KMS Server Explained

By Tarun Chhabra, Microsoft Support Engineer

KMS Overview

KMS is a client – server model. It is conceptually similar to DHCP Server. Instead of handing out IP addresses to clients on their request, KMS enables product activation. KMS is also a renewal model, with the clients attempting to reactivate on a regular interval. There are two roles: the *KMS host* and the *KMS client*.

- The **KMS host** runs the activation service and enables activation in the environment. The KMS host is the system where you will need to install a key (the KMS key from the Volume License Service Center (VLSC)) and then activate the service. The service is supported on Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2.
- The **KMS client** is the Windows operating system that is deployed in the environment and needs to activate. KMS clients can be running any edition of Windows that uses Volume Activation. These include the editions of Windows available to our volume license customers: Windows 7, Windows Vista, Windows Server 2008 R2, and Windows Server 2008. The KMS clients come with a key pre-installed, called the Generic Volume License Key (GVLK) or KMS Client Setup Key. The presence of the GVLK is what makes a system a KMS client. The KMS clients find the KMS host via a DNS SRV record (_vlmcs._tcp) and then automatically attempt to discover and use this service to activate themselves. When in the 30 day *Out of Box* grace period, they will try to activate every 2 hours. Once activated, the KMS clients will attempt a renewal every 7days.

From a troubleshooting perspective, we would need to look at both sides (KMS host and Client) to determine what is going on.

KMS Host

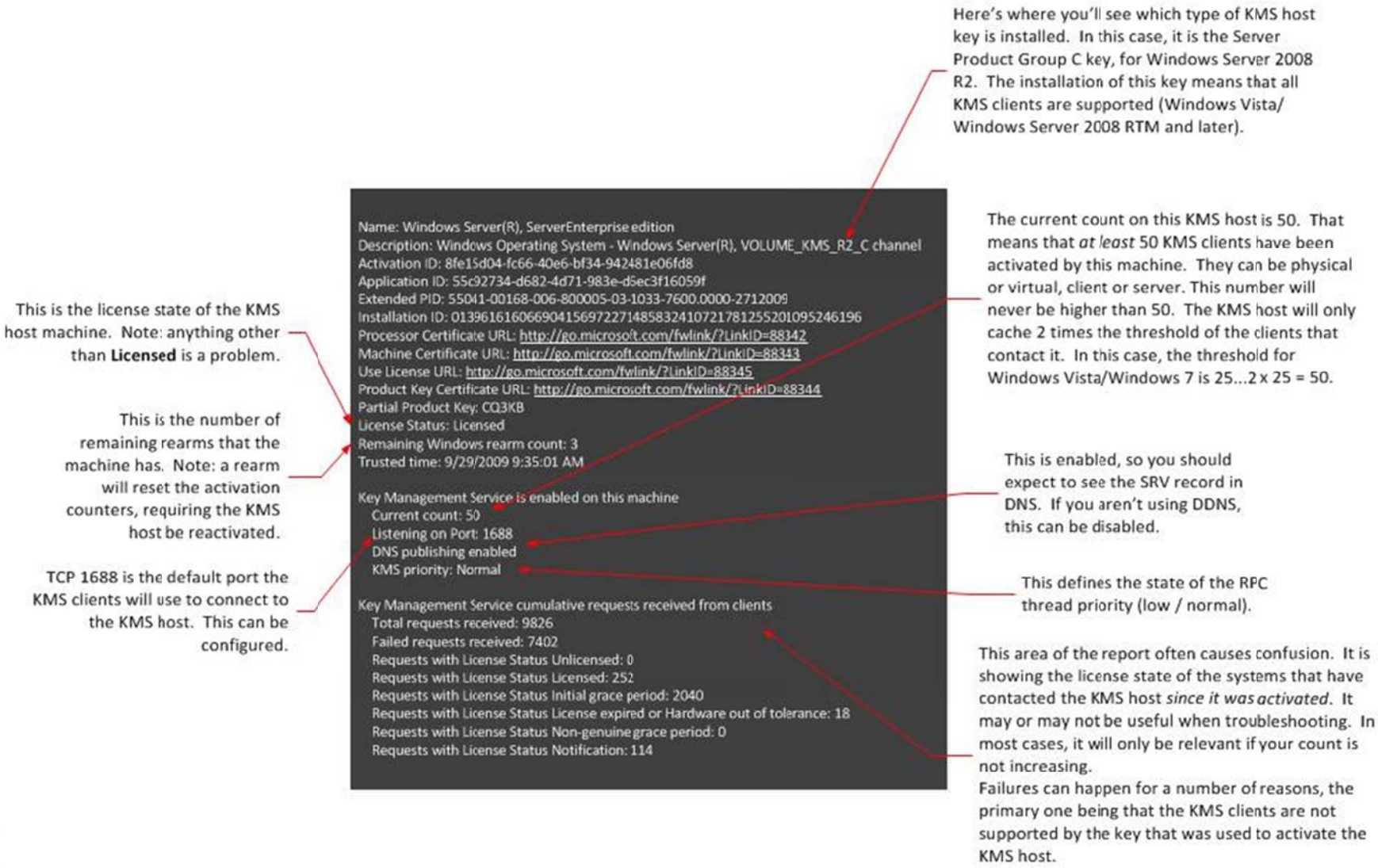
There are two areas of check on the KMS host. First, you'll want to check the status of the software license service on the host. Second, look in the Event Viewer.

