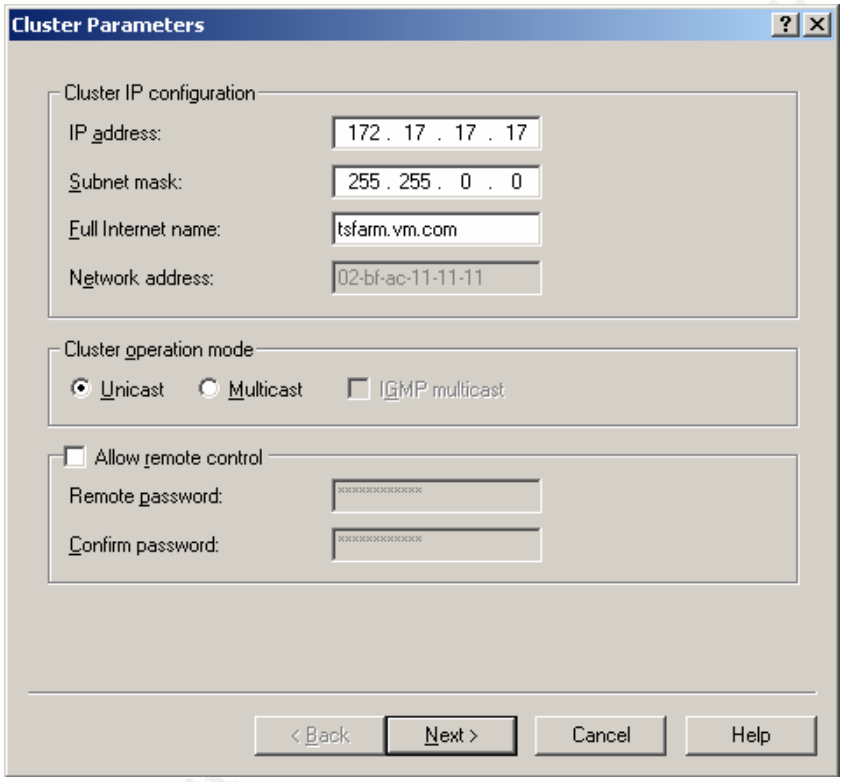
In order to run and configure NLB an administrator must run the Nlbmgr.exe configuration tool. This tool allows the administrator to create and configure NLB clusters. Again it must be remembered that servers configured with NLB are referenced as clusters, although they do not perform as a true hardware cluster, and only perform load balancing functions. To initiate the tool, simply run it from the Run menu, and the following initial screen will appear:



Once the tool is opened, the only process required is to right-click on the node for "Network Load Balanced Cluster" in the left-hand windows and choose "New Cluster" to open the Cluster Manager wizard. The first screen, shown below, prompts the administrator to choose an IP address for the virtual cluster and a name for the cluster. This should not be the IP address of one of the servers that will be a part of the TS

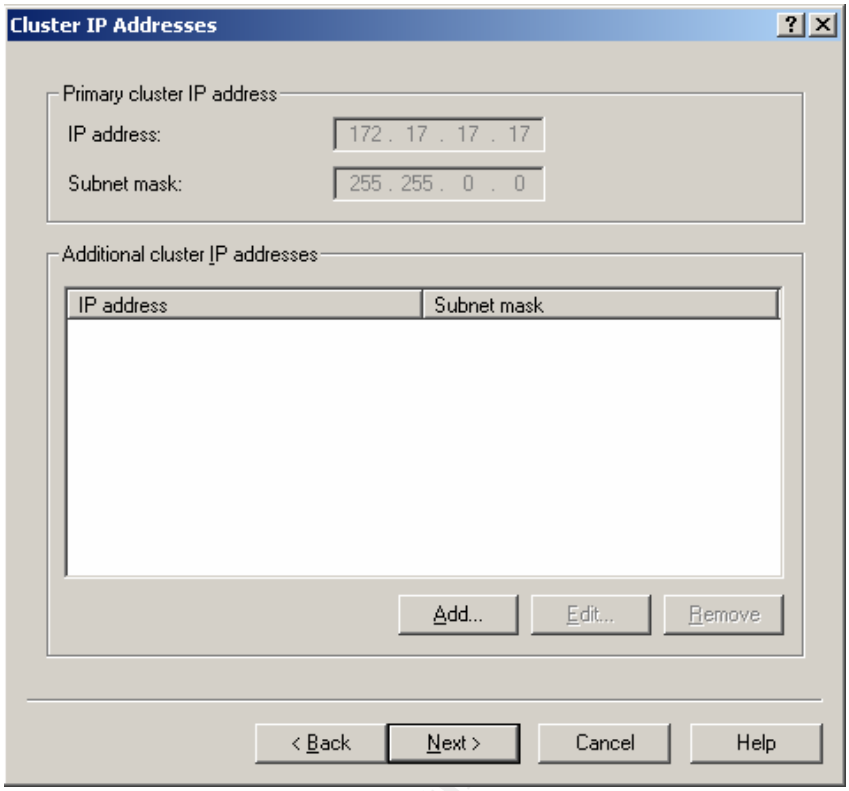
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

farm, but rather the IP of the "Virtual Cluster" that clients will use to connect to the farm. Also the administrator must choose here whether the operational mode of the cluster will be in unicast or multicast mode. Unicast mode restricts administration of the cluster to only the machine where the cluster is initially configured, while multicast mode allows the cluster to be administered from any server configured in the cluster. ACME network administrators will need to determine which mode is used based on the performance of their network infrastructure. While multicast mode is definitely the preferred choice, some LANs may not support the multicast traffic.



