Configuring Confidential Computing with AMD SEV-SNP and VMware ESXi 9.0

Planning / Implementation

The rapid migration of data and applications to cloud platforms is a defining characteristic of the evolving global computing infrastructure. This paradigm shift imposes novel challenges on security frameworks, necessitating adaptive measures to protect data across its lifecycle —including storage, network transmission, and active use. The escalating imperative for data protection, driven by industry regulations and the increasing threat landscape of cyberattacks, underscores the critical role of confidential computing. As such, confidential computing is positioned to become the de facto technological standard for secure cloud computing environments.

Cloud service providers are continually seeking innovative methodologies to protect and secure sensitive intellectual property (IP) and workload data. As the following figure shows, data protection strategies have focused on two primary domains:

- Encrypting data in transit through secure communication channels
- Encrypting data at rest via encrypted storage solutions

The advent of confidential computing, however, introduces a novel approach to protecting data in use. This is achieved through the utilization of hardware-based Trusted Execution Environment (TEE), which isolate data within a virtual machine, thereby shielding it from potential vulnerabilities posed by the hypervisor, host operating system, and cloud management components.

Attestation serves as the foundational process for establishing trust within Confidential Computing frameworks. This mechanism functions as a digital verification protocol, guaranteeing that confidential data is exclusively processed within TEEs that have undergone strict validation.

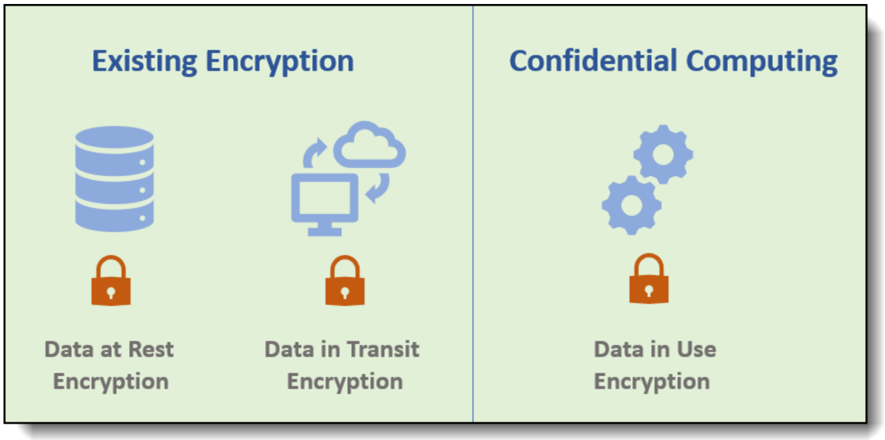


Figure 1. Confidential Computing data encryption

Confidential computing is particularly advantageous in scenarios where the entity responsible for the workload differs from the owner of the underlying physical infrastructure. This disparity may arise from heightened security concerns, apprehensions regarding the exploitation of vulnerabilities within cloud infrastructure by other tenants, or the inherent sensitivity of the data housed within the virtual machine. Sensitive information, such as customer data, financial records, and health information, often falls under strict regulatory or compliance frameworks. By leveraging confidential computing, the risk of data leakage while the data resides in the cloud is significantly mitigated.

AMD SEV-SNP

In 2016, AMD pioneered Secure Encrypted Virtualization (SEV), a foundational technology designed to launch encrypted virtual machine or Confidential VM (CVM), thereby facilitating support for confidential computing. This innovation was subsequently enhanced with the introduction of SEV Encrypted State (SEV-ES), which encrypts the CPU register state during periods of VM inactivity.

The most developed version of SEV, known as SEV Secure Nested Paging (SEV-SNP), represents a significant advancement. SEV-SNP builds upon the foundational capabilities of SEV and SEV-ES to enable the creation of confidential VMs that are isolated to external entities, including the bare-metal hypervisor, Basic Input/Output System (BIOS), other VMs, and even external input/output (I/O) devices. SEV-SNP incorporates robust memory integrity protection mechanisms to mitigate malicious hypervisor-based attacks, such as data replay and memory re-mapping, thereby establishing an isolated execution environment.

SEV-SNP also supports remote attestation, an attestation report can be generated, allowing any third party to verify the identity and state of a confidential VM, thereby ensuring the integrity and trustworthiness of the computing environment.

The SEV-SNP architecture enforces data integrity on guest private pages through the utilization of the Reverse Map Table (RMP) structure, which is globally shared by all logical processors. Conventionally, memory access is facilitated via CPU instructions, which employ an internal Memory Management Unit (MMU) to translate virtual addresses into physical addresses using page tables before accessing memory. In the SEV-SNP architecture, the hypervisor manages the page tables and the mapping to addresses within the physical address space. However, the RMP enforces access control within this physical address space. The RMP is a substantial in-memory data structure that tracks the ownership of each memory page. Each 4KB page of memory is associated with a 16-byte RMP entry, which contains the security attributes of the system physical page and specifies the entities permitted to write to that page.

As the following figure shows, during the translation of a virtual address to a physical address, an RMP check is typically performed as the final step in this process. The physical address that the software or device intends to access is used as an index for the RMP to verify that the assigned owner matches the entity attempting to access the page. If this verification fails, a fault is generated and access to the page is subsequently blocked.

