

Re: Slow Logon related to groups – Update!

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-09/msg03963.html>

- *From:* "Claus" <cjobs@xxxxxxxxxxxxxx>
 - *Date:* Wed, 26 Sep 2007 19:14:01 -0400
-

This is the only unusual thing I can detect:

Sent update to server : 192.1.1.1

Where is that IP address coming from?

My next step for troubleshooting this would be to create a new user, add the user to the domain admin group and try to log on from that same workstation. Does the same thing happen?

—

Claus

"Ferrell Ramey" <FerrellRamey@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:4D6D9331-6657-4151-9597-BB3CEB3DD7C5@xxxxxxxxxxxxxxxxxxxx>

I finally let the login process go through, it took about 15 minutes. This is logging the "Domain Administrator" to a workstation. Again, if I log the user into the same workstation this doesn't happen.

Here are the event log from the time I log out of the computer as my user name "Ferrell" through logging back into the same computer as the "Domain Admin".

Start: ===== Application Log ===== <

Event Type: Warning
Event Source: Userenv
Event Category: None
Event ID: 1517
Date: 9/26/2007
Time: 2:26:06 PM
User: NT AUTHORITY\SYSTEM
Computer: 28Y26B1
Description:

Re: Slow Logon related to groups – Update!

Windows saved user WESTERNVALVE\ferrell registry while an application or service was still using the registry during log off. The memory used by the user's registry has not been freed. The registry will be unloaded when it is no longer in use.

This is often caused by services running as a user account, try configuring the services to run in either the LocalService or NetworkService account.

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

Next: ===== <

Event Type: Error
Event Source: Userenv
Event Category: None
Event ID: 1054
Date: 9/26/2007
Time: 2:26:44 PM
User: NT AUTHORITY\SYSTEM
Computer: 28Y26B1
Description:
Windows cannot obtain the domain controller name for your computer network.
(The specified domain either does not exist or could not be contacted.).
Group Policy processing aborted.

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

Next: ===== <

Event Type: Error
Event Source: Userenv
Event Category: None
Event ID: 1053
Date: 9/26/2007
Time: 2:41:14 PM
User: NT AUTHORITY\SYSTEM
Computer: 28Y26B1
Description:
Windows cannot determine the user or computer name. (An internal error occurred.). Group Policy processing aborted.

Re: Slow Logon related to groups – Update!

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

Start: ===== System Log ===== <

This is where I couldn't stand it the first time and unplugged the patch cable. Then I logged off and tried to log right back on. The first couple of events are in regards...

Event Type: Information
Event Source: Tcpip
Event Category: None
Event ID: 4202
Date: 9/26/2007
Time: 2:26:36 PM
User: N/A
Computer: 28Y26B1

Description:

The system detected that network adapter
\\DEVICE\TCPIP_{137E9C4C-5431-4EB4-9D8C-C0EF69D18734} was disconnected from the network, and the adapter's network configuration has been released. If the network adapter was not disconnected, this may indicate that it has malfunctioned. Please contact your vendor for updated drivers.

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

Data:

0000: 00 00 00 00 02 00 50 00P.
0008: 00 00 00 00 6a 10 00 40 ...j..@
0010: 02 00 00 00 00 00 00 00
0018: 00 00 00 00 00 00 00 00
0020: 00 00 00 00 00 00 00 00

Next: ===== <

Event Type: Warning
Event Source: DnsApi
Event Category: None
Event ID: 11197
Date: 9/26/2007
Time: 2:26:36 PM
User: N/A
Computer: 28Y26B1

Description:

The system failed to update and remove host (A) resource records (RRs) for network adapter

Re: Slow Logon related to groups – Update!

with settings:

Adapter Name : {137E9C4C-5431-4EB4-9D8C-C0EF69D18734}
Host Name : 28Y26B1
Primary Domain Suffix : WesternValve.local
DNS server list :
192.168.1.2
Sent update to server : 192.1.1.1
IP Address(es) :
192.168.1.68

The reason the update request failed was because of a system problem. For specific error code, see the record data displayed below.

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

Data:

0000: 51 27 00 00 Q'..