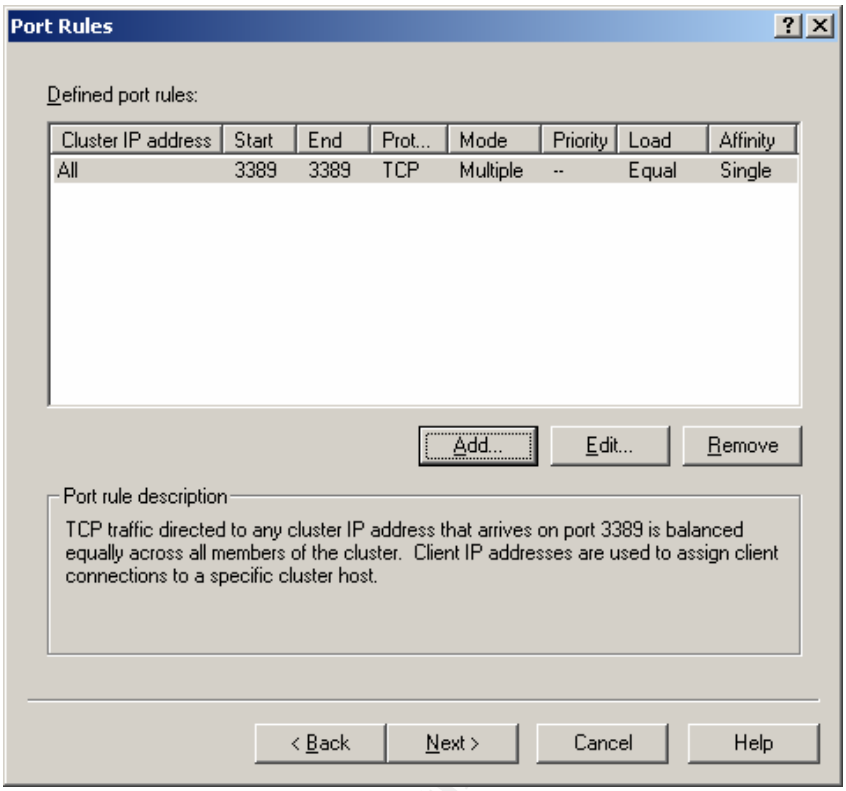
Once the initial IP has been assigned to the cluster the administrator has the option of assigning additional IP addresses to the cluster. This is an optional step, and has not been configured in this example (see below for the screen capture).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



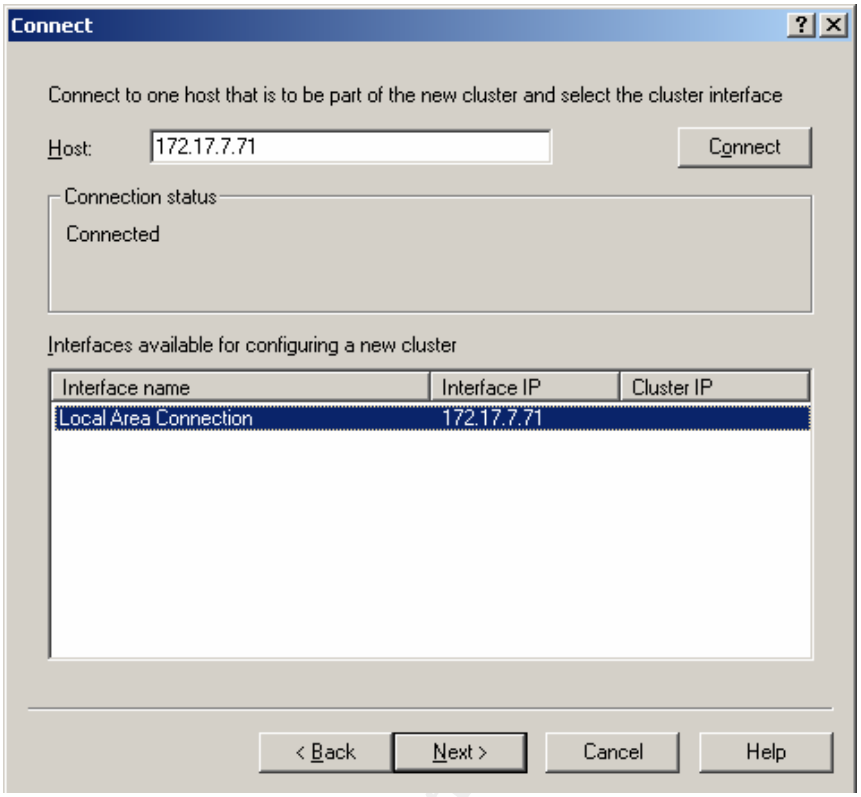
Once the IP addresses for the virtual cluster have been assigned the administrator has the option of assigning which ports will be load balanced as a part of this cluster. By default all IP ports, both TCP and UDP, are load balanced across the cluster. However since this cluster will only be used to load balance terminal services, only port 3389 TCP will be configured for this environment. Therefore the administrator should remove the initial port settings (clicking on the Remove button), and then add a new rule to only include TCP port 3389 (through the Add button).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

