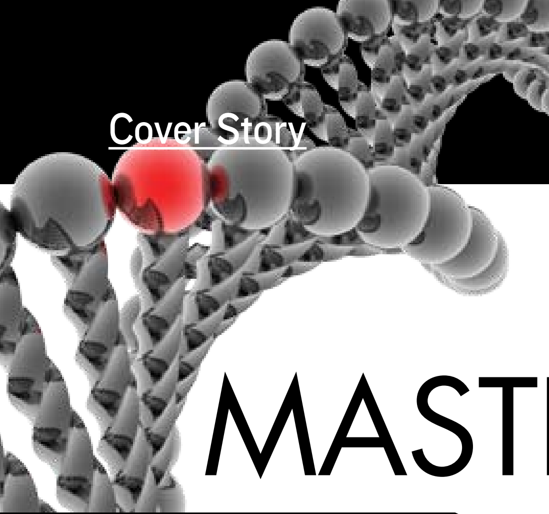


Cover Story

MASTERING RSoP

Your first step to Group Policy health

by Darren Mar-Elia

I spend a fair bit of time helping folks figure out problems with Group Policy. In the 8+ years I've been doing this, by far the biggest improvement in Group Policy management has been the introduction of the Resultant Set of Policies (RSoP) capability in Windows Server 2003 and Windows XP to help us figure out what the effective policy is on our desktops and servers. Understanding what RSoP is and knowing how to read an RSoP for a user or computer will help you ensure Group Policy is healthy and happy in your environment. And, while RSoP won't help solve every Group Policy problem that arises, an RSoP can point the way toward how to further investigate.

What Is RSoP?

The first thing to understand about the RSoP feature in Windows is that it's technology that Microsoft built into the Windows Management Instrumentation (WMI) infrastructure beginning with Windows XP. RSoP doesn't support Windows 2000 because Win2K's WMI infrastructure and Group Policy engine don't include the necessary components to collect RSoP information. The Windows 2000 Resource Kit does ship with a command-line utility called gpresult .exe that provides some of the information that RSoP delivers, but this first-try Gpresult doesn't paint as complete a picture of policy processing as the later RSoP.

When XP and later versions of Windows were introduced, Microsoft provided two main tools for accessing the WMI-based RSoP infrastructure. The Microsoft Management Console (MMC) Group Policy Management Console (GPMC) snap-in provides a graphical UI for accessing RSoP data, and the command line–based Gpresult is built into the OS. Don't confuse the RSoP-enabled version of Gpresult with the earlier Win2K Resource Kit version. Because the two tools use completely different mechanisms, they can return different information, with the RSoP-enabled version being the more accurate of the two.

So what exactly is RSoP? Well, essentially it's a mechanism to determine, for a given computer or user in Active Directory (AD), what that computer or user's effective Group Policy settings are. A user or computer can process many Group Policy Objects (GPOs) in a typical AD environment—with GPOs having possibly conflicting settings. GPOs are processed in a certain order that affects which policy settings will actually apply to a given user or computer, and GPOs can be filtered by using security groups and WMI filters. Given all these factors, you can see how knowing what the effective policy settings are for a given user or computer can be hard, especially in larger organizations. RSoP cuts through the confusion and tells you what's happening with your Group Policy settings.

RSoP Planning vs. Logging

The RSoP capability in Windows Server 2008, Windows Vista, Windows Server 2003, and XP comes in two flavors. The first, and by far the most common, is known as RSoP or Group Policy Results Logging. (Group Policy Results is the more common name for RSoP.) Group Policy Results Logging, as the name implies, lets you see what policies were applied to a given Windows computer or user. It answers the question, "What policy settings were processed by a given computer or user during the last policy processing cycle?" Logging relies on the Group Policy engine and each Client Side Extension (CSE) that processes the various policy settings to report to WMI on what it did when Group Policy was processed. When you run a GPMC Group Policy Results Logging report, which Figure 1, page 34, shows, or use Gpresult from your XP or Vista machine, you're essentially connecting to the machine you select—local or remote—and gathering the WMI logging data into a report.