Next: ===== <

Event Type: Warning
Event Source: DnsApi
Event Category: None
Event ID: 11191

Date: 9/26/2007

Time: 2:26:36 PM

User: N/A

Computer: 28Y26B1

Description:

The system failed to update and remove pointer (PTR) resource records (RRs) for network adapter with settings:

Adapter Name : {137E9C4C-5431-4EB4-9D8C-C0EF69D18734}
Host Name : 28Y26B1
Adapter-specific Domain Suffix : WesternValve.local
DNS server list :
192.168.1.2
Sent update to server : <?>
IP Address : 192.1.1.1

The system could not remove these PTR RRs because because of a system problem. For specific error code, see the record data displayed below.

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

Data:

Re: Slow Logon related to groups – Update!

0000: 51 27 00 00 Q'..

Next: ===== <

Event Type: Error
Event Source: NETLOGON
Event Category: None
Event ID: 5719
Date: 9/26/2007
Time: 2:26:44 PM
User: N/A
Computer: 28Y26B1
Description:
No Domain Controller is available for domain WESTERNVALVE due to the following:
There are currently no logon servers available to service the logon request.
.
Make sure that the computer is connected to the network and try again. If the problem persists, please contact your domain administrator.

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

Data:
0000: 5e 00 00 c0 ^..À

Next: ===== <

Event Type: Information
Event Source: Tcpiip
Event Category: None
Event ID: 4201
Date: 9/26/2007
Time: 2:26:51 PM
User: N/A
Computer: 28Y26B1
Description:
The system detected that network adapter
\DEVICE\TCPIP_{137E9C4C-5431-4EB4-9D8C-C0EF69D18734} was connected to the network, and has initiated normal operation over the network adapter.

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

Data:
0000: 00 00 00 00 02 00 50 00P.
0008: 00 00 00 00 69 10 00 40i..@
0010: 02 00 00 00 00 00 00 00
0018: 00 00 00 00 00 00 00 00

Re: Slow Logon related to groups – Update!

0020: 00 00 00 00 00 00 00 00</p></div>

Next: =====<

Event Type: Warning
Event Source: W32Time
Event Category: None
Event ID: 14
Date: 9/26/2007
Time: 2:26:53 PM
User: N/A
Computer: 28Y26B1
Description:
The time provider NtpClient was unable to find a domain controller to use as a time source. NtpClient will try again in 15 minutes.

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

Next: =====<

Event Type: Error
Event Source: W32Time
Event Category: None
Event ID: 29
Date: 9/26/2007
Time: 2:26:53 PM
User: N/A
Computer: 28Y26B1
Description:
The time provider NtpClient is configured to acquire time from one or more time sources, however none of the sources are currently accessible. No attempt to contact a source will be made for 14 minutes. NtpClient has no source of accurate time.

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

Next: =====<

Event Type: Warning
Event Source: LSASRV
Event Category: SPNEGO (Negotiator)
Event ID: 40960

Re: Slow Logon related to groups – Update!

Date: 9/26/2007

Time: 2:29:00 PM

User: N/A

Computer: 28Y26B1

Description:

The Security System detected an attempted downgrade attack for server cifs/sbserver.WesternValve.local. The failure code from authentication protocol Kerberos was "There are currently no logon servers available to service the logon request. (0xc000005e)".

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

Next: ===== <

Event Type: Warning

Event Source: LSASRV

Event Category: SPNEGO (Negotiator)

Event ID: 40961

Date: 9/26/2007

Time: 2:29:00 PM

User: N/A

Computer: 28Y26B1

Description:

The Security System could not establish a secured connection with the server cifs/sbserver.WesternValve.local. No authentication protocol was available.

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

Next: ===== <

Event Type: Warning

Event Source: LSASRV

Event Category: SPNEGO (Negotiator)

Event ID: 40960

Date: 9/26/2007

Time: 2:30:10 PM

User: N/A

Computer: 28Y26B1

Description:

The Security System detected an attempted downgrade attack for server LDAP/sbserver.WesternValve.local. The failure code from authentication protocol Kerberos was "There are currently no logon servers available to service the logon request. (0xc000005e)".

