Global Information Assurance Certification Paper

GIAC Certified Windows Security Administrator (GCWN) Practical Assignment v3.0

Securing Windows Terminal Server Using a Security Template

Date Prepared:
March 29, 2002

Prepared by:
Darwyne Tessier

Table of Contents

Introduction

This paper details a study of the steps necessary to improve the level of security of a Windows 2000 Terminal Server (WTS). A WTS establishes a multi-user environment that can be used by clients to access any program installed on the server. The security template chosen for this study as the base template to evaluate was the NSA Windows 2000 member or stand-alone server security template. Because this study revealed that the settings of this template were found to be inadequate for a WTS environment, modifications were made to the template configuration so that it would improve the levels of security of the WTS and at the same time allow normal access for the clients. Finally, with the template reconfigured and implemented, a number of tests were performed on the WTS to insure that it was fully functional.

A WTS in application server mode provides multi-user access to programs installed on the server. WTS users connect to the server and run applications as if they were physically logged on at the server. The WTS acts, therefore, as a remote workstation for the client because the complete user interface and all input and interaction with the application actually happen on the server. When a client connects to a WTS to start an application, the program starts on the WTS itself, and only screen changes and mouse and keyboard input are passed to the client's computer. In a regular application or file server environment the user's program is loaded on the client's computer and all processing occurs on it, but in a WTS environment none of the actual application program processing occurs at the client's workstation.

The NSA provides a standard template meant to improve the level of security of a Windows 2000 member or stand-alone server. Although a WTS is not a regular applications or file server, the NSA template provided the best starting point for this study. However, since this template was not designed to work specifically for WTS, it was expected that a number of changes would be required to allow normal client access. This study used the *NSA Guide to Securing Microsoft Windows 2000 Terminal Services* as well as a number of other sources to determine the modifications that would need to be made to the NSA Windows 2000 server security template. In this paper, the changes made to the template are documented in a checklist, and the reasoning behind each change is explained.

Once the checklist and settings were chosen, the template created was implemented using a group policy. The template was imported into this group policy and applied to the settings of the server. With the created template in place, updates and other changes to the security policy were easily made. Finally, after the template was implemented using a group policy to apply the settings on the server, a number of applications were tested to see that the changes did not affect the applications.

Environment

Server Hardware

3 IBM 300PL Desktops
- IBM 686241U
- 6 Gb hard drive
- 450 megahertz Intel Pentium II
- 256 Megabytes Installed Memory
- Realtek RTL8139(A) PCI Fast Ethernet Adapter

Server Software

Microsoft Windows 2000 Server, Service Pack 2 (Windows 2000 security rollup package applied)

Client Hardware and Software Used for Testing

Microsoft Windows 2000 Professional
Terminal Services Advanced Client installed

NOTE: Client workstation is not part of the domain.

Network Protocol

TCP/IP

Windows 2000 Domain Structure

GIACDC
- ADS Domain Controller
- DNS server
- DHCP server

Organizational Units
- TS60 OU with Terminal Server Security GPO applied.

GIACTS60
- Windows 2000 Terminal Server.
- Microsoft Excel and Word components installed from Office XP Pro CD.

NOTE: This is not a complete list of software and hardware installed.

Windows 2000 Terminal Server Setup

Operating System Installation

The server setup was done using a standard Windows 2000 Server installation. The server was installed in the domain as a member server only. The following options were chosen during the installation:

- The hard drive of each server was split into two partitions. Each was formatted as an NTFS partition, which provided a basic level of file system security for the Windows 2000 server.
- IIS was deselected during the installation.
- For the Terminal Services Setup the default selection was changed from Remote Administration Mode to Application Server Mode.
- Permissions Compatible with Windows 2000 Server was selected instead of the default Permissions Compatible with Terminal Server 4.0 Users because this setting will limit access to critical registry and file system locations. However, if backwards compatibility is required by applications, specific registry and file permissions could be reviewed at that point to see what access is required and whether the risks are acceptable.

No changes were made to any of the default file level permissions of the server.

After the installation of WTS, Service Pack 2 and the Microsoft Windows 2000 Security Rollup Package were installed.

Application Installation

In the terminal services environment any number of applications can be installed. Each application and any changes required to run securely in a WTS environment would need to be evaluated for that specific application. For the purpose of this paper Word and Excel were installed from Office XP to provide a set of applications to test after the implementation of the security template.