The second RSoP flavor, RSoP Planning (also known as Group Policy Modeling in GPMC), answers the question, "What policy should apply to a given computer or user during a future policy processing cycle?" As the name implies, RSoP Planning lets you perform a "what-if" calculation on the policy that a given

Learning Path

***WINDOWS IT PRO* RESOURCES**

For help troubleshooting Group Policy:

"Troubleshooting Group Policy–Related Problems," InstantDoc ID 44983

To use RSoP from the command line and in scripts:

"How can I view the Resultant Set of Policy (RSOP) from the command line?" InstantDoc ID 97129

"GPMC Scripting," InstantDoc ID 39529

To gather Group Policy deployment info for multiple computers or users:

"Monitor GPO Deployment," InstantDoc ID 50256 computer or user will receive. It goes one step better and lets you play with changes that might occur to users or computers to see what effect the changes will have on the users' or computers' effective policy.

For example, you can virtually move the user or computer into a new organizational unit (OU) or new security group to see how that will impact its effective policy. You can also simulate how policy would be affected if a slow network link were detected or if loopback policy were in place. All of these "modifications" that you can perform during the modeling phase will affect what policy settings a computer or user receives, and the Group Policy Modeling feature in GPMC lets you simulate these changes easily.

Unlike Group Policy Results, Group Policy Modeling doesn't require you to query a particular target computer to figure out what will happen. However, it does require access to a Server 2003 or Server 2008 domain controller (DC) to work. In fact, if you have only Win2K DCs in your AD domain, you won't even see the Group Policy Modeling node when you start up GPMC because the modeling feature uses a service called the Resultant Set of Policy Provider that runs only on the newer DCs. Without this service, modeling won't run.

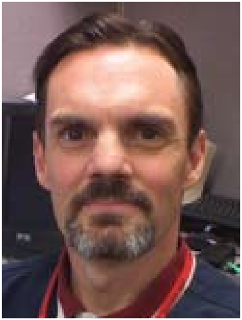
Using and Deciphering RSoP Logging

Now that you know what RSoP is, let's look at how you can use it to get more insight into your Group Policy settings. I find the version of Group Policy Results Logging that's available in GPMC easier to use than the command-line Gpresult utility, so let's start with the graphical version.

A note before we dive into the details: If you're working in a mixed environment of Server 2008, Vista, Server 2003, and/or XP, the rule of thumb is to run Group Policy Results on a machine that has the same or a more recent OS version than the machine whose results you're testing. So, if you're running Group Policy Results against a Vista machine, run it from a Vista machine, not an XP machine. You'll get more complete results this way.

The other thing to be aware of at this point is that the computer for which you're collecting Group Policy Results must be accessible on the network from your management station. That means it must be up and running and must not have a firewall blocking access to the ports and protocols required by Group Policy Results. Because Group Policy Results uses remote WMI calls to get access to this information, you typically need to ensure that the remote system allows the DCOM protocol. This protocol uses TCP port 135 for initial setup and random ports greater than 1024 for ongoing communication. If the target machine uses Windows Firewall, the easiest way to ensure that the necessary ports are unblocked is to use the built-in Remote Administration Exception provided in Group Policy. You can find this exception on XP and Server 2003 in GPMC under Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Standard (or Domain) Profile\Windows Firewall: Allow Remote Administration Exception and on Vista and Server 2008 under Computer Configu-

Keys to Group Policy Success? Prepare and Test!