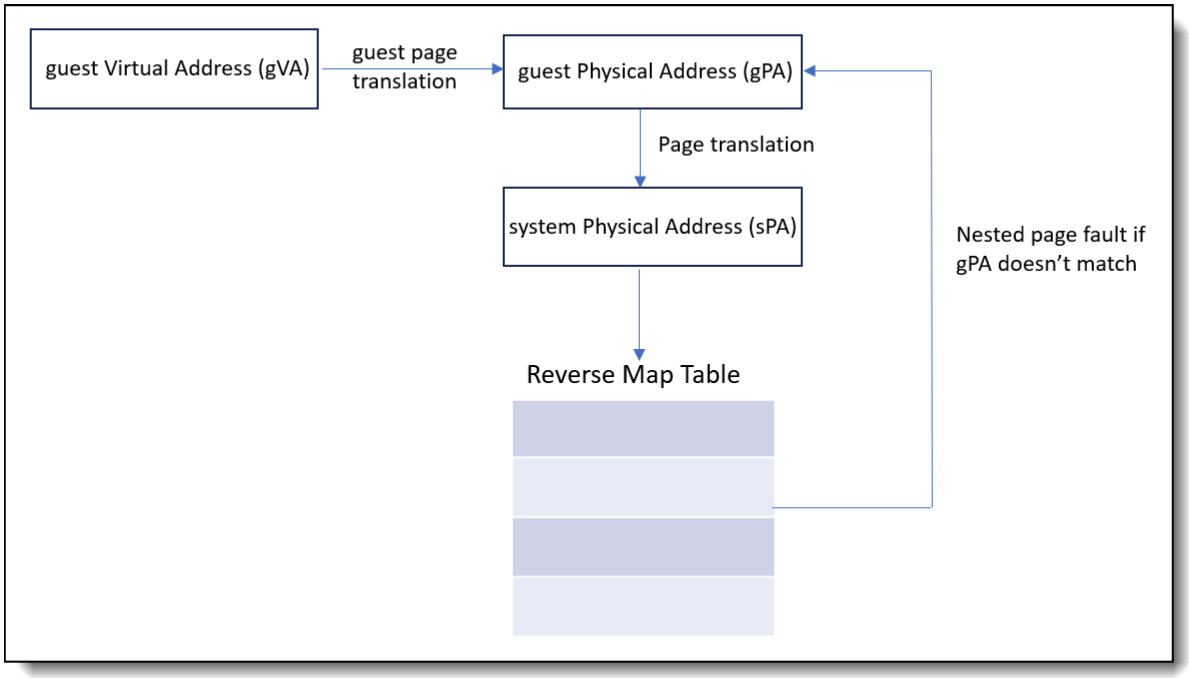

guest Virtual Address (gVA)
guest page translation
guest Physical Address (gPA)
Page translation
system Physical Address (sPA)
Nested page fault if gPA doesn't match
Reverse Map Table

Figure 2. Nested VM page table walk

Attestation workflow

Attestation is a cryptographic process wherein an entity, referred to as the attester, collects comprehensive information about its operational state and transmits this information to a client for verification purposes. The attester, in this context, is the entity responsible for generating evidence—a structured set of information pertaining to the TEE. Successful verification of this evidence assures the client that the TEE is executing the anticipated code on the designated hardware and is configured in accordance with specified parameters. Upon establishing the trustworthiness of the attester, the client proceeds to transmit confidential code and data to the attester, thereby initiating secure and verified communication.

The following figure depicts the standard attestation workflow.

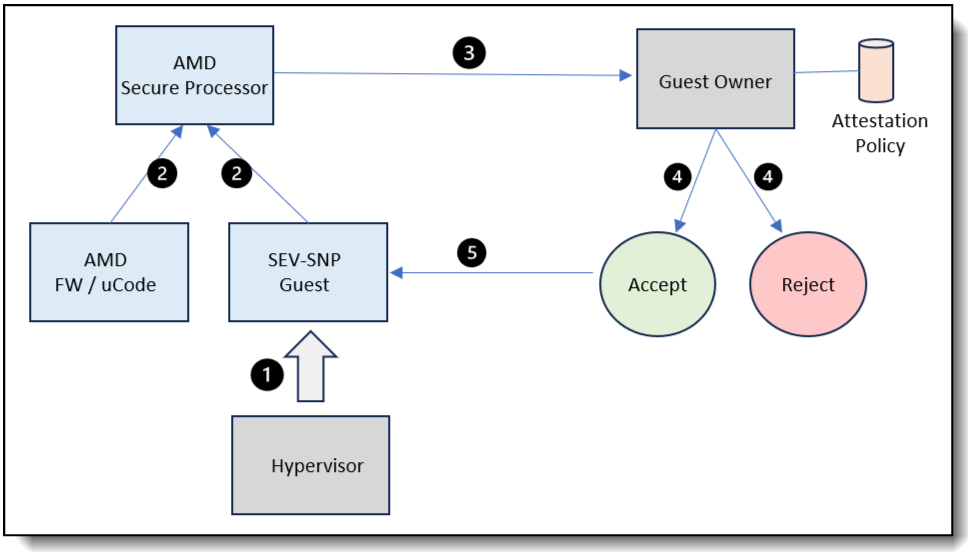
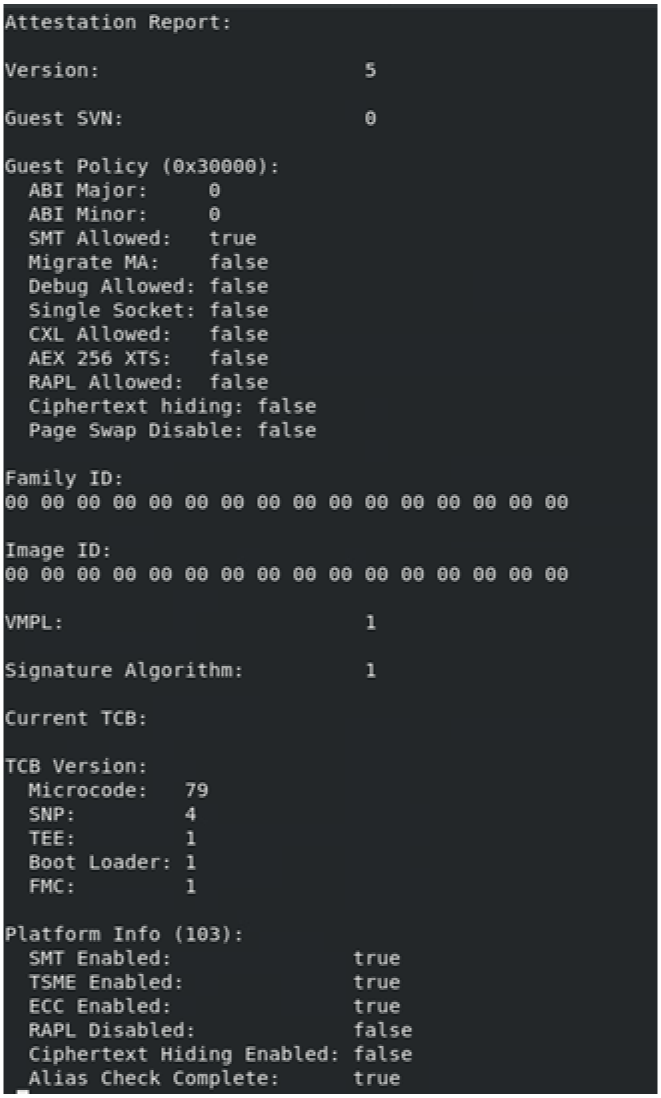