Word and Excel were installed into D:\Program Files\. Even though some files are still installed on the system partition, these applications were installed on a separate partition to control access to this partition and to help limit exposure to files on the system partition. Special security permission could be applied to this separate partition if certain applications required more access to files after they have been installed.

Group Policies and Organizational Units

Numerous features and settings can be limited through the use of group policies, such as limiting a client's access to applications or features available on the terminal server. However, the focus of this paper is on securing the server using a security template.

In a WTS environment multiple users have concurrent access to local files and applications just as if they were signing on directly to the server. A WTS requires specialized rights and policies that may not apply to any other workstations or servers in the organization. For this reason terminal servers need to be in their own organizational unit, making the implementation of specific policies and templates much easier.

Security Template Options and Settings

For this study, the template chosen to use as a starting point for the template to be applied to a WTS environment was the NSA Windows 2000 member or stand-alone server security template (w2k_server.inf). The Windows 2000 default security template used for a member server can be found in the file defltsv.inf in the INF directory of the system root. Since there was no standard template to choose from that was specifically developed for a server running terminal services, the NSA template developed for a member or stand-alone server provided a good base for a customized template. Modifications made to the NSA template were based upon what was found to work in the environment, as well as upon suggestions and research from a number of sources.

The following recommendations were considered requirements for a WTS environment before the implementation of the template:

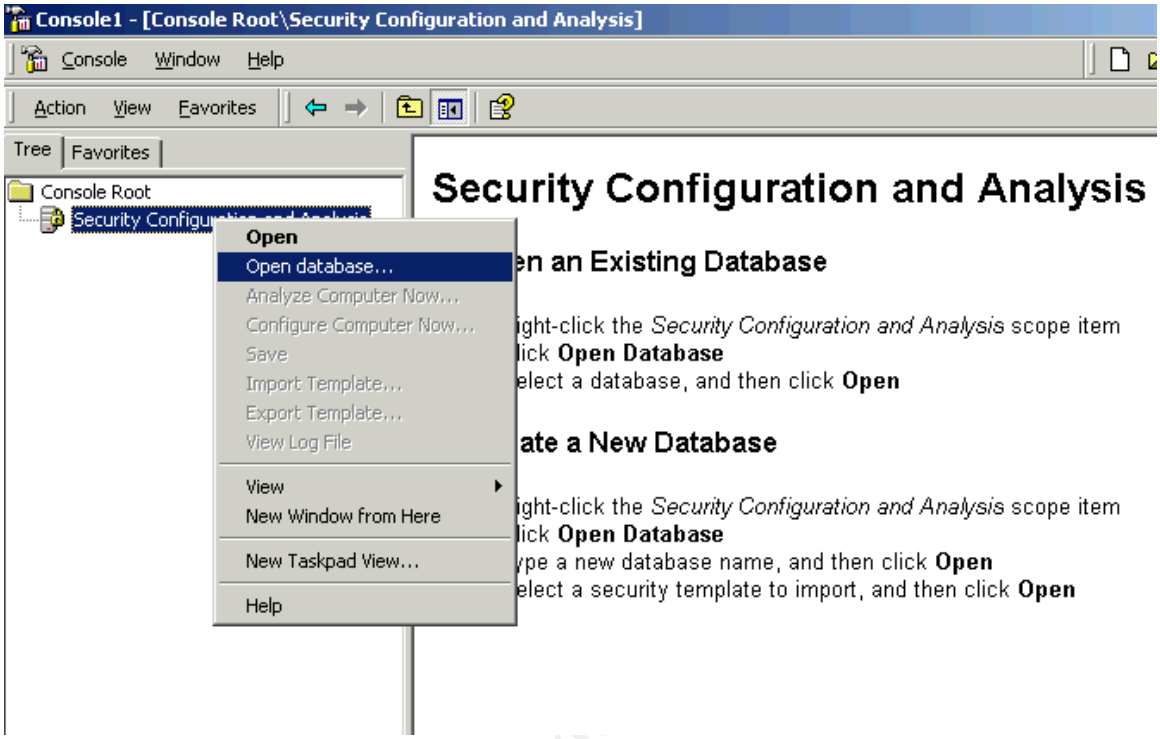
- When used in applications server mode, a WTS should be installed as a member server, never as a domain controller because users accessing the WTS required the right to log on locally to use the server.
- The default settings for each server should be modified so that the additional permissions that were granted to Terminal Services users are removed. *TechNet* article "Removing Additional Permissions Granted to Terminal Services Users" (Q238965) documents the procedures required to remove the extra permissions granted to the Terminal Services users.