LAN administrator Mike Foster gives advice on how to succeed using GPOs to deploy software

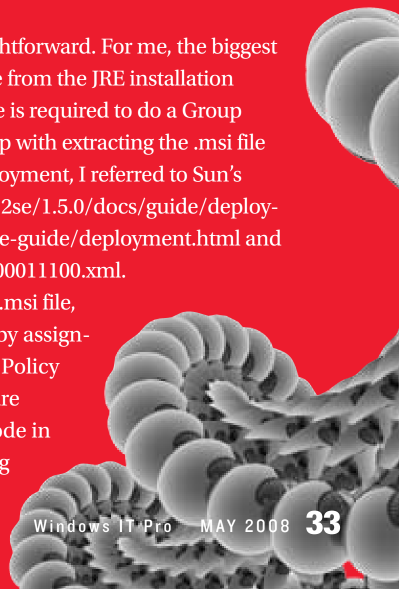
BY CAROLINE MARWITZ

Group Policy users typically can tell at least one horror story about settings gone wrong, but 10-year IT veteran Mike Foster says he hasn't really had what he'd call a horror story happen, even when his organization used Group Policy to install Sun Microsystems' Java Runtime Environment (JRE) on 800 computers. The success of that experience was due in no small part to Mike's preparatory steps. Mike is currently a junior LAN administrator for a US government organization that focuses on health care, but he gained his background in Group Policy as a Microsoft Certified Trainer working with Active Directory (AD). Besides asking him to share his experience with using Group Policy to install JRE, *Windows IT Pro* Web Site Strategic Editor Anne Grubb and I quizzed Mike about how to get up to speed with Group Policy resources. We even managed to glean an almost-horror-story from him, which he diplomatically calls a Group Policy "challenge," about deploying software at remote sites.

Q: Your organization needed to install JRE on 800-plus computers. How did you use Group Policy in this situation?

A: Deploying JRE was fairly straightforward. For me, the biggest hurdle was extracting the .msi file from the JRE installation executable (.exe) file. The .msi file is required to do a Group Policy–based installation. For help with extracting the .msi file and other aspects of the JRE deployment, I referred to Sun's documentation at java.sun.com/j2se/1.5.0/docs/guide/deployment/deployment-guide/upgrade-guide/deployment.html and java.com/en/download/help/5000011100.xml.

Once I obtained the required .msi file, I simply followed best practices by assigning the application in the Group Policy Computer Configuration/Software Settings/Software Installation node in Group Policy Editor and verifying



that I placed the required .msi file in an appropriately shared folder in an accessible network location, with the correct permissions configured on it. We didn't require any scripts or transform file for this installation, but we've used user logon scripts with Group Policy to configure the user environment, such as for modifying registry values required by applications or the users. We've also used computer startup scripts with Group Policy for various purposes.

Q: Was there anything special you did on this project that helped to make things work smoothly?

A: I conducted thorough testing on each client platform prior to rolling this out to our production environment. I also notified all users about the rollout in advance because Group Policy software installations occur during the computer boot phase, which leads to a delay when booting the computer. We notified our users well in advance so that calls to our Help desk would be minimized during the installation phase.

Q: What advice would you give others looking to deploy applications by using Group Policy?

A: First I recommend conducting thorough research in advance, so that you completely understand what the requirements are before you get started. Review white papers and best practices for using Group Policy. These are available via Microsoft's Web site and elsewhere on the Internet. I also recommend thoroughly testing the policies and deployment in a test environment on each client OS used in your production environment to ensure there are no issues once you get to production.

Q: Do you have any Group Policy horror stories?

A: I wouldn't call it a "horror story," but for me one of the biggest challenges with using Group Policy to perform software installations has been our remote sites and the WAN bandwidth issues we face. I created and targeted specific organizational units (OUs) within our AD so the computers at the remote sites wouldn't get large software installations over the WAN. We did do some smaller installs over the WAN, such as our Daylight Saving Time patch, but for the most part I recommend using multiple Group Policy Objects (GPOs), each with its own localized software source directory, and targeting specific OUs based on geographic location. Or you could do large software deployments manually on each client at the remote sites (which is something that we did for small remote sites where the bandwidth didn't support a software rollout using Group Policy.)

