Mt Wilson

Metering

# Background

Intel business managers need to know how customers use Mt Wilson: how many instances of Mt Wilson are installed, how many hosts are registered or attested, how many VMs are attested, how many VMs are encrypted, are asset tags being used, and which APIs are used.

In the future we might also want to limit the capabilities of the server based on the license purchased from Intel. However, initially we just need to get usage data. For that reason, what we need at this time is a blueprint for “metering” and not “licensing” or “locking” the product.

# Assumptions

Datacenter administrators are willing to routinely share Mt Wilson usage summaries but not detailed information about their network layout, server identities, or workloads

Datacenter administrators will not allow Mt Wilson to “call home” with a periodic report; they can easily block outside network access using a firewall

Datacenter administrators may want to see the Mt Wilson report prior to sending to verify it contains only summary information

Datacenter administrators are willing to perform an interactive step once every reporting period to send a Mt Wilson metering report to Intel in order to preview the report before it is sent

Datacenter administrators may be willing to allow automated report generation & submission to Intel without interactive steps if they can be cc’d on the report

Datacenter administrators may want a non-disclosure agreement to cover even the summarized information

We can make the periodic submission of the usage report part of the legal license agreement for using the software

# General requirements

Mt Wilson will maintain a log of activity covering the appropriate events with sufficient detail to enable generating the required reports (see reporting section for details)

The reporting component will be upgradable separately from other components

The reporting component will be able to read the logs, summarize the information, and generate a report

Mt Wilson must be able to take a new or existing generated report and send it by email to a configured address and cc: to zero or more configured addresses

Mt Wilson must be able to track which log entries were already included in a report, and which reports were already sent

Mt Wilson will automatically adjust the reporting period to align with Intel preferences such as monthly. For example if Mt Wilson is installed on the 20th of the month, and the reporting period is monthly, the first report would be generated on the 1st of the following month and would cover a short reporting period from the 20th thru the last day of the previous month.

If a report is missed due to Mt Wilson not running at the time it would generate a report, Mt Wilson will “catch up” by generating as many reports as necessary to cover monthly reporting periods since its last generated report, and send each one in a separate email in chronological order

# Reporting requirements

Every report will have an associated reporting period for the data it covers.

The report should have separate sections for Mt Wilson server data, host attestation data, and VM attestation data

Mt Wilson server data should include:

* how many times is each API invoked

Host attestation should include:

* how many hosts are registered/attested (same for Mt Wilson 2.x/3.x, different in 4.x)
* average number of attestations per host
* how many hosts have asset tags as part of the trust policy

VM attestation should include:

* how many unique VM images are attested
* how many unique VM instances are attested
* average number of attestations per instance
* how many VM images are encrypted
* average number of images on the same host
* average number of instances on the same host
* average number of instances of the same image on the same host

Because the information is summarized, each section must have an independent summary and all metrics must be tracked separately. There will be overlaps ( # instances > # images )

# Security requirements

The metering report is a function outside the scope of the solution for the customer; therefore security for this function (integrity of the report) is not critical. The typical customer is not considered to be a likely threat, and possible damage to Intel resulting from missing, understated, or overstated reports is estimated to be negligible. It may be acceptable to not apply any security at all beyond what is already part of the overall solution in the first release. Software-based and hardware-based mitigations may be considered but should not delay development of the feature.

Security efforts will be categorized in three levels:

**Level 1**. No specific protection besides what is provided by the main application software in any deployment scenario

**Level 2**. Software-based protection for metering logs or generated reports

**Level 3**. Hardware-based protection for metering logs or generated reports

# Roadmap

Integrate performance measurements into the logging and reporting to help Intel identify hotspots and bottlenecks