Using AMD Secure Encrypted Virtualization-Encrypted State (SEV-ES) on ThinkSystem Servers

Introduces the features AMD SEV-ES

Shows vSphere support of AMD SEV-ES

Explains the prerequisites and limitation for using AMD SEV-ES

Shows how to use AMD SEV-ES on Lenovo ThinkSystem servers

Chengcheng Peng

Abstract

AMD Secure Encrypted Virtualization-Encrypted State (SEV-ES) technology is used to protect a guest operating system from attacks on its register state from a malicious hypervisor. SEV-ES encrypts all CPU register contents when a VM stops running, which prevents the leakage of information in CPU registers to components like the hypervisor. It can even detect malicious modifications to a CPU register state.

This paper presents a briefly technical overview of the SEV-ES technology and describes how to configure and use SEV-ES in VMware vSphere 7.0 U1 on Lenovo® ThinkSystem™ servers. This paper is intended for IT specialists and IT administrators who are familiar with SEV-ES and VMware vSphere products.

At Lenovo Press, we bring together experts to produce technical publications around topics of importance to you, providing information and best practices for using Lenovo products and solutions to solve IT challenges.

See a list of our most recent publications at the Lenovo Press web site:

http://lenovopress.com

Do you have the latest version? We update our papers from time to time, so check whether you have the latest version of this document by clicking the **Check for Updates** button on the front page of the PDF. Pressing this button will take you to a web page that will tell you if you are reading the latest version of the document and give you a link to the latest if needed. While you're there, you can also sign up to get notified via email whenever we make an update.

Contents

Introduction

AMD Secure Encrypted Virtualization (SEV) integrates memory encryption capabilities with the existing AMD-V virtualization architecture to support encrypted virtual machines (VMs). Encrypted VMs can help protect not only from physical threats but also from other virtual machines or even the hypervisor itself. SEV provides additional assurances to help protect the guest VM code and data from the attacker.

SEV uses one key per virtual machine to isolate guests and the hypervisor from one another. The keys are managed by the AMD Secure Processor and are hardware isolated.

Figure 1 shows the brief overview workflow of AMD SEV.

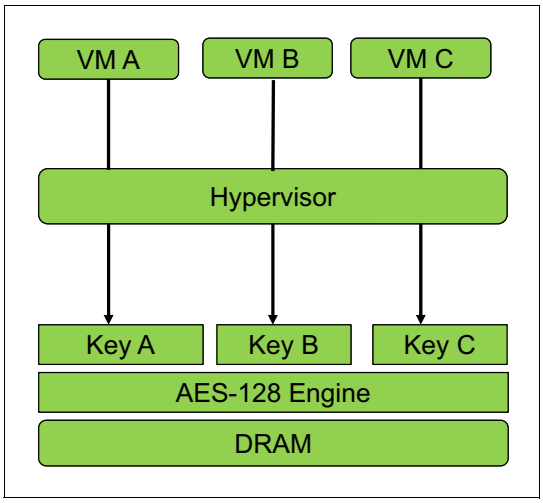

Figure 1 Workflow of AMD SEV

AMD SEV-ES builds upon AMD SEV to provide an even smaller attack surface and additional protection for a guest operating system (guest OS) from the hypervisor. The AMD SEV-ES feature provides additional hardware-enforced security for isolating guest VMs from the hypervisor. The AMD SEV-ES technology encrypts all CPU register contents when a VM stops running. This prevents the leakage of information in CPU registers to components like the hypervisor and can even detect malicious modifications to a CPU register state.

The AMD SEV-ES architecture is designed to protect guest VM register state by default, and only allow the guest VM itself to grant selective access as required. This additional security protection functionality is accomplished in two ways:

- First, all VM register state is saved and encrypted when a VM exit event occurs. This state is decrypted and restored on a VMRUN only.
- Second, certain types of VM exit events cause a new exception to be taken within the guest VM. This new Communication Exception (#VC) indicates that the guest VM performed some action which requires hypervisor involvement, an example of which would be an IO access by the VM.

The guest #VC handler is responsible for determining what register state is necessary to expose to the hypervisor for the purpose of emulating this operation. The #VC handler also inspects the returned values from the hypervisor and updates the guest state if the output is deemed acceptable.

