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

Planning / Implementation

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.

The following figure shows the brief overview workflow of AMD SEV.

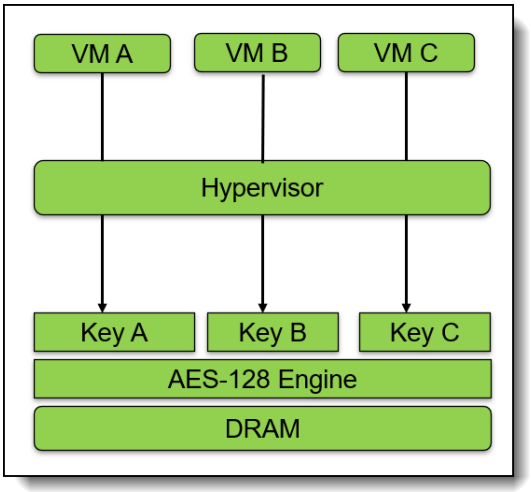

Figure 1. Workflow of AMD SEV

AMD Secure Encrypted Virtualization-Encrypted State (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.

The following figure shows the overview workflow of SEV-ES.

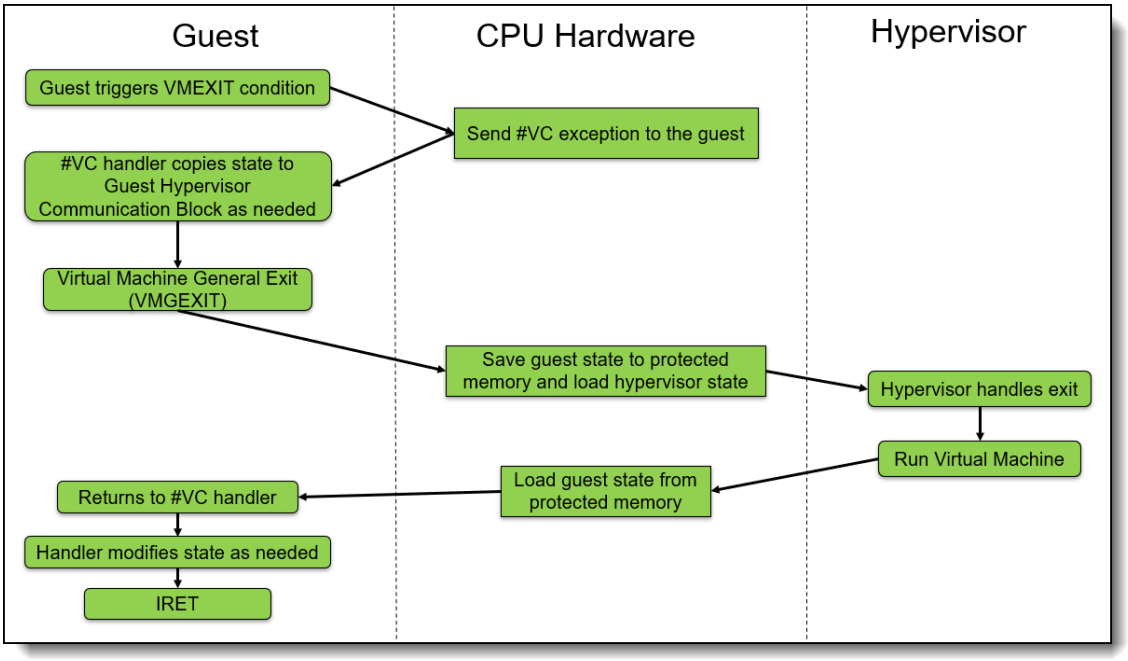

Figure 2. Workflow of AMD SEV-ES

Server and OS support

AMD SEV-ES supports AMD EPYC 7xx2 (“Rome”) and later processors. The following 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
ThinkSystem SR635 V3	2.10 and later	Yes
ThinkSystem SR645 V3	2.10 and later	Yes
ThinkSystem SR655 V3	2.10 and later	Yes
ThinkSystem SR665 V3	2.10 and later	Yes
ThinkSystem SR675 V3	1.30 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.