Since the NSA security template was not specifically designed for a member server, running terminal services a number of changes were required to the settings of the NSA template. This process began with a comparison between the default settings and that of the NSA template using the Security Configuration and Analysis tool.

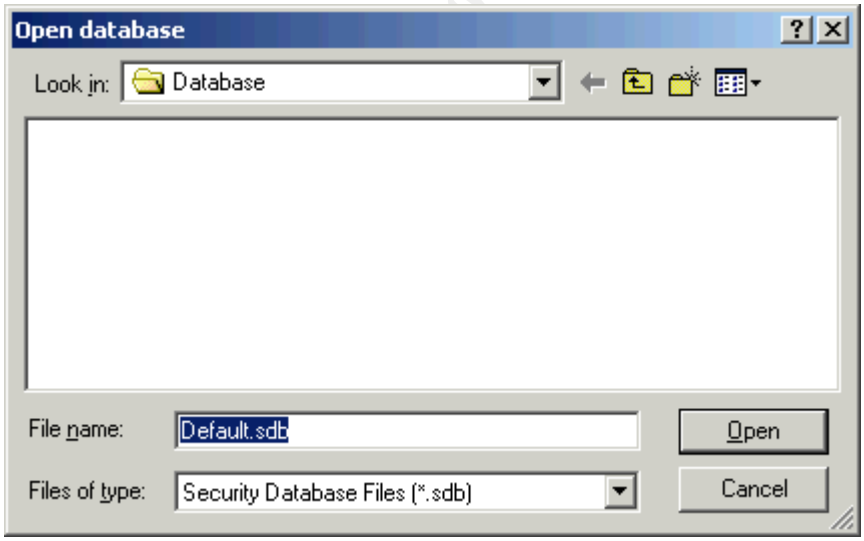
To duplicate the process taken in this study, complete the following steps:

1. Open a MMC console.
2. Add in the Security Configuration and Analysis snap-in.
3. Right-click Security Configuration and Analysis.

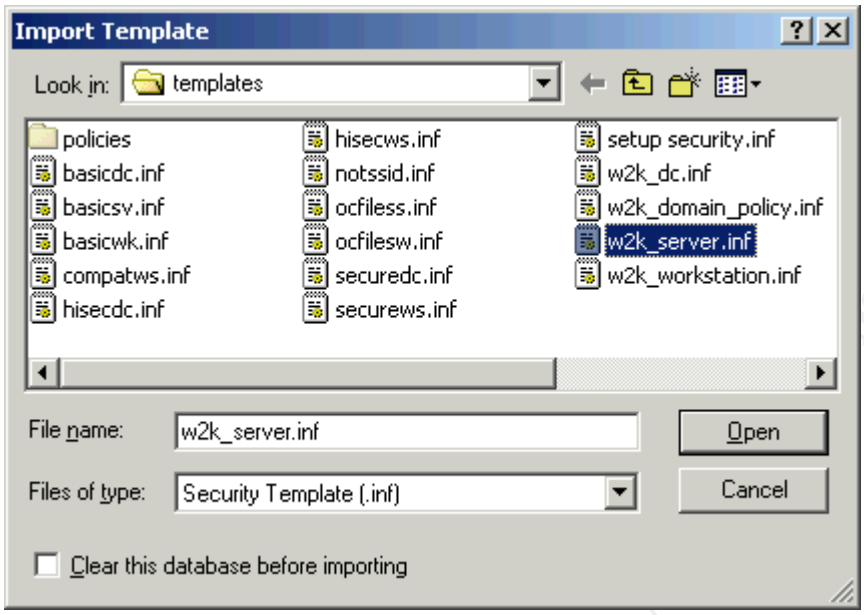
4. Choose Open database.



