INFORMATION TECHNOLOGY UPDATE

Windows Group Policy Management

You've heard the saying, "The devil is in the details." This is certainly true of group policy management within your Windows environment. Like many areas within Windows, the flexibility provided by Microsoft within Group Policy Management creates complexity in how policies are enforced. This often misunderstood area of Windows has become an area of emphasis within Snodgrass's Windows reviews. This article provides information to help clarify some areas where we have seen policies being commonly misapplied or applied settings that do not enforce optimal security.

Group policies can be applied at various points throughout your Active Directory structure including at the Domain level, at defined organizational units, and to specific users and computers within your Windows network. Experts have differing opinions on the most effective way to apply group policies. The common thread is that policy assignment should be properly planned. Users and computers that have common policies requirements should be organized within Active Directory, so policies can be readily applied without adding unnecessary complexity to the environment.

In addition to the Active Directory structure, there are additional factors to consider when determining policy enforcement including policy precedence (i.e.,, link order), inheritance, overrides, loopback policies, and default settings. This article does not attempt to explain all nuances of group policy management and enforcement. For more information on group policy enforcement, you can view plenty of good reference materials on the Internet through technet.microsoft.com including the following links:

> https://msdn.microsoft.com/en-us/library/bb742376.aspx - Step-by-Step Guide to Understanding the Group Policy Feature Set
> https://technet.microsoft.com/en-us/windowsserver/bb310732.aspx - Group Policy

First, let's look at some commands you can use to determine what policies are being enforced in your environment. One useful command is Gpresult. This command can be run on any server or PC for any user within your Windows environment to see what group policies and settings are effective. The command is run from a Command Prompt initiated with "run as administrator" to ensure it will return complete results. The syntax of the command is *Gpresult /r /z >>C:\gpresult.txt* (or a path and file name of your choosing). This will produce a verbose policy listing in text format for the system and user that run it.

2009 Mackenzie Way, Suite 340, Cranberry Township, PA 16066 | Phone (724) 934-0344 | Fax (724) 934-0345 | Email: info@srsnodgrass.com
1275 Glenlivet Drive, Suite 135 Allentown, PA 18106 | Phone (610) 530-8885 | Fax (610) 530-0409
2100 Renaissance Blvd., Suite 110 King of Prussia, PA 19406 | Phone (610) 278-9800

For more information on the Gpresult command syntax, see the following technet.microsoft.com posting:

https://technet.microsoft.com/en-us/library/cc755461(v=ws.10).aspx - Gpresult

The Gpresult listing has two sections: policies assigned to computers and policies assigned to users. The following excerpt shows the effective group policies assigned to this specific computer and the order the policies are enforced. Gpresult lists policies in order of precedence as determined by the link order within Active Directory. In other words, the policy listed first by Gpresult takes precedence over policies lower in the list for any conflicting settings among the policies. In the example below, the Default Domain Policy is listed first within the Applied Group Policy Objects list, so its settings would take precedence over the same settings from the other policies listed.

```
COMPUTER SETTINGS
------------------
    CN=Domain1, OU=Domain Controllers,DC=DC1,DC=local
    Last time Group Policy was applied: 6/1/2016 at 12:00:00 PM
    Group Policy was applied from:      Domain1.local
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        Domain1
    Domain Type:                        Windows 2000

    Applied Group Policy Objects
    -----------------------------
       Default Domain Policy
       Default Domain Controllers Policy
       Server Policy
       Audit Policy
       Removable Device Policy
```

In addition, the applied policies listed below for this user are also listed in the Gpresult. To further add to the complexity of policy enforcement, it is important to note there are rules regarding which policies take precedence. Computer configuration settings apply to computers, and user configuration settings apply to users. If set in a conflicting manner, user settings will usually take precedence. Again, this general rule can be changed based upon how policies are implemented within your environment.

```
USER SETTINGS
--------------
    CN=Joe User,OU=End Users,OU=Department1,OU=Acme Company, DC=DC1, DC=local
    Last time Group Policy was applied: 6/9/2016 at 12:00:24 PM
    Group Policy was applied from:      AD1.Domain1.local
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        Doamin1
    Domain Type:                        Windows 2000
```

```
    Applied Group Policy Objects
    -----------------------------
       Default Domain Policy
       Screen Saver Policy
       Removable Device Policy
```

The Gpresult listing shows the effective policy settings and which policy is enforcing these settings. In the following example, the Account Policies are coming from the Default Domain Policy with the highlighted MaximumPasswordAge setting also coming from the Server Policy. Because the Default Domain Policy is higher in the list of applied policy objects, it takes precedence, so in this case the MaximumPasswordAge setting enforced is 90 days. This example contains settings that **do not** provide an optimal level of security.

```
   Account Policies
   ----------------
            GPO: Default Domain Policy
                Policy:            LockoutDuration
                Computer Setting:  1

            GPO: Default Domain Policy
                Policy:            MaximumPasswordAge
                Computer Setting:  90

            GPO: Server Policy
                Policy:            MaximumPasswordAge
                Computer Setting:  42

            GPO: Default Domain Policy
                Policy:            MinimumPasswordAge
                Computer Setting:  0

            GPO: Default Domain Policy
                Policy:            ResetLockoutCount
                Computer Setting:  30

            GPO: Default Domain Policy
                Policy:            LockoutBadCount
                Computer Setting:  5

            GPO: Default Domain Policy
                Policy:            PasswordHistorySize
                Computer Setting:  0
```

```
    GPO: Default Domain Policy
        Policy:            MinimumPasswordLength
        Computer Setting:  6

Audit Policy
------------
    N/A
Security Options
----------------
    GPO: Default Domain Policy
        Policy:            PasswordComplexity
        Computer Setting:  Enabled

    GPO: Default Domain Policy
        Policy:            ClearTextPassword
        Computer Setting:  Not Enabled
```