SLMGR.VBS

From an elevated command prompt, type **SLMGR.vbs /dlv**. This will give you verbose output of the Software Licensing service. The screenshot below is from a KMS host

KMS Server Explained

By Tarun Chhabra, Microsoft Support Engineer



The most important fields for troubleshooting are listed below. What you are looking for may be different, depending on the issue to be solved.

- **Version Information**

KMS Server Explained

By Tarun Chhabra, Microsoft Support Engineer

- At the top of the **SLMGR.vbs /dlv** output is the Software Licensing Service Version. This may be useful to determine if the current version of the service is installed. For example, updates to the KMS service on Windows Server 2003 support different KMS host keys. This data can be used to evaluate whether or not the version is current and supports the KMS host key that you are attempting to install.

- **Name**
  - This will tell the edition of Windows that is installed on the KMS host system. This can be important when troubleshooting if you are having trouble adding or changing the KMS host key (e.g. to confirm the key is supported on that OS edition).
- **Description**
  - This is where you will see the key that is installed. Use this field to confirm which key was used to activate the service and whether or not it is the right one for the KMS clients that you have deployed.
- **License Status**
  - This is the status of the KMS host system. This should be Licensed. Anything but that means something is wrong and the host may need to be reactivated.
- **Current Count**
  - The count displayed will be between 0 and 50. The count is cumulative (between operating systems) and contains the number of valid systems that have attempted to activate within a 30 day period.
  - If the count is 0, it is a newly activated service or no valid clients have connected to the KMS host.
  - The count will not increase above 50, no matter how many valid systems exist in the environment. This is because they count is set to cache only 2 times the maximum license policy returned by a KMS client. The maximum policy today is set by the Windows client OS, which requires a count of 25 or higher from the KMS host to activate itself. Therefore, the highest count on the KMS host is 2 x 25, or 50. Note that in environments with only Windows Server KMS clients, the maximum count on the KMS host will be 10, as the threshold for server is 5 (2 x 5, or 10).
  - A common issue related to count is where the environment has an activated KMS host and a sufficient number of clients, but the count does not increase beyond 1. The core problem is that the deployed client image was not configured correctly (**sysprep /generalize**) and the systems do not have unique Clint Machine IDs (CMIDs).
  - Another reason why the count may not be increasing is that there are too many KMS hosts in the environment and the count is distributed over all of them.
- **Listening on Port**
  - Communication with KMS is via anonymous RPC. 1688 is the default TCP port used by the clients to connect to the KMS host. Make sure this port is open between your KMS clients and the KMS host. The port can be changed and can be configured on the KMS host. The KMS clients receive this port designation from the KMS host during their communication. If you change the port on a KMS client, it will be overwritten when that client contacts the host.