The supported VMware host versions that support AMD SEV-ES are as follows:

- VMware vSphere 7.0 Update 1 and later
- VMware vSphere 8.0 and later

The supported Guest OS versions that support AMD SEV-ES are as follows:

- RHEL 8.5 or later
- RHEL 9.0 or later
- SLES 15.3 or later
- Ubuntu 20.04.3 HWE kernel (v5.11)
- Ubuntu 22.04.0 or later
- 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 later processor.
2. Secure Memory Encryption (SME) and SEV-ES must be enabled in UEFI as described in Enabling SEV-ES in 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.

Enabling SEV-ES in UEFI

There are three ways to enable Secure Memory Encryption (SME) and SEV-ES in UEFI:

- Configure AMD SEV-ES in System Setup
- Configure AMD SEV-ES using Redfish REST API
- Configure AMD SEV-ES using OneCLI

Note: These instructions apply to all ThinkSystem servers with AMD processors except the SR635 and SR655. For these servers, see the Enabling SEV-ES in UEFI on the SR635 and SR655 section.

Configure AMD SEV-ES in System Setup

The following steps describe the process to configure SME and SEV-ES via System Setup on a ThinkSystem server.

1. In System Setup, navigate to the System Configuration and Boot Management page.
2. Enable SME by going to **System Settings > Memory** and set SMEE to **Enabled** as shown in the following figure.

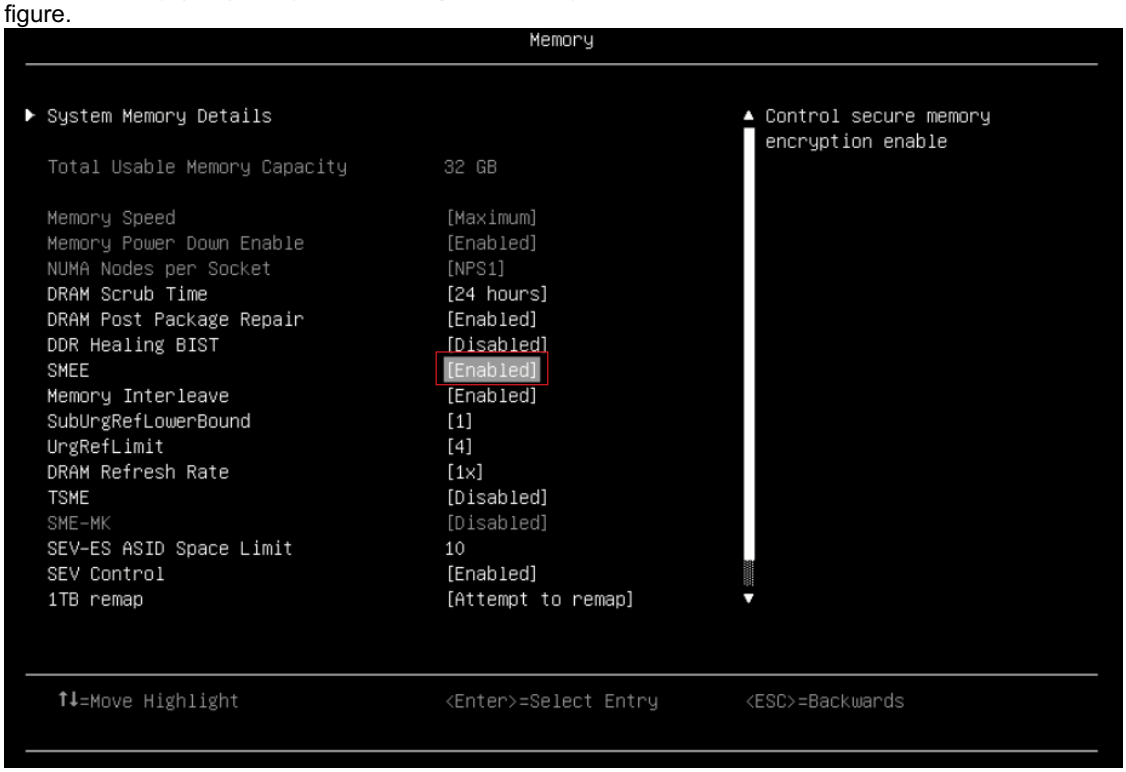

Figure 3. Enable SME via UEFI settings on SR665 V3

3. Enable AMD SEV-ES and configure SEV-ES ASID Space Limit Control via UEFI settings. Select **System Settings > Memory > SEV Control**, enable “SEV Control” and configure “SEV-ES ASID Space Limit” as shown in the following figure:

