

Troubleshooting Poor Windows Logon Performance In Active Directory Environments

Gary Olsen

Problems based around performance are often the most frustrating to resolve, mainly because there are so many variables to consider. In this article, I will focus on the difficult issue of diagnosing and resolving slow logon performance for users when logging in to their domain accounts.

When troubleshooting any performance problem, you must first define what is an acceptable delay. I've seen some environments where users experience 5-10 minute logon times and they don't complain simply because they are used to it. Then I've seen others scenarios where even a one minute delay is considered unacceptable. That's why it's important to first define what is reasonable so that you know when you have solved the problem.

Windows Logon Performance Factors

It's important to consider a variety of factors when looking for the cause of logon performance issues. Some of these factors include:

1. The proximity of domain controllers to your users
2. Network connections and available bandwidth
3. Hardware resources on the DCs (x64 vs. x86, memory, etc.)
4. The number of Group Policy Objects (GPOs) applied to the user and computer (which directly affects bandwidth)
5. The number of security groups the user and computer are members of (also directly affects bandwidth)
6. GPOs containing settings that require extra processing time such as:
 - loopback processing
 - WMI filters
 - ACL filtering
7. heavily loaded domain controllers caused by:
 - applications requiring authentication
 - inefficient LDAP queries from user scripts or applications (see my article on taming the LSASS.exe process for more details)
 - a DC hosting other apps such as Exchange, IIS, SQL Server, etc.
8. client configuration
 - memory, disk, processor, etc.
 - network Interface (10/100/1000)
 - subnet mapped properly to the site
 - DNS configuration

Define the Scope

I always spend time asking basic questions in order to define the true scope of the problem. This will take some effort because these problems are usually defined by users who complain, while there may also be users who have just learned to live with it. Below are some important questions to ask:

Troubleshooting Poor Windows Logon Performance In Active Directory Environments

Gary Olsen

- Are the problems defined to a single site, security group, OU, department, type of client (laptop or desktop), or OS?
- Does the problem happen at a particular time of day?
- Does the problem occur when you are in the office or connecting over the VPN?

Describe the symptoms:

- Does the delay occur at a specific point each time (i.e. "Network Settings" on the logon screen)
- Does it occur before or after the logon screen?
- When did this start happening?

Tools and Data Gathering

There are some basic tools that I use to gather data. For performance problems, I like to cast a wide net and collect all that I can. Here are some examples:

- Run Microsoft Product Support Reports (MPSreports) on clients and their authenticating DCs. This is a common tool that collects data for all event logs, MSINFO32, NetDiag, IPConfig, drivers, hotfixes and more. Hewlett-Packard also has its own version called HPS Reports which is, in my opinion, superior to Microsoft's tool and will collect specific Active Directory data if run on a DC. It also collects a plethora of hardware-related information, even for non-HP hardware.
- On the client, use Microsoft KB article 221833 to set verbose logging for Winlogon. This will provide excellent details in the %Systemroot%\Debug\UserMode\Userenv.log file. Note that this log does not contain date stamps, so you must:
 - delete the existing userenv.log from the client
 - enable verbose logging per KB 221833
 - logoff, logon, and save the userenv.log to a new location in order to limit data collection for the logon period.

Note that the userenv.log is excellent at following GPO and profile processing, and often you can clearly see where a logon delay occurs, indicated by a long interval between events.

- Enable Net Logon logging. The Netlogon log is located in %systemroot%\debug and will be empty if logging is not enabled. This is an excellent source of information. For instance, it will show you which clients in subnets that are not mapped to a site. This can cause a client to go to an out-of-site DC for authentication and result in a longer than expected logon time.
- Run Process Monitor from Sysinternals. Look in the Help section for details on enabling boot logging. You can capture the process information during the slow boot to see which processes might be affecting performance.

Other Tips For Troubleshooting Slow Client Logons

There are a few more quick things you can do to see if your logon performance is caused by a known issue.

Troubleshooting Poor Windows Logon Performance In Active Directory Environments

Gary Olsen

First, examine the GPRresult.exe and LOGONSERVER environment variable on the client. While MPSreports and HPS Reports collect the GPRresult for the logged on user, they don't collect the LOGONSERVER variable which points to the authenticating DC. This is important because each time a user logs in, the GPOs are downloaded to the client. SYSVOL -- which contains the GPOs -- is a DFS root, however, and does not obey client site awareness. Instead, it collects the DCs (hosting the SYSVOL DFS root) in a randomized order, then the GPOs are downloaded from the first DC in the list.