Figure 3. Attestation workflow

The following steps describe the standard attestation workflow on an AMD SEV-SNP platform.

1. The hypervisor initiates the launch of the SEV-SNP guest, during which the AMD Secure Processor cryptographically measures the content of the initial set of pages, generating a launch digest.
2. Platform measurements, including AMD firmware and microcode, along with guest measurements derived from the SEV-SNP guest, are aggregated to generate an attestation report from AMD secure processor. The data exchanged between the AMD secure processor and the VM is secured using the VM Platform Communication Keys (VMPCKs) to encrypt and decrypt the messages transmitted between these components.
   The following figure provides an example of an attestation report. The Trusted Computing Base (TCB) comprises a set of hardware, firmware, and software components that collectively provide a secure environment for operations. To ensure the integrity and trustworthiness of the VM, it is essential to trust the TCB components to function as intended. The TCB version is included within the attestation report and is represented as a 64-bit numerical value.



```
Attestation Report:

Version:                      5

Guest SVN:                    0

Guest Policy (0x30000):
  ABI Major:     0
  ABI Minor:     0
  SMT Allowed:   true
  Migrate MA:    false
  Debug Allowed: false
  Single Socket: false
  CXL Allowed:   false
  AEX 256 XTS:   false
  RAPL Allowed:  false
  Ciphertext hiding: false
  Page Swap Disable: false

Family ID:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Image ID:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VMPL:                         1

Signature Algorithm:          1

Current TCB:

TCB Version:
  Microcode:   79
  SNP:         4
  TEE:         1
  Boot Loader: 1
  FMC:         1

Platform Info (103):
  SMT Enabled:               true
  TSME Enabled:              true
  ECC Enabled:               true
  RAPL Disabled:             false
  Ciphertext Hiding Enabled: false
  Alias Check Complete:      true
```

Figure 4. Attestation report example

3. The attestation report is transmitted to the guest owner for subsequent verification.
4. The guest owner makes a determination regarding the trustworthiness of the guest. The regular attestation workflow involves retrieving the requisite signing certificates directly from the official AMD Key Distribution Service (KDS), thereby establishing a robust chain of trust that originates from AMD.

   Critically, the entire attestation report is cryptographically signed by a unique key embedded within the processor, known as the Versioned Chip Endorsement Key (VCEK). The VCEK is a private Elliptic Curve Digital Signature Algorithm (ECDSA) key that is unique to each AMD chip running a specific TCB version. The authenticity of the VCEK can be traced back to AMD's root keys through a certificate chain, as illustrated in the figure below.

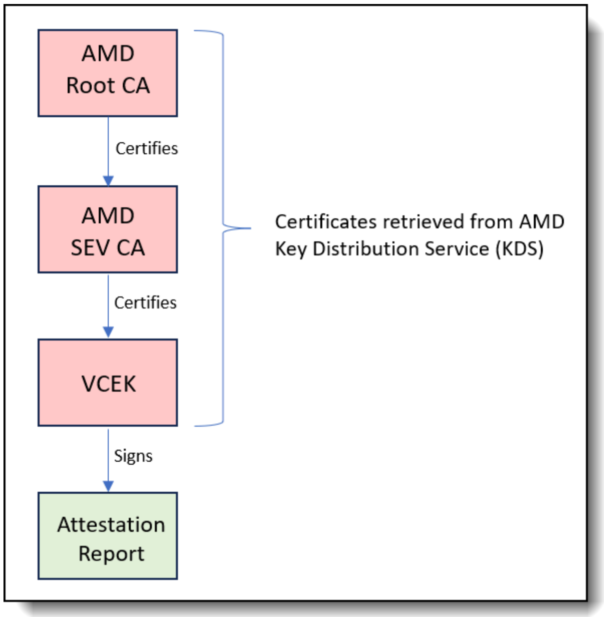


Figure 5. VCEK Certificate Trust Chain

The AMD Root Key (ARK) is the root of trust, so it is self-signed. The ARK then signed the AMD SEV Key (ASK), and the ASK, in turn, signs the VCEK, which is the certificate used to confirm the attestation report's authenticity and the system's configuration

5. Upon establishing trust, the guest owner authorizes the guest to handle sensitive information, thereby enabling the secure launch of the guest.