Q: What do you think of the Resultant Set of Policy (RSoP) snap-in?

A: I've used RSoP to troubleshoot Group Policy configuration settings, and I've also used the GPResult command-line tool. As somebody who came into the IT arena after the invention of the GUI, I really appreciate tools such as RSoP because I tend to grasp the information quicker from a GUI as opposed to the results of command-line tools such as GPResult. One of the benefits I've seen with RSoP is that it allows for reviewing the existing GPOs that are applied to a given computer and/or user (logging mode), which is great when you're troubleshooting Group Policy settings. RSoP also provides a way for the administrator to simulate the effect of applying a GPO (using planning mode), without actually applying the policy to the target computer and/or user.

InstantDoc ID 98477

MORE ON THE WEB

Read an expanded version of this article at www.windowsitpro.com, InstantDoc ID 98477.

Caroline Marwitz

(cmarwitz@windowsitpro.com) is an associate editor for *Windows IT Pro* and *SQL Server Magazine*, specializing in Active Directory, Group Policy, and desktop management.

ration\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Inbound Rules, under the Predefined Rules selection.

Ok, let's get started. Suppose you want to verify that a certain workstation has retrieved some policy settings. Start GPMC, right-click the Group Policy Results node, then select the Group Policy Results Wizard option. The first wizard screen lets you select a remote or local computer to connect to. If you're interested only in per-user settings, you can also select a check box to exclude any per-computer settings in the report that will be generated.

After selecting the computer you want to target, the next wizard screen lets you select a user who has logged onto that computer, if you want to return per-user Group Policy settings in addition to computer settings. The Group Policy Results wizard UI will show you only those users who have logged onto the remote system and generated RSoP data. If you don't see a user in the list, he or she likely hasn't logged onto that system. After you select the user, the Group Policy Results wizard collects the WMI data from the selected computer and displays it in the GPMC's right-hand results pane, as shown in Figure 1.

Interpreting the Results

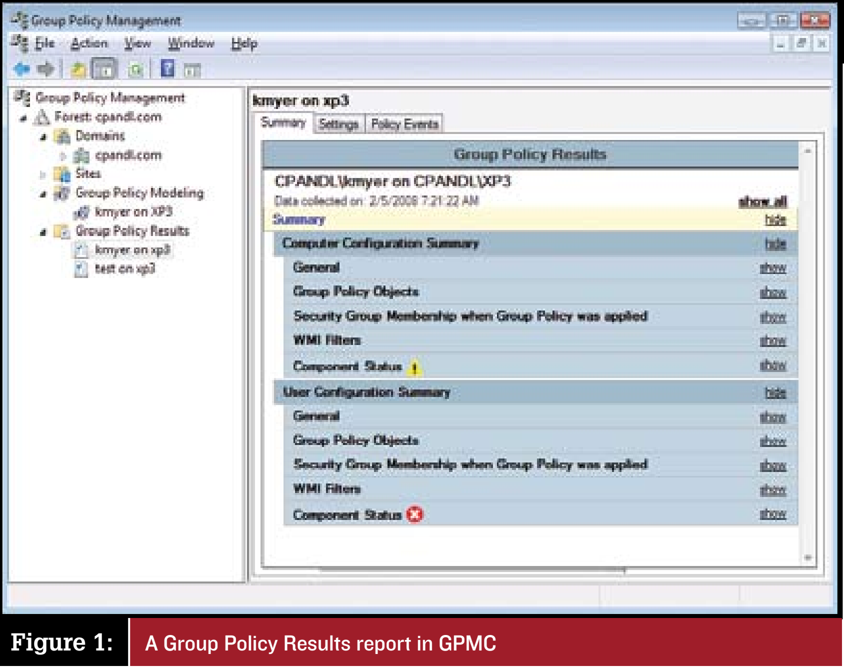
Once you've run the Group Policy Results wizard and the results are displayed, you can dive in and interpret those results. In the right-hand results pane are three tabs: Summary, Settings, and Policy Events. Table 1, page 36, describes the purpose of each.