I have seen situations where clients in a main hub site would go across a slow WAN link to an out-of-site DC in order to get the GPOs, causing very slow logon times. Since this could change on each logon, the problem was intermittent.

Examine the GPRresult for the DC that the GPOs were downloaded from and see if the GPOs are coming from an out-of-site DC. Also compare the LOGONSERVER variable to see if the client is being authenticated to an out-of-site DC. The logon delay could be explained through this "normal" behavior using known slow or busy links.

Another good test is to boot to Safe Mode with Networking and see if the delay occurs. If not, then do a Net Start and list all the services started. Then boot in normal mode and run Net Start and list all the services again. The difference should point to services that may be suspect, and eliminating them one at a time should help you identify the problem. You can also try disabling applications that start on boot to see if an application is getting in the way.

One final technique is usually to take a network trace using Netmon, Wireshark or another network capture utility. Since you are trying to capture the logon process, one good way to do this is to connect a dumb hub to the network cable going to the switch, then connect a cable from the hub to the problem PC and connect another cable to another PC or laptop that has Netmon or WireShark installed. Run the capture tool in promiscuous mode and reproduce the logon. This setup will ensure that the capture collects traffic in and out of the client and eliminates the network noise.

These are the basics to get you started. Just remember that there are no magic solutions – it really just takes time and detective work to find the problem. In an upcoming article, I will describe the methods I used in some case studies that should help tie this all together.

Debugging Windows Client Logon Delays: Narrowing The Scope

In my previous article, I described the basics of troubleshooting poor client logon performance in Windows. I will now dig a little deeper into how to develop an action plan to eliminate possible causes and, hopefully, find the problem.

Performance, of course, is always a challenge to write about because 1) everyone has a different view of acceptable performance and 2) there are many variables – hardware and software – that can affect performance. I do Active Directory-related troubleshooting for my day job, so that's the context in which I've put this article. I have worked on a number of these issues and will rely on that experience to describe how to attack these problems.

The first thing you need to do is prepare a list of possible causes for slow client logon in general. This could probably be developed into a flow chart, but for now we'll use a couple of lists and refer to them as we diagnose the problem.

Troubleshooting Poor Windows Logon Performance In Active Directory Environments

Gary Olsen

Known Causes Of Slow Client Logon Performance

As I wrote in my previous article, here is a quick summary of what I've found can cause client logon delays in Windows. These are not listed in any particular order, and each could be at fault for any given situation:

- Domain controller is unavailable or very busy
- DC overwhelmed by LDAP traffic
- DC also runs Exchange, SQL Server, File/print, etc.
- Client is getting Group Policy from an out-of-site DC
- Network traffic (startup/logon traffic is directly tied to the number of groups and GPOs that the computer and user are members of -- very predictable)
- Roaming profiles are slow to load
- Inefficient logon scripts
- Inefficient GPOs (filtering, restrictions)
- Large number of GPOs and/or security group memberships
- Viruses
- Network components (drivers, switches, link speeds, dual-homed, network cables, etc.)
- Applications and services are starting on the client at boot
- Antivirus updates, Windows Update downloads
- Faulty images

There are probably more possibilities, but this is a good list to start with.

Now let's examine some questions to ask in order to narrow the scope. This list is in the order that I would ask the questions. Each question is followed by a list of troubleshooting steps to resolve the issue. You will likely find more than one of these will apply, so organize the steps into a logical sequence for an action plan.

1. **When did this start?**

This is tough since you are relying on calls to the help desk, which may not be entirely accurate since some users often just learn to live with these issues. Interview the user and pin down the start of the problem. Then look at what changed, such as software installations, network changes, GPO changes or perhaps another problem that was solved with a hotfix. The answer to this will affect the rest of the questions you ask. (for example, it might be time to move to 64-bit DCs!)

2. **Who is affected?**

This is difficult because once again you have to rely on help desk complaints.