Hardware and OS requirements

The test configuration used in this paper is based on the Lenovo ThinkSystem SD535 V3 server. The configuration of the server is summarized in the following table.

Table 1. ThinkSystem SD535 V3 server configuration

Component	Configuration
Server	ThinkSystem SD535 V3 Server
CPU	1x AMD EPYC™ 9965 192-Core Processor
Memory	2x 16GB DDR5 6400MHz RDIMM
SSD	480GB SATA SSD
Host OS	ESXi 9.0 Custom Image for Lenovo ThinkSystem
Guest VM OS	Ubuntu server 25.04

To facilitate the attestation process, both the ESXi host and the guest VM must meet the following requirements:

- Processor: AMD EPYC 7003 Zen 3 "Milan" or subsequent generations.
- Host Firmware Configuration:
    - SME, SEV-ES, SEV-SNP must be enabled
    - When SEV-ES is activated, an appropriate value must be specified for the Minimum SEV non-ES Address Space Identifier (ASID) setting.
    - The Reverse Map Table (RMP) must be enabled for the entirety of host memory.
    - SNP features for IOMMU must be enabled.
- Guest Operating System: Ubuntu server 25.04, RHEL10.0, or SLES 15 SP6 (kernel version 6.9 or newer is recommended).
- Virtual Machine Hardware Version: The virtual machine hardware version must be 22 or later.

Restrictions to virtual machine functions

When AMD SEV-SNP is enabled, certain VM operations are unavailable. Specifically, the following functionalities are restricted:

- vMotion
- Suspending a VM
- Taking a snapshot of a VM
- Hotplug
- vTPM
- FT
- Secure Boot
- Quick boot
- Virtual IOMMU

Setting up Attestation in ESXi 9

VMware initially incorporated support for confidential computing five years ago, with the introduction of AMD SEV-ES. In VMware Cloud Foundation 9.0, this support was further extended to include AMD SEV-SNP. This technological advancement facilitates hardware-based encryption of data in use, employing per-Virtual Machine encryption keys. Additionally, it provides capabilities for workload and host attestation, thereby enhancing the security level of virtualized environments.

The remaining sections of the paper describe the steps required to enable the attestation process with a guest VM hosted on an ESXi 9.0 platform:

1. UEFI Configuration
2. ESXi Configuration
3. Guest OS Configuration

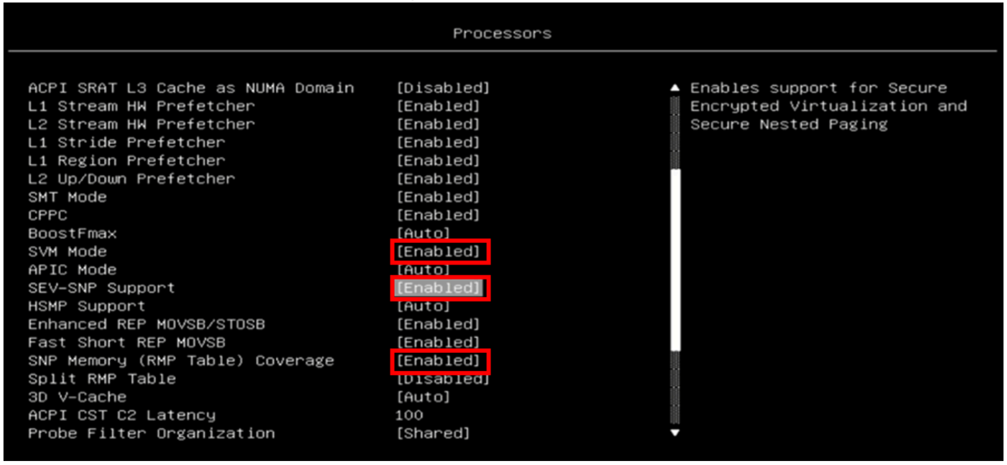
UEFI Configuration

The following steps describe the procedure for configuring AMD SEV-SNP through the System Setup or Lenovo XClarity Essentials OneCLI utility on a Lenovo ThinkSystem server.

Configure AMD SEV-SNP through the **System Setup**:

1. During the boot process, press the F1 key to access the System Setup utility.
2. Navigate to the Processor section and enable the following configurations, as the following figure shows.

   SVM Mode: **Enabled**
   SEV-SNP Support: **Enabled**
   SNP Memory (RMP Table) Coverage: **Enabled**