KMS Server Explained

By Tarun Chhabra, Microsoft Support Engineer

There is a section as “cumulative requests” in the **SLMGR.vbs /dlv** output. The KMS host will keep an ongoing record of the state of each KMS client that attempts to (re)activate. Failed requests indicate KMS clients that are not supported by the KMS host. For example, if a Windows 7 KMS client attempted to activate against a KMS host activated with a Windows Vista KMS key, the activation would fail. The “Requests with License Status” lines cover all of the possible license states, past and present. **From a troubleshooting perspective, this data will only be relevant if the count is not increasing (as expected). In that case, you should see the failed requests increasing and will know to check the product key used to activate the KMS host system. Note also that the values here will not reset unless the KMS host system is reinstalled.**
Event Viewer

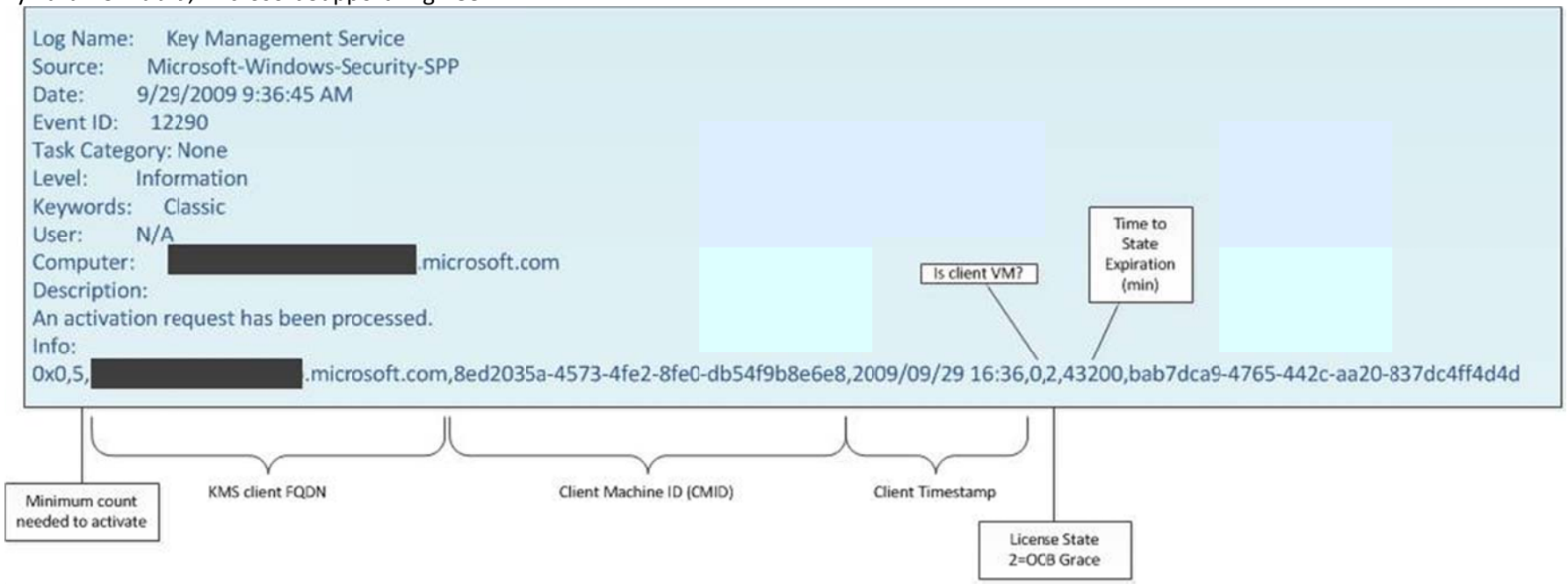
Below you will see a screenshot from the Key Management Service event log of KMS host. This event, 12290, shows that a KMS client contacted the host in order to attempt activation. There will be a 12290 entry in the Key Management Service log on the KMS host system for each client that attempts to activate. If you don’t see this event for a client that you are troubleshooting, that client is not connecting to the KMS host. There are two corresponding events on the KMS clients, 12288 and 12289, which will be covered in the KMS Client section. Some of the reasons why a 12290 event may not exist:

- Network outage
- Host not resolving/registered in DNS
- Firewall blocking TCP 1688
    - This can happen in many places within the environment, including on the KMS host system itself. By default, the exception for KMS exists in the firewall configuration dialog. However, it is not enabled automatically. You will need to turn on the exception.
- Log full

The 12290 event entry gives a significant amount of information that can be used to figure out what kind client contacted the host…and why a failure may occur.

