Microsoft-Windows-Kernel-General

The following tries to document the meaning behind some of the obscure events

EventID 15 (Registry Reorganization)

TBD

EventID 16 (Access Bits Cleared)

Message: `The access history in hive [HiveName] was cleared updating [KeysUpdated] keys and creating [DirtyPages] modified pages.` Fields: - HiveNameLength - HiveName - KeysUpdated - DirtyPages

This event is generated by the kernel when the `Access bits` flag of a registry hive is cleared. You can read more about the registry hive structure here.

The TL;DR is that the key node of a registry hive cell contain a field called `Access bits` that include information to help track when a key node was accessed since the last registry reorganization. Windows regularly reset the bits to 0 (hence the trigger the log).

You can use utilities such as Registry Explorer or yarp to view these values.

The clearing of the bits entails a reorganization of the registry as well. By default the kernel uses a value of 7 days to perform this. We can see from the following example using `yarp`.

```
Hive information:

Last written timestamp (UTC): 2012-05-22 00:00:19.594736
Last reorganized timestamp (UTC): 2023-10-06 08:24:12.068414
Serialization timestamp (UTC): None

Keys and values:

Root key
Last written timestamp (UTC): 2012-05-22 00:00:08.562312
Access bits: 2
Owner SID: S-1-5-32-544

---

Key path: LocalState
Last written timestamp (UTC): 2012-05-22 00:00:05.375980
Access bits: 0
Owner SID: S-1-5-32-544

---

Key path: RoamingState
Last written timestamp (UTC): 2012-05-22 00:00:13.752970
Access bits: 0
```

```
Owner SID: S-1-5-32-544

---
```

The above output is from the `settings.dat` hive of the Windows Maps application. As you can se the last reorganized timestamp is a couple of months old from the day of this writeup. But as soon as we launch this application and check with yarp again we can see an update to that value an a reset of the access bits event.

```
Hive information:

Last written timestamp (UTC): 2012-05-22 00:00:19.594736
Last reorganized timestamp (UTC): 2024-01-18 14:18:15.614622
Serialization timestamp (UTC): None

Keys and values:

Root key
Last written timestamp (UTC): 2012-05-22 00:00:08.562312
Access bits: 2
Owner SID: S-1-5-32-544

---

Key path: LocalState\PersistentSettingsModels
Last written timestamp (UTC): 2024-01-18 14:18:21.378170
Access bits: 2
Owner SID: S-1-5-32-544

---
...
...
...
```

```
The access history in hive \??\C:\Users\xxxx\AppData\Local\Packages\Micr
```

```
<EventData>
    <Data Name="HiveNameLength">99</Data>
    <Data Name="HiveName">\??\C:\Users\xxxx\AppData\Local\Packages\Micro
    <Data Name="KeysUpdated">1</Data>
    <Data Name="DirtyPages">1</Data>
</EventData>
```

Internally the log is written by the kernel (ntoskrnl.exe) `CmpLogClearAccessBitsEvent` function which is called by the `CmpClearKeyAccessBits` function. The latter is also part of the `CmpReorganizeHive` function which also compares the value of `CmpReorganizeDelayDays`.

> **Note**
>
> Some of the hives for Windows AppX packages initiated this process from service `AppXSvc` (AppXDeploymentServer.dll). Which seems to contain the concept of `DirtyPackages`. I didn't look too much into it but could be an interesting area to explore to determine how these packages handle and perhaps initiate the registry reorganization
>
> Another interesting DLL that contains potential functions related to clearing hive bits is the `daxexec.dll` with the function `ORClearBits` which might be related to all of this. Something further to explore in the future.

Appendix

The following resources were a of great help in order to understand these events

- https://github.com/msuhanov/yarp/blob/master/yarp/RegistryFile.py
- https://twitter.com/errno_fail/status/972914221779439618

- https://github.com/msuhanov/regf/blob/master/Windows%20registry%20file%20format%20specification.md#key-node
- Windows Internals Seventh Edition Part 2