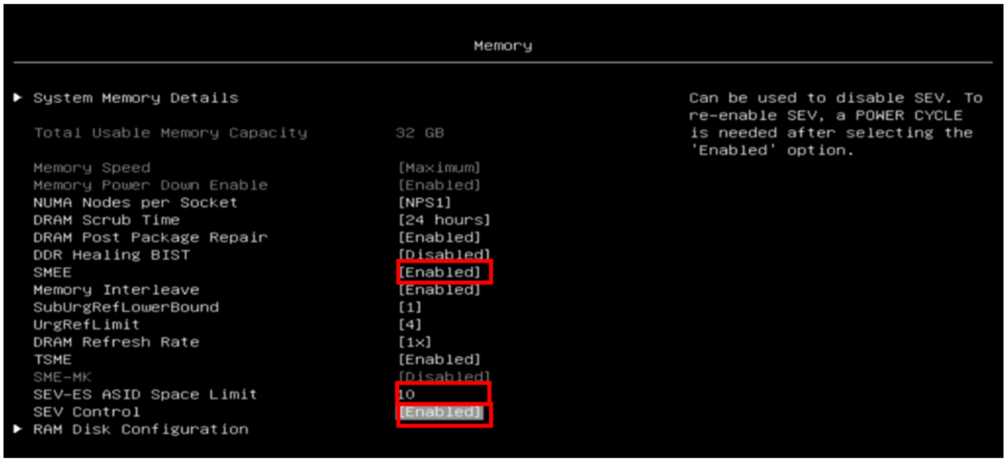


```
                                   Processors

ACPI SRAT L3 Cache as NUMA Domain     [Disabled]             Enables support for Secure
L1 Stream HW Prefetcher               [Enabled]              Encrypted Virtualization and
L2 Stream HW Prefetcher               [Enabled]              Secure Nested Paging
L1 Stride Prefetcher                  [Enabled]
L1 Region Prefetcher                  [Enabled]
L2 Up/Down Prefetcher                 [Enabled]
SMT Mode                              [Enabled]
CPPC                                  [Enabled]
BoostFmax                             [Auto]
SVM Mode                              [Enabled]
APIC Mode                             [Auto]
SEV-SNP Support                       [Enabled]
HSMP Support                          [Auto]
Enhanced REP MOVSB/STOSB              [Enabled]
Fast Short REP MOVSB                  [Enabled]
SNP Memory (RMP Table) Coverage       [Enabled]
Split RMP Table                       [Disabled]
3D V-Cache                            [Auto]
ACPI CST C2 Latency                   100
Probe Filter Organization             [Shared]
```

Figure 6. Processor settings in System Setup

3. Proceed to the Memory section and enable the following configurations, as the following figure shows.
   SMEE: **Enabled**
   SEV-ES ASID Space Limit: **10**
   SEV Control: **Enabled**



```
                                    Memory

▶ System Memory Details                                      Can be used to disable SEV. To
                                                             re-enable SEV, a POWER CYCLE
  Total Usable Memory Capacity        32 GB                  is needed after selecting the
                                                             'Enabled' option.
  Memory Speed                        [Maximum]
  Memory Power Down Enable            [Enabled]
  NUMA Nodes per Socket               [NPS1]
  DRAM Scrub Time                     [24 hours]
  DRAM Post Package Repair            [Enabled]
  DDR Healing BIST                    [Disabled]
  SMEE                                [Enabled]
  Memory Interleave                   [Enabled]
  SubUrgRefLowerBound                 [1]
  UrgRefLimit                         [4]
  DRAM Refresh Rate                   [1x]
  TSME                                [Enabled]
  SME-MK                              [Disabled]
  SEV-ES ASID Space Limit             10
  SEV Control                         [Enabled]
▶ RAM Disk Configuration
```

Figure 7. Memory settings in System Setup

4. Save the configurations and reboot the server to apply the configured settings.

5. Configure AMD SEV-SNP through the Lenovo XClarity Essentials OneCLI utility as follows:
    a. Enable the SVM Mode

    ```
    $ ./ OneCli config set Processors.SVMMode Enabled --bmc :@
    ```

    b. Enable the SEV-SNP Support

    ```
    $ ./ OneCli config set Processors.SEV-SNPSupport Enabled --bmc :@
    ```

    c. Enable the SNP Memory (RMP Table) Coverage

    ```
    $ ./ OneCli config set Processors.SNPMemoryRMPTableCoverage Enabled
    --bmc :@
    ```

    d. Enable the SMEE

    ```
    $ ./ OneCli config set Memory.SMEE Enabled --bmc :@
    ```

    e. Set the SEV-ES ASID Space Limit

    ```
    $ ./ OneCli config set Memory.SEV-ESASIDSpaceLimit 10 --bmc :@
    ```

    f. Enable SEV Control

    ```
    $ ./ OneCli config set Memory.SEVControl Enabled --bmc :@
    ```

    g. Dump the UEFI settings and confirm that the settings are configured correctly.

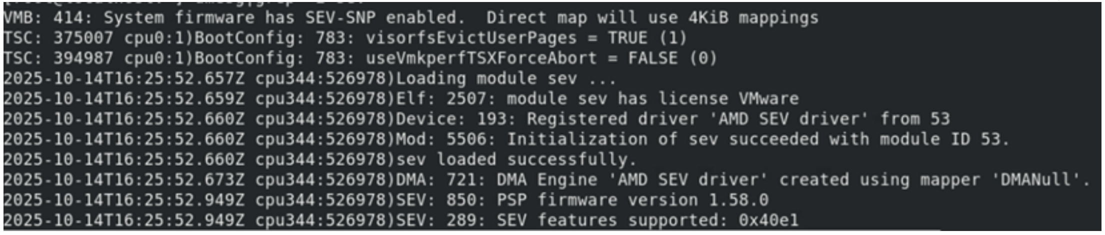
    ```
    $ ./ OneCli config show Processors --bmc :@
    $ ./ OneCli config show Memory --bmc :@
    ```

    h. Reboot the server to apply the configured settings.

ESXi Configuration

The following steps outline the procedure for configuring and enabling AMD SEV-SNP within the VMware vSphere environment. This process is demonstrated using vSphere ESXi 9.0 and an Ubuntu server 25.04 VM deployed on a Lenovo ThinkSystem server.

1. Proceed with the installation of ESXi 9.0 on the server. Upon reviewing the operating system boot log, it is evident that the system firmware has AMD SEV-SNP enabled. Additionally, the AMD Platform Security Processor (PSP) version is confirmed to be 1.58.0, as depicted in the following figure.