Figure 2 shows the overview workflow of SEV-ES.

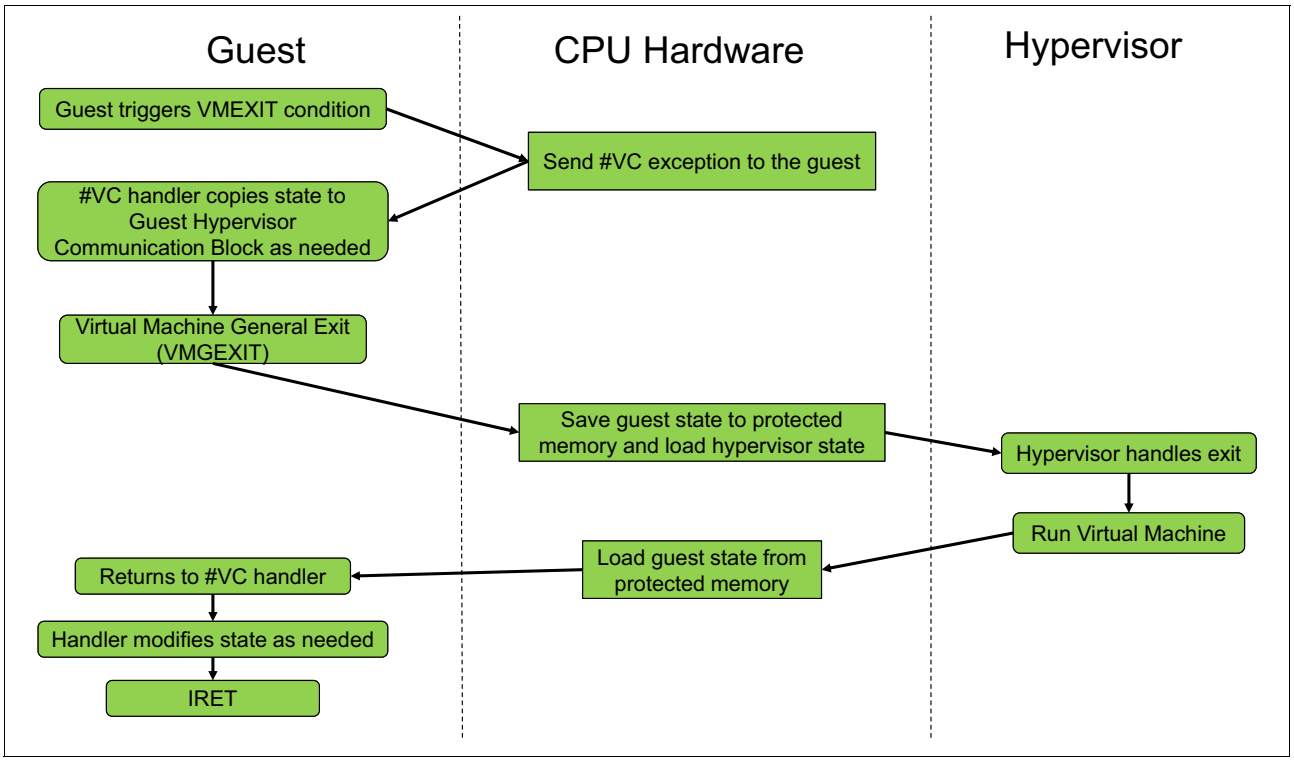

Figure 2 Workflow of AMD SEV-ES

vSphere support of AMD SEV-ES

AMD SEV-ES supports AMD EPYC 7xx2 (“Rome”) and EPYC 7xx3 (“Milan”) processors. Table 1 lists the Lenovo ThinkSystem servers which support AMD SEV-ES and the minimum version of UEFI firmware that supports the AMD SEV-ES.

Table 1 Lenovo servers that support AMD SEV-ES

Lenovo ThinkSystem Servers with AMD EPYC processors	Supported UEFI version	SEV-ES Support status
ThinkSystem SR635	6.01 and later	Yes
ThinkSystem SR645	2.0 and later	Yes
ThinkSystem SR655	6.01 and later	Yes
ThinkSystem SR665	2.0 and later	Yes

In vSphere 7.0 Update 1 and later, we can enable AMD SEV-ES on supported AMD EPYC CPUs and guest operating system. SEV-ES requires a supported guest operating system. A virtual machine with SEV-ES enabled won’t work if the guest OS does not support SEV-ES.