Re: Slow Logon related to groups – Update!

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

Next: ===== <

Event Type: Warning
Event Source: LSASRV
Event Category: SPNEGO (Negotiator)
Event ID: 40961
Date: 9/26/2007
Time: 2:30:10 PM
User: N/A
Computer: 28Y26B1
Description:
The Security System could not establish a secured connection with the server
LDAP/sbserver.WesternValve.local. No authentication protocol was available.

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

Next: ===== <

Finally it went to the desktop and seems to work fine after that.

Additional Info:

Logged in as the "Domain Administrator"
IP Config /all

Windows IP Configuration

Host Name : 28Y26B1
Primary Dns Suffix : WesternValve.local
Node Type : Hybrid
IP Routing Enabled. : No

Re: Slow Logon related to groups – Update!

WINS Proxy Enabled. : No

DNS Suffix Search List. : WesternValve.local

WesternValve.local

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : WesternValve.local

Description : Intel(R) PRO/100 VE Network
Connection

Physical Address. : 00-13-72-CD-CD-08

Dhcp Enabled. : Yes

Autoconfiguration Enabled : Yes

IP Address. : 192.168.1.68

Subnet Mask : 255.255.255.0

Default Gateway : 192.168.1.1

DHCP Server : 192.168.1.2

DNS Servers : 192.168.1.2

Primary WINS Server : 192.168.1.2

Lease Obtained. : Wednesday, September 26, 2007
2:26:51 PM

Lease Expires : Thursday, October 04, 2007
2:26:51 PM

GPRresult

is blank – when I run the gprresult, it gives me the following message:
INFO: The user "WESTERNVALVE\Administrator" does not have RSOP data.

Logged in as me "Ferrell" on the same workstation
IPConfig /all

Re: Slow Logon related to groups – Update!

Windows IP Configuration

Host Name : 28Y26B1
Primary Dns Suffix : WesternValve.local
Node Type : Hybrid
IP Routing Enabled. : No
WINS Proxy Enabled. : No
DNS Suffix Search List. : WesternValve.local
WesternValve.local

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : WesternValve.local
Description : Intel(R) PRO/100 VE Network
Connection
Physical Address. : 00-13-72-CD-CD-08
Dhcp Enabled. : Yes
Autoconfiguration Enabled : Yes
IP Address. : 192.168.1.68
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.1.1
DHCP Server : 192.168.1.2
DNS Servers : 192.168.1.2
Primary WINS Server : 192.168.1.2
Lease Obtained. : Tuesday, September 25, 2007
7:39:50 AM

Re: Slow Logon related to groups – Update!

Lease Expires : Wednesday, October 03, 2007
7:39:50 AM

GPRresult

Microsoft (R) Windows (R) XP Operating System Group Policy Result tool
v2.0
Copyright (C) Microsoft Corp. 1981–2001

Created On 9/26/2007 at 2:25:16 PM

RSOP results for WESTERNVALVE\Ferrell on 28Y26B1 : Logging Mode

OS Type: Microsoft Windows XP Professional
OS Configuration: Member Workstation
OS Version: 5.1.2600
Domain Name: WESTERNVALVE
Domain Type: Windows 2000
Site Name: Default-First-Site-Name
Roaming Profile:
Local Profile: C:\Documents and Settings\ferrell
Connected over a slow link?: No

COMPUTER SETTINGS

CN=28Y26B1,CN=Computers,DC=WesternValve,DC=local
Last time Group Policy was applied: 9/26/2007 at 1:51:28 PM
Group Policy was applied from: sbsserver.WesternValve.local
Group Policy slow link threshold: 500 kbps

Applied Group Policy Objects

Small Business Server Windows Firewall
Small Business Server Client Computer
Small Business Server Remote Assistance Policy
Small Business Server Lockout Policy
Small Business Server Domain Password Policy
Default Domain Policy

The following GPOs were not applied because they were filtered out

Small Business Server Internet Connection Firewall
Filtering: Denied (WMI Filter)
WMI Filter: PreSP2

Re: Slow Logon related to groups – Update!

