Confidential Computing concepts

This page discusses key concepts and terminology for Confidential VM. To get started using Confidential VM, see the quickstart (/compute/confidential-vm/docs/create-confidential-vm-instance).

Confidential Computing

Confidential Computing is the protection of data in-use with hardware-based Trusted Execution Environment (TEE). TEEs are secure and isolated environments that prevent unauthorized access or modification of applications and data while they are in use. This security standard is defined by the Confidential Computing Consortium (https://confidentialcomputing.io/).

End-to-end encryption

End-to-end encryption is comprised of three states.

- *Encryption-at-rest* protects your data while it is being stored.
- *Encryption-in-transit* protects your data when it is moving between two points.
- *Encryption-in-use* protects your data while it is being processed.

Confidential Computing provides the last piece of end-to-end encryption: *encryption-in-use*.

Confidential VM

A Confidential VM is a type of Compute Engine VM that ensures that your data and applications stay private and encrypted even while in use. You can use a Confidential VM as part of your security strategy so you do not expose sensitive data or workloads during processing.

Confidential VM runs on hosts with AMD EPYC processors which feature AMD Secure Encrypted Virtualization (SEV) (https://developer.amd.com/sev/). Incorporating SEV into Confidential VM provides the following benefits and features.

- **Isolation**: Encryption keys are generated by the AMD Secure Processor (SP) during VM creation and reside solely within the AMD System-On-Chip (SOC). These keys are

not even accessible by Google, offering improved isolation.

- **Attestation**: Confidential VM uses Virtual Trusted Platform Module (vTPM) (https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary/) attestation. Every time an AMD SEV-based Confidential VM boots, a launch attestation report event (/compute/confidential-vm/docs/monitoring#about_launch_attestation_report_events) is generated.
- **High performance**: AMD SEV offers high performance for demanding computational tasks. Enabling Confidential VM has little or no impact on most workloads, with only a 0-6% degradation in performance.

Enable Confidential VM

You can enable Confidential Computing whenever you create a new VM. Creating a Confidential VM (/compute/confidential-vm/docs/creating-cvm-instance) only requires an extra checkbox or 1-2 more lines of code than creating a standard VM. You can continue using the other tools and workflows you're already familiar with. Adding Confidential Computing requires no changes to your existing applications.

Other Confidential Computing services

Google Cloud also offers the following Confidential Computing services:

- Confidential Google Kubernetes Engine Nodes (/kubernetes-engine/docs/how-to/confidential-gke-nodes) enforce the use of Confidential VM for all of your GKE nodes.
- Dataproc Confidential Compute (/dataproc/docs/concepts/configuring-clusters/confidential-compute) features Dataproc clusters that use Confidential VMs.

What's next

- To quickly create a Confidential VM instance, try the quickstart (/compute/confidential-vm/docs/quickstart-creating-new-instance).
- For in-depth instructions about how to create a Confidential VM instance, see Creating a Confidential VM instance (/compute/confidential-vm/docs/creating-cvm-instance).

- Learn more about SEV in AMD's whitepaper, AMD Memory Encryption (http://developer.amd.com/wordpress/media/2013/12/AMD_Memory_Encryption_Whitepaper_v9-Public.pdf)

.

Last updated 2022-09-28 UTC.