Table 2 lists the version of vSphere and guest OS that support AMD SEV-ES.

Table 2 Supported vSphere and Guest OS version for AMD SEV-ES

Supported VMware vSphere Version	Supported guest OS Version
VMware vSphere 7.0 Update 1 and later	RHEL 8.5 RHEL 9.0 Photon OS version 3 and later

There are some VM operations unavailable when AMD SEV-ES is enabled. You cannot suspend, migrate with vMotion, or take or restore memory snapshots of such VMs.

The following features are not supported when SEV-ES is enabled:

- UEFI Secure Boot
- Suspend/Resume
- vMotion
- Hot add or remove of CPU or memory
- Powered-on snapshots (however, no-memory snapshots are supported)
- System Management Mode
- VMware Fault Tolerance
- Clones and instant clones
- Guest Integrity

How to configure and use AMD SEV-ES

Starting with vSphere 7.0 U1, PowerCLI can be used to enable and disable SEV-ES on virtual machines. Starting in vSphere 7.0 U2, either the vSphere Client or PowerCLI can be used to enable and disable SEV-ES on virtual machines. New virtual machines can be created with SEV-ES or SEV-ES can be enabled on existing virtual machines.

This section describes how to configure and use AMD SEV-ES in vSphere 7.0 Update 1 and later on Lenovo ThinkSystem servers with detailed steps.

Prerequisites

In order to use AMD SEV-ES, the system must meet the following requirements:

1. The system must be installed with an AMD EPYC 7xx2 or EPYC 7xx3 processor.
2. Secure Memory Encryption (SME) and SEV-ES must be enabled in the UEFI.
3. The number of SEV-ES virtual machines per ESXi host is controlled by UEFI. When enabling SEV-ES in the UEFI settings, enter a value for SEV-ES ASID Space Limit.
4. The ESXi host running in your host must be at ESXi 7.0 Update 1 or later.
5. The vCenter Server must be at vSphere 7.0 Update 2 or later.
6. The guest operating system must support SEV-ES. Currently only Linux kernels with specific support for SEV-ES are supported.
7. The virtual machine must be at hardware version 18 or later.
8. The virtual machine must have the Reserve all guest memory option enabled, otherwise power-on fails.

Configuration procedures

The following steps describe the process to configure and use AMD SEV-ES in vSphere 7.0 U3 on a Lenovo ThinkSystem SR635 server that is equipped with AMD EPYC 75F3 32-Core processor.

1. Enable advanced option in UEFI settings using the following command:

   # ipmitool -I lanplus -H $bmc-ip -U user -P pwd raw 0x3c 0x64 0x01 0x01

   Figure 3 shows an example of the command:

```
D:\ipmitool-1.8.17>ipmitool -I lanplus -H 10.245.39.89 -U USERID -P PASSWORD=0 raw 0x3c 0x64 0x01 0x01
```

   Figure 3 Enable advanced option on SR635

   Tip: We can use the following command to disable advanced option in UEFI settings:

   # ipmitool -I lanplus -H $bmc-ip -U user -P pwd raw 0x3c 0x64 0x01 0x00

2. Power on the server and press F1 when prompted to enter System Setup as shown in Figure 4.

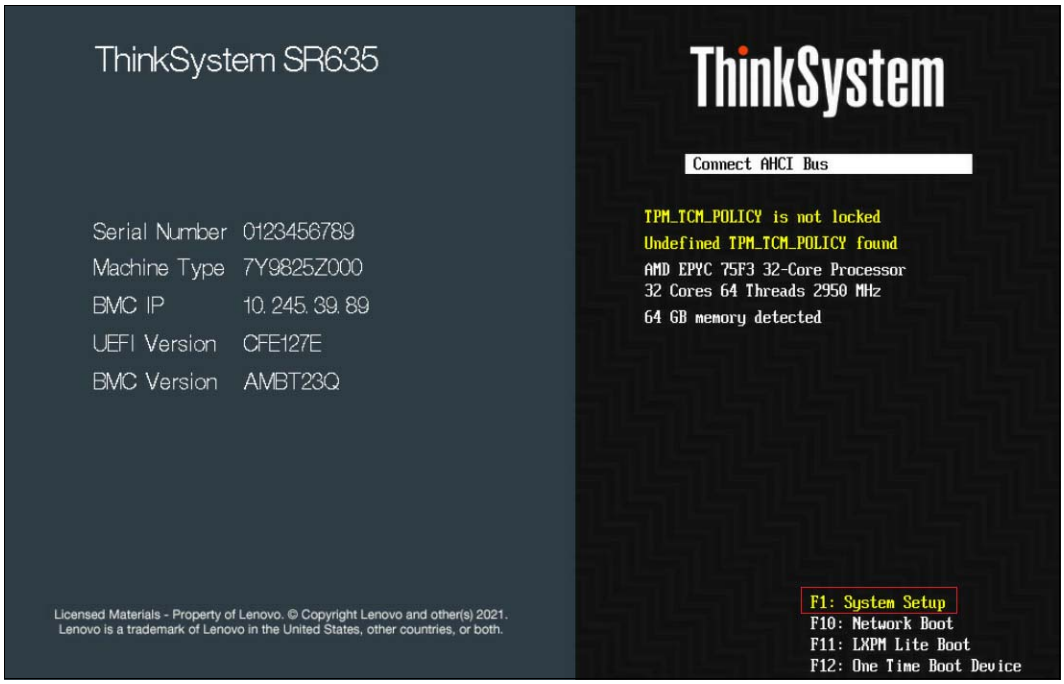

   Figure 4 Press F1 to enter System Setup on SR635

3. Use either UEFI settings or OneCLI to enable SME.

   To enable SME via UEFI settings, do the following:

   a. In System Setup, navigate to the System Configuration and Boot Management page.
   b. Select **Advanced** → **Memory Configuration** → **SMEE**.
   c. Enable SMEE setting as shown in Figure 5 on page 7.

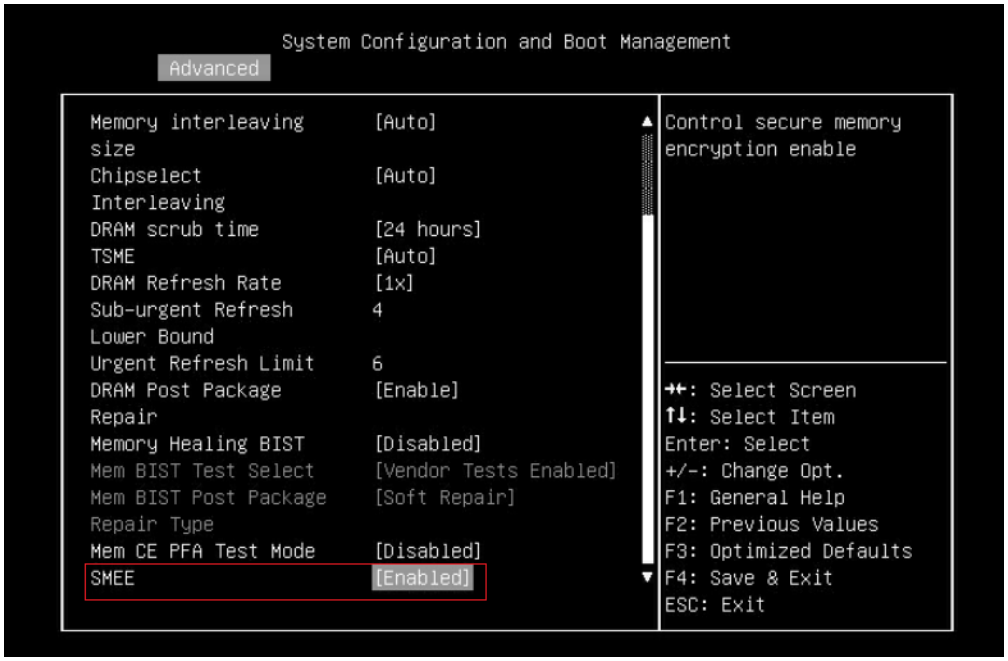

Figure 5 Enable SME in UEFI settings on SR635

To enable SME via OneCLI, do the following:

a. Download OneCLI from the Lenovo support site and install it.

   https://datacentersupport.lenovo.com/us/en/solutions/ht116433

b. Run the following OneCLI command to check the status of SME:

   ```
   OneCli.exe config show Bios.Q00094_SMEE --bmc <USERID>:<PASSWORD>@<IP>
   ```

   Figure 6 shows an example on how to check the status of SME via OneCLI command.