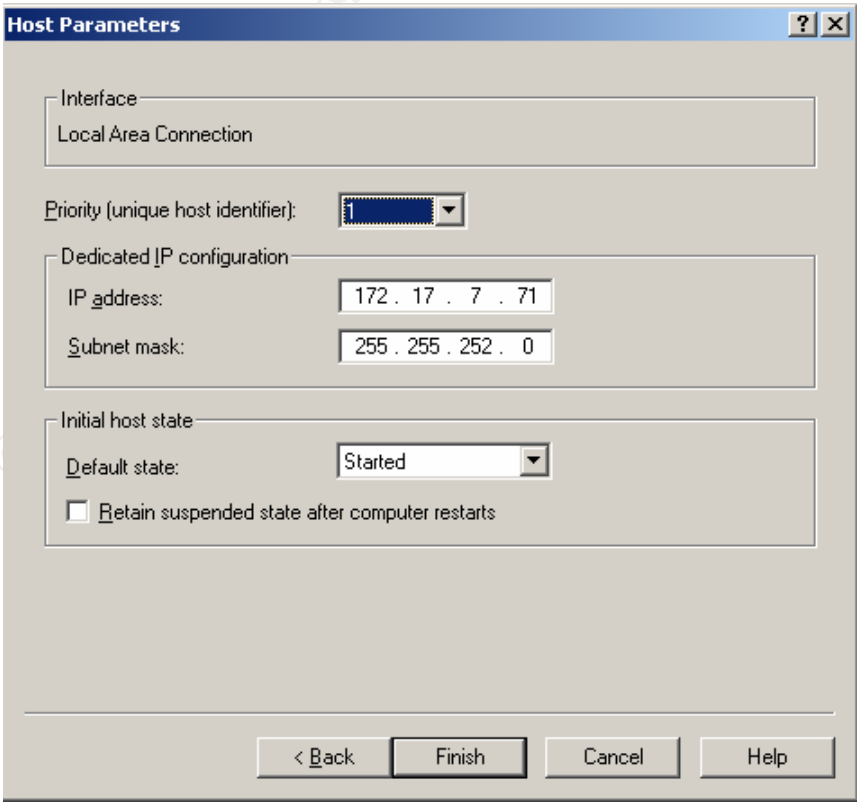


Once the IP and port assignments have been completed, the administrator is prompted to add servers to the TS farm. This is where the IPs of the already installed terminal servers should be added to the farm. Before this step can be accomplished the TS servers should be installed and configured, accessible from the server where NLB is being configured, and each server should be configured with a static address (the wizard will fail if the server has been assigned an address through DHCP). The server must be accessible for this process to complete and the server to be added to the virtual cluster. Once the IP for the server has been added, the server connection is verified, and then added to the list of servers in the TS farm (see below).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

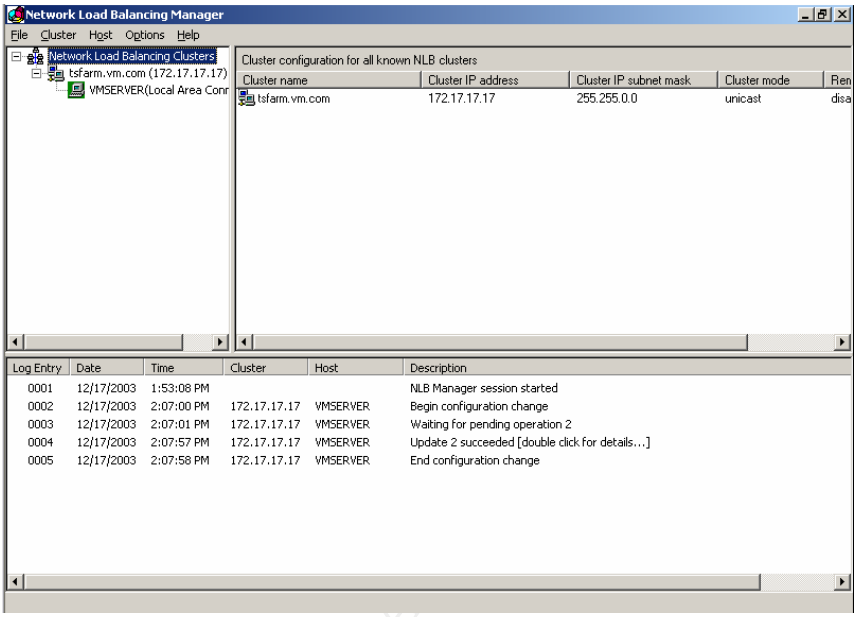


The final screen in the wizard (shown below), then prompts the administrator to confirm the configuration for the hosts added to the TS farm.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Once the virtual cluster configuration wizard completes, the new virtual cluster will appear in the Network Load Balancing Manger, as seen below. Also, each of the servers in the farm will appear beneath the virtual cluster name for future reference and monitoring purposes. Once each of the servers has been added to the NLB virtual cluster, the final step in configuring the TS farm is to setup the session directory.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

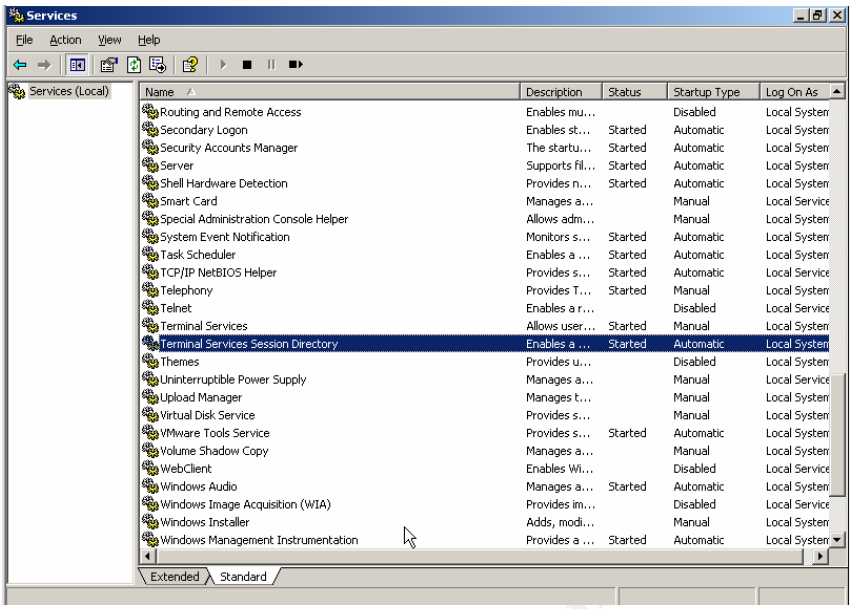
Session Directory Installation & Configuration