KMS Server Explained

By Tarun Chhabra, Microsoft Support Engineer



In the event entry, you will find the following relevant information:

- Minimum count needed to activate
  - The KMS client is reporting that the count from the KMS host must be 5 in order to activate. That means this is a Server OS, though whether it is Windows Server 2008 or Windows Server 2008 R2 will not be clarified, nor will the specific edition. If your clients are not activating, make sure that the count is sufficient on the host.
- Client Machine ID (CMID)
  - This is a unique value per system. If this is not unique it is because an image was not properly prepared for distribution (**sysprep /generalize**). This will manifest on the KMS host as a count that will not increase, despite a sufficient number of clients existing in the environment.
- License State and Time to State Expiration
  - This is the license state that the client currently has. It can help you differentiate a client that is trying to activate for the first time versus one that is attempting to reactivate. The time entry will tell you how much longer the client will be in that state, if nothing changes.

KMS Server Explained

By Tarun Chhabra, Microsoft Support Engineer

Another relevant event to look for on your KMS is the 12293. This event indicates that the host failed to publish the required records in DNS. That will definitely cause failures and is something you should confirm *after* setting up your host and *before* deploying clients.

KMS Client

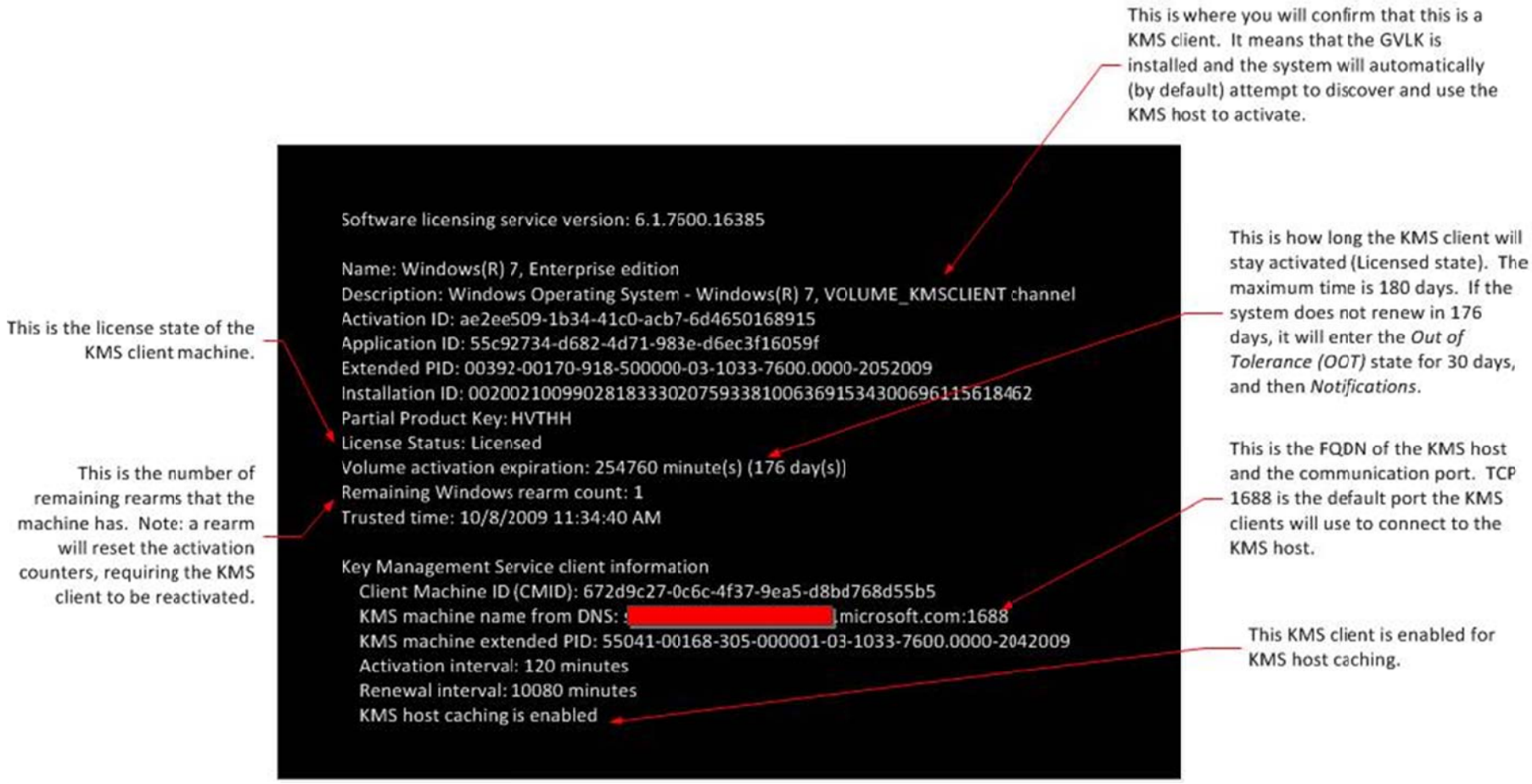
On the clients you will also use the same process (SLMGR and Event Viewer) to troubleshoot activation.