The Summary tab is probably the most interesting in terms of finding out what's going on with Group Policy on the remote system, so let's examine it in detail. Figure 2, page 36, shows an expanded Summary tab with all its sections.

Assuming you selected to show both per-computer and per-user Group Policy settings, the summary will be broken into two sections: Computer Configuration Summary and User Configuration Summary. In each of these sections are five subsections that provide details about what policies were processed. The most interesting subsections are Group Policy Objects and Component Status.

The Group Policy Objects subsection is further divided into Applied GPOs and

Denied GPOs. Applied GPOs lists the GPOs that were processed by the computer or user, to which AD container those GPOs were linked, and what their AD and SYSVOL version numbers were. This information is important because it lets you verify that a particular GPO that you think should be processed by the computer or user really is being processed. The version numbers are important because they should always be the same for a given GPO. If the AD and SYSVOL version numbers are different from each other, the GPO being processed could be out of sync on the DC that the computer is using to process policy, which could indicate a replication problem (or simply that you initiated Group Policy Results processing without leaving enough time for GPO changes to replicate to the DC).



Group Policy Management
Forest: cpandl.com
Domains
cpandl.com
Sites
Group Policy Modeling
kmyer on XP3
Group Policy Results
kmyer on xp3
test on xp3

kmyer on xp3

Summary | Settings | Policy Events

Group Policy Results

CPANDL\kmyer on CPANDL\XP3
Data collected on: 2/5/2008 7:21:22 AM — show all
Summary — hide
Computer Configuration Summary — hide
General — show
Group Policy Objects — show
Security Group Membership when Group Policy was applied — show
WMI Filters — show
Component Status ⚠ — show
User Configuration Summary — hide
General — show
Group Policy Objects — show
Security Group Membership when Group Policy was applied — show
WMI Filters — show
Component Status ✖ — show

Figure 1: A Group Policy Results report in GPMC

The Denied GPOs section is equally interesting because it tells you exactly why a GPO wasn't processed, even though it might be linked to a container in AD that includes the computer or user. The most common reasons for GPOs being denied—or, more correctly, not processed—include security group filters or WMI filters that prevent them from being processed, a link being disabled, or the GPO being empty (i.e., containing no settings). The Denied GPOs section can provide good information about how you're applying your policies and might indicate places where you can get rid of "dead" GPOs that computers or users are trying to process but can't.

The Component Status section of the results is the really interesting part! It's the portion of the report that tells you whether Group Policy processing actually worked for the computer or user in question. This section of the report is broken down into each part of the Group Policy processing cycle. The component named Group Policy Infrastructure represents what's called the core phase of Group Policy processing. During this phase, the computer or user account reads the list of GPOs it must process, finds out which ones it has access to, and creates the list of CSEs that must process the policy settings in those GPOs. If this part of the processing cycle fails, then the rest of the cycle will fail.

The subsequent components listed are the various CSEs that ran for the computer or user during the last processing cycle. These include the different policy areas such as Registry, Security, and Software Installation. The report shows whether each item succeeded or failed and, if it failed, will often show the related error information. In Figure 2, the Software Installation item is Pending. The software installation CSE requires a foreground processing event (i.e., a system reboot or user logon) to actually run, so while the component hasn't failed, it hasn't yet run. The Component Status section is also marked with a visual cue—a red X in the case of a failed event or a yellow ! in the case of a warning such as the pending state of software installation.

Table 1: The Group Policy Results Tabs in GPMC

Tab	Purpose
Summary	Provides summary information about which GPOs were and weren't processed by the computer and/or user, and why. Also states whether Group Policy processing actually succeeded on the target system and gives some other summary information, such as the security groups that the computer and/or user belonged to at the time of processing.
Settings	Shows the actual settings applied to the given computer and/or user and the "winning" GPOs that applied them.
Policy Events	Creates a filtered view of the Group Policy–related events from the Application event log on the remote computer.

