Modifying Shielded VM options

Use this topic to learn how to modify the Shielded VM (/security/shielded-cloud/shielded-vm) options on a VM instance. To see which images support Shielded VM features, see OS image security features (/compute/docs/images/os-details#security-features).

On a Shielded VM instance, Compute Engine enables the virtual Trusted Platform Module (vTPM) (/security/shielded-cloud/shielded-vm#vtpm) and integrity monitoring (/security/shielded-cloud/shielded-vm#integrity-monitoring) options by default. If you disable the vTPM, Compute Engine disables integrity monitoring because integrity monitoring relies on data gathered by Measured Boot (/security/shielded-cloud/shielded-vm#measured-boot).

Compute Engine does not enable Secure Boot (/security/shielded-cloud/shielded-vm#secure-boot) by default because unsigned drivers and other low-level software might not be compatible. Secure Boot helps ensure that the system only runs authentic software by verifying the signature of all boot components, and halting the boot process if signature verification fails. This helps prevent forms of kernel malware, such as rootkits or bootkits, from persisting across VM reboots. If appropriate for your specific workloads, that is, you can ensure that enabling Secure Boot doesn't prevent a representative test VM from booting, Google recommends enabling Secure Boot.

Before you begin

- If you want to use the command-line examples in this guide:
    1. Install or update to the latest version of the gcloud command-line tool (/compute/docs/gcloud-compute).
    2. Set a default region and zone (/compute/docs/gcloud-compute#set_default_zone_and_region_in_your_local_client).
- If you want to use the API examples in this guide, set up API access (/compute/docs/api/prereqs).

Permissions required for this task

To perform this task, you must have the following permissions (/iam/docs/overview#permissions):

- `compute.instances.updateShieldedInstanceConfig` on the VM

Modifying Shielded VM options on a VM instance

Use the following procedure to modify Shielded VM options:

Consolegcloud (#gcloud)API (#api)

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 instance name to open the **VM instance details** page.
3. Click **Stop**.
4. After the instance stops, click **Edit**.
5. In the **Shielded VM** section, modify the Shielded VM options:
   - Toggle **Turn on Secure Boot** to enable Secure Boot. Compute Engine does not enable Secure Boot (/security/shielded-cloud/shielded-vm#secure-boot) by default because unsigned drivers and other low-level software might not be compatible. Even so, if possible, Google recommends enabling Secure Boot.
   - Toggle **Turn on vTPM** to disable the virtual trusted platform module (vTPM). By default, Compute Engine enables the Virtual Trusted Platform Module (vTPM) (/security/shielded-cloud/shielded-vm#vtpm).
   - Toggle **Turn on Integrity Monitoring** to disable integrity monitoring. By default, Compute Engine enables integrity monitoring (/security/shielded-cloud/shielded-vm#integrity-monitoring).
6. Click **Save**.
7. Click **Start** to start the instance.

What's next

- Read more (/security/shielded-cloud/shielded-vm) about the security features offered by Shielded VM.
- Learn more about monitoring integrity on a Shielded VM instance (/compute/docs/instances/integrity-monitoring).

Last updated 2020-07-30 UTC.