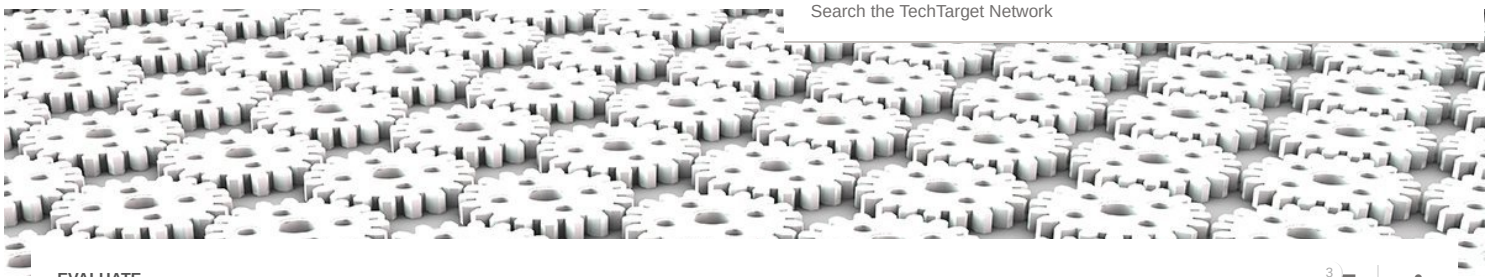

EVALUATE

Four utilities can verify Group Policy object settings

Client-side extensions could cause a Group Policy object to fail. Fortunately, there are a few different ways to track down Windows GPO settings.

Nirmal Sharma

In case a Group Policy object is applied for the first time, you would always want to know whether the GPO was applied. Once a GPO is applied to a Windows computer, the settings configured in it should also apply, but that is not always the case, because GPO settings are processed by the Winlogon process with the help of client-side extensions.

If a client-side extension fails, the related GPO settings will not apply. Built-in Windows tools enable desktop administrators to see whether a particular GPO and its settings are applied. Some of these tools can also be executed for remote computers.

Using GPResult to check application of Group Policy

GPResult is a powerful command-line tool that can report Group Policy settings applied on a Windows device. The tool has been available since Windows 2000 and supports the following parameters:

- **GPResult /R** -- This reports only the GPOs that have been applied to user and computer accounts. This is useful if you need to check only if a particular GPO was applied. The output is shown on the screen.
- **GPResult /Z** -- The /Z parameter can be used if you need to see both GPOs and policy settings applied to the computer.
- **GPResult /H <ReportFileName.html>** -- The /H parameter instructs the command to report GPOs and settings from each Group Policy that has been applied and saves the output to the ReportFileName.HTML file. The /H parameter is useful if you need to see both GPOs and policy settings applied to the local computer.
- **GPResult /S <Computer Name>** -- This instructs the command to get the GPResult from a remote computer.

Although the GPResult tool provides /S parameter to check the application of GPOs and its settings on a remote computer, the best option would be to use remote command execution tools such as PSExec.exe or Windows Management Instrumentation Command line (WMIC). PSExec.exe and WMIC tools run interactively on remote computers. Since GPResult is a command-line tool, it helps you script the operation and run against multiple computers.

Using the RSOP.MSC GUI tool

RSOP.MSC, which is a graphical user interface (GUI) tool, is the preferred utility for checking the GPOs and settings applied to a local or remote computer. With RSOP.MSC, you can quickly determine if there were any problems while applying GPOs from an Active Directory domain controller.

After running RSOP.MSC, you are presented with a Microsoft Management Console (MMC) snap-in. In case of any problems with the Computer or User configuration, you will see a red cross on top of the nodes as shown in Figure 1.