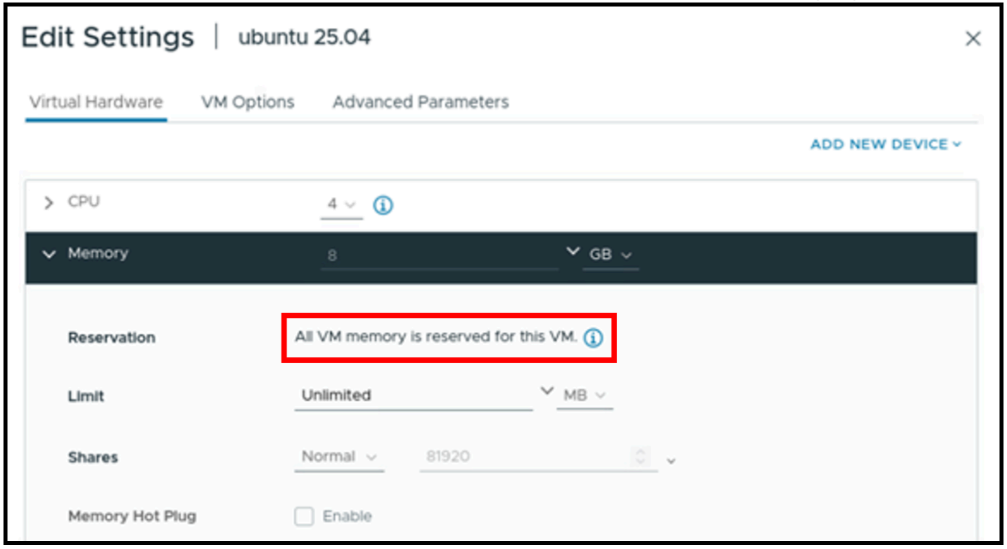
   

   ```
   VMB: 414: System firmware has SEV-SNP enabled.  Direct map will use 4KiB mappings
   TSC: 375007 cpu0:1)BootConfig: 783: visorfsEvictUserPages = TRUE (1)
   TSC: 394987 cpu0:1)BootConfig: 783: useVmkperfTSXForceAbort = FALSE (0)
   2025-10-14T16:25:52.657Z cpu344:526978)Loading module sev ...
   2025-10-14T16:25:52.659Z cpu344:526978)Elf: 2507: module sev has license VMware
   2025-10-14T16:25:52.660Z cpu344:526978)Device: 193: Registered driver 'AMD SEV driver' from 53
   2025-10-14T16:25:52.660Z cpu344:526978)Mod: 5506: Initialization of sev succeeded with module ID 53.
   2025-10-14T16:25:52.660Z cpu344:526978)sev loaded successfully.
   2025-10-14T16:25:52.673Z cpu344:526978)DMA: 721: DMA Engine 'AMD SEV driver' created using mapper 'DMANull'.
   2025-10-14T16:25:52.949Z cpu344:526978)SEV: 850: PSP firmware version 1.58.0
   2025-10-14T16:25:52.949Z cpu344:526978)SEV: 289: SEV features supported: 0x40e1
   ```

   Figure 8. ESXi OS log

2. Establish a connection between the ESXi 9.0 host and a vCenter Server utilizing the vSphere client.

3. Deploy an Ubuntu server 25.04 virtual machine. Prior to powering on the virtual machine, navigate to the Memory section within the virtual hardware settings. Ensure that the entirety of the VM memory is reserved for this specific VM, as illustrated in the following figure.

   Edit Settings | ubuntu 25.04

   CPU 4

   Memory 8 GB

   Reservation: All VM memory is reserved for this VM.

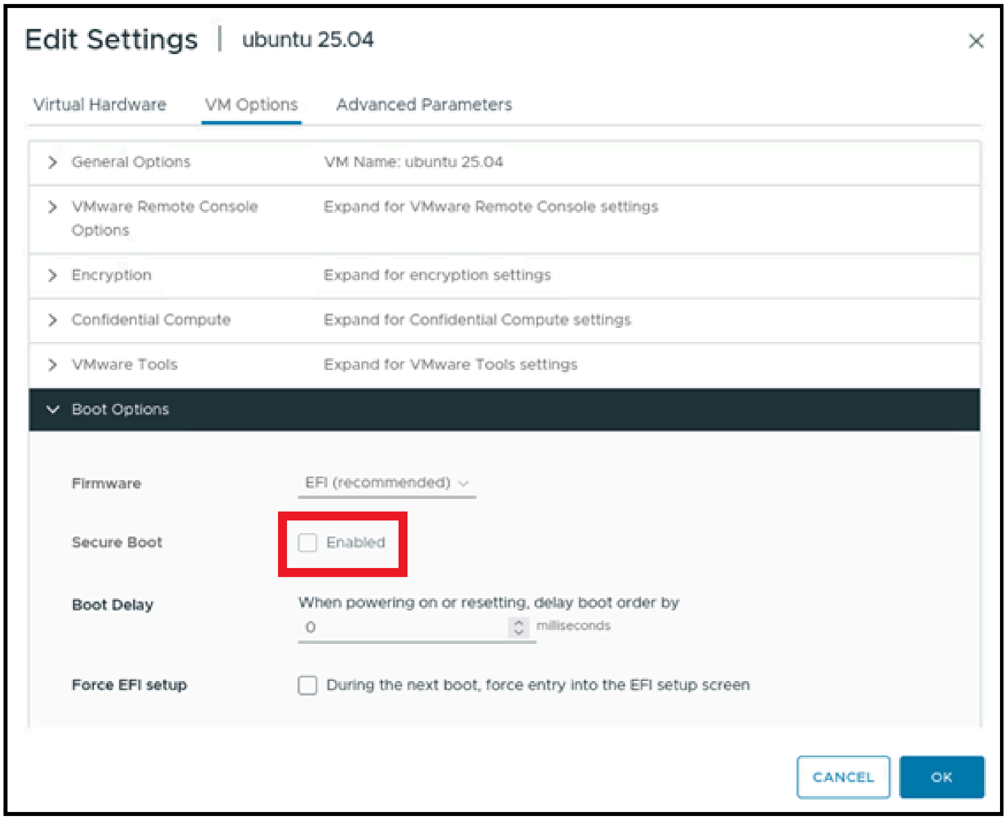
   Limit: Unlimited MB

   Shares: Normal 81920

   Memory Hot Plug: □ Enable

   Figure 9. Reserved all memory in VM setting

4. Proceed to the Boot Options within the VM Options tab and verify that UEFI Secure Boot is not enabled, as shown in the following figure.