SLMGR.VBS

From an elevated command prompt, type **SLMGR.vbs /dlv**. This will give you verbose output of the Software Licensing service. The screenshot below is from my machine, a KMS client within Microsoft.

KMS Server Explained

By Tarun Chhabra, Microsoft Support Engineer



The most important fields for troubleshooting are listed below. What you are looking for may be different, depending on the issue to be solved.

- **Name**
  - This will tell you the edition of Windows that is installed on the KMS client system. Use this to confirm that the version of Windows you are attempting to activate can use KMS. For example, our help desk has seen incidents where customers are attempting to install the KMS Client Setup Key on an edition of Windows that does not use volume activation, such as Windows Vista Ultimate.
- **Description**

KMS Server Explained

By Tarun Chhabra, Microsoft Support Engineer

- This is where you will see the key that is installed. VOLUME_KMSCLIENT indicates that the KMS Client Setup Key (or GVLK) is installed (default for volume license media) and that this system will automatically attempt to activate using a KMS host. If you see something else here, such as MAK, then you'll need to reinstall the GVLK for this system to be a KMS client.

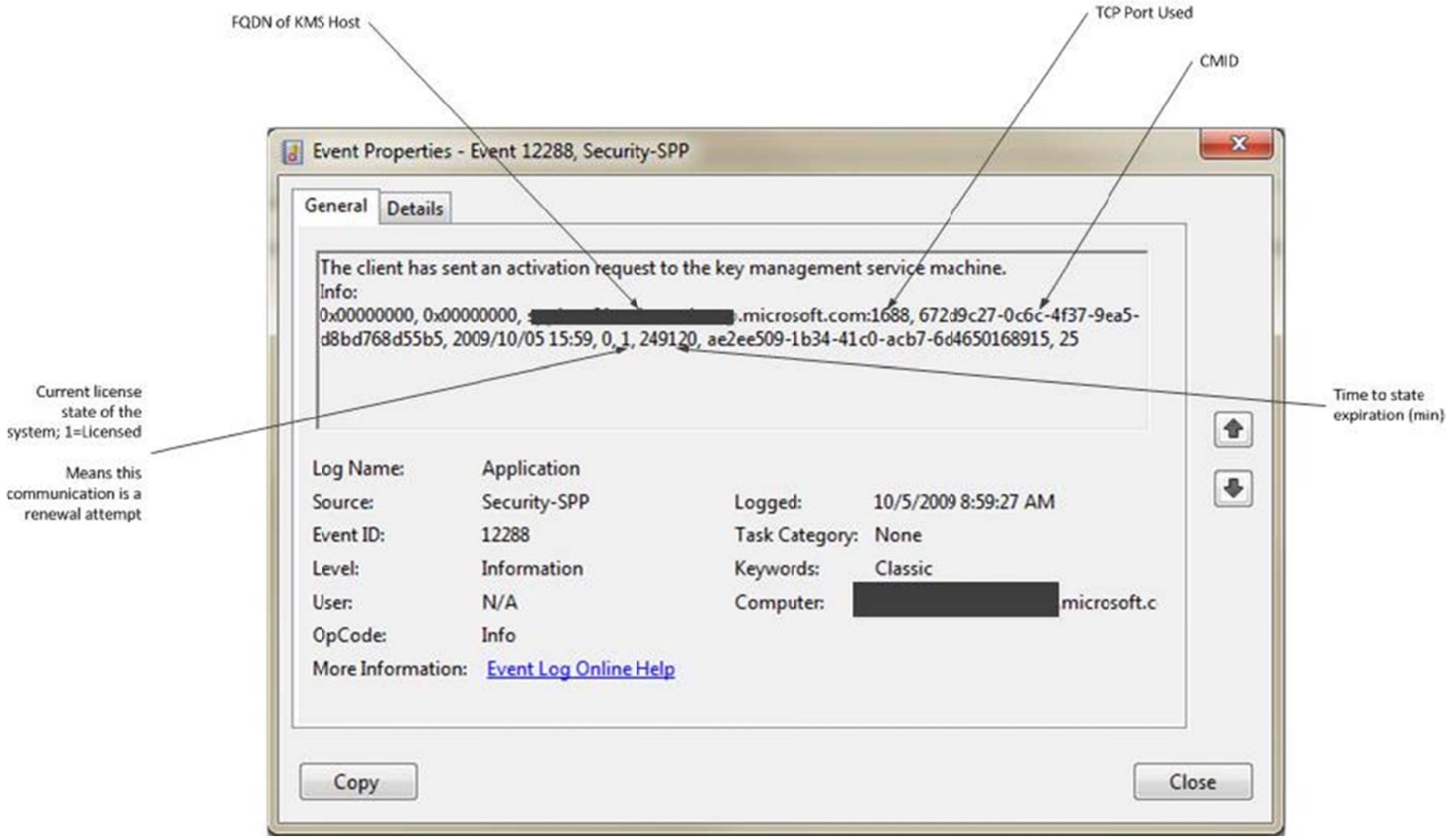
- **Partial Product Key**
  - As with the Name field above, you can use this information to determine that the correct KMS Client Setup Key is installed on this machine (e.g. matches the operating system that is installed on the KMS client). By default, the correct key will be present on systems built using media from the Volume License Service Center (VLSC) portal. In some cases, customers may use Multiple Activation Key (MAK) activation until there are a sufficient number of systems in the environment to support KMS activation. The KMS Client Setup key will need to be installed on these systems to transition them from MAK to KMS. VAMT can be used to install this key and ensure the correct one is applied.
- **License Status**
