SOLARWINDS WHITEPAPER

Top 5
WSUS Diagnostics Issues Solved!

Lawrence Garvin, WSUS MVP

Bonus!
Common Windows
Error Codes Explained

solarwinds

Table of Contents

Top 5 WSUS Diagnostics Issues Solved!

Summary

Are you using Microsoft's free patch management tool, Windows Sever Update Services or WSUS for patch management? If so, chances are you have some unresolved issues that you just haven't had time to fix. For example, do you have a few machines that won't report to WSUS? Are you wondering why some updates won't download? Or why WSUS has high CPU utilization? In this whitepaper, written by Microsoft MVP and WSUS Expert, Lawrence Garvin, you'll learn how to diagnose and solve the top 5 WSUS performance and configuration issues.

Top 5 WSUS Diagnostics Issues Solved

- Machines not reporting to WSUS? Use the Client Diagnostics Tool
- WSUS not working well? Use the Windows Update Log to identify & repair errors
- WSUS causing high CPU utilization? Determine the cause and fix it
- Duplicate SUSClientIDs in WSUS? Fix them and prevent them
- Excessive WSUS download time or failed downloads? Diagnose and repair
- Bonus: Recent Windows Update Agent Version Numbers
- Bonus: Common Windows Update Agent Error Codes

About the Author:

Lawrence Garvin, M.S., MVP, MCITP, has been working with Microsoft® Windows Server Update Services (WSUS) and Software Update Services (SUS) since the release of SUS SP1 in 2003, and update management, generally, since the creation of Windows Update in 1998. Prior to joining EminentWare (now part of SolarWinds) in 2009, he offered Windows Server Update Services expertise, as Principal/CTO of Onsite Technology Solutions to companies worldwide including deployment, implementation, and troubleshooting advice. Lawrence is also an independent WSUS evangelist and is a frequent contributor to WSUS forums and other online community sites.

Clients not showing up in WSUS?

Use the WSUS Client Diagnostics Tool to test that a client has the necessary functionality to talk to a WSUS Server

The WSUS Client Diagnostics Tool has been designed to aid the WSUS administrator in troubleshooting the client machines that are failing to report back to the WSUS Server. The tool will do a few preliminary checks and test the communication between the WSUS Server and the client machine. Once the tool has completed the tests, it will display the results in the console window. You also have the option to have the results logged to a file in addition to being displayed on the console.

NOTE: The WSUS Client Diagnostic Tool has some limitations as it is only available in 32-bit. It was written before there was a 64-bit WSUS. Specifically, it was written for the WSUS Version 2 environment and has not been updated regularly. It is still a very useful tool, but because it is not aware of WSUS Version 3, some of the results can be misleading.

Before you start, be aware that the Client Diagnostics Tool checks for the correct administrative rights to run this tool, so you must run it from an account with local administrative permissions.

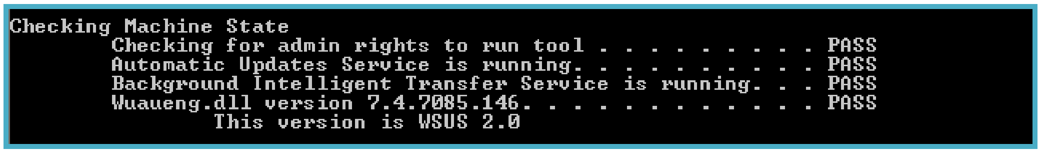
The Client Diagnostics Tool tests four areas to verify that a client has the necessary functionality to talk to a WSUS server:

- Issues about the machine state
- Verifies some automatic update settings
- Looks at the proxy configuration for the client
- Attempts to connect to the WSUS server that is configured in the policy

Verify the Machine State: In this function, the Client Diagnostics Tool will

- Check if the current logged on user running the tool has administrative access as this is required in order to obtain the information required to successfully complete the diagnosis of the machine.
- Check the current state of the Automatic Updates & Background Intelligent Transfer Service (BITS).
- Determine which version of the Windows Update Agent (wuaueng.dll binary) is currently installed.

If you PASS or FAIL the above tests, you will receive a report similar to Diagram 1, below:

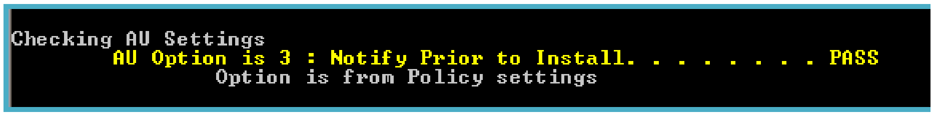


```
Checking Machine State
        Checking for admin rights to run tool . . . . . . . . . PASS
        Automatic Updates Service is running. . . . . . . . . . PASS
        Background Intelligent Transfer Service is running. . . PASS
        Wuaueng.dll version 7.4.7085.146. . . . . . . . . . . . PASS
                This version is WSUS 2.0
```

WSUS Client Diagnostics Tool, Diagram 1.