Edit Settings | ubuntu 25.04

General Options — VM Name: ubuntu 25.04

VMware Remote Console Options — Expand for VMware Remote Console settings

Encryption — Expand for encryption settings

Confidential Compute — Expand for Confidential Compute settings

VMware Tools — Expand for VMware Tools settings

Boot Options

Firmware: EFI (recommended)

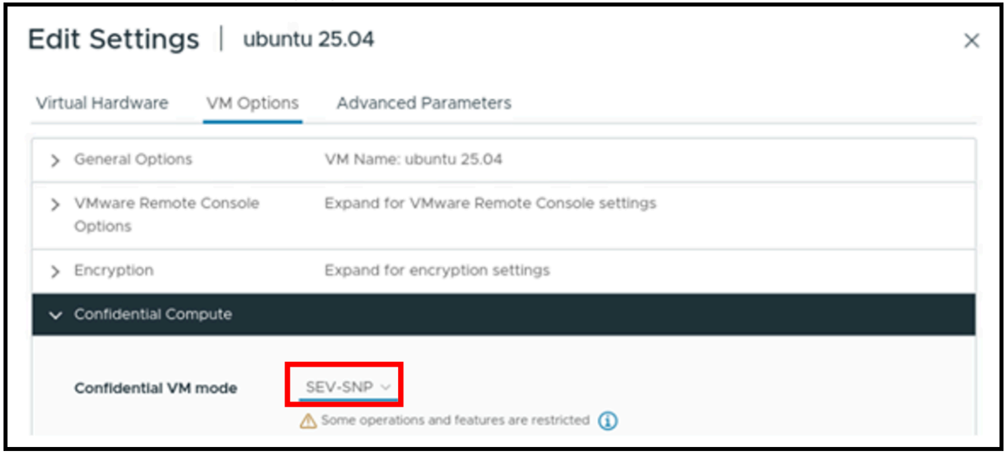
Secure Boot: □ Enabled

Boot Delay: When powering on or resetting, delay boot order by 0 milliseconds

Force EFI setup: □ During the next boot, force entry into the EFI setup screen

Figure 10. Secure Boot disabled in VM setting

5. Navigate to the Confidential Compute section and configure the Confidential VM mode to SEV-SNP, as shown in the following figure.



Edit Settings | ubuntu 25.04

General Options — VM Name: ubuntu 25.04

VMware Remote Console Options — Expand for VMware Remote Console settings

Encryption — Expand for encryption settings

Confidential Compute

Confidential VM mode: SEV-SNP

⚠ Some operations and features are restricted ⓘ

Figure 11. Enable AMD SEV-SNP in VM setting

6. Initiate the power-on sequence for the VM and proceed with the standard installation of the guest operating system.

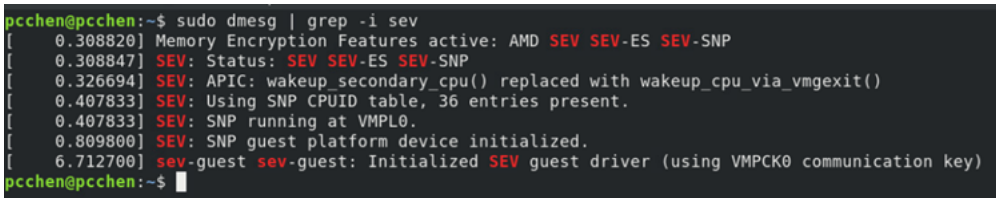
Guest OS Configuration

The **snpguest** utility is a command-line tool designed for managing an AMD SEV-SNP enabled guest. This utility facilitates user interaction with the guest firmware device, enabling a range of operations including attestation, certificate management, derived key fetching, and additional functionalities.

To enable and verify SEV-SNP attestation on a Linux guest operating system, follow to the below steps:

1. Upon launching the guest operating system, execute the following command to verify the status of SEV-SNP, as the following figure shows. The kernel log will contain messages that describe the state of AMD memory encryption features within the VM. The presence of the SEV-SNP feature in the kernel log, alongside other active memory encryption features, indicates that SEV-SNP is operational for the VM.