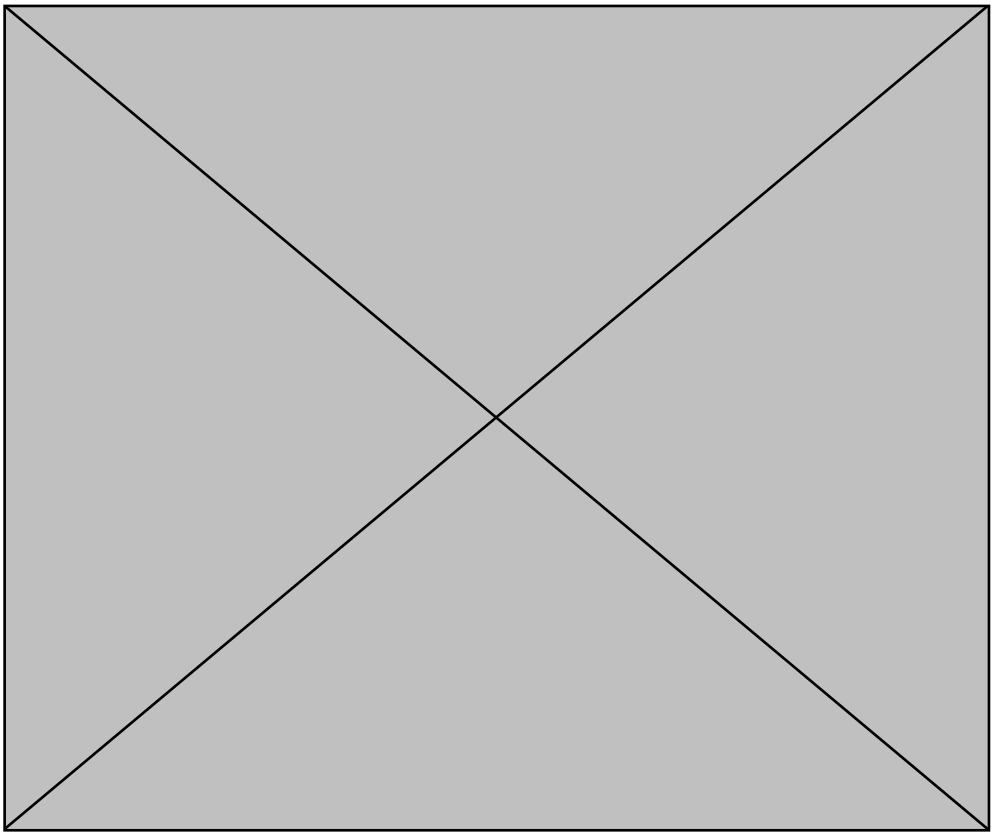
5. Choose a name for the new database (e.g. Default.sdb). Click Open to create the database.



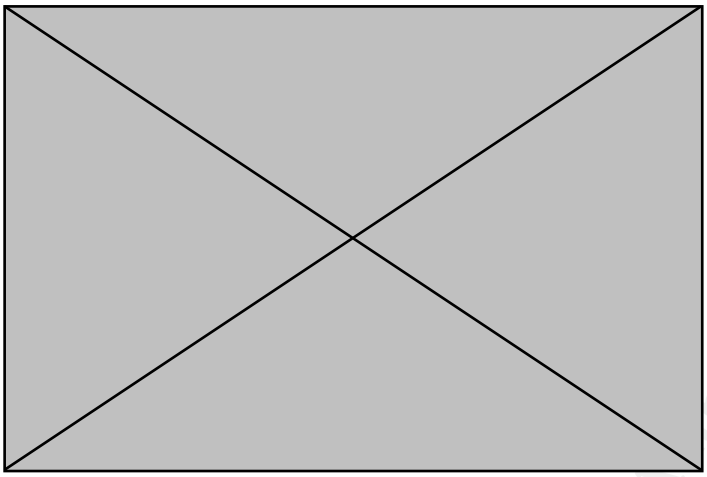
6. Choose the w2k_server.inf and click Open to load the security template so that it can be compared against default settings on the server.