AU Settings

After verifying that the machine may continue running the tool, the Client Diagnostics Tool will check the Automatic Update (AU) settings, including the AUOptions setting in the registry. This will verify that the settings match and determine whether the AUOption is being set from policy or from the control panel. This will verify that your Windows Update Agent policies are being applied correctly. If you receive a PASS, you will see an image similar to Diagram 2.

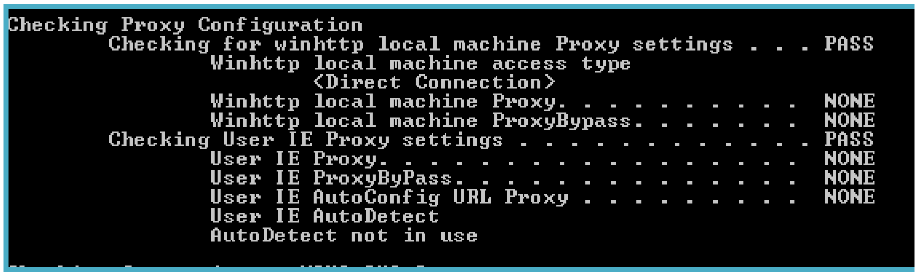


```
Checking AU Settings
        AU Option is 3 : Notify Prior to Install. . . . . . . . PASS
                Option is from Policy settings
```

WSUS Client Diagnostics Tool, Diagram 2

Proxy Configurations:

In this function, the Client Diagnostics Tool will obtain and display the proxy configuration settings for both the Local System (Win HTTP) and the current user Internet Explorer settings. This check is applicable to WSUS environments if the clients need to go through a proxy server to access the WSUS server, or the WSUS server is configured so the clients download the update files from the Microsoft Update service. Unfortunately, it does not provide advice on whether these settings are correct, it simply reports the information. So, if you have a proxy client configuration, verify the settings here.



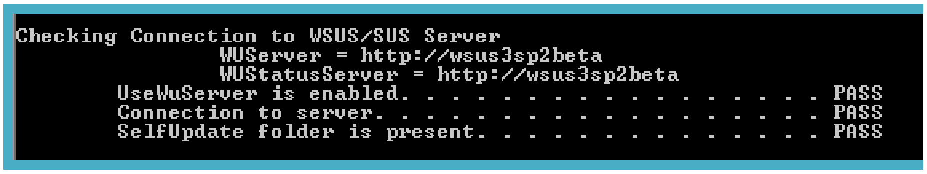
```
Checking Proxy Configuration
        Checking for winhttp local machine Proxy settings . . . PASS
                Winhttp local machine access type
                        <Direct Connection>
                Winhttp local machine Proxy. . . . . . . . . .  NONE
                Winhttp local machine ProxyBypass. . . . . . .  NONE
        Checking User IE Proxy settings . . . . . . . . . . . . PASS
                User IE Proxy. . . . . . . . . . . . . . . . .  NONE
                User IE ProxyByPass. . . . . . . . . . . . . .  NONE
                User IE AutoConfig URL Proxy . . . . . . . . .  NONE
                User IE AutoDetect
                AutoDetect not in use
```

WSUS Client Diagnostics Tool, Diagram 3

Test Connection to the WSUS Server:

For this function, the WSUS Client Diagnostics Tool connects to the WSUS server that is configured via policy. In this section, there are three items that you should check in order to identify problems:

- Ensure that the WUServer and the WUStatusServer values are identical. They must be identical in order for the Window Update Agent to work.
- Ensure that the “UseWUServer” registry value is set to “true.” This enables the Agent to use WSUS instead of using Automatic Updates from Microsoft.com.
- Connect to the server, and then verify that the self-update tree or folder is present on the server. If it is not, you’ll need to add it.



```
Checking Connection to WSUS/SUS Server
                WUServer = http://wsus3sp2beta
                WUStatusServer = http://wsus3sp2beta
        UseWuServer is enabled. . . . . . . . . . . . . . . . . PASS
        Connection to server. . . . . . . . . . . . . . . . . . PASS
        SelfUpdate folder is present. . . . . . . . . . . . . . PASS
```