The Settings tab of the Group Policy Results report, shown in Web Figure 1 (www.windowsitpro.com, InstantDoc ID 98442), gives you a breakdown of the actual policy settings that were applied to the computer or user and the name of the GPOs that delivered those settings. The report in Web Figure 1 shows the details of some Administrative Template Windows Firewall settings that were processed by the client. For Administrative Templates, the report actually includes the Explain text that goes along with the policy to remind you what the policy is for. Note also that, on Vista and Server 2008 systems, the report lets you know that Administrative Template policy descriptions were retrieved from the central store, which is the server-based file-system location where ADMX and ADML files can be kept.

When you select the Policy Events tab of the Group Policy Results report, you see a list of Group Policy–related events that occurred on the remote system. These look and feel like Windows Event Viewer events because that's where they come from. In many cases, the events that are the most interesting are the error or warning events, but frankly, I haven't found much of use in this information, due to the sheer volume of events and the lack of detail about them. However, it's worth looking at this view if you're having problems because some useful information could turn up.

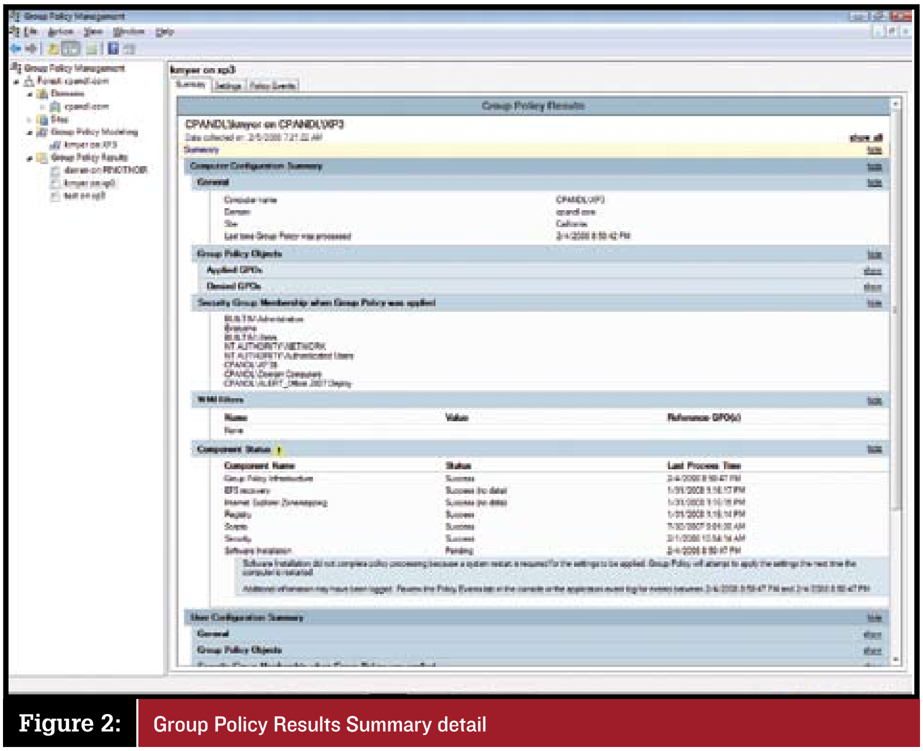
If you want to save the information from the Summary or Settings tabs, right-click over the area of either tab and select Save Report to send the report to an HTML or XML file. The XML file format is useful only if you plan to repurpose the raw data somewhere else.

You can view a five-minute screencast that shows how to run the Group Policy Results wizard and view the output at wms18.streamhoster.com/pentonmedia/windows/winscreencasts/RSOP-MarElia.wmv.