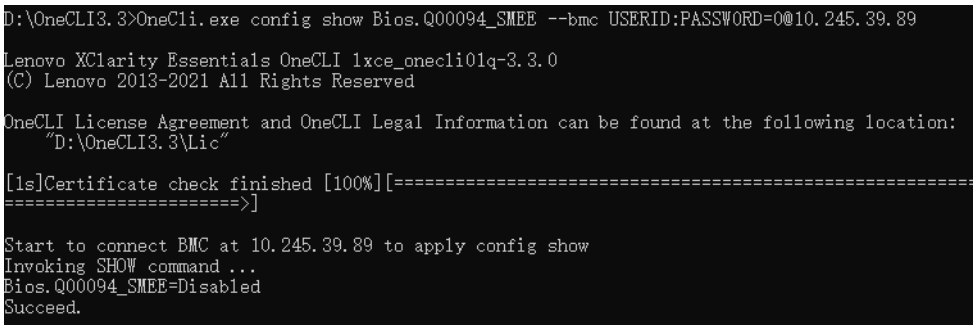

Figure 6 Check SME via OneCLI command

c. Run the following OneCLI command to enable the SME:

   ```
   OneCli.exe config set Bios.Q00094_SMEE Enabled --bmc <USERID>:<PASSWORD>@<IP>
   ```

Figure 7 shows an example on how to set the SME via OneCLI command.

```
D:\OneCLI3.3>OneCli.exe config set Bios.Q00094_SMEE Enabled --bmc USERID:PASSWORD=0@10.245.39.89

Lenovo XClarity Essentials OneCLI 1xce_onecli01q-3.3.0
(C) Lenovo 2013-2021 All Rights Reserved

OneCLI License Agreement and OneCLI Legal Information can be found at the following location:
    "D:\OneCLI3.3\Lic"

[1s]Certificate check finished [100%][==========================================================

Start to connect BMC at 10.245.39.89 to apply config set
Invoking SET command ...
Bios.Q00094_SMEE=Enabled
Changes completed successfully, but these changes will not take effect until next reboot.
Succeed.

D:\OneCLI3.3>OneCli.exe config show Bios.Q00094_SMEE --bmc USERID:PASSWORD=0@10.245.39.89

Lenovo XClarity Essentials OneCLI 1xce_onecli01q-3.3.0
(C) Lenovo 2013-2021 All Rights Reserved

OneCLI License Agreement and OneCLI Legal Information can be found at the following location:
    "D:\OneCLI3.3\Lic"

[1s]Certificate check finished [100%][==========================================================

Start to connect BMC at 10.245.39.89 to apply config show
Invoking SHOW command ...
Bios.Q00094_SMEE=Enabled
Succeed.
```

Figure 7 Enable SME via OneCLI command

4. Configure “SEV-ES ASID Space Limit Control” and “SEV-ES ASID Space Limit” in UEFI settings.
   a. In System Setup, navigate to the System Configuration and Boot Management page
   b. Select **Advanced** → **AMD CBS** → **CPU Common Options**
   c. Configure “SEV-ES ASID Space Limit Control” and “SEV-ES ASID Space Limit” as shown in Figure 8.