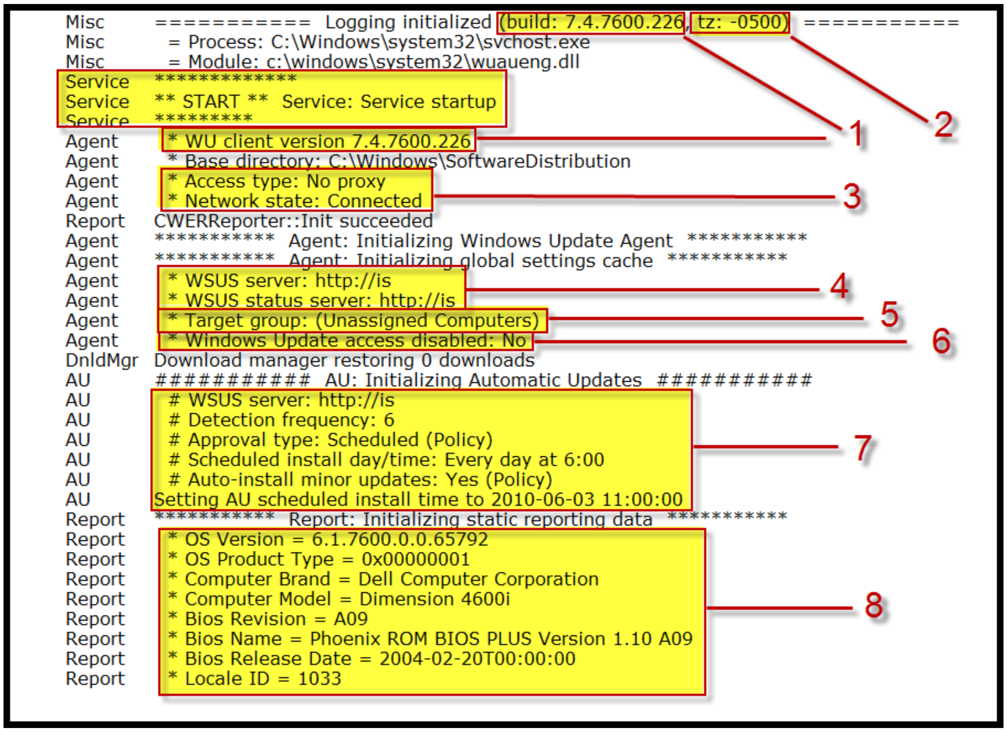
The issues above are some of the most common causes of connection problems, so if the WSUS Client Diagnostics Tool has any issues connecting to the server, it will most likely be detected here and error codes will be displayed.

WSUS simply not working?

Use the “Windows Update Log” to diagnose WSUS issues and identify errors

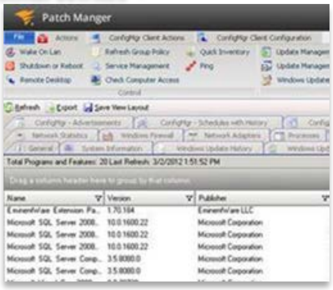
The Windows Update Log is a useful WSUS diagnostics tool that is a rolling log file. It generally contains about 30 days of entries or 2 MB of data, so be aware of these limitations. The Windows Update Log is located in the Windows Directory. The Windows Update Log provides many functions, but in this paper, we’ll discuss five features of the

Windows Update Log that provide useful WSUS diagnostics. These features will help you identify whether WSUS is configured and working correctly, whether there are errors, and ensure that all of your WSUS clients are successfully executing detection.



```
Misc      ===========  Logging initialized (build: 7.4.7600.226, tz: -0500)  ===========
Misc        = Process: C:\Windows\system32\svchost.exe
Misc        = Module: c:\windows\system32\wuaueng.dll
Service   *************
Service   ** START **  Service: Service startup
Service   *********
Agent     * WU client version 7.4.7600.226
Agent     * Base directory: C:\Windows\SoftwareDistribution
Agent     * Access type: No proxy
Agent     * Network state: Connected
Report    CWERReporter::Init succeeded
Agent     ***********  Agent: Initializing Windows Update Agent  ***********
Agent     ***********  Agent: Initializing global settings cache  ***********
Agent     * WSUS server: http://is
Agent     * WSUS status server: http://is
Agent     * Target group: (Unassigned Computers)
Agent     * Windows Update access disabled: No
DnldMgr   Download manager restoring 0 downloads
AU        ###########  AU: Initializing Automatic Updates  ###########
AU         # WSUS server: http://is
AU         # Detection frequency: 6
AU         # Approval type: Scheduled (Policy)
AU         # Scheduled install day/time: Every day at 6:00
AU         # Auto-install minor updates: Yes (Policy)
AU        Setting AU scheduled install time to 2010-06-03 11:00:00
Report    ***********  Report: Initializing static reporting data  ***********
Report    * OS Version = 6.1.7600.0.0.65792
Report    * OS Product Type = 0x00000001
Report    * Computer Brand = Dell Computer Corporation
Report    * Computer Model = Dimension 4600i
Report    * Bios Revision = A09
Report    * Bios Name = Phoenix ROM BIOS PLUS Version 1.10 A09
Report    * Bios Release Date = 2004-02-20T00:00:00
Report    * Locale ID = 1033
```

Windows Update Log, Diagram 1



Items Identified at Service Startup

You can find the service startup section by the banner in the log file that says “Service Startup.” At Service Startup, several items are logged which can be used to identify the particular machine and to verify that settings are correct. The items are:

- The build number of the Windows Update Agent (WUA)
- The time zone at which the entry was logged. All of the text entries in the Windows Update Log are recorded in GMT. The timestamps on the left-hand side are in the machine’s local time, but the log entries themselves are in GMT.
- The proxy configuration for the client and the network state. The Windows Update Agent is aware whether the machine is connected to the network or not. If a detection event is initiated during a disconnected time, the WUA will reschedule the detection to occur when the machine is reconnected to the network.