Troubleshooting Poor Windows Logon Performance In Active Directory Environments

Gary Olsen

- One user – Investigate other users that are in the same location and security groups, using the same hardware, etc. to make sure the problem is affecting only one user. Focus on local settings, profiles, workstation configurations, groups, and so on.
- Users in only one site – Look for problems at the domain controller or networking issues in the subnet(s). Examine domain controller performance to see if the DC is overwhelmed and can't handle the load. The LogonServer environmental variable should be examined on each client to determine which DC is authenticating them -- don't assume they are authenticating to a DC in the site as this can change. See if the "problem users" are all authenticating to one DC.
- Users across sites – This could be the result of a network issue, new patch installed, etc. Look for something in common among affected users, including when the problem was first seen.
- New clients installed since a certain date – Perhaps these users have a new image or OS?
- Terminal Services users – Look into local vs. roaming profile issues and terminal server load.

3. Does this happen at the same time every day?

Have the user log on and off at different times during the day, such as 10 a.m., 2 p.m., 7 p.m. or any other time when logon traffic is light. If the problem goes away, then you can focus on network traffic and DC performance during peak logon periods.

4. Do you have sites across slow-linked networks?

It is possible – and even common – for clients to authenticate to a local domain controller and get policy from another DC due to the way SYSVOL finds random DFS servers. It is also possible for a client to get policy from a DC in a poorly connected site, and it will change so the problem could be intermittent.

I don't know of a fix for this but have heard that a possible workaround is to hard code the LogonServer environmental variable to a specific DC. If this works in a test, then implement it only on problem clients. I have not done this, but it is worth consideration. The DC used for GPO loading is found in the GPResult output. Run GPRESULT /v on the client.

5. What did you change when this started?

The most common response to this is "nothing". After some digging however, you'll usually find something.

6. Can the affected user reproduce the problem by logging on to another computer?

In other words, does the problem follow the user? Or can another user who doesn't have the problem logon to the affected computer and experience the same issue? If you can determine that the problem is tied to the computer itself, it will narrow your attack.

7. Are you using roaming profiles (perhaps on some users and not others)?

Check the network share and look for roaming profile issues. Also, follow the steps in part one of this article to enable verbose logging for Userenv logs and examine it for more information.

8. Is the user having long delays when logging off?

This can also cause logon delays due to a bloated profile and registry. For Windows XP and earlier versions, consider implementing the Microsoft User Profile Hive Cleanup Service (UPHClean) to clean up local profiles and registry. UPHClean is implemented in Vista.

Troubleshooting Poor Windows Logon Performance In Active Directory Environments

Gary Olsen

9. Are the affected users remote access clients?

Perhaps the users only have a logon problem when using a remote access connection. Look at your remote connection software or VPN setup and try building a generic Windows connection rather than using your custom connection software. Your ISP and network performance could also be an issue here.

Digging Deeper

Here are some additional tips for finding the cause of these delays. You can find more details on some of these in my previous article.

- Find a test client. Ideally, you should be able to get a workstation and reproduce the problem without bothering a user.
- Download and run MPSreports from Microsoft on the client and DC. This collects data for all event logs, MSINFO32, NetDiag, drivers, hotfixes and more. remember, the more data you have, the easier it will be to track down the problem.
- Run PerfMon on the DC and client, and see if you can match the time of the client problem with some performance spike on the domain controller.
- Run a network trace and try to determine what is happening during the logon process that causes the delay.
- See if the problem happens at a specific time of day and if so, examine what is happening at that time. Suspects include AV and Windows updates, scheduled jobs, and client survey software.
- Review GPO settings. Known performance hits can come from ACL and WMI filters, loopback processing, etc. Determine if any GPO settings were implemented at the time this problem started. Check out my article on using Userenv logs to debug Group Policy and profile issues.
- If the problem follows the user (see item 6 in the question list above), try copying the user account to create a new user. If that account has no problem, recreate the account. I have seen this work in some cases. This test also eliminates the profile. You should try deleting the user's profile to see if that fixes the issue before recreating the account.
- Review the logon scripts. They can grow little by little until they become unwieldy and ineffective.

As I stated before, there are no easy solutions to this problem and it can take a lot of time to debug. The best attack is to review the possible causes, ask the right questions to narrow the scope, and use the tools noted here to gather and analyze data to locate the cause.