Once the TS farm has been configured for NLB, the next step in creating a fault tolerance set of servers is to configure the Terminal Services Session Directory (TSSD) service. The TSSD service is new to Windows Server 2003 and allows the administrator of a TS farm to configure servers into a fault-tolerant cluster without losing the capability to manage user sessions. The inherent problem with creating a NLB server farm with terminal services is that there's no guarantee that once a user disconnects from one server in the farm that he or she will be able to reconnect to the same session on the same server. In fact the odds are the bigger the farm, the less chance that a user will be able to reconnect to a session once it's been disconnected. That's where TSSD comes into play.

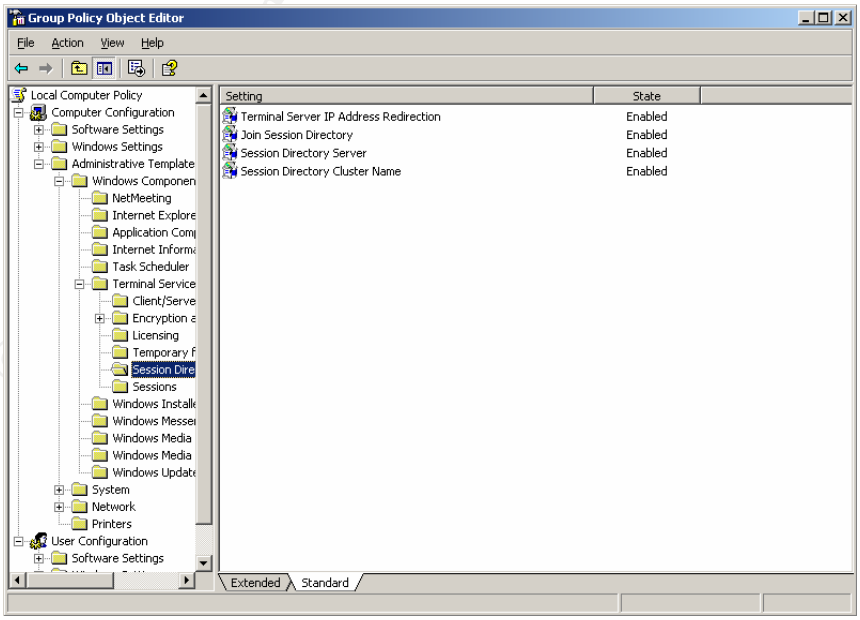
TSSD keeps track of each user connected to one of the servers in the TS farm. Each time a user connects to a server in the TS farm, TSSD records the user's name and the server that the session's been established with in a JET database located on the TSSD server. Once that user logs off of the farm, the TSSD server records that user's session as being cleanly ended. However, if the user is disconnected from the server unexpectedly, then the TSSD service keeps track of that user's name and which server the TS session had originally been established with. In this way when the user attempts to reconnect to the TS farm to reconnect to his or her original session, the user can reconnect to the same session, which is stored locally on that server. Thus the user is able to pick up his or her work from where he or she was before the session was disconnected.

In order to setup the session directory service, Windows Server 2003 Enterprise Edition must be installed on each of the TS servers attempting to be a part of the TSSD farm. This requires that the OS be installed cleanly on the server, as Windows Server 2003 standard edition cannot be upgraded to the enterprise edition. First the service must be installed on the server that will be hosting the TSSD service. By default the service is pre-installed on each Windows Server 2003 machine, although it is disabled. In order to initialize the service the administrator must simple set the startup type for the service to "Automatic" and then start the service (see screen capture below). From then on the service will accept connections from the TS farm and start whenever the server is rebooted.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