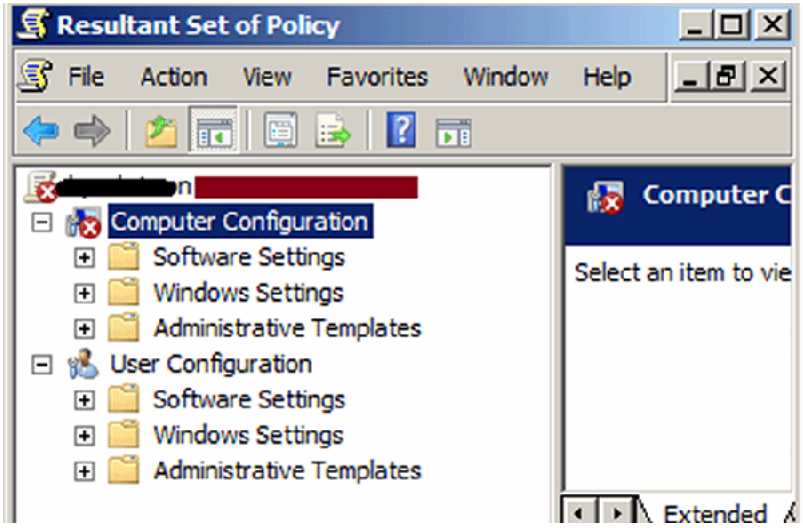

Figure 1. After running the RSOP.MSC tool, the MMC snap-in flags configuration problems.

If you need to see the reason for the failures, you can always go to the property page for the Computer/User Configuration and then click on the "Error Information" tab as shown in Figure 2.

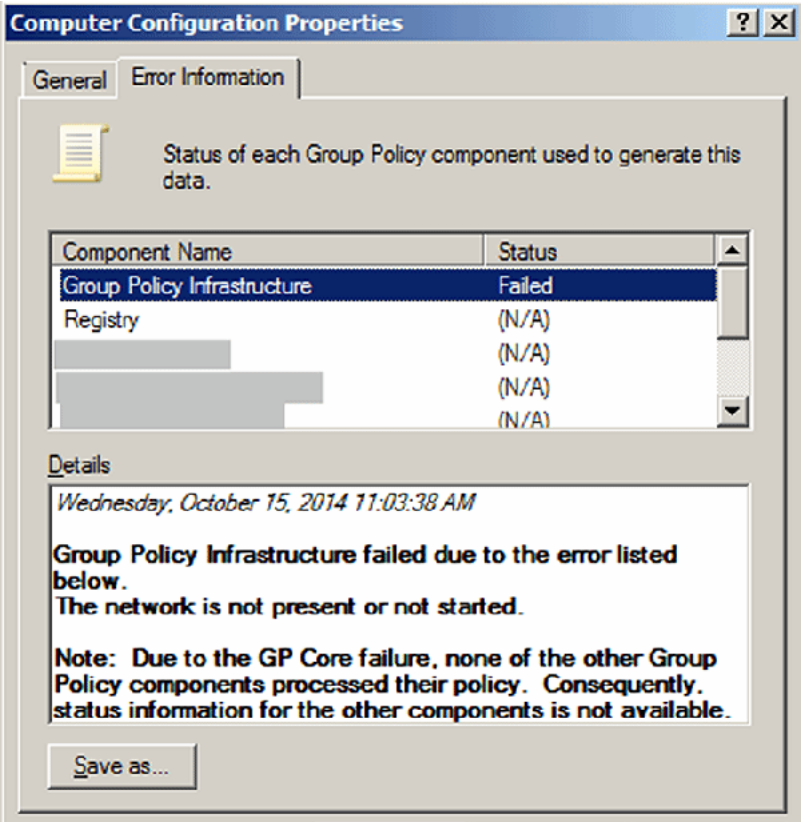

Figure 2. The properties box displays the reason for Group Policy failures.

To connect and collect the GPO RSOP data from a remote computer, in the RSOP.MSC snap-in, go to Action Menu, and then click on "Change Query."

The use of GPResult.exe is preferred over RSOP.MSC if you want to perform scripted tasks against several Windows computers.

Using Registry Editor to check if a GPO is in effect

To check whether or not a Group Policy was applied a local or remote computer, you can just use the Registry Editor. Note that it will show only which GPOs were applied. In other words, since the policy settings applied from a GPO are stored at a number of places in the registry, it would be difficult to know which settings were applied unless you know how and where GPO policy settings are stored in the registry.