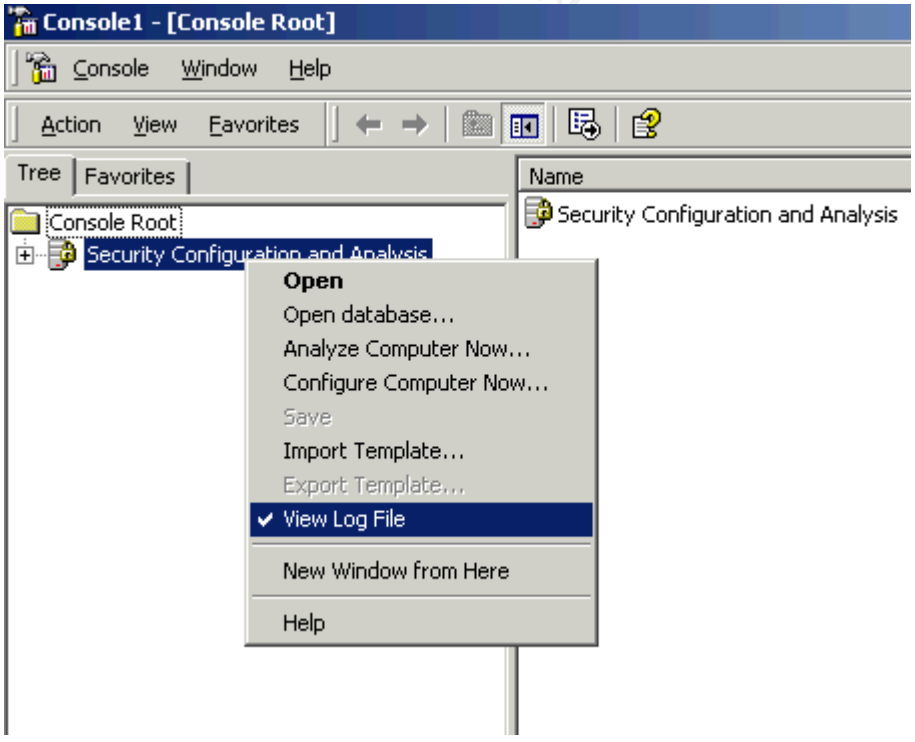
7. Right-click Security Configuration and Analysis and choose Analyze Computer Now to see what registry settings will be modified if the template is applied.



8. Enter a location and file name for the logs to be saved and click OK. The analysis is then performed to compare the settings from the default NSA template to the current installed settings on the WTS.



9. Right click on Security Configuration and Analysis and choose View Log File to view the differences.



10. Note that a red X indicates the differences between the security template and the default settings for the WTS.

By analyzing the differences between the WTS default settings and the NSA template, the customized settings for the template were determined. Some of the policies apply at both the domain and the local server to keep a consistent logon policy for the client workstations when they are authenticated. No local accounts are allowed to access a terminal server, but the policies are implemented locally on each server to remain consistent. Domain accounts are required to access a terminal services session. Some settings such as registry and file level security are set only at the terminal server OU level. Only the policies that have a direct affect on terminal servers were considered parts of this study. The following sections detail of the customized settings:

Account Policies

	Policy Setting	**Terminal Server OU or Domain Wide Policy**
Password policy		
Enforce password history	8 passwords remembered	Both
Maximum password age	42 days	Both
Minimum password age	1 day	Both
Minimum password length	8 characters	Both
Password must meet complexity requirements	Enabled	Both
Store password using reversible encryption for all users in the domain	Disable	Both
Account lockout policy		
Account lockout duration	9999 minutes	Both
Account lockout threshold	3 invalid logon attempts	Both
Reset account lockout after	15 minutes	Both

Many security templates use a password history of 24. This number is excessive. By using 42 days for password expiration and by keeping 8 passwords, users can reuse a password only once per year. The minimum password age is 1 day, and users could reuse

their password much more quickly but we do not anticipate that users would go through this trouble; so lowering the password history and password age settings are acceptable risks.

A domain-wide policy of 8 characters for the minimum password length that meets all the complexity requirements was lowered from the recommended setting of 12. The recommended length of 12 is too complex for the majority of users. However, for all administrative domain and local accounts, a separate security policy could be implemented to enforce a minimum password length of 12 that meets all complexity requirements.

The account lockout policy in effect follows the recommended guidelines. Users are locked out after 3 invalid attempts, and the invalid attempts are reset after 15 minutes. The biggest change from the NSA security policy is that accounts remain locked out until an administrator resets them. In the current environment with limited access to servers from the outside world, this is an acceptable risk and of little concern for potential denial of service attacks.