Small Business Server – Windows Vista policy
Filtering: Denied (WMI Filter)
WMI Filter: Vista

Local Group Policy
Filtering: Not Applied (Empty)

The computer is a part of the following security groups:

BUILTIN\Administrators
Everyone
BUILTIN\Users
NT AUTHORITY\NETWORK
NT AUTHORITY\Authenticated Users
28Y26B1\$
Domain Computers

USER SETTINGS

CN=Ferrell
Ramey,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=WesternValve,DC=local
Last time Group Policy was applied: 9/26/2007 at 1:09:42 PM
Group Policy was applied from: sbsserver.WesternValve.local
Group Policy slow link threshold: 500 kbps

Applied Group Policy Objects

Default Domain Policy

The following GPOs were not applied because they were filtered out

Small Business Server Client Computer
Filtering: Not Applied (Empty)

Small Business Server Lockout Policy
Filtering: Disabled (GPO)

Small Business Server Internet Connection Firewall
Filtering: Denied (WMI Filter)
WMI Filter: PreSP2

Small Business Server Domain Password Policy
Filtering: Not Applied (Empty)

Small Business Server – Windows Vista policy
Filtering: Denied (WMI Filter)
WMI Filter: Vista

Local Group Policy

Re: Slow Logon related to groups – Update!

Filtering: Not Applied (Empty)

Small Business Server Remote Assistance Policy
Filtering: Disabled (GPO)

Small Business Server Windows Firewall
Filtering: Not Applied (Empty)

The user is a part of the following security groups:

Domain Users
Everyone
BUILTIN\Administrators
BUILTIN\Users
NT AUTHORITY\INTERACTIVE
NT AUTHORITY\Authenticated Users
LOCAL
Web Workplace Users

On the server as the "Domain Admin"

IPConfig /all

Windows IP Configuration

Host Name : sbsserver
Primary Dns Suffix : WesternValve.local
Node Type : Unknown
IP Routing Enabled. : Yes
WINS Proxy Enabled. : Yes
DNS Suffix Search List. : WesternValve.local

PPP adapter RAS Server (Dial In) Interface:

Connection-specific DNS Suffix . :
Description : WAN (PPP/SLIP) Interface

Re: Slow Logon related to groups – Update!

Physical Address. : 00-53-45-00-00-00

DHCP Enabled. : No

IP Address. : 192.168.1.57

Subnet Mask : 255.255.255.255

Default Gateway :

NetBIOS over Tcpi. : Disabled

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :

Description : Intel(R) PRO/1000 MT Network
Connection #2

Physical Address. : 00-13-72-F7-4F-E0

DHCP Enabled. : No

IP Address. : 192.168.1.2

Subnet Mask : 255.255.255.0

Default Gateway : 192.168.1.1

DNS Servers : 192.168.1.2

Primary WINS Server : 192.168.1.2

GPRresult

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
Copyright (C) Microsoft Corp. 1981-2001

Created On 9/26/2007 at 2:24:15 PM

RSOP data for WESTERNVALVE\Administrator on SBSERVER : Logging Mode

OS Type: Microsoft(R) Windows(R) Server 2003 for Small
Business Server
OS Configuration: Primary Domain Controller
OS Version: 5.2.3790
Terminal Server Mode: Remote Administration
Site Name: Default-First-Site-Name
Roaming Profile:
Local Profile: C:\Documents and Settings\Administrator
Connected over a slow link?: No

COMPUTER SETTINGS

CN=SBSERVER,OU=Domain Controllers,DC=WesternValve,DC=local
Last time Group Policy was applied: 9/26/2007 at 2:20:34 PM
Group Policy was applied from: sbserver.WesternValve.local
Group Policy slow link threshold: 500 kbps
Domain Name: WesternValve
Domain Type: Windows 2000

Applied Group Policy Objects

Small Business Server Auditing Policy
Default Domain Controllers Policy
Small Business Server Client Computer
Small Business Server Remote Assistance Policy
Small Business Server Lockout Policy
Small Business Server Domain Password Policy
Default Domain Policy
Local Group Policy

The following GPOs were not applied because they were filtered out

Small Business Server Internet Connection Firewall
Filtering: Denied (WMI Filter)
WMI Filter: PreSP2

Small Business Server – Windows Vista policy
Filtering: Denied (WMI Filter)
WMI Filter: Vista

Small Business Server Windows Firewall
Filtering: Denied (WMI Filter)
WMI Filter: PostSP2

The computer is a part of the following security groups

BUILTIN\Administrators
Everyone

Re: Slow Logon related to groups – Update!