  - This is the status of the KMS client system. This should be Licensed for a system that has been activated with KMS. Anything but that may indicate there is a problem. For example, if the KMS host is good and the KMS client will not activate (e.g. in a Grace state) then there may be something preventing the client from reaching the host system (such as firewall issues, network outage, etc.).
- **Client Machine ID (CMID)**
  - The CMID should be a unique value per KMS client. As I mentioned in the KMS host section, a common issue related to count is where the environment has an activated KMS host and a sufficient number of clients, but the count does not increase beyond 1.
- **KMS Machine Name from DNS:**
  - Here is where you will find the FQDN of the KMS host that the client successfully activated with and the TCP port used for the communication.
- **KMS Host Caching**
  - The final entry is to show whether or not caching is enabled. It is by default. What this means is that the KMS client will cache the KMS host that it was able to activate with and will communicate directly with this host when it is time to reactivate (instead of querying DNS). If the client cannot contact the cached KMS host, discovery with DNS will be used.

Event Viewer

Below you will see a snippet from Application event log from my machine. A successful activation/reactivation on the client will have two events, 12288 and 12289. If you only see the 12288 event (without a corresponding 12289) it means that the KMS client was not able to reach the KMS host or it did not respond/response was lost. In this case, confirm that the KMS host is discoverable and reachable by the KMS client systems.

KMS Server Explained

By Tarun Chhabra, Microsoft Support Engineer



In the 12288 event entry, the most relevant piece of information is data in the Info section. For example, the FQDN and TCP port used by the client to attempt activation is shown, along with the current state of the client. The FQDN can also help to troubleshoot cases where the count