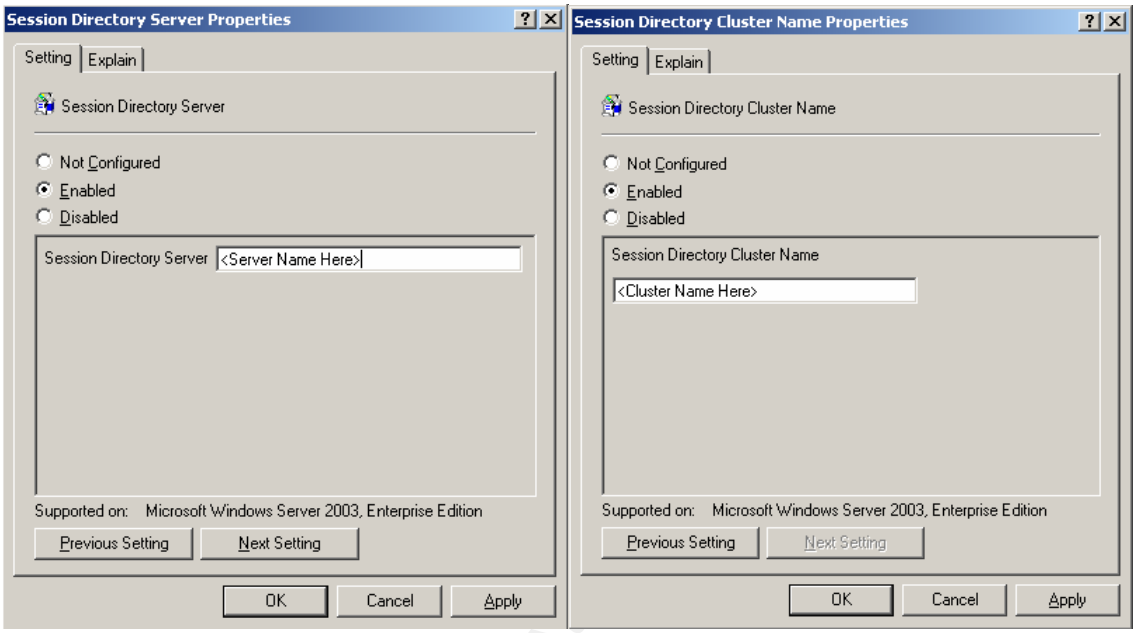


Once the service has been configured on the TSSD server, the server side of the installation is complete. Next each of the TS servers in the farm needs to be configured to join the session directory farm. This is accomplished through the use of group policies at either the local system level (if the server is not a part on an AD domain) or at the OU level (if the server is a part of an AD domain). Microsoft always recommends that this configuration be completed at an OU level whenever possible for ease and consistency of management. There are four settings in the GPO which must be set in order to join the TS server to the TSSD service, all of which must be set to “Enabled.” These are located under Computer Configuration – Administrative Templates – Terminal Services – Session Directory (see the following screen capture for details).



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Not only must all of the settings be set to “Enabled,” but two of them must be specifically configured to instruct the server as to which server is hosting the TSSD service and what the name of the TSSD cluster is (configured earlier through NLB). The following screens demonstrate the simple configuration of this service through the two GPO settings, “Session Directory Server” and “Session Directory Cluster Name.”



Once each of these settings has been configured the TS farm is ready for production and can start allowing users to connect to a fault-tolerant, secure configuration of a Microsoft TS farm.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Administration & Maintenance

Administering the Server

Once the TS farm has been installed and configured and then properly secured using local security policies, software updates, etc, the administrators responsible for the system must have a way of administering the system securely. There are six primary ways ACME administrators could administer the TS farm described in this paper:

1. Through the physical server console
2. Through the built in HP / Compaq RILO board
3. Through the TS client software (Remote Desktop Connection)
4. Through the "mstsc.exe" command line utility
5. Through the "tsmmc.msc" Microsoft Management Console
6. Through the TS Web Client ActiveX control (TSWeb)

The first method is the most obvious way of administering the system. However many administrators within the organization will find the need to remotely administer these systems and thus this method isn't always practical.

Another way is through the built in RILO board. This method is perfect for administering the system through a complete startup or shutdown procedure when access to the system regardless of the operating system's state is required. This can be done via accessing the RILO's web server built into the system's ROM. The other nice feature of this hardware is that console access is not an issue, since you are connecting via the hardware. While this method is great for controlling all aspects of the server, the interface can be clunky and isn't the best for day to day administrative purposes. Configuration of this hardware is described earlier in this document.

Other options for remote administration are through the terminal services service itself. These utilities are great for day to day tasks which must be performed on the server; however often the administrator is called on to perform tasks such as software installations or updates, which should only be done through a console session with the server. The first of these methods, the TS client software, unfortunately does not allow the administrator to access a console session on the server without creating a customized *.rdp file which can be cumbersome to manage in a multiple server environment.

Another choice for administering the server through the TS service is through the "mstsc.exe" command line utility. This allows the administrator to connect to a TS session using either regular user mode or through a console session via the use of different switches, but is identical to the TS client in every other way. The syntax for using this command, as taken from the help file, is:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Remote Desktop Connection **MSTSC [<Connection File>] [/v:<server[:port]>] [/console] [/f[ullscreen]] [/w:<width> /h:,height>] | /Edit"ConnectionFile" | /Migrate | /?**	
<Connection File>	Specifies the name of an .rdp file for the connection.
/v:<server[:port]>	Specifies the terminal server to which you want to connect.
/console	Connects to the console session of a server.
/f	Starts the client in full-screen mode.
/w:<width>	Specifies the width of the Remote Desktop screen.
/h:<height>	Specifies the height of the Remote Desktop screen
/edit	Opens the specified .rdp file for editing.
/migrate	Migrates legacy connection files that were created with Client Connection Manager to new .rdp connection files.
/?	Generates the Usage message.

Yet another way of administering a terminal server is through the "tsmmc.msc" Microsoft Management Console. This allows the administrator to access a Terminal connection with console access through selecting a checkbox for the connection. More importantly it allows an administrator to pre-configure multiple TS sessions through one management console, thus allowing the administrator to toggle between open sessions with terminal servers. This tool is available through the "AdminPak.msi" installation package for Windows Server 2003. In order to install this, the client machine must be running Windows XP, service pack one or later, or Windows Server 2003. There are two other inconveniences with this tool. First of all the connections that are created cannot be alphabetized or sorted for easy filtering of the connections, which can be difficult when trying to manage large numbers of servers. The second issue is that if an administrator attempts to open too many TS sessions at a time, mouse control becomes sporadic within the TS session itself. Regardless of the downfalls, this MMC console will likely be the tool of choice for most ACME employees administering large numbers of TS machines.

