



7

Managing and Maintaining Group Policy

CERTIFICATION OBJECTIVES

- 7.01 Troubleshoot Issues Related to Group Policy Application and Deployment
- 7.02 Troubleshoot Group Policy Software Installation Issues

✓ Two-Minute Drill
Q&A Self Test

Now that we have covered practically every aspect of Active Directory that architects and administrators are likely to face on a daily basis, we need to take a final look at group policies and what methodologies and tools can be used to assist in troubleshooting problems, which are not uncommon in the initial cycles of Active Directory deployment.

CERTIFICATION OBJECTIVE 7.01

Troubleshoot Issues Related to Group Policy Application and Deployment

Chapter 6 described how complex the settings within a group policy object can be, and just how much they cover. Earlier chapters have shown that group policy objects may be applied to Active Directory containers—domains, sites, and organizational units—and discussed in detail how inheritance and blocking work and how administrators can control the mechanism of application of group policy settings. Now, you've established which settings to implement on which levels, you have created a well-organized and logical organizational unit structure that suits the business needs, and created group policy objects and applied them on the respective levels; yet you've found that some of the configuration settings either did not get through as planned, or did get applied, but in the wrong way.

Luckily, there are a few troubleshooting tools administrators can take advantage of. Chapter 6 introduced RSoP—the Resultant Set of Policy MMC snap-in—and its use in planning. This is one of the mainstream tools in Windows Server 2003 when it comes to troubleshooting group policy application problems.

Viewing Effective Group Policy Settings

Determining which policy or policies are in effect is the first thing administrators must investigate if a certain policy is not applied as expected. Windows Server 2003 features at least two GPO troubleshooting tools that administrators are expected to be familiar with—RSoP and Gpresult. In the following exercise, you review how to use the RSoP tool step-by-step.

EXERCISE 7-1**Viewing Effective Policy Settings Using RSoP**

In this exercise you use the RSoP console to view group policy object settings applied to the local machine. You run RSoP in logging mode to achieve this.

1. Log on to the network using the administrator account.
2. Click on Start | Run, type **mmc**, and press ENTER.
3. In the menu, click on File | Add/Remove Snap-in.
4. In the Add/Remove Snap-in window, click on Add and find Resultant Set of Policy in the list of installed snap-ins.
5. Select Resultant Set of Policy, click Add, Close, and then OK to close all open dialog windows.
6. Next, in the console, right-click on the Resultant Set of Policy node and click on Generate RSoP Data. A wizard screen will appear.
7. Click Next on the welcome screen. On the Mode Selection screen, leave the Logging Mode selection unchanged and click Next. The Planning Mode selection would be helpful if you wish to test-apply group policy objects against a certain machine and a certain user to see how that would work if implemented. Logging mode is used to view already applied settings, which is needed in troubleshooting.
8. On the Computer Selection screen, leave the default setting (This Computer) and click Next. Alternatively, you can select another computer if you wish to troubleshoot the policy applied on a remote computer.
9. On the User Selection screen, select which user you will be running the policy settings against. The default setting is the currently logged on user (Current User). Leave the setting unchanged and click Next.
10. You are presented with the final screen of this wizard, which summarizes the RSoP settings. Click Next to proceed with the gathering process and then Finish to close the wizard and review RSoP data.

Note that you can cancel collecting RSoP data for users or computers and just focus on one section of the group policy object. To achieve this, use the corresponding check boxes on either the Computer Selection or User Selection screen.

4 Chapter 7: Managing and Maintaining Group Policy

RSoP presents effective policy settings in a familiar way—containers in the left-hand pane and individual nodes in the right-hand pane. This is similar to how group policy objects are presented in tools like the Group Policy Object Editor, with two slight exceptions. First, you may note that some settings are not shown; this is because they were not configured in the policy object. Second, there is now a Source GPO column next to the configured settings, which shows the group policy object that enforced the settings in question. This is useful in cases where you have to troubleshoot cascading group policies within an OU structure and you want to confirm which policy is in effect.

In addition, RSoP in logging mode can be an effective tool to diagnose policy refresh or processing errors. If there was a problem refreshing or applying the latest version of the policy, RSoP will display an exclamation mark in the appropriate section of the policy, alerting you to the fact (either in user settings or computer settings). If you right-click on the section that is displaying a warning sign, and click on Properties, you will see the Error Information tab that will list applicable errors and corresponding descriptions. It also presents a time stamp of the latest policy processing run and status of application of various policy sections.

The second troubleshooting tool, Gpresult, can be used to display information about policies in effect on the machine. Gpresult is a command-line utility that produces output similar to the following:

```
C:\Documents and Settings\Administrator.JOVIDUDE>gpresult
Microsoft (R) Windows (R) Oper numbered list 2,wsnl2cy Result tool v2.Worksheet numbered
list,wsnl1loft Corp. 1981-2001{Label,lCreated On 10/6/2003 at 10:36:17 AM
{Table Heading,thata for WIN2K3-2\administrator onTable paragraph,tp Mode
-----Table spacing,ts-----{neAlert Separator,as
Microsoft(R) WiPicture3 Large 2003, Enterprise Edition
OS Configuration:           Primary Domain Controller
OS Version:                  5.2.3790
Terminal Server Mode:       Remote Administration
Site Name:                   Default-First-Site-Name
Roaming Profile:
Local Profile:               C:\Documents and Settings\Administrator.JOVIDUDE
Connected over a slow link?: No

COMPUTER SETTINGS-----
CN=JOVIDUDE,OU=Domain Controllers,DC=sales,DC=flexecom,DC=com
Last time Group Policy was applied: 10/6/2003 at 10:35:21 AM
Group Policy was applied from:   jovidude.sales.flexecom.com
Group Policy slow link threshold: 500 kbps
Domain Name:                   WIN2K3-2
Domain Type:                   Windows 2000

Applied Group Policy Objects
-----
```

Default Domain Controllers Policy
Default Domain Policy

The following GPOs were not applied because they were filtered out

Local Group Policy
Filtering: Not Applied (Empty)

The computer is a part of the following security groups

BUILTIN\Administrators
Everyone
BUILTIN\Users
BUILTIN\Pre-Windows 2000 Compatible Access
Windows Authorization Access Group
NT AUTHORITY\NETWORK
NT AUTHORITY\Authenticated Users
This Organization
JOVIDUDE\$\
Domain Controllers
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS

USER SETTINGS

CN=Administrator,CN=Users,DC=sales,DC=flexecom,DC=com
Last time Group Policy was applied: 10/6/2003 at 10:07:36 AM
Group Policy was applied from: jovidude.sales.flexecom.com
Group Policy slow link threshold: 500 kbps
Domain Name: WIN2K3-2
Domain Type: Windows 2000

Applied Group Policy Objects

Default Domain Policy

The following GPOs were not applied because they were filtered out

Local Group Policy
Filtering: Not Applied (Empty)

The user is a part of the following security groups

Domain Users
Everyone
BUILTIN\Administrators
Remote Desktop Users
BUILTIN\Users
BUILTIN\Pre-Windows 2000 Compatible Access
REMOTE INTERACTIVE LOGON
NT AUTHORITY\INTERACTIVE

6 Chapter 7: Managing and Maintaining Group Policy

```
NT AUTHORITY\Authenticated Users
This Organization
LOCAL
Domain Admins
Group Policy Creator Owners
```

In the three distinct sections, Gpresult lists some basic information about the computer it was executed on, then goes on to collect computer settings and user settings, which represent effective (resultant) settings on the machine in question. Note that Gpresult is simply a command-line tool that uses RSOP APIs to retrieve this information using logging mode. In the Applied Group Policy Objects subsections in computer and user settings, you can see which policy objects are effective on the machine. Also note the filtering sections that list all policy objects that were rejected due to security or WMI filtering. Gpresult can be used with the following switches:

- **/v - verbose mode** This adds group policy extensions such as ADM registry-based templates, disk quotas, scripts, IPsec settings, and folder redirection settings, but only those with the highest precedence.
- **/z - super verbose mode** In addition to the standard output depicted in the preceding listing, and all of the information exposed in the verbose mode, Gpresult will list registry values applied by the policy, software distribution settings, certificates, and group policy version numbers, regardless of the precedence of these settings.
- **/SCOPE COMPUTER** Computer settings only. This option will restrict output to settings delivered through the computer settings portion of the policy object.
- **/SCOPE USER** User settings only. This option will restrict output to settings delivered through the user settings portion of the policy object.
- **/s <system>** This allows connecting to a remote system.