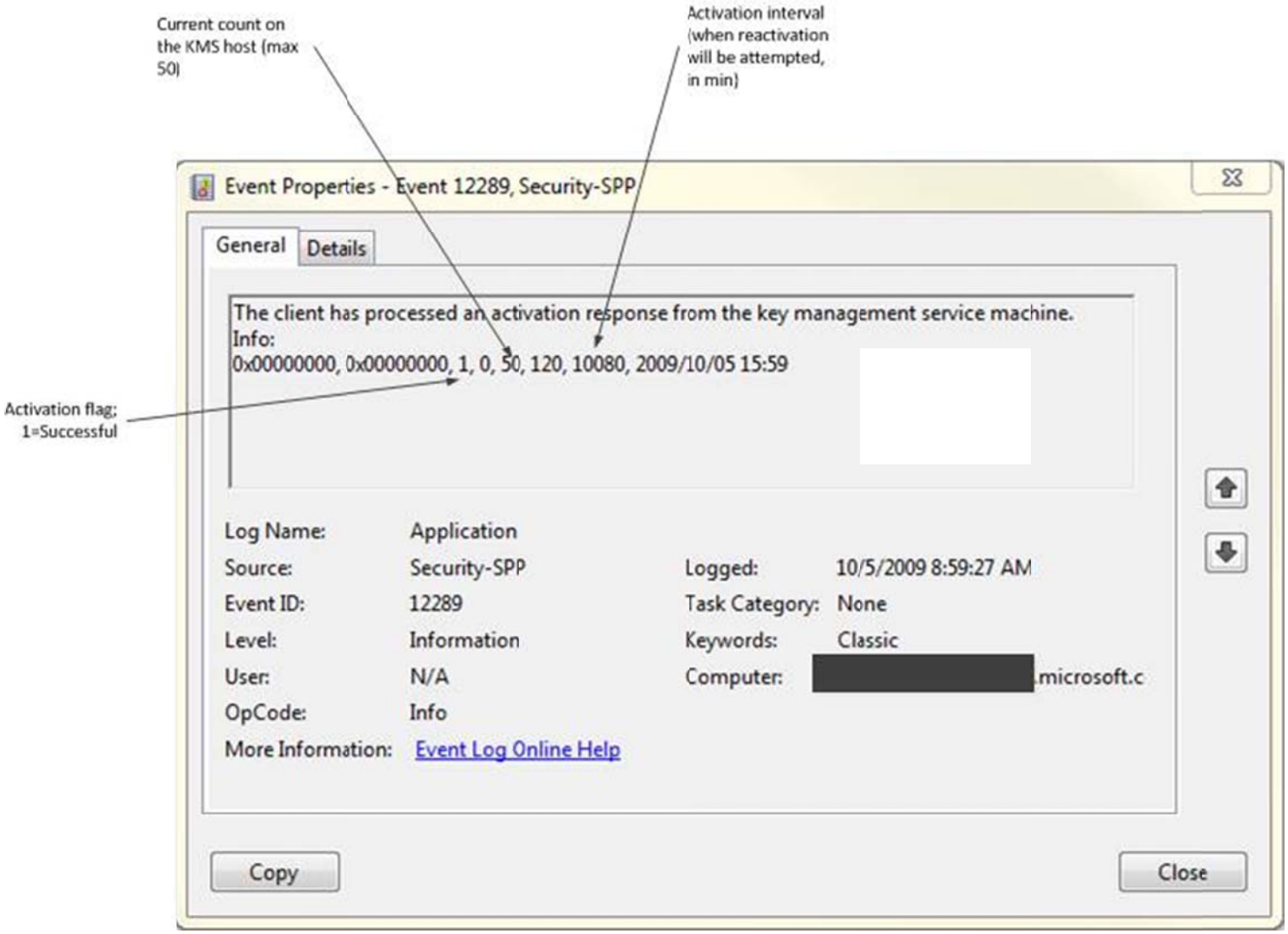
By Tarun Chhabra, Microsoft Support Engineer

on a KMS host is not increasing. For example, if there are too many KMS hosts available to the clients (either legitimate or rogue systems) then the count may be distributed over all of them.

An unsuccessful activation will not always mean that the client has 12288 and not 12289. A failed activation/reactivation may also have both events. This is where you need to examine the second event to confirm the reason for the failed attempt.

KMS Server Explained

By Tarun Chhabra, Microsoft Support Engineer



In the 12289 event entry, the Info section is also where you will look to find what you need:

- **Activation Flag**

By Tarun Chhabra, Microsoft Support Engineer

- This will be a 1 (successful) or 0 (failure) on the attempt.

- **Current Count on the KMS Host**
  - The client will log the count received by the KMS host. If activation fails, it may be because the count is not sufficient for this client OS or that there are not enough systems in the environment to build the count.