Validating Confidential VMs using Cloud Monitoring

oduct is covered by the Pre-GA Offerings Terms (/terms/service-terms#1) of the Google Cloud Platform Term
e. Pre-GA products may have limited support, and changes to pre-GA products may not be compatible with ot
versions. For more information, see the launch stage descriptions (/products#product-launch-stages).

Cloud Monitoring (/monitoring/docs) and Cloud Logging (/logging/docs) let you monitor and validate your Confidential VM instances. This topic details what you can monitor, how to view logged reports, and what to look for in reports.

Integrity monitoring

Integrity monitoring is a feature of both Shielded VM and Confidential VM that helps you understand and make decisions about the state of your VM instances.

The remainder of this section contains information about using integrity monitoring with Confidential VMs.

Enable integrity monitoring

Integrity monitoring is enabled by default in new Confidential VM instances. To learn how to change integrity monitoring settings—including toggling Secure Boot, vTPM, and integrity monitoring itself—see Modifying Shielded VM options (/compute/docs/instances/modifying-shielded-vm).

View integrity reports

You can view integrity reports in Cloud Monitoring and set alerts on integrity failures. You can review the details of integrity monitoring results in Cloud Logging. To learn how to view integrity validation events and set alerts on them, see Monitoring VM boot integrity by using Monitoring (/compute/docs/instances/integrity-monitoring#monitoring).

View launch attestation report events

Confidential VM generates a unique type of integrity validation event, called a *launch attestation report event*. Every time an AMD Secure Encrypted Virtualization (SEV)- based Confidential VM boots, a launch attestation report event is generated as part of the integrity validation events for the VM.

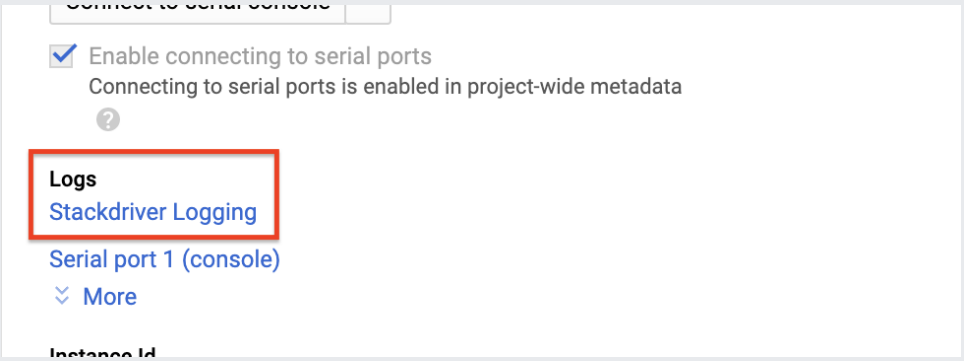
To view the launch attestation report event from the integrity report:

1. In the Google Cloud Console, go to the **VM instances** page.

   Go to the **VM instances** page (https://console.cloud.google.com/compute/instances)

2. Click the Confidential VM instance name to open the **VM instance details** page.

3. Under **Logs**, click **Stackdriver Logging**.



4. Logging opens, and the integrity report populates with integrity validation events.

   The following screenshot shows a typical integrity report:

(/compute/confidential-vm/docs/images/sev-integrity-report.png)

   Look for the string `sevLaunchAttestationReportEvent`.