Finally, there is yet another way to gather similar information that might be helpful when you are troubleshooting an issue over the phone with a user who does not have enough knowledge to do much of the administrative legwork. If you click on Start | Help and Support, under Support Tasks, you will find a System Information link. Clicking on this link pulls up another menu. Choose View Advanced System Information to continue. In the third menu you are presented with, select View Group Policy Settings Applied. It will take a few seconds for the results to appear on the screen. The resulting information may remind you of the Gpresult output, but then it adds information such as applications listed in the Add/Remove Programs applet,

deployment state of software packages, Internet Explorer settings and any scripts enforced by the policy, as well as registry settings received through ADM templates.

This method also relies on the RSoP engine to gather policy information, but goes one step further than Gpresult. It allows administrators to determine not only which policies are in effect but also how software distribution settings are affecting the machine in question, which registry settings specifically were applied by which source policy object, and how filtering affected the process. Also note that this method exposes specific security settings that were applied to individual objects and indicates which policy object delivered the setting.

Refreshing Group Policy Settings

By using RSoP-derived tools such as Gpresult, and viewing group policy settings via the Help and Support console, you can determine when the policy was applied. In the initial stages of policy implementation, administrators need to fine-tune their policy settings, which may result in numerous changes applied to group policy objects throughout the day. If a certain setting is not being propagated to client machines as expected, or if a policy is not getting applied in the first place due to other issues that may be taking place elsewhere in the system, checking the latest group policy application time stamp will help establish whether the new setting has been replicated to the machine. If the policy on the client machine was refreshed since it was reconfigured on a domain controller, chances are the setting was overwritten by another policy or setting. Otherwise, the newer policy object has not made it to the client workstation yet. You can confirm whether policy refresh was successful from the Application section of the Event Log, information event ID 1704:

```
Event Type:      Information
Event Source:    SceCli
Event ID:        1704
Description:
Security policy in the Group policy objects has been applied successfully.
```

Remember that the default policy refresh interval is 90 minutes for client computers and member servers, and 5 minutes for Windows 2000 and Windows Server 2003 domain controllers. If administrators make changes to the policy objects, the settings may not become effective for a period of time. Certain settings such as software distribution may not become effective until a reboot or logon event takes place.

To avoid logging off and on or even rebooting your test machine manually while you are experimenting with group policy changes, use the `gpupdate` command in Windows XP or Windows Server 2003 (logoff or reboot in this case only occurs

8 Chapter 7: Managing and Maintaining Group Policy

if settings that require these events have been modified). It replaces the **secedit /refreshpolicy** command available in Windows 2000 and serves the purpose of forcibly refreshing policy settings regardless of the refresh interval. The syntax of this command as is follows:

```
GPOupdate [/Target:{Computer | User}] [/Force] [/Wait:<value>] [/Logoff] [/Boot] [/Sync]
```

You can execute **gpupdate** without specifying any parameters, but if you want to test or troubleshoot settings like software distribution, you might need to use some of the parameters provided with the command:

- **/Target** Indicates which portion of the GPO should be refreshed—by default, refreshes both.
- **/Force** Force-applies all policy settings—by default, only changed settings are applied.
- **/Wait** Causes the command line to wait for **gpupdate** to finish processing group policy objects.
- **/Logoff** Forces a logoff if the policy refresh implemented changes that are normally applied in the foreground mode (during logon). Note that logoff will not be forced if settings implemented with the latest policy do not require it.
- **/Boot** Forces a reboot if the policy refresh implemented changes that are normally applied during computer start-up. Note that reboot will not be forced if settings implemented with the latest policy do not require it.
- **/Sync** Results in the next foreground process (computer bootup or user logon updates) to be performed synchronously; that is, the user interface will not start loading until policy processing and application is complete.

Network-Related Issues

Network-related problems are often overlooked when dealing with group policy issues, but it is vital that every aspect of network communication between client and server is configured and operating as prescribed. In addition to most basic network connectivity that must be in place, DNS resolution should be functioning correctly for the client to be able to resolve server names to IP addresses.

Network troubleshooting is a subject perhaps deserving of its own discussion; for the purposes of this chapter, only the most common tools, introduced in Chapter 2, will be covered: **NSLOOKUP** and the **ipconfig** and **ping** commands. The **NSLOOKUP** command-line utility is used to verify DNS functionality and resolve DNS fully

qualified domain names into IP addresses. The **ipconfig** command outputs the interface configuration with pertinent connection parameters. Finally, the **ping** command can be used to send test packets and verify end-to-end connectivity.

Traditional network troubleshooting is based on a seven-layer OSI model that takes the guesswork out of the process. If network connectivity is the suspect, you should first run the **ipconfig** command to see if the network interface is disconnected. If that is not the case, you proceed to **ping** and its three tests—pinging the loopback address 127.0.0.1, then pinging the local IP address, and finally, pinging the default gateway address. (You will find these addresses in the **ipconfig** output.) To wrap it up, you should verify connectivity to the DNS server by pinging its IP address, and then run the **nslookup** command to resolve domain controller names. In firewalled networks, this may not be acceptable because pings in many cases are filtered out. In this case you would need to use telnet to connect on port 53 to verify connectivity to the DNS server and check availability of the service.

This being said, administrators often begin from the last step of this process; if it works, all underlying troubleshooting steps immediately become redundant. If you are able to telnet to the DNS server on port 53 using its hostname, you have tested all seven OSI layers successfully. This means your interface is connected to the network and you can ping the loopback, local IP, and, depending on the DNS server location in the network, the default gateway address as well. In other words, network connectivity problems are ruled out. You just have to make sure that the IP address returned by the DNS server is indeed the right address (DNS configuration may also be a problem). And in more complex routed networks, you might also want to run the **tracert** command from the client to the domain controller in question to make sure there are no routing loops and to see that packets are taking expected routes.



Recall the Netdiag utility from Chapter 4. It may save you time to start network troubleshooting with this tool. Depending on the results, you may need to fall back to other tools mentioned in this section, but if no problems are detected by Netdiag, it would make sense to proceed to the next phase in your troubleshooting—replication.

Correct name resolution is paramount in the group policy application process simply because clients need to be able to locate domain controllers in order to locate policy configuration and copy policy files. They use DNS to locate hostnames and IP addresses of the servers providing network services, preferably in their local Active Directory sites—services such as Active Directory. If there is a name resolution problem in the network, most likely, group policy will not be the only component of Active Directory that will be affected.

Policy Replication Issues

After you establish that network connectivity and name resolution are functioning as expected, the next thing to look at would be replication. Remember that group policy files are stored in SYSVOL shares on domain controllers, and the content of these shares must be consistent throughout your Active Directory environment. The File Replication Service (FRS) is used to replicate the content, so it is not actual Active Directory replication that you should be focusing on while troubleshooting group policy replication. That being said, it is vital to ensure that Active Directory replication also works, due to the fact that FRS uses the same connection objects (created manually and automatically), the same topology, and the same replication schedules as Active Directory.