Under the Covers

GPMC and Gpresult hide the complexity of how RSoP data is collected in WMI, but if you're familiar with WMI and know how to query its contents, you can get directly at the WMI data that underlies those nice RSoP reports. RSoP data is held in a special namespace within WMI specifically for that purpose. Whereas you might be familiar with querying information in the root\CIMv2 namespace, RSoP data is held in root\RSOP. The data is broken down into a number of different classes, each representing different policy areas (e.g., registry, folder redirection, security). Figure 3 shows a view into this namespace through a WMI browser tool called WMIX, which you can download at www.pjtec.com/WMIX.

What you see here is a number of containers in the RSOP namespace. The containers that start with NS followed by a bunch of alphanumeric characters are called RSoP Sessions. They represent me running RSoP reports remotely against this system, called XP3. In Figure 3, I've drilled down into one of these sessions and you can see a number of WMI classes representing the various policy areas that you'd typically look at in an RSoP report. If I viewed the instances on these classes, I would see the raw Group Policy settings data that the GPMC report returned.



kmyer on xp3

Group Policy Results

CPANDL\kmyer on CPANDL\XP3
Data collected on: 2/5/2008 7:21:22 AM

Summary

Computer Configuration Summary

General

Computer name	CPANDL\XP3
Domain	cpandl.com
Site	California
Last time Group Policy was processed	2/4/2008 8:50:42 PM

Group Policy Objects

Applied GPOs

Denied GPOs

Security Group Membership when Group Policy was applied

BUILTIN\Administrators
Everyone
BUILTIN\Users
NT AUTHORITY\NETWORK
NT AUTHORITY\Authenticated Users
CPANDL\XP3$
CPANDL\Domain Computers
CPANDL\ALERT_Office 2007 Deploy

WMI Filters

Name	Value	Reference GPO(s)
None		

Component Status

Component Name	Status	Last Process Time
Group Policy Infrastructure	Success	2/4/2008 8:50:47 PM
EFS recovery	Success (no data)	1/31/2008 1:16:17 PM
Internet Explorer Zonemapping	Success (no data)	1/31/2008 1:16:15 PM
Registry	Success	1/31/2008 1:16:14 PM
Scripts	Success	7/30/2007 9:01:20 AM
Security	Success	2/1/2008 11:58:16 AM
Software Installation	Pending	2/4/2008 8:50:47 PM

Software Installation did not complete policy processing because a system restart is required for the settings to be applied. Group Policy will attempt to apply the settings the next time the computer is restarted.

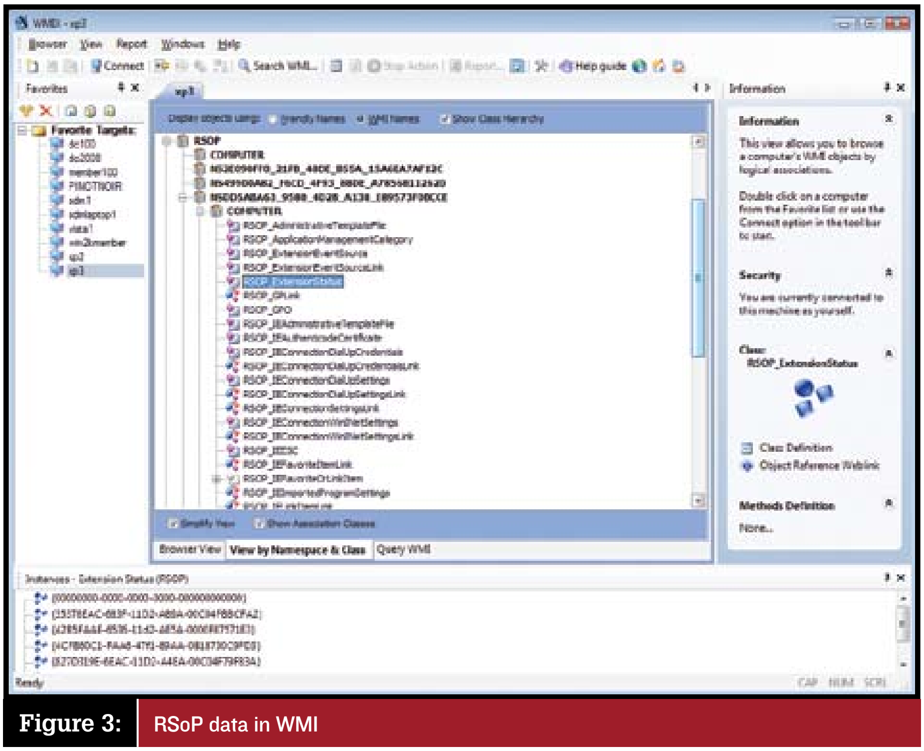
Additional information may have been logged. Review the Policy Events tab in the console or the application event log for events between 2/4/2008 8:50:47 PM and 2/4/2008 8:50:47 PM.