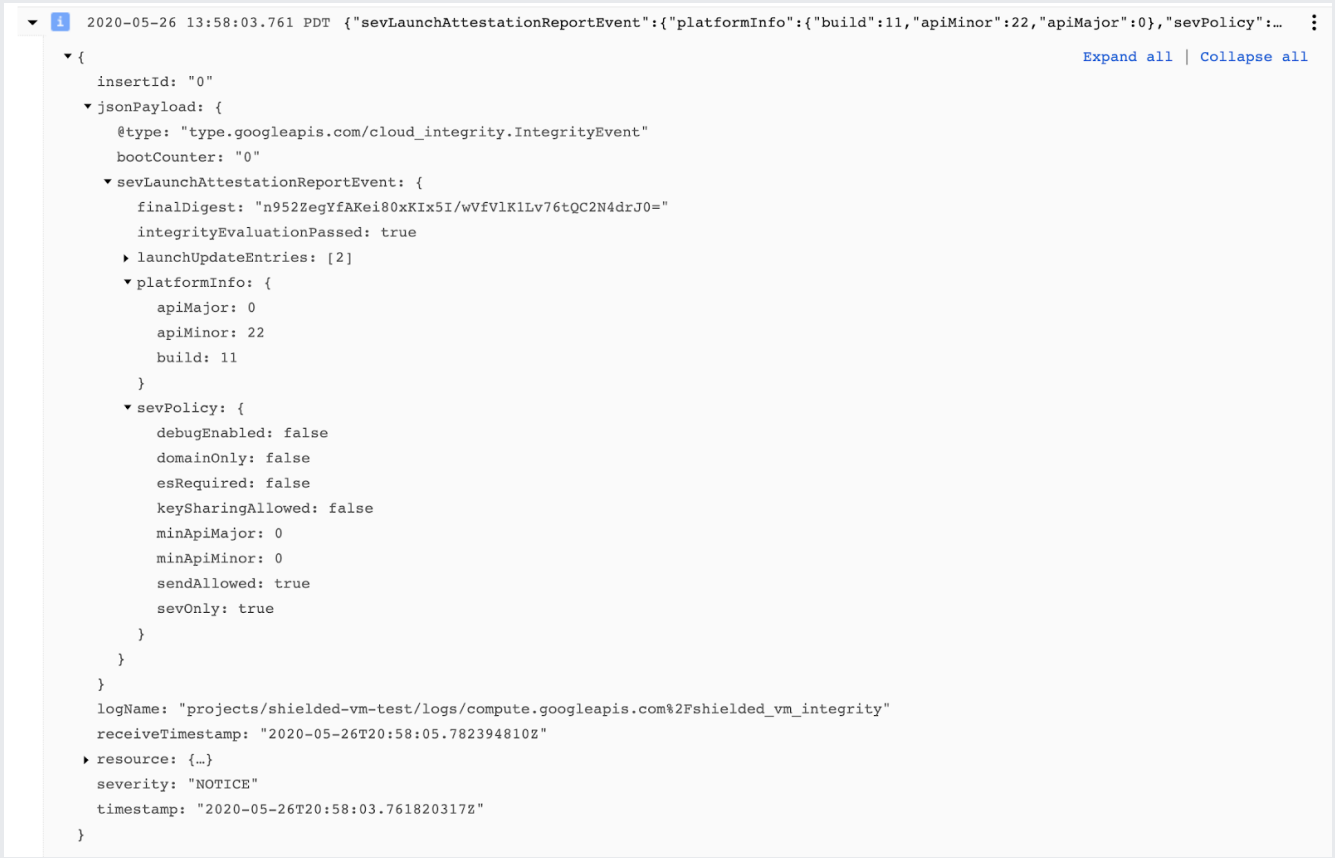
To view detail about a specific event, click the ▸ expander arrow. You can open all the nodes in the tree at one time by clicking **Expand all**.

About launch attestation report events

Launch attestation report events validate whether a VM is an AMD SEV-based Confidential VM. A launch attestation report event contains information such as the following:

- `integrityEvaluationPassed`: The result of an integrity check performed by the Virtual Machine Monitor on the measurement computed by AMD SEV.
- `sevPolicy`: The AMD SEV policy bits set for this VM; policy bits are set at Confidential VM launch to enforce constraints such as whether debug mode is enabled.

The following screenshot shows a typical launch attestation report event:



(/compute/confidential-vm/docs/images/launch-attestation-event.png)

Related security technologies

You can also take advantage of Secure Boot and Measured Boot, both of which leverage Shielded VM.

Secure Boot

Secure Boot helps ensure that the Confidential VM instance's system only runs authentic software by verifying the digital signature of all boot components and ending the boot process if signature verification fails. Firmware that is signed and verified by Google's Certificate Authority establishes the root of trust for Secure Boot, which verifies your VM's identity and checks that it is part of your specified project and region.

Secure Boot is not enabled by default. To learn how to enable this feature and for more information, see Secure Boot (/security/shielded-cloud/shielded-vm#secure-boot).

Measured Boot

Measured Boot is enabled by a Confidential VM's Virtual Trusted Platform Module (vTPM) and helps guard against malicious modifications to the Confidential VM. Measured Boot monitors the integrity of a Confidential VM instance's bootloader, kernel, and boot drivers.

Measured Boot is enabled by default in new Confidential VM instances. Learn more about Measured Boot (/security/shielded-cloud/shielded-vm#measured-boot).

What's next

- Learn how to set alerts on integrity validation events (/compute/docs/instances/integrity-monitoring#setting-alerts) and determine the cause of boot integrity validation failure (/compute/docs/instances/integrity-monitoring#diagnosing-failure).
- Learn about one approach to automating responses to integrity monitoring events (/security/shielded-cloud/automating-responses-integrity-failures).

Last updated 2020-08-12 UTC.