Most of the tools that administrators use to troubleshoot AD/FRS replication are discussed in Chapter 4, in the section “Monitor Active Directory Replication.” The tools listed here can assist in obtaining a variety of diagnostic information regarding the health of the domain controller, replication partners, topology information, the latest replication attempts and outcomes, and so forth.

- **Dcdiag** This tool runs a series of diagnostic tests on a domain controller; these tests include replication and topology integrity checks.
- **Repadmin** This tool is used to analyze replication mechanisms in great detail. Repadmin exposes information such as the time stamp of the last successful replication, error codes if it was not successful, the history of all replication metadata, and replication settings, among many other things.
- **File Replication Service log in Event Viewer** The log provides a very convenient and fast way to verify whether FRS is having problems replicating SYSVOL data to other domain controllers.
- **FRS debug logs** Ntfrsapi.log files and Ntfrs_000X.log files (where X is a sequential number) located in the %systemroot%\debug folder also expose FRS configuration and diagnostic information that may capture detailed information as to what is causing the problem. These logs are not enabled by default. For more information on how to configure FRS logging, see the “Monitor File Replication Service” section in Chapter 4.
- **Ntfrsutil** This utility is used to view FRS tables, memory, and thread information, and may be helpful in troubleshooting complex FRS issues. It also allows for listing transactions from the FRS database (%systemroot%\ntfrs\jet\ntfrs.jdb).
- **Replmon** This allows you to view replication topology and replication information and settings, such as connection object properties, using a convenient GUI application.

- **Sonar.exe** Sonar is a GUI-based tool written specifically for FRS monitoring and troubleshooting. Administrators can use it to gather statistics on replicas and monitor traffic levels, backlogs, free space, and other parameters. This tool presents read-only information per each replication partner, not per connection or per session, so you might think of it as a more convenient way to get a view of your FRS landscape from 30,000 feet.



Sonar.exe is not included in Windows Server 2003 Support Tools, but it is featured in Windows Server 2003 Resource Kit. You can also download it separately from www.microsoft.com, Windows Server 2003 Downloads/Tools section. Along with the tool, when downloaded separately from the Resource Kit, Microsoft includes a lengthy white paper dedicated to troubleshooting FRS issues and providing an in-depth overview of how the service works and where and how it can be used.

Recovering from Group Policy-Related Disasters

There are several ways to back up and restore group policy objects. The SYSVOL share, located on all domain controllers and replicated by means of FRS, is used, among other things, for storing files that implement group policy settings. You should include SYSVOL shares in your backup routines and perform backups regularly. Microsoft discourages administrators from modifying SYSVOL share content and structure manually, even by restoring it from a backup. Microsoft knowledge base article 324175 discusses this in a fair bit of detail; it has to do with so-called juncture points.

You will want to avoid tampering with the structure of this share, so if you must restore group policies from a backup, it is recommended that you use advanced options in NTBACKUP (or use the appropriate option in backup software used in your company) to restore SYSVOL content to another directory and then copy actual policy files into the SYSVOL directory.

A more elegant solution to group policy backup and restore problems may be implemented using the Group Policy Management Console (GPMC). This console allows backing up and restoring individual group policy objects, giving administrators a flexible mechanism to implement GPO backups before and after policy object modifications are performed. This may also be indispensable in change management processes, in addition to disaster recovery, where administrators may require a quick and reliable way to back out of an unsuccessful policy change. Although it does not back up “external” configuration of group policy objects, such as WMI filtering, it does save GPO configuration information, which administrators can view later on when they restore GPOs.

12 Chapter 7: Managing and Maintaining Group Policy

Follow these steps to back up group policy objects (assuming that the GPMC is already installed):

1. Log on as domain administrator, click on Start | Run, type **gpmc.msc**, and press ENTER.
2. In the left-hand pane, expand your forest, expand the Domains container, expand domain GPOs that you want to back up, and then expand the Group Policy Objects container. You should see at least two GPOs listed there—Default Domain Controllers Policy and Default Domain Policy. Any additional GPOs you created in this domain should also appear in the list.
3. Right-click on the GPO you wish to back up, and click on the Back Up option in the context menu. The Back Up Group Policy Object dialog box will appear next.
4. Type in a backup location where you wish to save the group policy object, provide a description if necessary, and click Back Up. The Backup progress window will appear next.
5. When the process finishes, you will be presented with warning and error messages (if any). Click OK to finish.

Note that a GPO, when backed up, is not saved as a single file. Instead it is saved as a structure of folders, representing different configuration sections, and several files inside this structure.

The process of restoring a group policy object is likewise pretty straightforward:

1. Log on as domain administrator, click on Start | Run, type **gpmc.msc**, and press ENTER.
2. In the left-hand pane, expand your forest, expand the Domains container, expand the domain GPOs that you want to restore, and then expand the Group Policy Objects container.
3. Right-click on the policy object you wish to restore, and in the context menu, choose the option Restore from the Backup. A wizard welcome screen will appear.
4. Click Next to continue. You will be prompted to provide a location of the backup folder. Type in the path to the root of your backup folder and click Next.

5. The wizard will read the content of the folder provided and display existing backups for the group policy you are performing a restore on. Select the backup version you wish to restore, and click on View Settings if you wish to examine external configuration of this object. Click Next to continue.
6. The next screen provides a confirmation of what the wizard is about to do. Click Finish. The Restore progress window appears next. Once the restore operation is finished, you will be presented with warning and error information if applicable. Click OK to exit.

If you are trying to restore a group policy object that is no longer listed in the Group Policy Objects container, you may want to create a new group policy object and then use the context menu to import GPO settings from the corresponding backup. Just like restoring, importing does not re-create external settings such as WMI filtering, delegation, or GPO links; you would have to reconfigure this manually. Alternatively, you can restore any GPO from an existing backup, regardless of whether this GPO exists in Active Directory. To do this, you need to call up the Manage Backups screen by selecting the Manage Backups option in the Group Policy Objects container context menu.

Managing backups and restores in an organization of significant size may get more complicated than backing up one or two policy objects. To back up all of the policies at once, you can choose the Back Up All option in the Group Policy Objects container context menu. From the same context menu, you can also invoke the Manage Backups dialog box to take a look at all existing GPO backups and to view their “external” configuration at the time the backup was created.



Keep in mind that the GPMC delivers a set of COM objects that implement functionality delivered through the user interface tool. Administrators can write their own scripts or otherwise automate group policy management using the same objects. More information on this can be obtained from <http://www.microsoft.com/windowsserver2003/gpmcl>.

Finally, if an outage damaged the SYSVOL share or otherwise disabled your existing group policy objects, and you do not have a backup of SYSVOL or a backup of individual group policy objects, you will need to resort to the DcGPOFix utility, which restores the Default Domain Policy and Default Domain Controllers Policy to their original post-Dcpromo state. As you can see from the following code, this option should only be used in terminal cases where nothing else can be done to recover current versions of policies.

14 Chapter 7: Managing and Maintaining Group Policy

```
C:\Documents and Settings\Administrator.JOVIDUDE>dcgpofix
Microsoft(R) Windows(R) Operating System Default Group Policy Restore Utility v5.1
Copyright (C) Microsoft Corporation. 1981-2003
Description: Recreates the Default Group Policy Objects (GPOs) for a domain
Syntax: DcGPOFix [/ignoreschema] [/Target: Domain | DC | BOTH]
```

This utility can restore either or both the Default Domain Policy or the Default Domain Controllers Policy to the state that exists immediately after a clean install. You must be a domain administrator to perform this operation.