Based upon the settings above, it appears the Account Policies are coming from the Default Domain Policy; however, these settings do not provide an optimal level of security. Snodgrass recommends the following settings for most confidential systems:

Settings	Snodgrass Recommended Settings
Minimum Length	8 characters
Expiration (maximum age)	42 days
Minimum Age	10 days
Complexity enabled?	Yes
Clear test passwords enabled?	No
Password History	24 passwords
Bad Attempts Allowed	3 attempts
Reset Bad Logon Count	1440 (24 hours)
Lockout Duration	Forever (0)

Additionally, in the above Gpresult example, there is no Audit Policy being enforced through the effective group policies (N/A). So, to determine what default or local policies may apply, you can run the "Auditpol" command which lists the actual settings from the computer's registry.

The Auditpol command syntax is: *auditpol /get /category:* >> C:\auditpol.txt* (or specify the output file and path of your choosing). For more information on the Auditpol command syntax, see the following technet.microsoft.com article:

https://technet.microsoft.com/en-us/library/cc731451(v=ws.11).aspx - Auditpol

Following is an example of Auditpol command output. The settings are the Windows 2008 Server default settings which record very few categories of events.

System Audit Policy

Category/Subcategory	Setting
System	
Security System Extension	No Auditing
System Integrity	Success and Failure
IPsec Driver	No Auditing
Other System Events	Success and Failure
Security State Change	Success
Logon/Logoff	
Logon	Success
Logoff	Success
Account Lockout	Success
IPsec Main Mode	No Auditing
IPsec Quick Mode	No Auditing
IPsec Extended Mode	No Auditing
Special Logon	Success
Other Logon/Logoff Events	No Auditing
Network Policy Server	Success
Object Access	
File System	No Auditing
Registry	No Auditing
Kernel Object	No Auditing
SAM	No Auditing
Certification Services	No Auditing
Application Generated	No Auditing
Handle Manipulation	No Auditing
File Share	No Auditing
Filtering Platform Packet Drop	No Auditing
Filtering Platform Connection	No Auditing
Other Object Access Events	No Auditing
Privilege Use	
Sensitive Privilege Use	No Auditing
Non Sensitive Privilege Use	No Auditing
Other Privilege Use Events	No Auditing

```
Detailed Tracking
  Process Termination                     No Auditing
  DPAPI Activity                          No Auditing
  RPC Events                              No Auditing
  Process Creation                        No Auditing

Policy Change
  Audit Policy Change                     Success
  Authentication Policy Change            Success
  Authorization Policy Change             No Auditing
  MPSSVC Rule-Level Policy Change         No Auditing
  Filtering Platform Policy Change        No Auditing
  Other Policy Change Events              No Auditing

Account Management
  User Account Management                 Success
  Computer Account Management             No Auditing
  Security Group Management               Success
  Distribution Group Management           No Auditing
  Application Group Management            No Auditing
  Other Account Management Events         No Auditing

DS Access
  Directory Service Changes               No Auditing
  Directory Service Replication           No Auditing
  Detailed Directory Service Replication  No Auditing
  Directory Service Access                No Auditing

Account Logon
  Kerberos Service Ticket Operations      No Auditing
  Other Account Logon Events              No Auditing
  Kerberos Authentication Service         No Auditing
  Credential Validation                   No Auditing
```

Audit policy determines what events are recorded in the Windows Event Viewer log. As a general rule, recoding both success and failure events would provide a more complete set of logs in the event activity, such as that a potential breach would need to be researched. There are good tools available to report targeted events for review, so the extra “noise” created by recording success and failure events would not impact your ability to review the log. The only adverse result is some extra \archive storage requirements for the logs, but storage is relatively cheap. Therefore, we recommend setting all audit policies to record both success and failure events. Other things to consider for your audit log are the size and retention. Here, it is important to specify an adequate log size within your Event Viewer settings, so events are not overwritten before they are archived. Also, you should retain logs for an adequate period of time so they are available for review in the event activity needs to be researched. We recommend log retention of 60 days.

If your policy management has been properly planned, you can avoid some of the pitfalls that unnecessary complexity can create. Using the commands discussed in this article and additional commands and information within the referenced links, you should be able to confirm that your Windows policies are being enforced as intended.

If you have any questions regarding this Update, please feel free to contact Jeremy Burris, Rob Haller, or Chris Kreutzer at (724) 934-0344 or (800) 580-7738, or email jburris@srsnodgrass.com, rhaller@srsnodgrass.com, or ckreutzer@srsnodgrass.com.