A computer keeps its information about applied GPOs at the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\History registry location. That key contains subkeys, which contain the names of GPOs that have been applied to the computer as shown in Figure 3.

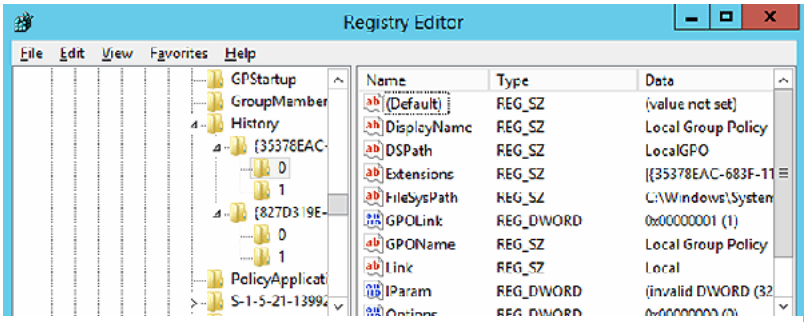

Figure 3. Subkeys in the registry history contain the names of applied Group Policies.

Registry Editor also allows admins to connect to the registry of a remote computer, provided the "Remote Registry" service is running on the remote device. In order to check the application of a GPO on a remote computer, connect to the remote registry and then navigate to the above registry location.

GPO PowerShell modules

Undoubtedly, you can use GPResult.exe and RSOP.MSC to get the GPO results from a Windows computer, but Microsoft also implemented the same functionality in Windows PowerShell. GPO PowerShell cmdlets, which are available as part of the Remote Server Administration Tool, can be run in Windows 7 and later operating systems.

Prev

1

Next

Nirmal Sharma asks:

Have you had any problems applying or verifying Group Policy object settings?

Join the Discussion

There are many PowerShell cmdlets available to perform GPO related tasks, one of which can help you generate GPO settings from a local or remote computer -- the **Get-GPResultantSetOfPolicy** PowerShell cmdlet.

This cmdlet is the quickest and easiest way to get the GPO RSOP data for a user, computer or both from a local or remote computer. The Get-GPResultantSetOfPolicy cmdlet is very similar to the RSOP.MSC, except it supports reporting GPO RSOP to XML format and allows commands to run against a remote computer from the command line. To check GPOs and policy settings applied to the local computer, execute the following command:

- Get-GPResultantSetOfPolicy -ReportType XML -path C:\MyReports\GPOReport.XML

In case you need to run the command against a remote computer and store the output to a local computer, execute this command:

- Get-GPResultantSetOfPolicy -ReportType HTML -Computer PC1.TechTarget.com -Path C:\MyReports\GPOReport_PC1.html

Similarly, the command below generates a report for the computer PC1 and user James in the TechTarget.com domain.

- Get-GPResultantSetOfPolicy -User James -Computer TechTarget.com\PC1 -ReportType html –Patch C:\MyReports\PC1_GPOReport.html.

Although Get-GPResultantSetOfPolicy supports the –Computer parameter, you can specify only one computer name to collect the GPO RSOP data. To run the command for multiple computers, you can use the "ForEach" PowerShell cmdlet to read the computer names from a text file and then process the Get-GPResultantSetOfPolicy command.

Next Steps

How to check refresh status of Group Policy Object settings

Remotely refresh Windows 8 Group Policy with one of two methods

Control the Windows 8.1 UI with Group Policy settings

Manage the Windows 8 UI, configuration with Group Policy settings

How do GPOs vary among Windows editions?

Use Group Policy settings to lock down enterprise desktops

Check the Winlogon component for missing GPO settings

PowerShell isn't just for servers; use it to manage Windows 7 desktops

This was last published in November 2014

Dig Deeper on Microsoft Windows 7 operating system

ALL NEWS GET STARTED EVALUATE MANAGE PROBLEM SOLVE