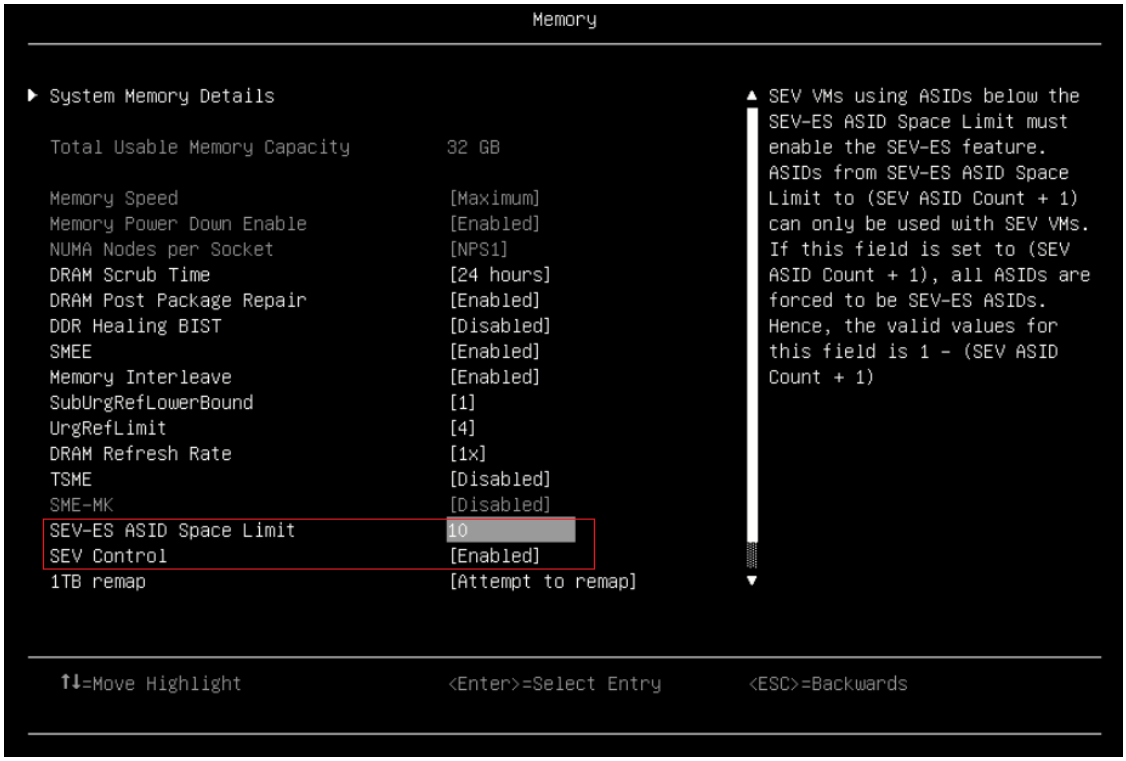

Figure 4. Enable SEV and configure SEV-ES ASID Space Limit via UEFI Settings on SR665 V3

4. Press F4 to Save & Exit.
5. Reboot host to make configuration take effect.

Configure AMD SEV-ES using Redfish REST API

Redfish is a next-generation systems management interface standard, which enables scalable, secure, and open server management. It is a new interface that uses RESTful interface semantics to access data that is defined in model format to perform out-of-band systems management. We can use Redfish REST API to configure AMD SEV-ES on Lenovo ThinkSystem servers.

Lenovo provides some Python and PowerShell sample scripts to use Redfish. These are available as open source code on Lenovo's Github page, https://github.com/lenovo/.

