Supplemental Reading for Group Policy Troubleshooting

Group Policy Troubleshooting

This reading expands upon a previous topic on various approaches to troubleshooting common Group Policy problems.

Terminology

Important terminology used with Microsoft Windows Server Group Policies:

- **Group Policy Object (GPO):** A set of Active Directory (AD) Group Policy configurations that controls the appearance and behaviors for groups of computer systems and/or groups of end users.
- **Group Policy Management Console (GPMC):** A console that is used to create, manage, edit, and link GPOs. The GPMC provides thousands of options for computer and user settings such as Control Panel items, Registry settings, and environmental variables. Policy settings are refreshed every 90 minutes, so changes are not applied immediately. The GPMC can be used to create GPOs that control registry-based policies and software installations, as well as options for:
  - security
  - maintenance
  - scripts
  - folder redirection
- **Active Directory (AD) containers:** AD containers can be linked to GPOs. AD containers include:
  - **Sites:** Physical sites or aspects of a network, which are linked to AD Domains. Can be used to group and connect geographically dispersed locations into the same domain.
  - **Domain:** A collection of objects in an AD network, such as computers, users, and groups. Can contain multiple AD Sites and be linked to multiple GPOs.
  - **Organizational Unit (OU):** Collectively groups end users, computers, groups, and/or other OUs. OUs can reflect an organization's hierarchy and business divisions. For example, an organization might have separate OUs for executives, administration, accounting, IT, sales, marketing, vendors, etc.
- **GPOs process order:** Windows will apply GPOs in the following order:
  1) The Local GPO
  2) GPOs linked to Sites
  3) GPOs linked to Domains
  4) GPOs linked to OUs
- **Resultant Set of Policies (RSoPs):** A report of AD Group Policy settings that indicates how all GPO settings are hierarchically inherited by end users and computers. RSoP reports can be collected for evaluation using RSoPs logging.
- **Windows Management Infrastructure (MI) and Windows Management Instrumentation (WMI):** MI is the next generation of WMI. However, both MI and WMI are fully supported by Microsoft and MI is backwards-compatible with WMI. MI/WMI provide the operations infrastructure and management data in Windows. They also are used for scripting administrative tasks to run on remote systems.

Group Policy troubleshooting tools

The following command line tools can be used for troubleshooting Group Policy issues:

- **gpresult:** Displays the RSoP report or values for a computer and user account. This information can help to ascertain which configuration settings have been applied and which settings were overridden. A few of the switches available to the gpresult command include:
  - **/s** *host* - Displays the RSoP values of a remote computer.
  - **/u** *user-account* - Displays the RSoP values of an end-user.
  - **/p** *password* - Displays the RSoP values of an end-user password policy.
  - **/r** - Displays the RSoP summary of applied GPOs.
  - **/z** - Turns on verbose mode to display details of the RSoP applied settings.
- **gpedit:** The Group Policy Editor, which is a robust tool for changing Registry settings related to the Control Panel, Settings, user profiles, system configurations, third-party software, and more.

Settings, user profiles, system configurations, third-party software, and more.

- **gpupdate:** Command that can be used to force a new or edited GPO to be applied immediately using the /force switch. If the policy setting requires the users to logoff or reboot, the switches /logoff or /boot can be added to the command.

Additionally, system event logs are important tools for most Windows troubleshooting issues:

- **Event Viewer and Windows Logs:** The Windows Event Viewer is an invaluable tool for viewing Windows Logs. These tools help IT Support specialists track system problems and events related to items like applications, user logins, security, and systems. To open the Windows Event Viewer, click on the Start menu and type "Event Viewer". Any error messages or codes found in the logs can be investigated using the Microsoft Knowledge Base (support.microsoft.com), as well as through an internet search. The main Windows Logs include:
- **System log:** Records Windows OS events like hardware conflicts, driver load failures, service load failures, network issues, and more.
- **Application log:** Records application processes and utilities events/errors.
- **Security log:** Records system security audit information.
- **Setup log:** Records installation events and errors.

Resources for more information

- Group Policy troubleshooting documentation for Windows Server - Extensive troubleshooting guide for Group Policies. Topics can be accessed from the left side menu.
- Group Policy processing and precedence - Additional information about GPO processing order and exceptions.
- Active Directory documentation - Extensive troubleshooting guide for AD. Topics can be accessed from the left side menu.
- Use Resultant Set of Policy logging to gather computer policy information - Microsoft article that provides information on how to use the RSoPs utility (Rsop.msc) to gather computer-specific policy information.
- Suggested hotfixes for WMI related issue on Windows platforms - Provides information on symptoms and resolutions for WMI issues.
- How the Windows Time Service Works - (from the video on troubleshooting Group Policies) Microsoft article that includes information on how to manually force a domain computer to resync.
    - W32tm - Syntax for using the **w32tm /resync** command, which can be used to diagnose problems related to Windows Time.
- 6.3.2.3 SRV Records - (from the video on troubleshooting Group Policies) Information from Microsoft on the SRV DNS Resource Record.