WARNING: YOU WILL LOSE ANY CHANGES YOU HAVE MADE TO THESE GPOs. THIS UTILITY IS INTENDED ONLY FOR DISASTER RECOVERY PURPOSES.

```
You are about to restore Default Domain policy and Default domain Controller policy for
the following domain
sales.flexecom.com
Do you want to continue: <Y/N>?
```

Policy Application Issues

When troubleshooting policy application issues, you will need to determine what is causing group policies to conflict or what is causing them to be ineffective.

Application, Inheritance, Blocking, No Override, and Loopback Processing

Inheritance and blocking are the most obvious places to start sorting out conflicts in complex Active Directory environments where one or two policies just don't cut it. Remember how group policies are applied: local policy is applied first (although it is not really a "group" policy, it may have an effect on local computer security settings), then site policy, followed by domain policy, followed by the OU policy. Policies on all four levels are processed and overwritten by those GPOs applied later in the process. Therefore, it would make things easier if group policies were designed to apply the bulk of settings on the least specific level—that is, site or domain—with only a few more particular settings applied on the most specific level—organizational units. If your OU structure features several levels and each of those levels has a link to its own GPO, policies will be processed in the order from least specific OU (parent levels) to the most specific OU (child levels).

Settings not explicitly defined in the policies that are applied in the later stages are inherited either from defaults, or from the policies applied earlier in the process, unless administrators modify the Blocking and No Override options. The No Override setting takes precedence over policy blocking. Of course, to quickly determine which policies are in effect, you can use Gpresult, as noted earlier in the chapter—it explicitly lists all effective policies for a given user and computer.

You have to keep one more thing in mind when figuring out the order of application of group policy settings: some setting areas between user and computer configurations overlap. If you configure the same setting in the computer configuration section and user configuration section, the end result will be determined based on the User Group Policy Loopback Processing Mode setting, as described in Chapter 6. Merge will add user settings to computer settings, Replace will cancel user settings and apply computer settings; by default, if there is a conflict of settings between user and computer configuration sections, computer settings receive higher precedence.

Security and WMI Filtering

Next, you need to look at GPO ACEs, also known as security filtering, and WMI filtering. Users need at least two rights granted to them, such as Read and Apply, in order to be able to apply policies. Not only that, you also need to make sure that none of the users who need to access the policies in question have membership in security groups that were assigned an explicit Deny on the group policy ACL list. Explicit Deny will prevent users from reading the policy, and therefore it will not be applied. You can access either the GPMC (if it is installed), or Active Directory Users and Computers (ADUC)/Active Directory Sites and Services (ADSS) consoles, to modify security filtering settings for each individual group policy object.

WMI filtering has similar effects on policy application in the sense that if your WMI filter does not match the user or computer in question, the policy will not be applied. To determine whether a policy was filtered out because of a WMI filter match (or lack of it), use Gpresult.

Disabled GPOs or Configuration Sections

Disabled GPOs or turned-off user or computer configuration sections also present a potential problem. GPOs can be disabled entirely or in portions, only affecting either user or computer configuration sections. You can check to see if these conditions are true using the same tools—Gpresult and ADUC/ADSS or GPMC (by checking properties of the respective policy objects).

GPO Links and Object Location in AD

Finally, GPO links should also be verified. First of all, they need to exist—that is, the policies should be applied to containers where you expect them to be applied. Second, if you are working with policy links that span several domains, you need to make sure that at least one domain controller is available in each domain. The reason is rather

straightforward: cross-domain policy links need trust relationships and authentication available to them in order to access a GPO not located in their own domain.

Another consideration when verifying group policy links is user or computer location in the OU structure. If it changes, the client may not be aware of the fact for about 30 minutes, because client computers cache their domain location information. If you need to enforce policy settings immediately, you must make sure that the user logs off and logs back on (if the user account location changed), or reboot the client computer (if the computer account location changed).

Policy Tattooing

Last but not least, you might want to ensure that policy tattooing is not preventing your settings from becoming effective on target machines. The concept of policy tattooing needs to be explained a little further. *Tattooing* refers to custom registry settings applied with group policies that are persistent in nature. Administrators who worked with System Policies in Windows NT 4.0 should remember how this older implementation of group policies used to work: when you configure settings using `poledit.exe` and distribute these settings in `ntconfig.pol` files through NETLOGON shares, they are committed to the registry and will not revert to their original state, unless another policy is applied that explicitly assigns original values. In other words, user logoff, computer reboot, and removal of policy assignment would have no effect on the modified registry values on client machines—settings are persistent.

In contrast to Windows NT 4.0-style policies, Windows 2000 (and Windows Server 2003) group policies distribute nonpersistent settings: user configuration is removed every time the user logs off, and computer configuration is likewise lost upon reboot. If you revoke an assigned policy, client systems will likewise pick it up upon the next policy refresh. All is well then, right? Not if you use custom administrative templates that apply registry settings to keys that are not maintained by the group policy engine.

example

Watch

An easy way to distinguish these settings is that nonpersistent settings appear in a GPO with a blue icon, and persistent/tattooed policy settings appear with a red icon.

If you apply computer settings to `HKEY_LOCAL_MACHINE\SOFTWARE\Policies` or `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies`, and user settings to `HKEY_CURRENT_USER\SOFTWARE\Policies` or `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies`, then tattooing

will not be a problem in your network. However (and you've probably guessed it by now), this depends on how the software you manage with group policies has been engineered. If your applications were not written to store their settings in the keys mentioned here, you may have to deal with occasional tattooing problems.

Logging Policy Processing Information

Policy processing logging may shed light on internal errors that happen during the processing and application of policy files. What you are looking for is the `userenv.log` log file located in the `%systemroot%\debug\usermode` folder. By default though, this log file is disabled. To enable it, you need to modify registry settings to add the `UserenvDebugLevel` value to the `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon` registry key. You need to assign this `REG_DWORD` setting a value of `0x10002`. This modification kicks in on the fly, and you should start seeing some diagnostic information logged in the `userenv.log` file the next time a policy refresh is performed (every 90 minutes, or whenever triggered manually).

For performance reasons, the active log file will rotate during the logon if its size is over 1MB. A new `userenv.log` file is created while the existing one is saved as `userenv.bak`. `Userenv.log` will keep growing in excess of 1MB during the user session. Here is an example of what you should expect to see in the log:

```

USERENV(1b8.168) 20:37:30:262 ProcessGPO: Searching
<CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=sales,DC=flexecom,DC=com>
USERENV(1b8.168) 20:37:30:262 ProcessGPO: Machine has access to this GPO.
USERENV(1b8.168) 20:37:30:262 ProcessGPO: GPO passes the filter check.
USERENV(1b8.168) 20:37:30:262 ProcessGPO: Found functionality version of: 2
USERENV(1b8.168) 20:37:30:262 ProcessGPO: Found file system path of:
<\\sales.flexecom.com\sysvol\sales.flexecom.com\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}>
USERENV(1b8.168) 20:37:30:272 ProcessGPO: Found common name of:
<{6AC1786C-016F-11D2-945F-00C04fB984F9}>
USERENV(1b8.168) 20:37:30:272 ProcessGPO: Found display name of: <Default Domain
Controllers Policy>
USERENV(1b8.168) 20:37:30:272 ProcessGPO: Found machine version of: GPC is 1, GPT is 1
USERENV(1b8.168) 20:37:30:272 ProcessGPO: Found flags of: 0
USERENV(1b8.168) 20:37:30:272 ProcessGPO: Found extensions:
[ {827D319E-6EAC-11D2-A4EA-00C04F79F83A} {803E14A0-B4FB-11D0-A0D0-00A0C90F574B} ]
USERENV(1b8.168) 20:37:30:272 ProcessGPO: =====
USERENV(1b8.168) 20:37:30:272 GetGPOInfo: GPO Local Group Policy doesn't contain any data
since the version number is 0. It will be skipped.
USERENV(1b8.168) 20:37:30:272 GetGPOInfo: Leaving with 1
USERENV(1b8.168) 20:37:30:272 GetGPOInfo: *****
USERENV(1b8.168) 20:37:30:272 ProcessGPOs: Logging Data for Target <JOVIDUDE>.
    
```