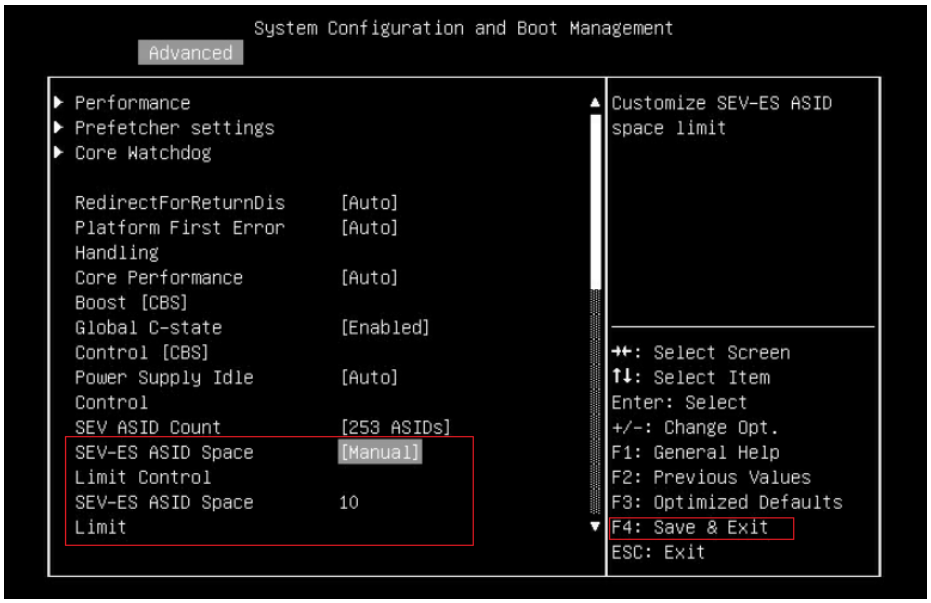

Figure 8 Configure SEV-ES ASID Space Limit on SR635

   d. Press F4 to Save & Exit.

5. Install vSphere 7.0 U3 on the server.
6. Connect to vCenter Server by using the vSphere Client.
7. Create a virtual machine and install a guest OS (e.g., RHEL8.5) that supports AMD SEV-ES.
8. Enable SEV-ES on virtual machines. Starting in vSphere 7.0 U2, you can use either the vSphere Client or PowerCLI to enable SEV-ES on virtual machines:

   To enable SEV-ES on the VMs using the vSphere Client, do the following:

   a. Right click the virtual machine RHEL8.5 in the inventory and click **Edit Settings**.

   b. Under **VM Options** → **Boot Options**, ensure that EFI is selected, and Secure Boot is unselected, as highlighted in Figure 9.