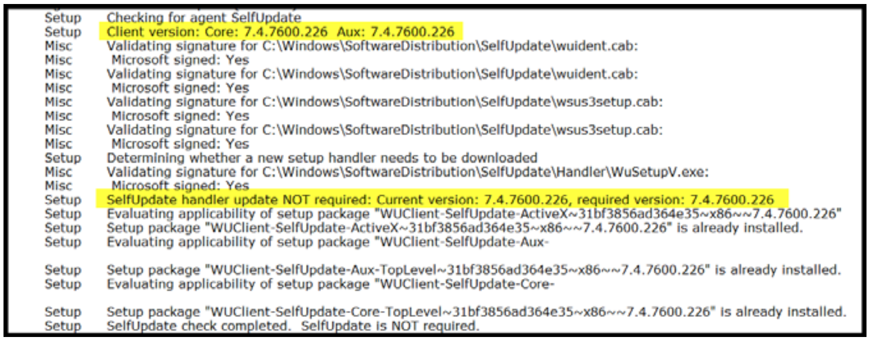
This is particularly useful for notebook machines that are not always connected to the network.

- Configuration parameters for the agent including the WUServer value and the WUStatusServer values
- The target group membership(s) of the machine when client-side targeting is being used.
- The value of the setting for “WindowsUpdateAccessDisabled” which is “yes” or “no.” This policy value can be used to block the user’s ability to access any Windows Update (WU) or Microsoft Update (MU) functionality.
- The WSUS Server URL, the detection frequency, how the updates are being installed, when scheduled events occur, and the next scheduled installation time.
- Inventory information including the operating system version, build number, the computer hardware that it is configured on, and language information

Self-Update

In this section, the machine looks at the current version of the client, looks at the version of the client that’s available from the WSUS server, and then ensures that the client has the latest available version.

See Diagram 2 for an example.



```
Setup   Checking for agent SelfUpdate
Setup   Client version: Core: 7.4.7600.226  Aux: 7.4.7600.226
Misc    Validating signature for C:\Windows\SoftwareDistribution\SelfUpdate\wuident.cab:
Misc     Microsoft signed: Yes
Misc    Validating signature for C:\Windows\SoftwareDistribution\SelfUpdate\wuident.cab:
Misc     Microsoft signed: Yes
Misc    Validating signature for C:\Windows\SoftwareDistribution\SelfUpdate\wsus3setup.cab:
Misc     Microsoft signed: Yes
Misc    Validating signature for C:\Windows\SoftwareDistribution\SelfUpdate\wsus3setup.cab:
Misc     Microsoft signed: Yes
Setup   Determining whether a new setup handler needs to be downloaded
Misc    Validating signature for C:\Windows\SoftwareDistribution\SelfUpdate\Handler\WuSetupV.exe:
Misc     Microsoft signed: Yes
Setup   SelfUpdate handler update NOT required: Current version: 7.4.7600.226, required version: 7.4.7600.226
Setup   Evaluating applicability of setup package "WUClient-SelfUpdate-ActiveX~31bf3856ad364e35~x86~~7.4.7600.226"
Setup   Setup package "WUClient-SelfUpdate-ActiveX~31bf3856ad364e35~x86~~7.4.7600.226" is already installed.
Setup   Evaluating applicability of setup package "WUClient-SelfUpdate-Aux-

Setup   Setup package "WUClient-SelfUpdate-Aux-TopLevel~31bf3856ad364e35~x86~~7.4.7600.226" is already installed.
Setup   Evaluating applicability of setup package "WUClient-SelfUpdate-Core-

Setup   Setup package "WUClient-SelfUpdate-Core-TopLevel~31bf3856ad364e35~x86~~7.4.7600.226" is already installed.
Setup   SelfUpdate check completed.  SelfUpdate is NOT required.
```

Windows Update Log, Diagram 2

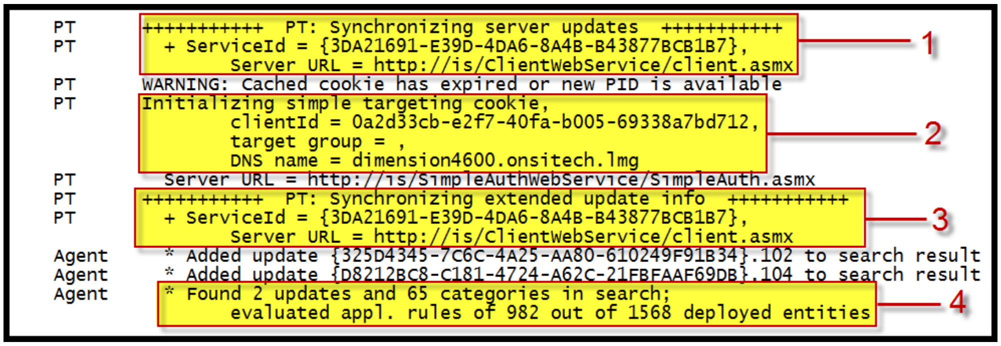
Detection Process

This process involves four steps. If any of these four steps encounter an issue, the Windows Update Agent will log an error message.

- Call the client web service.
- Initialize the targeting cookie and a call to the “simpleauth” web service.

- Call against the client web service to get the extended update information.
- Produce a log entry showing how many updates were detected, how many product categories were searched, and how many updates were tested.

See Diagram 3 for an example.

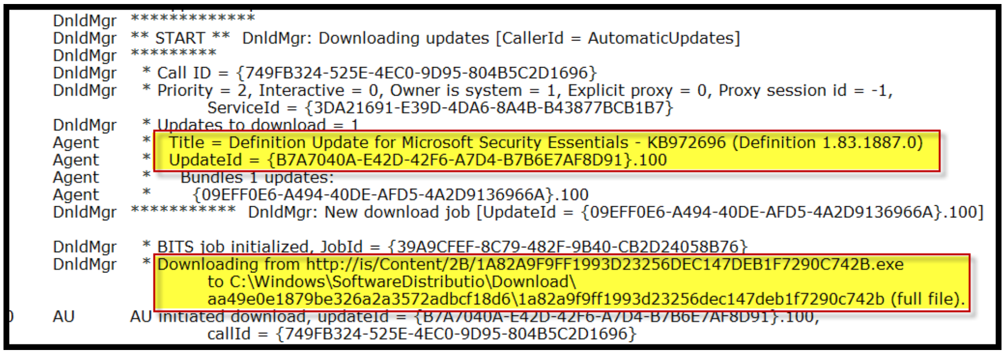


```
PT          ++++++++++++  PT: Synchronizing server updates  ++++++++++++
PT            + ServiceId = {3DA21691-E39D-4DA6-8A4B-B43877BCB1B7},
                      Server URL = http://is/ClientWebService/client.asmx
PT          WARNING: Cached cookie has expired or new PID is available
PT          Initializing simple targeting cookie,
                      clientId = 0a2d33cb-e2f7-40fa-b005-69338a7bd712,
                      target group = ,
                      DNS name = dimension4600.onsitech.lmg
PT            Server URL = http://is/SimpleAuthWebService/SimpleAuth.asmx
PT          ++++++++++++  PT: Synchronizing extended update info  ++++++++++++
PT            + ServiceId = {3DA21691-E39D-4DA6-8A4B-B43877BCB1B7},
                      Server URL = http://is/ClientWebService/client.asmx
Agent         * Added update {325D4345-7C6C-4A25-AA80-610249F91B34}.102 to search result
Agent         * Added update {D8212BC8-C181-4724-A62C-21FBFAAF69DB}.104 to search result
Agent         * Found 2 updates and 65 categories in search;
                      evaluated appl. rules of 982 out of 1568 deployed entities
```

Windows Update Log, Diagram 3

Downloading:

Downloading creates simple log entries. The download initiates then the agent hands the download off to the Background Intelligent Transfer Service (BITS). Two items are logged in the Windows Update Log. The first is the title of the update (this is the only place that the actual title of the update is logged.) Secondly, the log tracks where the update is being downloaded from, where it's being downloaded to, and the actual file name on the WSUS server that is being transferred. If there are any issues downloading, you'll see it in the Windows Update Log. See Diagram 4 for an example.



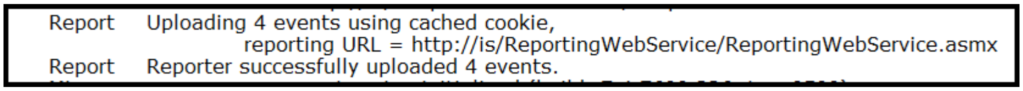
```
DnldMgr  *************
DnldMgr  ** START **  DnldMgr: Downloading updates [CallerId = AutomaticUpdates]
DnldMgr  *********
DnldMgr    * Call ID = {749FB324-525E-4EC0-9D95-804B5C2D1696}
DnldMgr    * Priority = 2, Interactive = 0, Owner is system = 1, Explicit proxy = 0, Proxy session id = -1,
                  ServiceId = {3DA21691-E39D-4DA6-8A4B-B43877BCB1B7}
DnldMgr    * Updates to download = 1
Agent      *  Title = Definition Update for Microsoft Security Essentials - KB972696 (Definition 1.83.1887.0)
Agent      *  UpdateId = {B7A7040A-E42D-42F6-A7D4-B7B6E7AF8D91}.100
Agent      *    Bundles 1 updates:
Agent      *      {09EFF0E6-A494-40DE-AFD5-4A2D9136966A}.100
DnldMgr  ***********  DnldMgr: New download job [UpdateId = {09EFF0E6-A494-40DE-AFD5-4A2D9136966A}.100]

DnldMgr    * BITS job initialized, JobId = {39A9CFEF-8C79-482F-9B40-CB2D24058B76}
DnldMgr    * Downloading from http://is/Content/2B/1A82A9F9FF1993D23256DEC147DEB1F7290C742B.exe
                  to C:\Windows\SoftwareDistributio\Download\
                  aa49e0e1879be326a2a3572adbcf18d6\1a82a9f9ff1993d23256dec147deb1f7290c742b (full file).
AU       AU initiated download, updateId = {B7A7040A-E42D-42F6-A7D4-B7B6E7AF8D91}.100,
                  callId = {749FB324-525E-4EC0-9D95-804B5C2D1696}
```

Windows Update Log, Diagram 4

Reporting

Reporting also creates simple log entries. WSUS tracks reporting calls to the ReportingWebService. At a minimum, this executes an event that will always upload two events. See Diagram 5, for an example. If there are any issues executing the call, you'll see an error in the Windows Update Log



```
Report    Uploading 4 events using cached cookie,
                    reporting URL = http://is/ReportingWebService/ReportingWebService.asmx
Report    Reporter successfully uploaded 4 events.
```

Windows Update Log, Diagram 5

WSUS causing high CPU utilization?

Check for high CPU utilization on the servicehost.exe process

The Window Update Client runs on the svchost.exe process. If you notice high CPU utilization caused by this process, there are several common issues that may be the cause. Here is a list of questions that will help you diagnose the issue:

Are you running WSUS Version 2? If yes and you are experiencing high CPU utilization issues, then the best fix is to upgrade to WSUS 3 or the most recent version of WSUS.

Are you using Outlook 2003 with Office XP? If yes and you are experiencing svchost.exe performance issues, the best resolution is to upgrade Office XP to a newer version of Office. This issue primary occurs in SBS 2003 environments where Outlook 2003 may have been deployed on older Windows XP/Office XP machines.

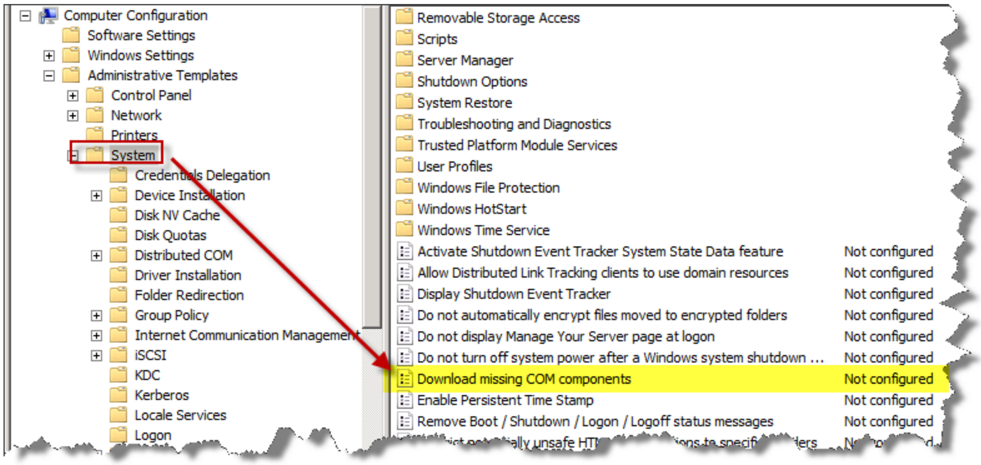
Are you using Office 2003 with a large number of updates already applied on the client? The svchost.exe process may run slowly because the Windows Installer folder has a large number of packages. The client must scan these updates each time to inventory what is on the machine. The recommended fix is to uninstall Office 2003, which will clear out that folder, reinstall Office 2003, and apply Service Pack 3 directly to the machine. This will minimize the number of files contained in the installer folder.

Do you have superseded updates on the WSUS server that have not been declined? If so, and you are experiencing high CPU utilization, are you also using the v7.1 client? There were known performance issues in the v7.1 client with large volumes of updates being scanned. To fix this issue, you need to do two things:

- Mark the superseded updates as “declined.”
- Upgrade to the latest client. This can be done by upgrading to WSUS 3 Service Pack 2 which has a new build of the Windows Update Agent (v7.4) which will fix the issue. You can also browse to Windows Update or Microsoft Update, or download the Windows Update Agent 3.0 installer.

Do you have a Group Policy conflict with Windows Update Agent v7.4?

If you have updated the WUAgent to v7.4, there is a known conflict with the WUAgent v7.4 client and a particular Group Policy setting shown to the right. To eliminate the conflict, verify that the Group Policy setting “Download missing COM components” is Disabled or Not Configured. You will find this setting in Computer Configuration\Administrative Templates\System.



- Computer Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates
    - Control Panel
    - Network
    - Printers
    - System
      - Credentials Delegation
      - Device Installation
      - Disk NV Cache
      - Disk Quotas
      - Distributed COM
      - Driver Installation
      - Folder Redirection
      - Group Policy
      - Internet Communication Management
      - iSCSI
      - KDC
      - Kerberos
      - Locale Services
      - Logon

Removable Storage Access	
Scripts	
Server Manager	
Shutdown Options	
System Restore	
Troubleshooting and Diagnostics	
Trusted Platform Module Services	
User Profiles	
Windows File Protection	
Windows HotStart	
Windows Time Service	
Activate Shutdown Event Tracker System State Data feature	Not configured
Allow Distributed Link Tracking clients to use domain resources	Not configured
Display Shutdown Event Tracker	Not configured
Do not automatically encrypt files moved to encrypted folders	Not configured
Do not display Manage Your Server page at logon	Not configured
Do not turn off system power after a Windows system shutdown ...	Not configured
Download missing COM components	Not configured
Enable Persistent Time Stamp	Not configured
Remove Boot / Shutdown / Logon / Logoff status messages	Not configured

Try disabling the Group Policy Setting “Download missing COM components”

Duplicate SUSClientIDs?

Clean up and prevent them to keep WSUS running well

Duplicate SUSClientIDs are caused when a machine is cloned from a master image that already has a SusClientID stored in the registry. It is an issue that becomes more complicated to fix over time, so it’s in your best interest to solve this as soon as you realize it’s an issue.

The Duplicate SUSClientID can cause two problems

- First, your WSUS console will only show a percentage of the machines in your environment. While the names of the machines change, the physical number of machines in the list is fixed. This number shown by WSUS is the number of unique SusClientIDs in the environment, but not the actual number of client systems. If you have 1000 machines, WSUS could show as little as one machine if every machine in the environment has been incorrectly cloned from a single master image.
- Secondly, certain error codes can be directly traced to duplicate SusClientIDs. If you’re seeing any of these error codes, duplicate SusClientIDs are most likely the reason. (See Page 9 for a description of common WSUS error codes.)

How to fix duplicate SUSClientIDs

In older versions of WSUS, prior to version 3, the problem automatically resolved itself by comparing the machine SIDS and the Windows Update Agent Version 5 client registry value called AccountDomainSID. If they didn't match, the Windows Update Agent would automatically generate a new SUSClientID.

However, if you're using WSUS 3 which installs the Windows Update Agent Version 7 release, the AccountDomainSID value was removed from the registry. So there is nothing to tell the Windows Update Agent that it should generate a new SusClientID. To fix the problem, you must delete the SUSClientID from the registry. Then the Windows Update Agent sees that the ID is missing and will generate a new one.

There are two places to find the SUSClientID:

- In the registry in the CurrentVersion\WindowsUpdate key.
- It is also logged in the "Initializing Simple Targeting Cookie" log entry in the Windows Update Log.

The Solution

The preferred fix would be to remove the applicable registry key from your master image before cloning. If you are unable to do this, you must remove the duplicate ID from each of the cloned machines and then restart the Automatic Updates service, which will generate a new unique value and replace the old one.

Luckily, the Windows Update Agent v7.4 has been enhanced to auto-detect and remediate duplicate SusClientIDs. Therefore, the duplicate SUSClientID issue should cease to exist in the future for environments running WSUS v3 SP2 and the WUAgent v7.4!,

Long-running or failed downloads?

Use WSUS Server-Side Diagnostics to analyze and repair

If a download is taking a very long time, first determine how many approved updates you have waiting. If you have 50 or more updates, simply put, you have a lot of content to be downloaded. Numerous waiting updates makes BITS run slowly. This service runs based upon available bandwidth.

If downloads are actually failing, you will need to check for errors in the Application Event Log on the WSUS server. There are two common error codes that will show reasons for a download failure:

HTTP v1.1 Range Protocol Header

The failure is caused by a firewall, proxy server, or other network appliance between the WSUS Server and Microsoft that is not properly configured or that is not capable of supporting the HTTP Version 1.1 Range Protocol Header that is being used in the download instance. The solution: There are some third-party firewall and proxy server appliances that either do not support or have not been configured to support the WSUS range protocol header. This behavior has also been observed to be caused by some web filtering appliances. If you see an Application Event Log entry that says something about Range Protocol Headers, the most likely cause is a device that is sitting between you and the Internet. This is a very common issue with SonicWall appliances. A fix is available on SonicWall's website, or visit the website of the appliance in question for advice.

Permissions on the non-SYSVOL volume

If content is being stored on a volume other than the system volume, most likely, access is being denied on that other volume. You will often see this as "access denied" for drive D or drive E, etc. The solution: This is actually a defect in the .NET Framework. Unfortunately, .NET does not automatically give the Network Service account read access to the ROOT of non-SYSVOL drives. So when WSUS is configured to write to those drives, the Network Service account cannot read the ROOT of the drive and find the path to write. To fix this issue, you must add the Network Service account to the ROOT drive and give it "read" permissions. Simply select the drive, go to the security tab, add the Network Service account, and add "read" permissions.