18 Chapter 7: Managing and Maintaining Group Policy

```
USERENV(1b8.168) 20:37:30:302 ProcessGPOs: OpenThreadToken failed with error 1008,  
assuming thread is not impersonating  
USERENV(1b8.168) 20:37:30:302 ProcessGPOs: -----  
USERENV(1b8.168) 20:37:30:302 ProcessGPOs: Processing extension Registry  
USERENV(1b8.168) 20:37:30:302 ReadStatus: Read Extension's Previous status successfully.  
USERENV(1b8.168) 20:37:30:302 CompareGPOLists: The lists are the same.  
USERENV(1b8.168) 20:37:30:302 CheckGPOs: No GPO changes and no security group membership  
change and extension Registry has NoGPOChanges set.
```

This is just a tiny portion of the full log, and the amount of detail it delivers about the processing, as you can see, is remarkable. You don't want to keep it logging for no reason though. As you know, excessive logging and auditing is taxing, and small things tend to add up and slow the system down.

If your environment relies heavily on group policy, and its functionality is critical while group policy files are modified quite often, you may also want to enable verbose group policy logging in the Event Log to see a bigger picture. To achieve this, you need to add a REGDWORD value `RunDiagnosticLoggingGroupPolicy` to the `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics` registry key and assign it a value of 1.

This will cause a significant portion of diagnostic group policy information to be logged in the Application log; so depending on your log settings, you might want to increase its size or change the log record retaining mode to overwrite as needed. Otherwise, this registry setting will cause your application log to fill up rather quickly.

Administrators are better off troubleshooting GPO problems using `userenv.log` because, even with verbose logging, information logged in the Event Log will not reveal some errors and warning messages that are logged in `userenv.log`.

Generally, this log should be used to confirm that there are no group policy core failures or client-side extension failures. Core failures result in total loss of group policy processing and application due to reasons outlined earlier in this chapter: network connectivity problems, DNS resolution issues, or inconsistent SYSVOL content (replication issues). Client-side extension failures may result in individual policy sections being skipped. Areas that may be affected by this problem include software distribution, scripts, folder redirection, IPSec settings, administrative templates, and security settings, all of which are implemented using separate client-side extensions. `Userenv.log` will help you confirm whether each of these extensions was processed correctly, whether changes in policy were detected, and so on. A typical example of a problem that may cause script client extension errors is incorrectly defined script paths.

CERTIFICATION OBJECTIVE 7.02

Troubleshoot Group Policy Software Installation Issues

In the final section of this chapter, we will look into some aspects of using group policy objects and software management, as well as troubleshooting of problems commonly associated with this technology. You may recall from Chapter 6, in the section “Installing Software Using Group Policies,” that administrators need to use MSI packages (or ZAP files in worst-case scenarios) in order to install software, and that the software can be assigned or published (assigned to users or computers, or published to users).

If your software package is assigned to a computer object, it will install the next time the workstation is rebooted, before the logon prompt is displayed. If the package is assigned to a user object, administrators can either force software installation upon user logon or trigger installation if the user clicks on application icons or attempts to open files associated with the yet-to-be-installed application. Publishing software packages is only available to users, and applications published through group policies can be found in the Add/Remove Programs applet in Control Panel.

When dealing with software installation issues, potential problems can be divided into three main categories: client-side extension problems, group policy processing or application problems, and Windows Installer problems. Since group policy processing and application problems were reviewed earlier in the chapter, we will skip to client-side extensions and Windows Installer.

A large portion of the errors and warnings generated from software distribution-related processes is published to the Event Log, Application log section. The source of these events appears as Application Management. Typical software distribution errors, such as those generated during installation due to insufficient free space or inability to access the distribution point, are logged by MsiInstaller, also in the Application section of the Event Log.

However, if the logging level configured by default does not reveal enough details about why the installation is failing, you may need to enable verbose logging. This can be achieved by adding the REGDWORD value Appmgmtdebuglevel to the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\

Diagnostics registry key and assigning it a value of 0x0000009b. Doing so will force the software installation client-side extension of the group policy engine to perform extensive logging using the %windir%\debug\usermode\appmgmt.log file.

MsiInstaller can also be configured to perform verbose logging. To enable this, add the following values to the HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer key:

- Debug = REGDWORD 0x00000003
- Logging = REGSZ “voicewarmup”

Once these values are configured, MsiInstaller will start logging in two separate directories, depending on what sort of installation is being performed:

- %systemroot%\temp\MSI*.log
- %temp%\MSI*.log

Outside of logging and all other troubleshooting methods, and group policy application, replication, and refresh concerns discussed to this point, keep in mind the following information:

- Paths to distribution shares should not contain IP addresses or domain names. They should be UNC paths made up of hostnames and sharenames, as in \\servername\sharename.
- The software distribution point must be accessible to client computers. If there is a network problem or permissions issue, installations will most likely fail. Computers use the local system account when accessing distribution shares.
- Distribution shares should not be hosted by Windows NT 4.0 servers or older. They are not supported by software installation in group policies.
- The distribution share must be in the same Active Directory forest.
- Software distribution (publishing) will not work on servers running Terminal Services in application mode.
- If you assign applications to users, desktop icons may not appear until the user logs off and logs on again.
- MsiInstaller installations triggered by group policy are executed with elevated permissions. ZAP installations of legacy applications require users to have either Power User or Administrator privileges on the local machine.

Software Update Services and Windows Update

Patch and service pack distribution may be somewhat troublesome using group policies for several reasons. First, Microsoft may not always provide MSI packages; most commonly, patches are released as executable files. This creates more work for administrators if they are to create their own MSI packages. Second, it would not be practical to maintain a list of dozens, if not hundreds, of patches in your group policies. Group policy objects would take more space and network bandwidth and would be more resource intensive to process and nearly impossible to manage, as some patches get revised and updated, and others are added almost on a daily basis.

An optional workaround to using group policies is to manually download all the patches into a centralized location and create an install script that applies these patches. Although acceptable, depending on the size of the network, this may also be counterproductive. Microsoft originally came out with the Automatic Update service that can be set to check for updates on a periodic basis, alerting users to the fact that new updates are available for their platform, and optionally downloading and installing the patches. This service, at the time, was the best alternative, and here's a piece of good news: it is fully configurable through group policies.

Still, two problems existed in the early going. First, Microsoft did not initially provide an option not to reboot computers automatically after the patches were installed. It was a good alternative to manual installation, to MSI packages, and to asking users to run Windows Update, but it did create the problem of user workstations running important overnight processes getting rebooted without warning. The second problem with individual patch download from the Internet is bandwidth—it has to be available, and it has to be sufficient for all computer nodes to download those latest service pack distributions. That's 120+ MB times the number of managed computers—not very efficient.

Enter Software Update Services (SUS). The SUS concept is essentially the same as Windows Update and Automatic Update combined, but it introduces some important improvements to the patch management process that may suit many production environments. It replaces the Windows Update online servers with an internal company server running SUS. This eliminates the need to download patches more than once, thus preserving bandwidth. In addition, individual servers no longer need the Internet connection and the ability to talk to the outside world, communicating directly with the Microsoft update services (and this is not to mention MSBLAST-type worm scenarios when Microsoft's online servers are offline).

The new process essentially allows system administrators to review, download, and test patches locally. Once approved, they are published on the internal SUS server, and become available to Windows clients and servers. The SUS server is implemented as a system service called Software Update Services Synchronization Service. It is provided with an HTML-based management console where administrators can define the synchronization schedule (when your SUS server should poll updates from Microsoft).