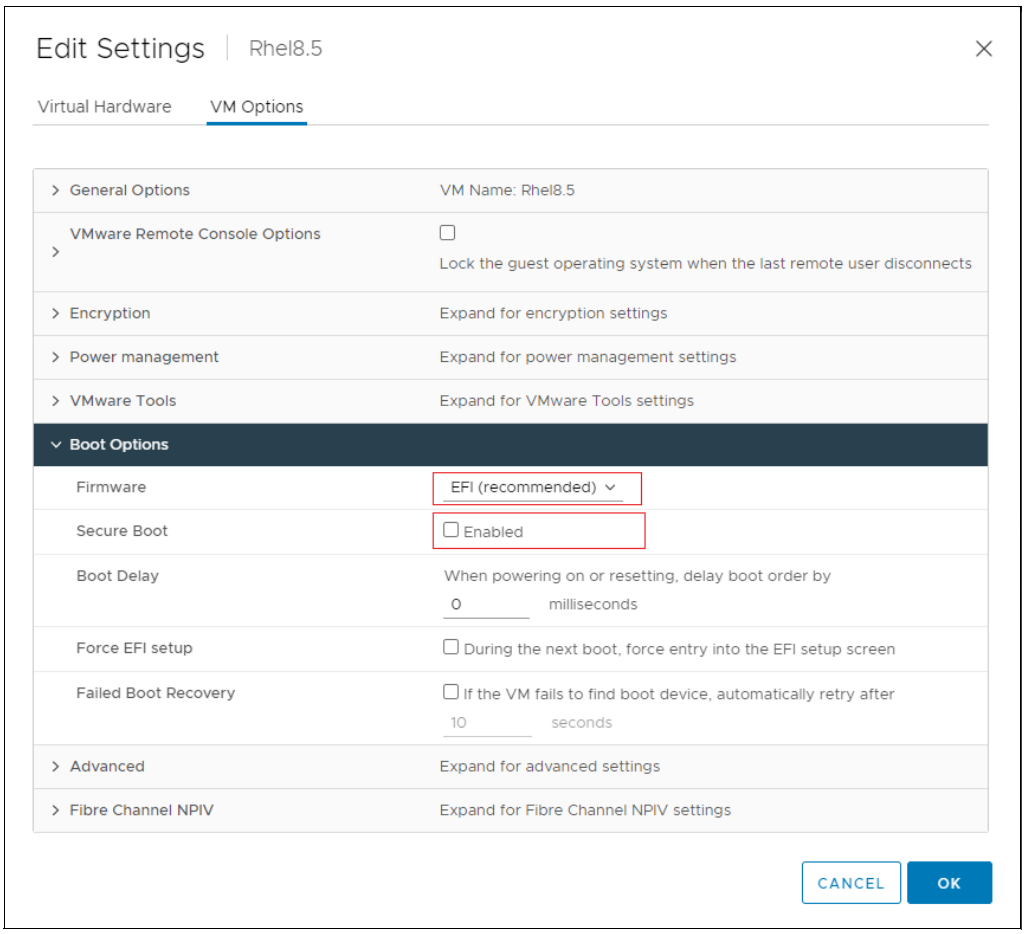

Figure 9 Configure Boot Options on vSphere client

c. In the Edit Settings dialog box, go to **VM Options** → **Encryption**, click the **Enabled** check box for AMD SEV-ES, and then click the OK button, as shown in Figure 10.

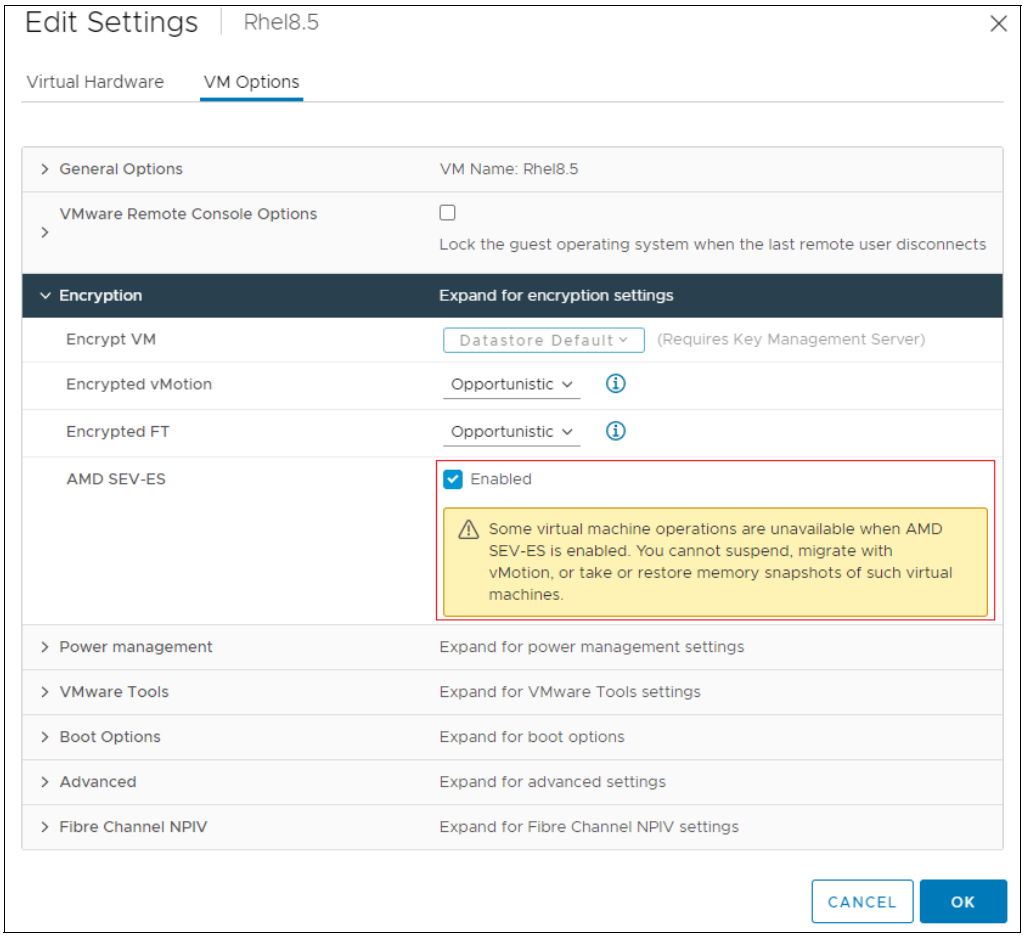

Figure 10 Enable AMD SEV-ES on vSphere client

To enable SEV-ES on the VMs using PowerCLI, do the following:

a. Download the PowerCLI from the PowerCLI home page, and install PowerCLI.