BUILTIN\Users
BUILTIN\Pre-Windows 2000 Compatible Access
Windows Authorization Access Group
NT AUTHORITY\NETWORK
NT AUTHORITY\Authenticated Users
This Organization
SBSERVERS\$
Domain Controllers
Exchange Domain Servers
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
Exchange Enterprise Servers
RAS and IAS Servers

USER SETTINGS

CN=Administrator,CN=Users,DC=WesternValve,DC=local
Last time Group Policy was applied: 9/26/2007 at 1:54:48 PM
Group Policy was applied from: sbserver.WesternValve.local
Group Policy slow link threshold: 500 kbps
Domain Name: WESTERNVALVE
Domain Type: Windows 2000

Applied Group Policy Objects

Default Domain Policy

The following GPOs were not applied because they were filtered out

Small Business Server Client Computer
Filtering: Not Applied (Empty)

Small Business Server Lockout Policy
Filtering: Disabled (GPO)

Small Business Server Internet Connection Firewall
Filtering: Denied (WMI Filter)
WMI Filter: PreSP2

Small Business Server Domain Password Policy
Filtering: Not Applied (Empty)

Small Business Server – Windows Vista policy
Filtering: Denied (WMI Filter)
WMI Filter: Vista

Local Group Policy
Filtering: Not Applied (Empty)

Small Business Server Remote Assistance Policy
Filtering: Disabled (GPO)

Re: Slow Logon related to groups – Update!

Small Business Server Windows Firewall
Filtering: Denied (WMI Filter)
WMI Filter: PostSP2

The user is a part of the following security groups

Domain Users
Everyone
BUILTIN\Administrators
BUILTIN\Users
REMOTE INTERACTIVE LOGON
NT AUTHORITY\INTERACTIVE
NT AUTHORITY\Authenticated Users
This Organization
LOCAL
Group Policy Creator Owners
Domain Admins
QuickbooksGroup
SBS Report Users
OfficeGroup
TimeclockGroup
Enterprise Admins
ManagementGroup
SalesGroup
Schema Admins
SBS Mobile Users
AccountingGroup
ProductionGroup
EngineeringGroup
Offer Remote Assistance Helpers
Debugger Users

Server Event Logs

No events are logged between the login time(s) [9/26/2007 at 2:20PM – 2:45PM, or within 5 minutes either way.

////////////////////////////////////

Note:

When I log into the server at the server as the "Domain Admin"; it does not exhibit this behavior. It logs in quickly and works fine.

Thanks again.

Ferrell Ramey

Re: Slow Logon related to groups – Update!

"Lanwench [MVP – Exchange]" wrote:

Ferrell Ramey <FerrellRamey@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

I have a small business server and have created different security and distribution groups. I've not been able to narrow down which group(s) are causing an issue, but if I try to login to a workstation as the domain admin; the computer will hang for 5–10 minutes or until I unplug the network patch cable.

If I create a brand new user and don't put them into any groups, the computer logs in quickly. I've been going through and adding that user to the different groups and combination of groups trying to figure out what is going on.

This happens on multiple computers with different users, I've been removing the users from all of the groups and then adding them back in one-by-one.

Anyone have any ideas? I'd hate to have to blow away all of the groups and start from scratch. This started in March, the server had always been real quick, and users were able to login into the server quickly, then over night this started.

It seems like my group(s) got corrupted?, is there a "repair" or a way to export, blow away and rebuild them that won't turn into a nightmare?

What do your groups do, exactly?
What do you see in your event logs?
Rsop.msc give you any errors?

I agree with Claus that this is normally a DNS problem – but if you have a

Re: Slow Logon related to groups – Update!

vanilla workstation, and user A can log in with no lag if she's not in Group A, but it takes 10 minutes if she *is* in Group A, then that could be a red herring.