The final method of managing a TS server is through the web client, TSWeb. This client, like the TS client for desktops is limited in that console access is not available through this client. Also, as noted earlier, installing the TSWeb client requires the installation of IIS on the server where it is installed, which opens up the server to multiple vulnerabilities. Therefore because of these factors this method of accessing terminal servers within ACME should not be used.

Regular Maintenance Activities

Beyond simply connecting to the server farm, there are regular administrative tasks which need to be performed on these systems for performance, optimization, and security reasons. These tasks need to be performed on each of the servers in the farm,

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

not just on the virtual address of the NLB cluster. The administrator should perform each of these tasks on a regular basis to ensure the continued confidentiality, integrity, and availability of the systems. Any series of servers such as this must be constantly maintained in order to keep it in optimal shape for the end users.

The following table outlines some of the regular maintenance activities which should be performed on these servers, as well as how often they should be performed on each server in the system:

Maintenance Activity	Maintenance Interval
Run system backups on the servers in the TS farm & perform a test restore.	System backups of system specific configuration information should be run on a weekly basis. Since images of these systems will be created after system changes and no data will be stored on the system, daily backups and full system backups will not be necessary for these servers.
Create an image of a server in the TS farm & perform a test restore.	An image should be created of the original server in the farm, and whenever new applications are installed or there is a major change to the servers in the farm.
Install Microsoft Windows Server 2003 service packs and hotfixes on the system.	As they become available. Microsoft currently releases hotfixes once a month which need to be tested and then installed on each server in the farm.
Conduct security audits of the system's configuration.	Annual security audits should be performed against the servers in the TS farm. These should be used to verify proper configuration of the farms as well as look for new vulnerabilities to the systems.
Delete temporary data from the servers.	Monthly, administrators should delete temporary data from the servers to free up disk space and optimize the system. Scripts could also be utilized to delete data at regular intervals.
Defragment the server's hard drives.	This should be done on a monthly basis on the same schedule as deleting temporary data from the system. This can also be scheduled using task scheduler to run at off peak hours.
Reboot the servers.	Monthly the servers should be rebooted using the `tsshutdn /reboot` command. This should be done at off hours and can be scheduled using the system's task scheduler.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Managing Risks to Terminal Services

Before terminal services or any technology should be deployed in an organization the risks of deploying that system must be weighed against the potential benefits of the technology. Many of the benefits of terminal services have already been discussed in this paper; however the risks to the system also need to be considered. The following table of risks to the system attempts to address the major risks to the TS farm from a security standpoint. In order to do so, first a baseline definition of risk must be identified. A simple formula that describes information system security risk is:

Threat + Vulnerability + Impact > Risk

Or said another way, threats, combined with vulnerabilities, combined with potential negative impacts to a system, yield the security risk to the system. Therefore the following table will address each of these elements of risk, as well as define whether the risk exists in an internal TS farm configuration, and external TS farm configuration, or in either of the two architectures. Remember, this chart assumes that the Terminal Service Web Client (TSWeb) has not been installed on the system, nor the Internet Information Service (IIS) on which TSWeb depends as these services open a large number of unnecessary vulnerabilities to the system.

Threats	Vulnerabilities	Impacts	Internal / External / Both
Password Guessing / Dictionary Attacks *Medium Level of Risk*	Attackers have access to multiple ways of performing dictionary or password guessing attacks against a Terminal server. Some of those ways are: 1. **Manually** – By guessing random usernames or passwords. 2. **Using Social Engineering** – Convincing a real user of the system to give their username and/or password to the attacker. 3. **Using TSCrack** – This is an automated, free TS password cracker which can be	If an attacker is able to discover the password of a legitimate user of the TS farm, the attacker would have the capability to perform any of the tasks available to that user. This is primarily a concern for any users with administrative access to the server.	Both

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	downloaded from the Internet. However it is very slow, only allowing 1-2 attempts per minute. 4. **Using TSGrinder** – Another free, automated tool which can be downloaded. Much faster than TSCrack.		
Denial of Service (DOS) Attacks *Medium Level of Risk*	There have been many advertised flaws in the RDP protocol which can lead to DOS attacks against a TS server. At the time of this document these attacks are only successful on Windows 2000 servers running TS. One of these vulnerabilities, as advertised on SecurityFocus, is BugTraq ID 5376. These servers are also vulnerable to traditional TCP/IP DOS attacks as are most servers (Ping of Death, Teardrop, SYN Flooding, Land, Smurf, etc).	An attacker performing a denial of service attack against the TS farm has the capability of overwhelming the farm, thus denying legitimate users access to the systems. This will deny system users from performing their normal tasks and being productive users of the system.	Both (Primarily external issue)
Network Traffic Sniffed *Low Level of Risk*	In order to be successful with this type of attack a user must first sniff traffic off of the network using a tool such as Ethereal, Sniffer Pro, EtherPeek, etc. The traffic gathered can then be filtered to display only TS traffic. Once the TS traffic is isolated, the attacker now has encrypted network traffic from the server. If the attacker has the computing power, or the encryption keys, this data can then be read and analyzed. But it is difficult for an attacker to be able to compromise the data.	If an attacker is able to sniff the traffic between a terminal server and the TS client, the attacker has the ability to compromise the confidentiality of the system's data. This can result in misuse of information, trade secrets lost, violation of government regulations, negative publicity, or worse.	Both (Primarily external issue)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

TS Service Advertised *Low Level of Risk*	The default installation of terminal services runs the RDP service on port 3389. Administrators can change this port and attempt to hide the service by editing the registry on the terminal server. However even if the TS listening port has been changed the attacker can utilize tools such as TSenum or TSprobe to discover servers running this service on the network. Another more manual way would be to utilize banner grabbing through utilities such as telnet or nmap. However this can be a painfully long process to do manually.	If the TS service is running with the default settings and listening on the default port, an attacker may notice the port and attempt a more directed attack against the system.	Both (Primarily external issue)

Each of these risks needs to be evaluated when considering whether or not to implement terminal services as a part of a HIPAA compliant secure architecture. This is especially true when considering whether or not to provide terminal services as an Internet accessible service, potentially as a replacement of a corporation's VPN for certain types of remote access. ACME must consider in either of these scenarios whether to mitigate the risk, lower the level of risk, or accept the risk for any of these items before implementing the technology into their system.