User Configuration Summary

General

Group Policy Objects

Figure 2: Group Policy Results Summary detail



Favorite Targets:
dc100
dc2008
member100
PIMOTHOR
sdm1
sdmlaptop1
vista1
win2kmember
xp2
xp3

RSOP
COMPUTER
NS2E090F70_21F8_480E_B55A_15A6EA7AF12C
NS49900A62_F6CD_4F93_880E_A7855811252D
NSDD5A8A63_9588_4028_A138_E89573F08CCE
COMPUTER
RSOP_AdministrativeTemplateFile
RSOP_ApplicationManagementCategory
RSOP_ExtensionEventSource
RSOP_ExtensionEventSourceLink
RSOP_ExtensionStatus
RSOP_GPLink
RSOP_GPO
RSOP_IEAdministrativeTemplateFile
RSOP_IEAuthenticodeCertificate
RSOP_IEConnectionDialUpCredentials
RSOP_IEConnectionDialUpCredentialsLink
RSOP_IEConnectionDialUpSettings
RSOP_IEConnectionDialUpSettingsLink
RSOP_IEConnectionSettingsLink
RSOP_IEConnectionWinINetSettings
RSOP_IEConnectionWinINetSettingsLink
RSOP_IEESC
RSOP_IEFavoriteItemLink
RSOP_IEFavoriteOrLinkItem
RSOP_IEImportedProgramSettings
RSOP_IELinkItemLink

Information

This view allows you to browse a computer's WMI objects by logical associations.

Double click on a computer from the Favorite list or use the Connect option in the tool bar to start.

Security

You are currently connected to this machine as yourself.

Class:
RSOP_ExtensionStatus

Methods Definition

None...

Instances - Extension Status (RSOP)

{00000000-0000-0000-0000-000000000000}
{35378EAC-683F-11D2-A89A-00C04FBBCFA2}
{4285FAA8-6536-11d3-A85A-000F8757183}
{4CFB80C1-FAA8-4791-89AA-0818730C9FD3}
{827D319E-6EAC-11D2-A4EA-00C04F79F83A}

Figure 3: RSoP data in WMI

RSoP data provides a powerful mechanism for discovering how Group Policy is working on your remote Windows systems. Using GPMC or Gpresult, you can both model what should happen with Group Policy for a given user or computer, as well as what did happen. And not only do you get to see the actual settings that were processed, but you can also see whether any errors occurred during processing that might have prevented settings from being delivered. This important tool goes a long way toward guaranteeing that Group Policy is doing what it's supposed to do—keeping your systems secure and locked down.

InstantDoc ID 98442

Darren Mar-Elia
(dmarelia@windowsitpro.com) is a contributing editor for *Windows IT Pro* and is CTO and founder of SDM Software (www.sdmsoftware.com). He maintains a Group Policy resource Web site (www.gpoguy.com) and is coauthor of *Microsoft Windows Group Policy Guide* (Microsoft Press).