The first synchronization cycle needs plenty of time and bandwidth, as your SUS server will be downloading hundreds of megabytes of updates. From that point onward, it is practical to set up the synchronization process to occur nightly. You will also use this HTML console to review and approve patches and service packs. Nothing will be made available to local clients by default, unless updates have been approved by an administrator. By default, this management console is configured on the local IIS server and is accessible through `http://servername/SUSadmin`.

On the client side (with clients being desktop or server systems), the Automatic Update service is configured to work with the local SUS server. SUS needs either Active Directory or, in the absence of it, a slight modification in the registry that tells the update service on client systems where to look for updates. Since our discussion is Active Directory-centric, we will continue accordingly.



The SUS server is available for free from <http://www.microsoft.com/sus/>. As of this writing, the latest version is SUS 1.0 SPI. The SUS client is called Automatic Update, it runs as a system service, and it is configurable using its own Control Panel icon. The SUS client is included in Windows 2000 SP3 and later, and in Windows XP and Windows Server 2003. It is also downloadable. You must update the Automatic Update client on pre-SPI Windows XP computers in order to include pre-SPI Windows XP computers into your SUS management game plan.

Let's fire up GPEdit.msc and see how to configure Windows Update using group policies.

EXERCISE 7-2

Using Group Policies to Configure the Windows Update/SUS Client

In this exercise you use the GPOE console to view and modify group policy object settings as they pertain to Windows Update.

1. Log on to the network using the administrator account.
2. Click on Start | Run, type **gpedit.msc**, and press ENTER.
3. The settings we are after are located in the computer configuration portion of group policies, Administrative Templates, Windows Components, and finally, Windows Update. Go ahead and expand these containers.
4. Configure the Automatic Updates option. This is the main configuration setting for choosing the mode of operation for Automatic Update and defining the polling schedule. This configuration works with or without an intranet SUS server. In the absence of an intranet server, it will simply configure the Automatic Update client service to poll Windows Update servers maintained by Microsoft (unless Windows Update is disabled—see the following information). Options available for the mode of operation are Notify for Download and Notify for Install, Auto Download and Notify for Install, and Auto Download and Schedule the Install.
5. Use the Specify Intranet Microsoft Update Service Location option to add your intranet SUS server. Here, you need to specify two URLs: one for the patch download and another one for the statistics upload.
6. The Reschedule Automatic Updates Scheduled Installations setting can be used to reschedule the installation process *N* minutes after the system boot process is complete in cases when a previously scheduled installation was missed.
7. The No Auto-Restart for Scheduled Automatic Updates Installations setting is useful if you want to prevent automatic reboots upon patch installation. Enable it to reduce the stress level of users who leave important processes running on their workstations overnight.
8. One last group policy setting that concerns Windows Update can be found in the user configuration section, Administrative Templates, Windows Components, Windows Update. If you switch to this container, you will see one setting: Remove Access to Use All Windows Updates Features. If this setting is configured, it effectively removes the Windows Update/SUS Client functionality from your clients.

Remember that these settings are only supported by Windows 2000 SP3 or later, Windows XP Professional SP1 or later, and Windows Server 2003 computers. Microsoft did not support installing service packs prior to SUS SP1.

SCENARIO & SOLUTION

<p>What is the difference between logging mode and planning mode in RSoP?</p>	<p>Logging mode is used to display actual permissions applied for a specific computer and specific user during the natural course of group policy processing and application, whereas planning mode is a simulation process of applying a given policy to a selected user and computer. Logging mode is useful in troubleshooting, whereas planning mode is more suitable for designing group policy settings and hierarchy.</p>
<p>What is policy tattooing?</p>	<p>Tattooing refers to custom registry settings applied with group policies that are persistent in nature. They are committed to the registry and will not revert to their original state, unless another policy is applied that explicitly reverts original values.</p>
<p>Why is it important to ensure that FRS is healthy and file replication works well?</p>	<p>FRS is responsible for replication of the SYSVOL share content between domain controllers. In terms of group policies, if SYSVOL shares are inconsistent, the client will get unpredictable results when attempting to apply policy settings.</p>
<p>How do you restore default group policies in the event that they are deleted?</p>	<p>First, try restoring individual policies from a recent backup using the GPMC. If none exist, restore the SYSVOL share to an alternate location and copy policy files into the actual SYSVOL share. If no SYSVOL share backups exist, you will need to use DcGPOFix to revert to post-Dcpromo versions of default policies.</p>

Using SUS and group policy together can fully automate patching and make prompt deployment of the latest security updates enterprise-wide a breeze. The only portion of the process that administrators will still have to take care of is patch QA testing and timely approval using the SUS console.

CERTIFICATION SUMMARY

The closing chapter of this book described troubleshooting techniques and mechanisms available in Windows Server 2003. We started with an exercise on how to use the RSoP tool in logging mode to collect effective user and computer settings from a machine you

are troubleshooting, and then covered details of the Gpresult tool. We then moved on to look at tools for refreshing group policy settings, such as Gpupdate.

If a problem persists after reviewing effective settings, modifying group policy objects, and refreshing policy settings, you may need to move on to the next stages of troubleshooting. Network troubleshooting steps and tools were discussed, and then you learned why replication problems and FRS are important factors when troubleshooting group policy.

You need to ensure that there is a backup of every piece of the system you are dealing with; however, having a full backup of everything may not necessarily satisfy various recovery scenarios. In the event of a lost policy, you want to have a quick and efficient way of restoring the necessary files from a backup, certainly avoiding downtime, or even worse, Active Directory rollbacks. The GPMC tool allows backing up and restoring individual policies in a way that is transparent to the rest of the system and its users.

Next, you need to go through the group policy application process with a fine-tooth comb. Concepts such as inheritance, blocking, no override, loopback processing, security and WMI filtering, disabled GPOs or configuration sections, failed or missing GPO links, object location in Active Directory, and finally, policy tattooing all have distinct effects on the end result. If the environment you are dealing with is complex due to its nature and/or poor planning, collecting information that deals with these concepts and how they are being used in your environment would be step one of any troubleshooting initiative. You may also need to look into the internals of group policy processing (verbose logging of various components will help achieve this).

The final section of the chapter covered some basic information pertinent to software installation troubleshooting and the advantages of using Software Update Services (SUS) in Windows Server 2003 networks.



TWO-MINUTE DRILL

Troubleshoot Issues Related to Group Policy Application and Deployment

- Use RSoP in logging mode to get a full set of effective permissions.
- Gpresult should be used to collect policy information on a machine; it can identify specific policies that were applied and filtered out.
- Gpupdate is the Windows Server 2003 equivalent of **secedit /refreshpolicy** on Windows 2000.
- For troubleshooting network issues related to group policy application, you can use tools like Netdiag, Dcdiag, NSLOOKUP, and the **tracert** and **ping** commands.
- FRS is used to replicate SYSVOL content (and group policies) between domain controllers. It uses the same replication engine as Active Directory.
- Backup and restore of individual policies is possible using the GPMC. You should also back up the SYSVOL share, but it is not recommended to restore its contents directly from backup to the original location.
- When troubleshooting policy application issues, pay special attention to inheritance, blocking, no override, loopback processing, security and WMI filtering, disabled GPOs or configuration sections, failed or missing GPO links, object location in Active Directory, and policy tattooing.
- Userenv.log can be enabled through the registry to expose detailed information about group policy application and processing.
- The Event Log can be switched to display verbose information about group policy application and processing.