The following table addresses how the above risks can be successfully mitigated in a production environment, either an internal only TS farm or one that is exposed to the Internet:

Threat	How to Mitigate Risk
Password Guessing / Dictionary Attacks *Medium Level of Risk*	Password guessing is one of the most common attacks which will threaten a TS farm. This will be true both for internal only TS farms as well as Internet facing systems. In fact there are even dedicated applications whose role is to use a dictionary file to break passwords on terminal services accounts (TSGrinder by Thor). The simplest and most effective way of protecting a system against this type of attack is to enforce account lockouts on the system. While doing this may lead to higher administrative costs associated with the machine, and may result in a higher occurrence of users causing

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	their own personal DOS, this is still a necessary configuration. Should an attacker guess someone else's password he or she will have full access to the system just as that user. By implementing a conservative account lockout policy of 5-8 attempts to login to the system, most password guessing or dictionary attacks will fail. However, even by implementing a policy such as this there is one account that is immune to the setting, the Administrator account. This super account can only enforce account lockouts by installing and running the Passprop.exe program (found in the Windows 2000 Server Resource Kit, and must be extracted from the Netmgmt.cab file). By running the command: `Passprop /adminlockout` The administrator account will be locked out if it is attacked. Another option is to rename the administrator account to protect it from being compromised. This can be done with or without the use of the Passprop utility, but provides a stronger level of defense when used together. Because this is such a common threat, but one that is easily remedied, it is given a Medium level of risk.
Denial of Service (DOS) Attacks *Medium Level of Risk*	This particular threat can often be one of the most difficult threats to protect a system against, especially one that is facing the Internet. In order to protect against this threat, a series of controls must be implemented in order to secure the server. Some of the most important are: 1. Keep the server's software updated with service packs and hotfixes. 2. For Internet facing systems, employ the use of a firewall with DOS filtering capabilities to filter such attacks from hitting the server. 3. Configure the host operating system with the Local Security Settings described earlier to make the OS itself more resistant to DOS attacks. While DOS attacks are common, and new ones are constantly being discovered, by implementing the above three controls, a system administrator

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	will protect against the majority of attacks. Thus this threat is given a Medium level of risk.
Network Traffic Sniffed *Low Level of Risk*	In order to protect a terminal server's data from being sniffed off of the network the administrator should follow best practices for encrypting all TS traffic. The easiest way of accomplishing this is to enable either High or FIPS encryption level in the terminal server's RDP settings (as described earlier in this paper). The other common method for encrypting this traffic in organizations with a higher need for data security is to apply IPsec filters to all terminal services (TCP 3389) traffic and require its usage to access the TS farm. Either or both of these methods can be used to encrypt the traffic to and from the servers in the TS farm. Since either of these methods is simple to configure and maintain, this threat is given a Low level of overall risk.
TS Service Advertised *Low Level of Risk*	In order to mitigate against this risk the administrator may choose to change the default listening port for the terminal services service. While Microsoft does provide information on their web site on how to change this port, this process is not recommended. Not only does this make the administration of the farm more difficult and costly, but there are tools available which will discover this service regardless of what port is used (TSEnum or TSProbe both by Thor) and Microsoft will not support an installation of terminal services that does not listen on the default port of TCP 3389. It must also be considered that even if an attacker discovers a 'hidden' terminal server, he or she will still need to exploit the service using one of the above mentioned threats. Thus this is listed as a Low Risk Threat.

© SANS Institute 2004, Author retains full rights.

Conclusion

Terminal services with Microsoft Windows Server 2003 have many potential benefits to an organization, especially when considered in the healthcare vertical market. ACME Health System is starting to realize some of these benefits, and the benefits of thin client computing more and more as new enterprise systems are being configured and deployed using a thin client model. As has been noted already, through deploying this technology there are gains in manageability and security which can contribute to a lower total cost of ownership for information technology systems and improve the end user's ability to access the right information, when they need it, where they need it.

Within ACME, more and more local systems are rolling out applications using thin client computing. Unfortunately each system seems to be moving in its own direction, utilizing its own resources, and moving in their own direction on this topic. While in the past ACME has operated as a federacy of local systems, there is a lot that can be gained through collaboration and joint efforts to solve common problems. This document has sought to provide a framework for deploying terminal services as a thin client platform in a standardized way in order to promote the sharing of information between systems. Each local system will continue to be unique, and continue to have needs that are different from others in the organization, but hopefully papers such as this will contribute to the sharing of information and resources which will help us to better utilize the talent our organization has.

© SANS Institute 2004, Author retains full rights.