   ```
   sudo dmesg | grep -i sev
   ```

   ```
   pcchen@pcchen:~$ sudo dmesg | grep -i sev
   [    0.308820] Memory Encryption Features active: AMD SEV SEV-ES SEV-SNP
   [    0.308847] SEV: Status: SEV SEV-ES SEV-SNP
   [    0.326694] SEV: APIC: wakeup_secondary_cpu() replaced with wakeup_cpu_via_vmgexit()
   [    0.407833] SEV: Using SNP CPUID table, 36 entries present.
   [    0.407833] SEV: SNP running at VMPL0.
   [    0.809800] SEV: SNP guest platform device initialized.
   [    6.712700] sev-guest sev-guest: Initialized SEV guest driver (using VMPCK0 communication key)
   pcchen@pcchen:~$ 
   ```

   Figure 12. Check SEV-SNP in guest OS

2. Install the Rust toolchain and Cargo package manager.

   ```
   $ curl --proto '=https' --tlsv1.2 -sSf https://sh.rustup.rs | sh
   ```

3. Compile the snpguest utility from the source repository.

   ```
   $ git clone https://github.com/virtee/snpguest.git
   $ cd snpguest
   $ cargo build -r
   $ cd target/release
   ```

4. Execute the following command to request the AMD Secure Processor to generate an attestation report (report.bin). This report will include random data to ensure its uniqueness and integrity:

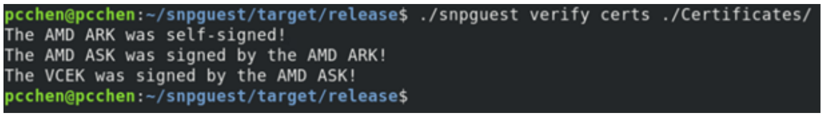
   ```
   $ ./snpguest report report.bin requtest-file.txt --random
   ```

5. Execute the following command to retrieve the AMD certificate chain and the VCEK certificate from the AMD KDS:

   ```
   $ ./snpguest fetch ca -r report.bin pem ./Certificates
   $ ./snpguest fetch vcek pem ./Certificates ./report.bin
   ```

6. Execute the following command to verify the validity of the certificate chain. Successful verification of these relationships is represented in the following figure.

   ```
   $ ./snpguest verify certs ./Certificates
   ```

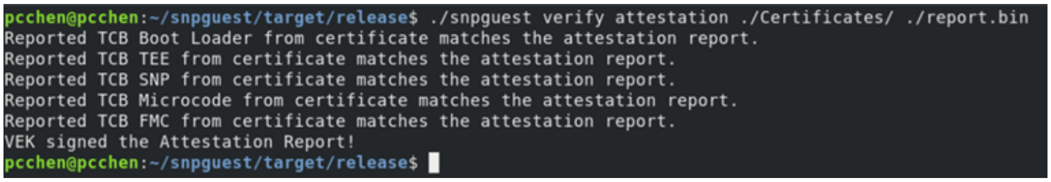


```
pcchen@pcchen:~/snpguest/target/release$ ./snpguest verify certs ./Certificates/
The AMD ARK was self-signed!
The AMD ASK was signed by the AMD ARK!
The VCEK was signed by the AMD ASK!
pcchen@pcchen:~/snpguest/target/release$
```

Figure 13. Verify the certificate chain

7. Execute the following command to validate the attestation report, as the following figure shows. This process involves utilizing the VCEK certificate to examine the cryptographic signature on the report.bin file. Additionally, it compares the TCB version numbers embedded within the VCEK certificate to those documented in the attestation report. It is imperative that these version numbers match to ensure the integrity and authenticity of the report, with the final line confirming the validity of the certificate.

```
$ ./snpguest verify attestation ./Certificates ./report.bin
```



```
pcchen@pcchen:~/snpguest/target/release$ ./snpguest verify attestation ./Certificates/ ./report.bin
Reported TCB Boot Loader from certificate matches the attestation report.
Reported TCB TEE from certificate matches the attestation report.
Reported TCB SNP from certificate matches the attestation report.
Reported TCB Microcode from certificate matches the attestation report.
Reported TCB FMC from certificate matches the attestation report.
VEK signed the Attestation Report!
pcchen@pcchen:~/snpguest/target/release$
```

Figure 14. Verify the attestation report

Summary

AMD SEV-SNP was the first commercially available x86 technology to offer VM isolation—including confidentiality and integrity—for the cloud and is deployed in the form of confidential VMs on Microsoft Azure, AWS, and Google Cloud.

Confidential VM takes advantage of security technologies to offer the following benefits:

- Isolation: CPUs are equipped with an AES hardware memory encryption engine, the encryption key itself is stored in the hardware root of trust, inaccessible to the hypervisor.
- Attestation: We can verify the identity and the state of the VM, to make sure that key components haven't been tampered with. The measurement is cryptographically signed and can be attested to a remote verifier

Resources

For more information, see these resources:

- Securing Virtual Machines with AMD Secure Encrypted Virtualization-Secure Nested Paging
https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/9-0/vsphere-security/securing-virtual-machines-in-the-vsphere-client/securing-virtual-machines-with-amd-secure-encrypted-virtualization-secure-nested-paging.html
- snpguest on github
https://github.com/virtee/snpguest
- General overview of AMD SEV-SNP and Intel TDX
https://sys.cs.fau.de/extern/lehre/ws22/akss/material/amd-sev-intel-tdx.pdf
- AMD SEV SNP Attestation: Establishing Trust in Guests
https://www.amd.com/content/dam/amd/en/documents/developer/lss-snp-attestation.pdf

Author

Alpus Chen is an OS Engineer at the Lenovo Infrastructure Solutions Group in Taipei, Taiwan. As a specialist in Linux and VMware technical support for several years, he is interested in operating system operation and recently focuses on VMware OS.

Related product families

Product families related to this document are the following:

- Processors

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION ”AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

This document, LP2349, was created or updated on January 5, 2026.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/LP2349
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/LP2349.

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at https://www.lenovo.com/us/en/legal/copytrade/.

The following terms are trademarks of Lenovo in the United States, other countries, or both:
Lenovo®
ThinkSystem®
XClarity®

The following terms are trademarks of other companies:

AMD and AMD EPYC™ are trademarks of Advanced Micro Devices, Inc.

Intel®, the Intel logo is a trademark of Intel Corporation or its subsidiaries.

Linux® is the trademark of Linus Torvalds in the U.S. and other countries.

Microsoft® and Azure® are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.