Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Revise asset and identity lookup memory usage behavior in Splunk Enterprise Security

Generated: 6/13/2022 8:38 am

Revise asset and identity lookup memory usage behavior in Splunk Enterprise Security

Prior to the release of Splunk Cloud Platform 8.0.2004, KV Store backed lookups do not respect the `max_memtable_bytes` setting. This means that KV Store backed lookups are always stored in memory on the indexer.

With the release of Splunk Cloud Platform 8.0.2004, KV Store backed lookups do respect the `max_memtable_bytes` setting. This means that a KV Store backed lookup is stored in memory until it exceeds the definition in the `max_memtable_bytes` setting.

You might experience the following behavior after upgrading. Using Splunk Enterprise 8.0 as an example, consider a KV Store lookup of 1 GB in size that is used as an automatic lookup, with `max_memtable_bytes=25MB`. If you upgrade to a Splunk Cloud Platform version of 8.0.2004 or higher, the 1 GB size exceeds the `max_memtable_bytes` setting, so an index file is created and the lookup occurs on disk, which is slower.

The default setting in Splunk Cloud Platform is `max_memtable_bytes=100MB`. Splunk Cloud Platform customers need to contact technical support if necessary to revise this behavior.

To revise this behavior in an on-premises environment, increase your `max_memtable_bytes` in the `$SPLUNK_HOME/etc/system/local/limits.conf` file. See lookup of limits.conf in the Splunk Enterprise *Admin Manual*.