Group Policy Troubleshooting FAQ

By Darren Mar-Elia

CTO & Founder

SDM Software, Inc.

2008

First, before you do anything, make **sure** the GPO is really not being processed or not being processed correctly. Run gpresult.exe on the affected client to ensure that you're actually not getting the policy you expect.

1. Your AD domain controllers are not correctly registered in DNS. While it may not seem like there is any relationship between Group Policy and DNS, there is. In fact, your users may be able to authenticate to the domain just fine without DNS being healthy but GPOs will not process. GPO processing requires that the various SRV records related to LDAP be located in order to successfully complete. Specifically, the _ldap._tcp.._sites.dc._msdcs. record must be found for domain in which the GPO resides. This name allows a machine to find a DC to query for the list of GPOs that it must process. If you have determined that GPOs simply aren't being processed, check DNS first. You can simply do an nslookup on the LDAP name above from the problem workstation to ensure its correctly being resolved to a valid DC as follows:

nslookup _ldap._tcp.mysite._sites.dc._msdcs.gpoguy.com

If the name is not resolved correctly, try restarting the Netlogon service on the missing DC to refresh SRV registration. Check the DC's event logs to make sure there aren't other issues. In larger environments this problem is usually rare, since there are usually some DCs that can be found, even if they're not in the local site.

2. Basic GPO processing infrastructure items are not available. Often times you can't simply get GPO processing going. I've pointed some reasons for this in this list but there are a few other things that you need to check to ensure that all the infrastructure is in place for healthy GPO processing. Specifically, on all client machines that process GPO, the TCP/IP NetBIOS Helper service must be running in order to successfully connect to the SYSVOL share. Additionally, sometimes a DC will have trouble sharing out SYSVOL, especially after it's just been DCPromo'd. In order to ensure that the

DC your workstation is using to get at the SYSVOL portion of a GPO is available, open a command shell and enter the following:

net use \\<DomainName>\sysvol

where <DomanName> is the DNS name of your AD domain (e.g. abccompany.com)

If SYSVOL is successfully shared out, then this command should succeed with the message, “The command completed successfully”.

3. You have No Override or Block Inheritance Set on a GPO or Container. Sometimes, we can cause our own problems. You can set a GPO link as Enforced, which means any downstream GPOs that conflict with the settings in that GPO are simply not processed. Or, you can set a domain or OU with Block Inheritance, which prevents upstream GPOs from being processed. Note that Enforced overrides Block Inheritance in cases where both are in place.

4. GPO synchronization is “whacked”. A GPO is composed of two pieces– the GPC that resides in AD under System\Policies and the GPT that resides in SYSVOL\Policies. These two pieces replicate by default from the PDC emulator DC to all other DCs in a domain. Each piece has a version number associated with it. You can see if these version numbers are in sync by using the GPMC (under the Details tab on a given GPO or the Infrastructure Status screen on a given domain). If all is well, both the DS Version (a.k.a. the GPC) and the SYSVOL Version (a.k.a. the GPT) will have the same number of revisions, meaning that their versions are identical and the GPO is in sync.

If these version numbers are not in sync (i.e. the GPC doesn’t get replicated at the same time as the GPT or vice-versa), then the GPO will not be processed. If you find them, check the event logs on the affected DCs for

DFS-R or, if you are still using it, NTFRS or AD replication problems. If SYSVOL replication is functioning correctly, try making a benign change on the GPO and see if that forces another replication event that cleans things up.

5. GPOs don't get processed unless they change. This one trips up a lot of people. By default, GPO are processed at machine startup and user logon. They are also processed in the background every 90 min. (with a 30 minute randomizer) on member servers and workstations and every 5 min. on DCs. However, in most cases, a GPO is not processed by a client unless something on that GPO has changed. The client machine will keep a history of GPO versions in the registry and will compare them to the versions of each GPO that gets processed during a processing cycle. If nothing changes on the GPO, it will not be processed unless you force it to via Administrative Template policy (specifically under Computer Configuration|Administrative Templates|System|Group Policy). The problem arises when people make changes to workstation or server configurations and expect them to get cleaned up automatically via policy. It won't happen until the AD-based GPO changes, or unless you force it using the policy referenced above or by issuing a "gpupdate /force" from GPMC or the command line. Also note that the policy to force a GPO to be processed even if it hasn't changed is set per Client-Side Extension (CSE). That is, if you look in the policy area above, it will have a number of processing policy options by CSE (e.g. Registry, IE Maintenance, Software Installation, etc.).

6. Slow link detection prevents certain Policy from Processing.
By default, if a client processing policy from a DC detects a slow link (<500Kb/s) to that DC, then certain policy is not processed. This includes Software Installation and Folder Redirection policy. Therefore, if for some reason the client detects a slow link, these policies won't get processed. This can be confusing, since part of the policy is being processed and part isn't. You can change the default slow link threshold on a per-CSE basis via Admin. Template policy (Computer Configuration|Admin. Templates|System|Group Policy) if you find this happening.

You can also verify if a slow link is being detected by viewing the Group Policy Operational Log within the Event Log under “Applications and Services Logs\Microsoft\Windows\GroupPolicy”. Event ID 5314 indicates the results of the slow link detection process, as shown below: