

# Troubleshooting the Infamous Event ID 333 Errors

Use Tips And Microsoft Tools To Diagnose And Resolve These Elusive Errors

Michael Morales

(Reprinted From WindowsItPro Magazine)

## Executive Summary

Event ID 333 errors are some of the most difficult Windows System event log errors to troubleshoot. Learn how to diagnose and resolve event ID 333 errors more quickly, using Microsoft's Performance Monitor, poolmon.exe, and dureg.exe tools and troubleshooting tips from a Microsoft support professional.

Windows Server 2003 SP1 introduced event ID 333 into the System event log. This particular event ID is quickly becoming one of the most frequent generators of Microsoft support calls—some of which have taken weeks to resolve. During such calls, we spend much time trying to figure out which general category the event 333 errors fall into. Because of its cryptic description, the error is time-consuming to diagnose and resolve. I'll give you some pointers for understanding troubleshooting an event ID 333 error, so that you can either solve the problem yourself or obtain information about it that will speed up a support call.

## Event ID 333 Symptoms

Event ID 333's description is An I/O operation initiated by the Registry failed unrecoverably. The Registry could not read in, write out, or flush, one of the files that contain the system's image of the Registry. This means that the image of the registry held in memory could not be written to disk. Windows uses what's called the lazy writer to periodically write modified pages of memory to disk. When the lazy writer fails, an event ID 333 is recorded in the System event log.

The symptoms that might accompany the event ID 333 errors include these:

- Server hangs: Your server may completely stop responding to keyboard or mouse movements and appears completely locked up, requiring a hard reboot.
- Server sluggishness: The server is extremely slow to respond at the console, and processing information is significantly delayed.
- Delayed Terminal Services connections: Users trying to log on to a terminal server could experience slow or delayed logons. Once they log on, they may be able to work without a slow experience; however, the logon takes several minutes instead of a few seconds.

Generally, event ID 333 can be classified into three categories:

- Memory resource depletion: At the time the lazy writer attempted to write the modified pages in cache to disk, there weren't enough resources to complete the operation. Often this type of problem is accompanied by either an event ID 2020 or 2019.
- Disk was too busy or inaccessible: Sometimes a busy disk might not respond quickly enough to handle the lazy writer's request to commit modified pages of memory to disk.
- Registry bloat: The registry suddenly grows in size, which makes it increasingly difficult for the lazy writer to commit the changes to disk, commonly occurring on terminal servers.

# Troubleshooting the Infamous Event ID 333 Errors

Use Tips And Microsoft Tools To Diagnose And Resolve These Elusive Errors  
Michael Morales

(Reprinted From WindowsItPro Magazine)

Especially frustrating is how the events continue to flood the System event log (many times per minute) until the server is rebooted. All it takes is one time for the lazy writer to fail for the event flooding to begin. Although the condition that caused the lazy writer to fail might have been brief (such as a short spike in memory usage), event ID 333 continues to be logged even during normal memory utilization. The event is still logged because the system recognizes that a failure to sync the registry has occurred and the registry version contained in memory is out of sync with the version on disk. As a result, the number and frequency of event ID 333 messages isn't a good indicator of the problem's severity. By default the lazy writer tries to flush to disk every five seconds.

## Event ID 333 Troubleshooting Tools

When troubleshooting event ID 333 errors, first you must determine which general category the error falls into. Also it's useful to check the System event log for any other event IDs that accompany the 333 error, such as event ID 2020, which indicates a lack of paged pool memory, or event ID 2019, which indicates a leak in nonpaged pool memory.

These tools can assist in further diagnosing event ID 333 messages:

- Performance Monitor: The counters to track are the system, memory, disk, and process objects.
- Memory object: Look for a rise in nonpaged or paged memory.
- Process object: Look for continuous rises in a process's handles just prior to the event ID 333's being logged.
- System object: The %Registry Quota In Use counter can be useful in displaying how much of the allowed registry quota is being utilized. The higher the percentage, the more likely that the problem is related to a growing registry.
- Physical disk: Look for increases in the Avg Disk Queue Length counter, which tracks the average number of read and write requests to the selected disk. If this counter spikes during the problem, start investigating the filter drivers (i.e., antivirus or backup software) on your system.
- Poolmon.exe: This tool, which is included in the Windows Debugging Tools, is used to track kernel pool memory usage by pool-allocation tag name. Using poolmon.exe can halve your troubleshooting time by enabling you to find the tag that's leaking memory.
- Dureg.exe: This tool lets you view the size of the entire registry per hive. Dureg.exe is great for finding which registry hive is consuming the most space, which helps to determine what software might be causing the problem.

## Case 1: Finding a Memory-Leaking Driver

I recently worked on an issue where the customer's Windows 2003 SP2 server completely hung. Accompanying the event ID 333 was also event 2019, The server was unable to allocate from the system nonpaged pool because the pool was empty. The addition of the 2019 error told me that this

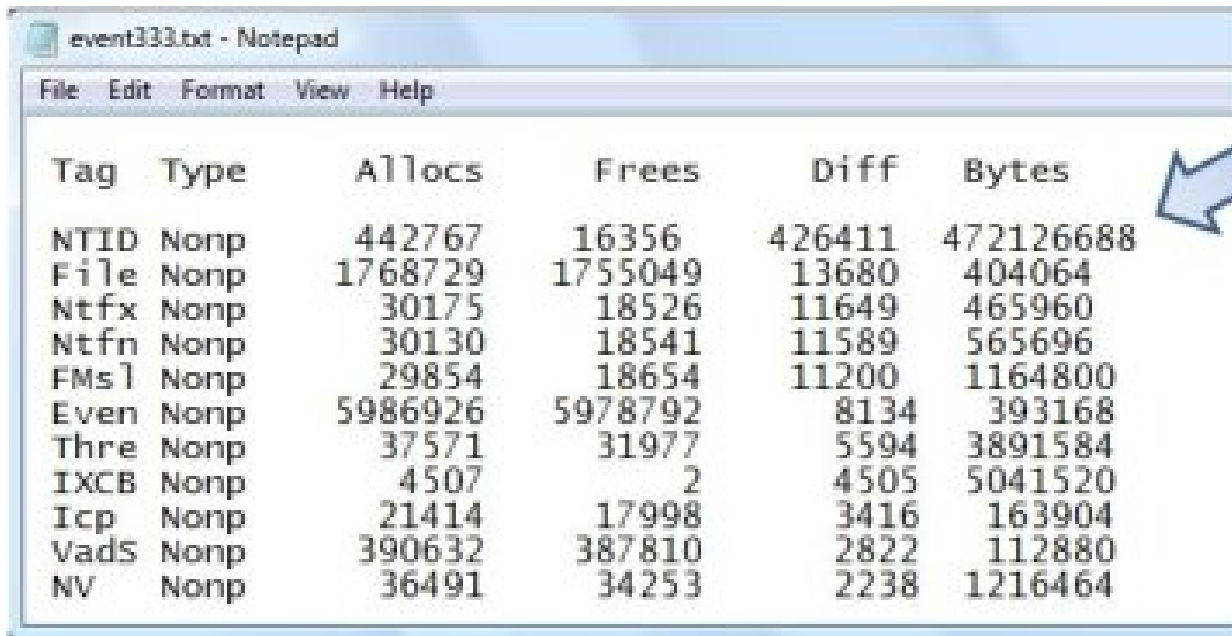
## Troubleshooting the Infamous Event ID 333 Errors

Use Tips And Microsoft Tools To Diagnose And Resolve These Elusive Errors  
Michael Morales

(Reprinted From WindowsItPro Magazine)

was a resource-depletion issue, so the next step was to determine which driver was leaking. As Figure 1 shows, the output that poolmon.exe captured helped to pinpoint which tag allocated the highest amount of memory.

**Figure 1**  
**Poolmon.Exe Output Indicating A Leaking Tag**



Tag	Type	Allocs	Frees	Diff	Bytes
NTID	Nonp	442767	16356	426411	472126688
File	Nonp	1768729	1755049	13680	404064
Ntfx	Nonp	30175	18526	11649	465960
Ntfn	Nonp	30130	18541	11589	565696
FMsl	Nonp	29854	18654	11200	1164800
Even	Nonp	5986926	5978792	8134	393168
Thre	Nonp	37571	31977	5594	3891584
IXCB	Nonp	4507	2	4505	5041520
Icp	Nonp	21414	17998	3416	163904
Vads	Nonp	390632	387810	2822	112880
NV	Nonp	36491	34253	2238	1216464

To help in quickly identifying the leaky tag, use the -b switch, which will sort the output based on byte usage for each tag. The tag at the top of the output is the tag that has consumed the most amount of memory (in bytes).

Our next step was to use the built-in Windows Findstr utility to find the driver associated with the NTID tag, by running this command:

```
C:\>findstr /m /s "NTID" *.sys
```

The /m switch tells Findstr to list only the filename in the output, and the /s switch searches in only the current folder and its subfolders. The Findstr output yielded the driver C:\WINDOWS\SYSTEM32\DRIVERS\CPQTEAM.SYS.

Armed with the pool-allocation tag and name of the driver leaking memory, our final step was to do a simple search on "NTID CPQTEAM". In the search results, we found a link to HP's tech forum that discussed a memory leak associated with a specific version of the Cpqteam.sys driver.

# Troubleshooting the Infamous Event ID 333 Errors

Use Tips And Microsoft Tools To Diagnose And Resolve These Elusive Errors  
Michael Morales

(Reprinted From WindowsItPro Magazine)

## Case 2: Tracking Heavy Registry Usage

Not all event ID 333 errors are a result of a resource problem, however. It's possible to have event ID 333 errors and be unable to correlate them with any resource depletion. One such issue I worked on occurred on a Terminal Services server on which event ID 333 was flooding the System event log. Using Performance Monitor, we noticed that the counter %Registry Quota In Use was greater than 98 (i.e., the system was using more than 98 percent of the allowed system quota for registry size). Knowing that the system was heavily utilizing the registry, we took another look at the Application event log entries during the problem period and found an event ID 1517, which Figure 2 shows.

**Figure 2**  
**Event ID 1517**

```
Event Type: Warning
Event Source: Userenv
Event Category: None
Event ID: 1517
Date: Date
Time: Time
User: NT AUTHORITY\SYSTEM
Computer: ComputerName
Description:
Windows saved user User_Name 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.
```

Event 1517 indicates that the registry isn't being freed when users log off. Our Performance Monitor counter %Registry Quota in Use correlates this information. We searched Microsoft Help and Support for "1517" and "registry" and found an article at [support.microsoft.com/kb/944984](http://support.microsoft.com/kb/944984) that fixed our problem.

Dureg.exe is another utility that's becoming increasingly popular to use for troubleshooting event ID 333 errors. Dureg.exe output needs to be collected once before users experience a problem and again during the problem period to determine whether the registry is becoming bloated. The first run of dureg.exe (before the problem) would look like this:

```
C:\>dureg.exe /a
Size of HKEY_CLASSES_ROOT : 11627272
Size of HKEY_USERS : 56739224
Size of HKEY_LOCAL_MACHINE : 47719408
Total Registry data size: 115985904
```

The second time you'd run dureg.exe would be when the slow logon and event ID 333 problems are occurring, like this:

## Troubleshooting the Infamous Event ID 333 Errors

Use Tips And Microsoft Tools To Diagnose And Resolve These Elusive Errors  
Michael Morales

(Reprinted From WindowsItPro Magazine)

```
C:\>dureg.exe /a
Size of HKEY_CLASSES_ROOT : 11879338
Size of HKEY_USERS : 335257592
Size of HKEY_LOCAL_MACHINE : 46006166
Total Registry data size: 392142994
```

Notice the large change in the HKEY\_USERS key, from 56MB to 334MB. Although this size discrepancy doesn't necessarily resolve the problem, the information provides a valuable starting point for tech support that can drastically reduce the time needed to resolve the problem.

For this particular example, you'd want to run regedit and navigate to:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Terminal
Server\Install\Software.
```

Then look for duplicate registry keys associated a particular application because the values of this key are copied to a user's profile (HKEY\_USERS) when the user logs on to a terminal server. An application might be flooding the Software key with values that end up bloating the registry and causing the Event ID 333 errors. Merely deleting any duplicate values under the HKEY\_USERS key would be inadequate because the next time the user logged on, all those duplicate keys would be copied from the Software key to the HKEY\_USERS key, and the problem would continue.

### Faster Problem-Solving

Although troubleshooting Event ID 333 errors can be tricky, you've now learned ways to make the process easier. With help from Performance Monitor, poolmon.exe, and dureg.exe, you can more easily spot causes of Event ID 333 problems and use that information to resolve such problems faster.