Troubleshoot Group Policy Software Installation Issues

- When troubleshooting issues related to software installation with group policies, look at group policy processing, client-side extension problems, and Windows Installer issues.
- MsiInstaller and software installation client-side extensions keep separate logs, but they are not enabled by default. A limited amount of information is posted to the Event Log.
- You can use the SUS server with Automatic Updates on client machines to distribute patches and service packs automatically. Group policies can be used to configure Automatic Update on client machines to get Windows updates from your intranet server.

SELF TEST

The following questions will help you measure your understanding of the material presented in this chapter. Read all the choices carefully because there might be more than one correct answer. Choose all correct answers for each question.

Troubleshoot Issues Related to Group Policy Application and Deployment

1. You are troubleshooting group policy application issues. Objects in one of the OUs do not get the settings from the Default Domain Policy. Clients from that OU do not complain of any problems logging on or accessing Active Directory search functions. What is likely to be causing this issue? (Choose all that apply.)
 - A. Failed GPO link
 - B. Policy is blocked
 - C. Client-side extensions fail to process policy
 - D. Policy is disabled
2. You want to enable detailed logging of group policy processing and application. How would you achieve this? (Choose all that apply.)
 - A. Use the Event Log.
 - B. Turn on verbose logging.
 - C. Use the userenv.log log.
 - D. Turn on userenv.log.
3. You are troubleshooting a policy application issue, and you need to find out which policies were applied on a client computer. Which of the following tools can you use? (Choose all that apply.)
 - A. RSoP in planning mode
 - B. RSoP in logging mode
 - C. Gpresult
 - D. Help and Support console
4. You need a list of all custom registry settings applied to a client machine. How would you do this using Gpresult?
 - A. Use the /z switch.
 - B. Use the /v switch.
 - C. Don't use any switches.
 - D. Gpresult cannot collect this information.

28 Chapter 7: Managing and Maintaining Group Policy

5. Your company is developing a custom office productivity application. Software developers ask your advice on how they should develop the configuration mechanism of a few application parameters. You want to manage this application using group policy. What should you suggest? (Choose all that apply.)
 - A. Use schema modification.
 - B. Use logon scripts and use group policy to deploy them.
 - C. Create a custom .adm registry file configuration, and use group policy to deploy it.
 - D. Store application registry settings in keys supported by the policy engine to avoid tattooing.
6. You want to enable userenv.log logging. How should you configure values in the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon key to achieve this? (Choose all that apply.)
 - A. Set Appmgmtdebuglevel to 0x0000009b.
 - B. Set Debug to 0x00000003.
 - C. Set UserenvDebugLevel to 0x10002.
 - D. Set RunDiagnosticLoggingGroupPolicy to 1.
7. Your company has offices on three continents. You are an administrative delegate responsible for group policy implementation in the South African branch. The Active Directory environment is implemented as one domain with three sites and a comprehensive OU structure. You attempt to open one of the group policy objects in the Group Policy Object Editor but get an error. You verify group policy permissions and confirm that you have Read access. What is the most likely cause of this problem?
 - A. In order to use the Group Policy Object Editor, you have to have the Full Control access right for the group policy objects in question.
 - B. You must be a member of the Domain Admins security group in order to use the Group Policy Object Editor.
 - C. In addition to Read rights, you need Change permission in order to modify object settings.
 - D. None of the domain controllers are available in your local site. Check whether they are online and accept connections as expected.
8. You are troubleshooting a policy application issue. Some of the settings you expect to be applied on the site level are not becoming effective. Upon further investigation, you find out that there are domain and OU policies that apply similar sets of settings. What is the most likely cause of this problem?
 - A. There is no problem; this behavior is by design.
 - B. There is not enough information to diagnose the problem. You should enable userenv.log logging and look into GPO processing.

- C. Set the No Override option on the site-level policy to enforce its settings.
 - D. You should enable verbose logging in the Event Log to collect more information about client-side extension processing of policy settings.
- 9.** After extensive planning and a bit of tinkering, you have created a policy that fits all requirements. Knowing that it will have to be modified sooner or later, you need to make sure that you have a backup in case you ever need to restore this policy. Which of the following is the optimal strategy?
- A. System state backup
 - B. SYSVOL folder backup
 - C. GPMC policy backup
 - D. This cannot be done.
- 10.** What is the purpose of RSoP planning mode and RSoP logging mode?
- A. RSoP planning mode allows you to plan policies for Windows XP and Windows 2000 clients.
 - B. RSoP planning mode CIMOM database is compiled by an emulator service based on assigned group policies. RSoP logging mode is used to see the content of the CIMOM database that was compiled as a result of the actual policy application.
 - C. RSoP planning mode does not process security policies.
 - D. RSoP planning mode and RSoP logging mode differ in how you can view and save the results.
- 11.** You are troubleshooting a group policy application issue. You notice that group policy is not applied to some members of the security group, which is located in one of the OUs that is a child of a parent OU where the policy is applied. What is the most likely cause of this problem?
- A. Check to see if the policy is blocked on the child OU level.
 - B. Check to see if the policy is disabled.
 - C. This is by design—policies are not applied to security groups, only to users and computers.
 - D. You need to link the child container to the GPO in question for the policy to become effective.
- 12.** You work for a consulting and software development firm. You need to troubleshoot a group policy application issue for one particular user. The rest of the users in the same OU have no problems applying this policy. Upon investigation, you discover that the policy in question is not getting to the client computer, but there are no network problems reported or observed on this machine. What is the most likely cause of this problem?
- A. The policy may be blocked for this particular user.
 - B. Check user membership in security groups, especially if some of them have Deny on the ACL of the policy in question.

30 Chapter 7: Managing and Maintaining Group Policy

- C. The user configuration section may be turned off.
 - D. Check to make sure that the policy is not disabled for this user.
13. You are deploying a few legacy applications that do not have associated MSI packages. How can you do this? (Choose all that apply.)
- A. Create an installation package using Windows Installer.
 - B. Use ZAP files.
 - C. Use a custom setup script to launch setup.exe.
 - D. You cannot install applications that do not have MSI packages.
14. You are troubleshooting a group policy issue. The Default Domain Policy and Default Domain Controllers Policy appear to be corrupt. Upon investigation, you determine that there are no backups of policy taken using GPMC or by direct file backup of the SYSVOL share. What should you do to resolve the issue?
- A. Use the Dcpromo utility.
 - B. Use the Ntdsutil utility.
 - C. Use the Dcdiag utility.
 - D. Use the DcGPOFix utility.
15. The concept known as policy tattooing is best described by which of the following?
- A. Applying registry settings to keys not maintained by group policy
 - B. Applying custom registry settings
 - C. Applying system policies using *.pol files
 - D. Applying custom ADM administrative templates
16. Which of the following events trigger group policy refreshes?
- A. Computer boot sequence and user logon process
 - B. Refresh interval expiration
 - C. Execution of the Gpupdate tool in Windows XP or **secedit** in Windows 2000.
 - D. Clicking OK in the Group Policy Object Editor.
17. Which of the following statements about user environment policies are correct?
- A. User and computer environment policies modify different registry sections.
 - B. User policies are only applicable to Windows 2003/XP clients.
 - C. User policies are applied only upon user logon, whereas computer policies are applied at the end of the boot process and upon user logon.
 - D. User policies are applied only upon user logon, whereas computer policies are applied at the end of the boot process.