b. Open the PowerCLI console and use the following command to verify that the VMware Power CLI modules is installed successfully, as shown in Figure 11.

```
Get-Module -Name VMware.* | Select-Object -Property Name,Version
```

```
PS C:\Users\pengcc1> Get-Module -Name VMware.* | Select-Object -Property Name,Version

Name                                Version
----                                -------
VMware.Vim                          7.0.3.18730922
VMware.VimAutomation.Cis.Core       12.4.0.18627057
VMware.VimAutomation.Common         12.4.0.18627061
VMware.VimAutomation.Core           12.4.0.18627056
VMware.VimAutomation.Sdk            12.4.0.18627054
```

Figure 11 Check VMware Power CLI modules

c. In PowerCLI console, run the following command to allow execution of local scripts, as shown in Figure 12.

```
Set-ExecutionPolicy RemoteSigned
```

```
PS C:\Users\pengcc1> Set-ExecutionPolicy RemoteSigned
```

Figure 12 Set execution policy

d. In PowerCLI console, run the following **`Connect-VIServer`** cmdlet as an administrator to the vCenter server, as shown in Figure 13.

```
Connect-VIServer -server vCenter_Server_ip_address -User admin_user
-Password 'password'
```

```
PS C:\Users\pengcc1> Connect-VIServer -server 10.245.39.187 -User 'Administrator@vSphere.local' -Password 'L123.com'

Name                           Port  User
----                           ----  ----
10.245.39.187                  443   VSPHERE.LOCAL\Administrator
```

Figure 13 Connect to vCenter server

e. Add SEV-ES to the virtual machine with the following **`Set-VM`** cmdlet, as shown in Figure 14.

```
$vm=Get-VM -Name Rhel8.5
Set-VM -VM $vm  -SEVEnabled $true
```

```
PS C:\Users\pengcc1> $vm=Get-VM -Name Rhel8.5
PS C:\Users\pengcc1> Set-VM -VM $vm  -SEVEnabled $true

Confirmation
Proceed to configure the following parameters of the virtual machine with name 'Rhel8.5'?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): Y

Name                 PowerState Num CPUs MemoryGB
----                 ---------- -------- --------
Rhel8.5              PoweredOff 1        2.000
```

Figure 14 Enable SEV-ES via PowerCLI

9. Power on the virtual machine (we used RHEL 8.5) and use the following command to check the SEV-ES, as shown in Figure 15.

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

```
[root@localhost ~]# dmesg | grep -i sev
[    0.001000] AMD Memory Encryption Features active: SEV SEV-ES
[root@localhost ~]#
```

Figure 15 Check SEV-ES in RHEL8.5

References

For additional information, see these resources:

- AMD Secure Encrypted Virtualization developer page

  https://developer.amd.com/sev/

- Protecting VM Register State with SEV-ES

  https://www.amd.com/system/files/TechDocs/Protecting%20VM%20Register%20State%20with%20SEV-ES.pdf

- AMD64 Architecture Programmer's Manual Volume 2

  https://www.amd.com/system/files/TechDocs/24593.pdf

- VMware vSphere documentation, Securing Virtual Machines with AMD Secure Encrypted Virtualization-Encrypted State

  https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-F1F913CB-05F9-4D4F-B8A7-970A43532003.html

Author

Chengcheng Peng is a VMware Engineer at the Lenovo Infrastructure Solutions Group in Beijing, China. As a VMware engineer with 6 years' experience, she mainly focuses on vSphere security and storage.

Thanks to the following people for their contributions to this project:

- Boyong Li, Lenovo OS Technical Leader
- Alpus Chen, Lenovo VMware Engineer
- David Hsia, Lenovo VMware Engineer
- Chia-Yu Chu, Lenovo Advisory Engineer
- Gary Cudak, OS Architect and WW Technical Lead
- David Watts, Lenovo Press

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.
1009 Think Place - Building One
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 was created or updated on January 10, 2022.

Send us your comments via the **Rate & Provide Feedback** form found at
http://lenovopress.com/lp1545

Trademarks