Appendix A – Unattended Installation Script (TSfarm.txt)

The following is the results of running Windows Setup Manager in order to create an unattended installation script for installing the core operating system on one of the servers in the TS farm. In order to use this script the following text must be cut and pasted into notepad, and the file saved as “TSfarm.txt”:

```
;SetupMgrTag
[Data]
    AutoPartition=1
    MsDosInitiated="0"
    UnattendedInstall="Yes"

[Unattended]
    UnattendMode=DefaultHide
    OemPreinstall=No
    TargetPath=\WINDOWS

[GuiUnattended]
    EncryptedAdminPassword=NO
    OEMSkipRegional=1
    TimeZone=35

[UserData]
    ProductKey=PVY8R-YHJDT-JFP22-7CH7Y-TRCMB
    FullName="ACME"
    OrgName="ACME"

[LicenseFilePrintData]
    AutoMode=PerSeat

[TapiLocation]
    CountryCode=1
    Dialing=Tone

[RegionalSettings]
    LanguageGroup=1
    Language=00000409

[Identification]
    JoinWorkgroup=WORKGROUP

[Networking]
    InstallDefaultComponents=Yes
```

© SANS Institute 2004, Author retains full rights.

Appendix B – Automatic Update Script (AutoUpdateTS.vbs)

The following script can be used to configure a server that's a member of a TS farm to automatically update itself through the use of an internal Microsoft Software Update Services (SUS) server. Please note that this script should only be used on new servers which follow the guidelines noted in this guide. Do not apply this script to any production terminal servers without thoroughly testing it first. Making many of these changes on a production system without proper prior testing is likely to break the live system.

Also before implementing this script the portion of the script where it states <SUSServerName> should be replaced by the name of the internal Software Update Services (SUS) server that will provide automatic updates to the server farm. This script can be cut and pasted into Notepad and should be saved as AutoUpdateTS.vbs:

```
'*********************************************************************
***
'* This script will update the Automatic Windows Update Server to be
'* the McAfee server in Site A. It also sets the updates to
'* run automatically, without user intervention, at 12:00pm every day.
'* by James Tarala 10/1/2003
'*********************************************************************
***
set WshShell = CreateObject("WScript.Shell")
WshShell.regwrite
"HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\W
UServer","http://<SUSServerName>","REG_SZ"
WshShell.regwrite
"HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\W
UStatusServer","http://<SUSServerName>","REG_SZ"
WshShell.regwrite
"HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\A
U\NoAutoUpdate",0,"REG_DWORD"
WshShell.regwrite
"HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\A
U\AUOptions",4,"REG_DWORD"
WshShell.regwrite
"HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\A
U\ScheduledInstallDay",0,"REG_DWORD"
WshShell.regwrite
"HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\A
U\ScheduledInstallTime",12,"REG_DWORD"
WshShell.regwrite
"HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\A
U\UseWUServer",1,"REG_DWORD"
```

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

"Guide to Securing Microsoft Windows 2000 Terminal Services." July 2001. National Security Agency. 21 December 2003.http://nsa2.www.conxion.com/win2k/guides/w2k-19.pdf

"Hammer of God Utilities Download." 2003. 2003. Hammer of God. 21 December 2003. http://www.hammerofgod.com/download.htm

"Locking Down Windows Server 2003 Terminal Services Sessions." 2003. Microsoft Corporation. 21 December 2003. http://www.microsoft.com/windowsserver2003/techinfo/overview/lockdown.mspx

"Microsoft Case Studies – Avanade" 2003. Microsoft Corporation. 21 December 2003. http://www.microsoft.com/resources/casestudies/casestudy.asp?casestudyid=13212

"Remote Desktop Connection Client 1.0.2 for Mac OS X" 2003. Mactopia. 21 December 2003. http://www.microsoft.com/mac/downloads.aspx?pid=download&location=/mac/DOWNLOAD/MISC/RDC.xml&secid=80&ssid=9&flgnosysreq=True

"Remote Desktop Connection Software Download." 2003. Microsoft Corporation. 21 December 2003. http://www.microsoft.com/windowsxp/pro/downloads/rdclientdl.asp

"Scalability and Performance of HP Proliant DL360 G3 Servers." 2003. HP / Compaq ActiveAnswers. 21 December 2003. http://activeanswers.compaq.com/aa_downloads/6/100/225/1/72358.pdf

"Session Directory and Load Balancing Using Terminal Server." 2003. Microsoft Corporation. 21 December 2003. http://www.microsoft.com/windowsserver2003/techinfo/overview/sessiondirectory.mspx

"Technical Overview of Windows Server 2003 Terminal Services." 2003. Microsoft Corporation. 21 December 2003. http://www.microsoft.com/windowsserver2003/techinfo/overview/termserv.mspx

"Terminal Services." 2003. Microsoft Corporation. 21 December 2003. http://www.microsoft.com/windowsserver2003/technologies/terminalservices/default.mspx

"Using Software Restriction Policies to Protect Against Unauthorized Software." 2003. Microsoft Corporation. 21 December 2003. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/maintain/rstrplcy.asp

"What's New in Terminal Server." 2003. Microsoft Corporation. 21 December 2003.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/terminalserver.mspx

"Windows @ The University of Michigan." 2003. University of Michigan. 21 December 2003. http://www.umich.edu/~lannos/windows/w2k-termserv.html

"Windows Server 2003 Terminal Server Capacity and Scaling" June 2003. Microsoft Corporation. 21 December 2003. http://www.microsoft.com/windowsserver2003/docs/TSscaling.doc

Smith, Del. "Appsec can help restrict application access in Win2K." Sept 2002. TechRepublic. 21 December 2003. http://techrepublic.com.com/5100-6268-1054829.html

Lewis, Morris. "Terminal Services Security." February 2001. Windows 2000/.NET Magazine. 21 December 2003. http://www.winnetmag.com/WindowsSecurity/Article/ArticleID/16524/16524.html

© SANS Institute 2004, Author retains full rights.