Local Policies

	Policy Setting	**Terminal Server OU or Domain wide policy**
Audit Policy		
Audit account logon events	Success, Failure	Both
Audit account management	Success, Failure	Both
Audit directory service access	No auditing	N/A Domain only
Audit logon events	Success, Failure	OU
Audit object access	Failure	OU
Audit policy change	Success, Failure	Both
Audit privilege use	Failure	Both
Audit process tracking	No auditing	OU
Audit system events	Success, Failure	Both
User Rights		
Access this computer from the network	Administrators	OU
Bypass traverse checking	Users	OU
Log on locally	Administrators, Users	OU
Shutdown the system	Administrators	OU
Security Options		
Additional Restrictions for anonymous connections	No access without explicit permissions	OU
LAN Manager Authentication Level	Send NTLMv2 response only\refuse LM & NTLM	OU
Do not display the last user name in logon screen	Enable	OU
Number of previous logons to cache to cache	0 logons	OU
Shut down system immediately if unable to log security events	Disable	OU

By auditing events at both the domain level and the local server level, all necessary monitoring is in place to log any potential problems. There are no local accounts except the administrator account accessing the server. The policy settings are in place only to monitor and log any suspicious events. All access to the server is through domain accounts, which is why events such as successful and failed logon attempts, policy changes, and privilege use need to be audited on domain controllers as well. Auditing of the account logon events track successful and failed login attempts by domain accounts. These events will be logged on the domain controller. Auditing of logon events also captures failed account logon attempts at the WTS by any account, domain or local.

These events will be logged on the WTS.

Auditing of object access is used at the server level to monitor failed access to local resources, such as directories and files. Auditing is enabled for all local drives. Auditing failed attempts to access local directories and files helps identify problems with any applications that need additional rights. It also helps identify any accidental or malicious attempts by users to access critical operating system or application files.

The user rights assignment is also modified to allow users to logon locally to the server. The Users group, which contains the Domain Users group as well as the local Administrators group, is granted the right to logon locally. When clients logon to a WTS session they are actually logging on locally to the server so this change is required to allow access. A special group of terminal services users only called, WTSUsers, could also be created and put in the local Users group, but all Domain Users are allowed to run applications on the WTS. However, unlike other Windows 2000 servers the "Access this computer from network" is limited to the Administrators group. Users do not need to connect to shares on the WTS because all file shares and printer shares required by a user exist on other member servers that provide these services.

Anonymous access is not allowed in the environment. All users accessing the server are required to have a domain account. The only account that is not disabled locally is the local Administrators account. Membership in the local groups is controlled using the Restricted Group portion of the security template. The authentication on the server is set to "Send NTLMv2 response only\refuse LM & NTLM" to provide the strongest possible challenge response authentication. Since all client workstations and servers run versions of Windows 2000, this authentication method does not cause problems in the environment.

The system does not shutdown if the security logs are full. This setting is too strong. Forcibly shutting down the system causes problems for the users logged on to the server. The logs are monitored weekly and are not overwritten. If they did begin to fill up, an administrator would manually clear them.

Event Log

	Policy Setting	**OU or Domain wide policy**
Settings for event logs		
Maximum application log size	204800 Kb	Both
Maximum security log size	204800 Kb	Both
Maximum system log size	204800 Kb	Both
Restrict guest access to applications log	Enable	Both
Restrict guest access to security log	Enable	Both
Restrict guest access to system log	Enable	Both
Retention method for application log	Manually	Both
Retention method for security log	Manually	Both
Retention method for system log	Manually	Both
Shutdown the computer when the security log is full	Disable	OU

The event log settings are set to keep up to 200 MB of data in each log, which provides more than enough space for the logs. The logs are never overwritten and in the event that the security log does fill, shutting down the server is too strong a policy to implement and has a negative impact on users running on the terminal server.

Restricted Groups

Group Name	Members
Administrators	Domain Admins, Local Administrator account
Backup Operators	No members
Guests	No members
Power Users	No members
Users	Domain Users, Authenticated Users, Interactive

By restricting all local groups on the terminal server, group membership cannot change - either maliciously or mistakenly - and give unauthorized users elevated rights on the server. If users are added to the groups listed in the template, anyone not specifically listed in the restricted group of the template is removed.

System Services

Because the following services are not required they are disabled through the template:

- Alerter
- Computer Browser
- Distributed File System
- Distributed Link Tracking Client
- Messenger
- Remote Registry Service
- Removable Storage

All other services remain not defined in the template. Each of the services that are set to disable also have the default ACL changed so that Administrators and SYSTEM have full control and Authenticated Users have read only access to the service.