Troubleshoot Group Policy Software Installation Issues

- 18.** Your network is running an SUS server, and group policy is used to configure client computers to retrieve updates daily. However, after a while you notice that SUS updates are not taking place, and whenever you try running Windows Update manually, you get an error. What is the most likely cause of this problem? (Check all that apply.)
- A. Policy loopback processing is configured incorrectly.
 - B. Remove Access to Use All Windows Updates Features has been enabled.
 - C. The SUS server is not synchronized with Microsoft Windows Update servers.
 - D. The SUS administrator has not approved any updates yet.
- 19.** You are configuring software distribution packages for your organization. You verified that group policy objects are applied on client machines successfully and that they are up-to-date, yet somehow software distribution changes are not becoming effective on user workstations. What is the most likely cause of this issue? (Choose all that apply.)
- A. For published software distribution changes to become effective, users have to log off and log on again.
 - B. For assigned software distribution changes to become effective, computers have to be rebooted.
 - C. There may be something wrong with policy processing. Enable userenv.log to gather details.
 - D. User accounts must be able to access software distribution shares in order for software packages to be downloaded successfully.
- 20.** You are troubleshooting MSI package installation problems. You log on using the administrator account and enable MsiInstaller logging using the registry settings. What are the locations of these log files? (Choose all that apply.)
- A. C:\Windows\System32\LogFiles\MsiInstaller\MSI*.log
 - B. C:\WINDOWS\Debug\UserMode\MSI*.log
 - C. C:\Windows\temp\MSI*.log
 - D. C:\Documents and Settings\Administrator\Local Settings\Temp\MSI*.log

SELF TEST ANSWERS

Troubleshoot Issues Related to Group Policy Application and Deployment

- B** is correct. In this scenario, the policy is most likely blocked for this individual OU.

A is incorrect. The Default Domain Policy is applied on the domain level by default and not on the individual OU level; hence, OUs do not have a GPO link, and the policy settings are applied by virtue of inheritance. **C** is incorrect because client-side extensions are only responsible for subcomponents of the group policy, such as scripts and folder redirection, and not the bulk of standard settings. **D** is an unlikely candidate here due to the fact that the policy is only having problems in one of the OUs.
- C** and **D** are correct answers. In this situation you will need to use the `userenv.log` log file, but since it is not enabled by default, you will also need to turn it on.

A is incorrect because the Event Log does not provide enough information about group policy processing; it may log severe errors and warnings of major significance, which only alerts you to a problem and carries no information about policy processing. **B** is incorrect. Although verbose logging through the Event Log will reveal more details about the process, it still will not log all of the errors and warnings, and in addition, it will result in the Event Log flooding, putting additional stress on the system.
- B**, **C**, and **D** are correct answers. All of these tools can be used to display information about effective group policies, with varying levels of detail.

A is incorrect because planning mode only runs a simulation and does not present actual applied settings.
- A**. The `Gpresult /z` switch enables super-verbose output and will display required registry information with any level of precedence.

B is incorrect. Although the `/v` switch will enable verbose output and result in extensive information being displayed, it may not list all of the settings, depending on their precedence level. **C** is incorrect because you need to use one of the verbose switches to see this information. **D** is incorrect because `Gpresult` can be used for this purpose.
- C** and **D** are correct answers. The ADM file is flexible, manageable, and a simple enough way to configure client computer registry settings with group policies. By applying these settings to dynamic registry keys serviced by group policies, administrators can avoid tattooing policy settings elsewhere in the registry.

A is incorrect because schema modification is a complex process that may or may not be suitable. You will be forced to develop your own way to configure these settings. **B** is incorrect because this method is more complex than **C** and **D**, and it may not perform consistently 100 percent of the time.
- C**. Setting `UserenvDebugLevel` to 10002 (hex) in the registry key presented in the question will achieve the desired result.

- A, B, and D** are incorrect. All of these values are valid for other logging purposes and not for the registry key in question.
- 7.** **A.** To be able to open a group policy object in the GPEdit.msc console, you need to have Full Control rights on the object in question.
- B, C, and D** are incorrect. Domain Admin membership would achieve the desired result, but in this case it may not be desirable to add a remote administrator to the Domain Admin group if all he or she needs to do is edit a group policy object. Likewise, if domain controllers are not available in the local site, an attempt will be made to access domain controllers in remote sites.
- 8.** **A.** Remember LSDOU: Local, Site, Domain, OU. The later in the process the policy is applied, the more effective it is. In this case, OU policy may be overwriting some of the settings set on higher levels.
- B, C, and D** are incorrect because **A** is correct.
- 9.** **C.** The GPMC console allows administrators to back up and restore group policy objects.
- A and B** are incorrect because copying SYSVOL via SYSTEMSTATE backup or directly from the file system will not allow you to restore group policy objects, but may help fix policy file corruption issues. **D** is incorrect because it can be done using GPMC. You can restore a policy object using a different name, without overwriting the existing object, if that is necessary.
- 10.** **A and B.** The main difference is how the group policy settings database is compiled.
- C** is incorrect because both modes process all applicable policies. **D** is incorrect because both modes allow viewing and saving results in a similar fashion.
- 11.** **C** is correct. Group policies are not applicable to security groups, only to user and computer objects.
- A, B, and D** are incorrect because **C** is correct.
- 12.** **B.** It is very likely that the user in question may be affected by some form of group policy filtering, either WMI or security. Checking to see if the user belongs to any security groups that may have an explicit Deny defined in the ACL of the group policy object in question would be step one.
- A** is incorrect because it is not possible to block policy on the user level. **C** is likewise incorrect because the question suggests that the policy in general works as expected for the majority of users. **D** is incorrect largely for the same reason.
- 13.** **A and B.** These are the correct ways to deal with situations if you have to install an application that did not come with an MSI package.
- C** is incorrect because this will not guarantee successful installation, and applications cannot be published this way. **D** is incorrect because you can use methods described in **A** and **B**.

34 Chapter 7: Managing and Maintaining Group Policy

14. **D**. The DcGPOFix utility is the intended solution in this question.
 A, B, and C are incorrect because none of them are designed to restore default policies. Ntdsutl may be used to restore the domain controller's SYSVOL and Active Directory to its predisaster state, but this is a very dramatic approach to the problem. Likewise, Dcpromo will fix the policies, but if there is only one domain controller, it will destroy the existing Active Directory environment. If there is more than one domain controller, then Dcpromo will copy corrupt policies from other domain controllers.
15. **A**. This is the correct answer that summarizes the rest of the options in the most generic way.
 B, C, and D, are incorrect. **B** is incorrect because it is possible to apply custom registry settings without tattooing them into registry keys not serviced by group policy. **C** is incorrect. While system policies are applied in a static fashion, they are not the best description of what tattooing is. **D** is incorrect because it is possible to apply ADM templates in a dynamic fashion, as long as they modify dynamic registry keys.
16. **A, B, and C**. All of these events trigger group policy to be refreshed.
 D is incorrect because the GPEdit console does not really have OK or APPLY buttons that are applicable to policies and not to their properties or specific settings. Only clients can request and apply policy objects. Forced update from a central location would grind the network to a halt if it triggers, say, a few dozen concurrent installations of Microsoft Office.
17. **A and D**. User and Computer sections of the policy modify different registry areas and apply at different stages.
 B and C are incorrect statements.

Troubleshoot Group Policy Software Installation Issues

18. **B** is correct. If you configure Remove Access to All Windows Updates Features, Windows Update will get disabled on the computers affected by this policy.
 A is incorrect because loopback processing has no effect in this case, due to the fact that the policy settings in question do not overlap. **C** and **D** are incorrect because, although they are required before any internal update will take place, they would not be causing an error message or preventing users from running a manual Windows Update process using the Internet.
19. **A and B** are correct. In order for the software distribution changes to become effective, a logoff/logon event or a reboot event must occur first, depending on the distribution method.
 C is incorrect, because **A** or **B** should be done first before any troubleshooting takes place. **D** is incorrect because user accounts are not used to access distribution shares; local system accounts are used to download packages.
20. **C and D** are correct. These are the correct locations for log files, providing that default environment variables and Windows amd user profiles locations have not changed.
 A and B are incorrect because MsiInstaller log files are not maintained in these directories.