Recent Windows Update Agents: Details

- Version 7.6 is an upgrade available for Windows 7 SP1 and Windows Server 2008 R2 SP1 systems to fix a defect in the 7.5 agent.
- Version 7.5 shipped in the Service Pack 1 upgrade for Windows Server 2008 R2.
- Version 7.4 is the current primary production release. It shipped with WSUS Version 3 Service Pack 2
- Version 7.3 shipped in Windows 7 and Windows Server 2008 R2
- Version 7.2 was released in Summer, 2008, to Windows Update and Microsoft Update clients
- Version 7.1 comes from WSUS Version 3 Service Pack 1
- Version 7.0 client comes from WSUS Version 3, the release version from 2007
- Finally, there are the older version 5 clients, which are relevant to WSUS Version 2 and Software Update Services-

Common Windows Update Agent Error Codes

HTTP 401 error codes

(0x80190191 or 0x80244017)

These are access issues and are typically caused because the virtual server, the default website, the WSUS administration website, or one or more of the virtual directories don't have the correct IIS permissions – and anonymous access has been removed. This may be caused where permissions have been set on the IIS web server before WSUS installed.

HTTP 403 error codes

(0x80190193 or 0x80244018)

Commonly caused when the proxy client configuration for Win HTTP is not correct or when the proxy server is interfering. These may also occur on the server side if the Options|Proxy Configuration setting for the WSUS server is improperly set and the Internet firewall or proxy server is interfering. You may also see these on Windows Server 2008 systems or down level systems if the firewall has been enabled and the proper ingress filters for the web service ports are not enabled. (By default, a WSUS server needs to have port 80 open to support basic content. If you're using the WSUS administration alternate site, you'll need 8530, if you're using SSL, you'll also need 443 or 8531.)

HTTP 404 errors

(0x80190194 or 0x80244019)

This typically occurs after WSUS 3 Service Pack 1 has been applied. It may also occur when content has been inadvertently deleted from the WSUS content folder, and the WUA tries to download the missing file. This may happen after using the Server Cleanup Wizard while the client is still trying to download content that that was previously approved or because the files have actually been removed from the folder tree. Use the wsusutil reset command to have the WSUS server identify any content that should be there and download it again.

0x80072EE5 is an invalid URL error code

Typical cause: there are trailing slashes in the URL in the policy definition, resulting in a double-slash when the rest of the path name is appended for a file download. The trailing slash should not be in the URL name and should be removed.

0x80072EE6 error, identified as an unrecognized scheme

This is a URL problem. A URL may have missing or invalid characters; URLs have backslashes instead of forward slashes, the URLs are missing the prefix entirely, or the URLs have been defined with a UNC machine name rather than a URL. To fix, check all URLs to ensure that they are correct.

HTTP 401 error codes

(0x80190191 or 0x80244017)

These are access issues and are typically caused because the virtual server, the default website, the WSUS administration website, or one or more of the virtual directories don't have the correct IIS permissions – and anonymous access has been removed. This may be caused where permissions have been set on the IIS web server before WSUS installed.

HTTP 403 error codes

(0x80190193 or 0x80244018)

Commonly caused when the proxy client configuration for Win HTTP is not correct or when the proxy server is interfering. These may also occur on the server side if the Options|Proxy Configuration setting for the WSUS server is improperly set and the Internet firewall or proxy server is interfering. You may also see these on Windows Server 2008 systems or down level systems if the firewall has been enabled and the proper ingress filters for the web service ports are not enabled. (By default, a WSUS server needs to have port 80 open to support basic content. If you're using the WSUS administration alternate site, you'll need 8530, if you're using SSL, you'll also need 443 or 8531.)

HTTP 404 errors

(0x80190194 or 0x80244019)

This typically occurs after WSUS 3 Service Pack 1 has been applied. It may also occur when content has been inadvertently deleted from the WSUS content folder, and the WUA tries to download the missing file. This may happen after using the Server Cleanup Wizard while the client is still trying to download content that that was previously approved or because the files have actually been removed from the folder tree. Use the wsusutil reset command to have the WSUS server identify any content that should be there and download it again.

0x80072EE5 is an invalid URL error code

Typical cause: there are trailing slashes in the URL in the policy definition, resulting in a double-slash when the rest of the path name is appended for a file download. The trailing slash should not be in the URL name and should be removed.

0x80072EE6 error, identified as an unrecognized scheme

This is a URL problem. A URL may have missing or invalid characters; URLs have backslashes instead of forward slashes, the URLs are missing the prefix entirely, or the URLs have been defined with a UNC machine name rather than a URL. To fix, check all URLs to ensure that they are correct.