- Lenovo Python Redfish Scripts: https://github.com/lenovo/python-redfish-lenovo
- Lenovo PowerShell Redfish Scripts: https://github.com/lenovo/powershell-redfish-lenovo

Since Redfish is a REST API, standard REST clients can be used to interact with the service. Postman is an easy-to-use HTTP REST client tool. The tool is available from https://www.getpostman.com/.

The following steps describe the process to configure AMD SEV-ES via Redfish REST API with Postman tool on ThinkSystem servers with AMD EPYC processors:

1. Use the GET method to retrieve properties in BIOS resource for Redfish service with Postman as shown in the following figure.

   ```
   https://<BMC_IPADDR>/redfish/v1/Systems/1/Bios
   ```

   The following figure shows the result on the SR655 V3:

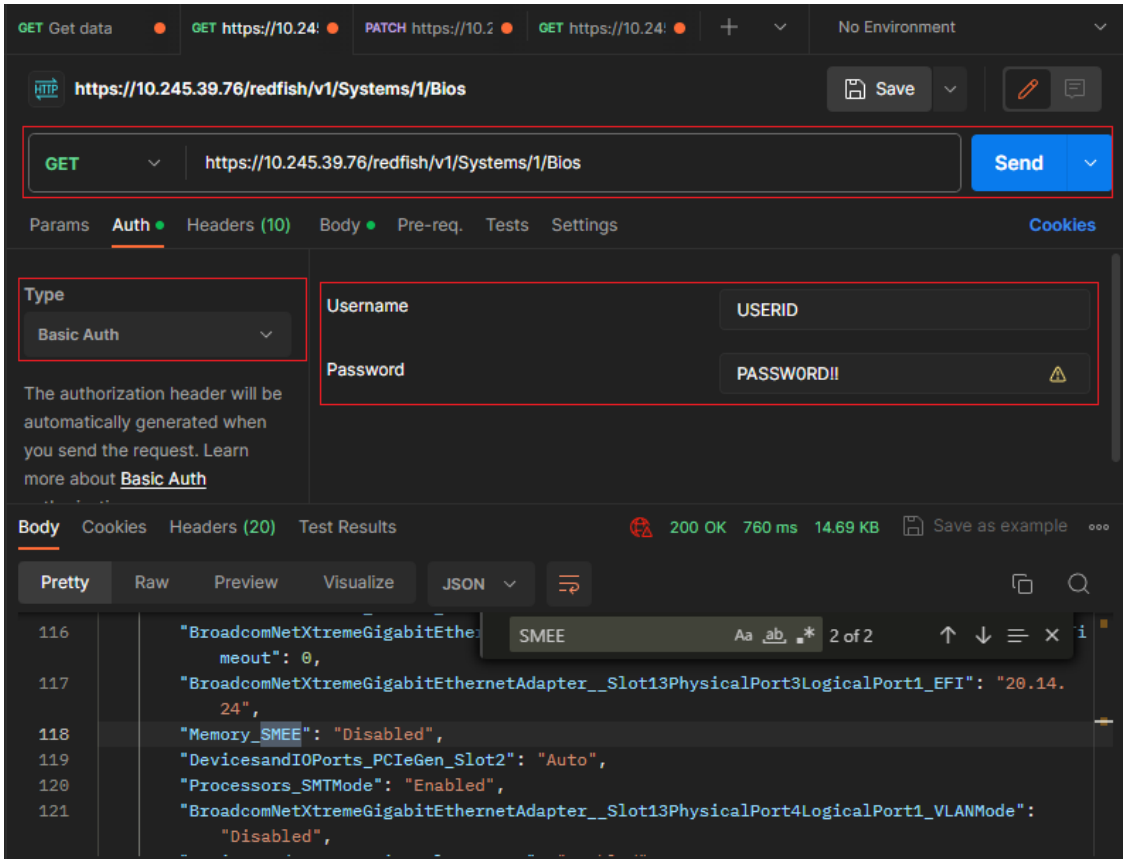

Figure 5. Get BIOS properties via Redfish on SR655 V3

2. Use the PATCH method to update AMD SEV-ES properties in BIOS resource for Redfish service with Postman as shown in the following figure.

```
https://<BMC_IPADDR>/redfish/v1/Systems/1/Bios/Pending
```

The following figure shows the result on the SR655 V3:

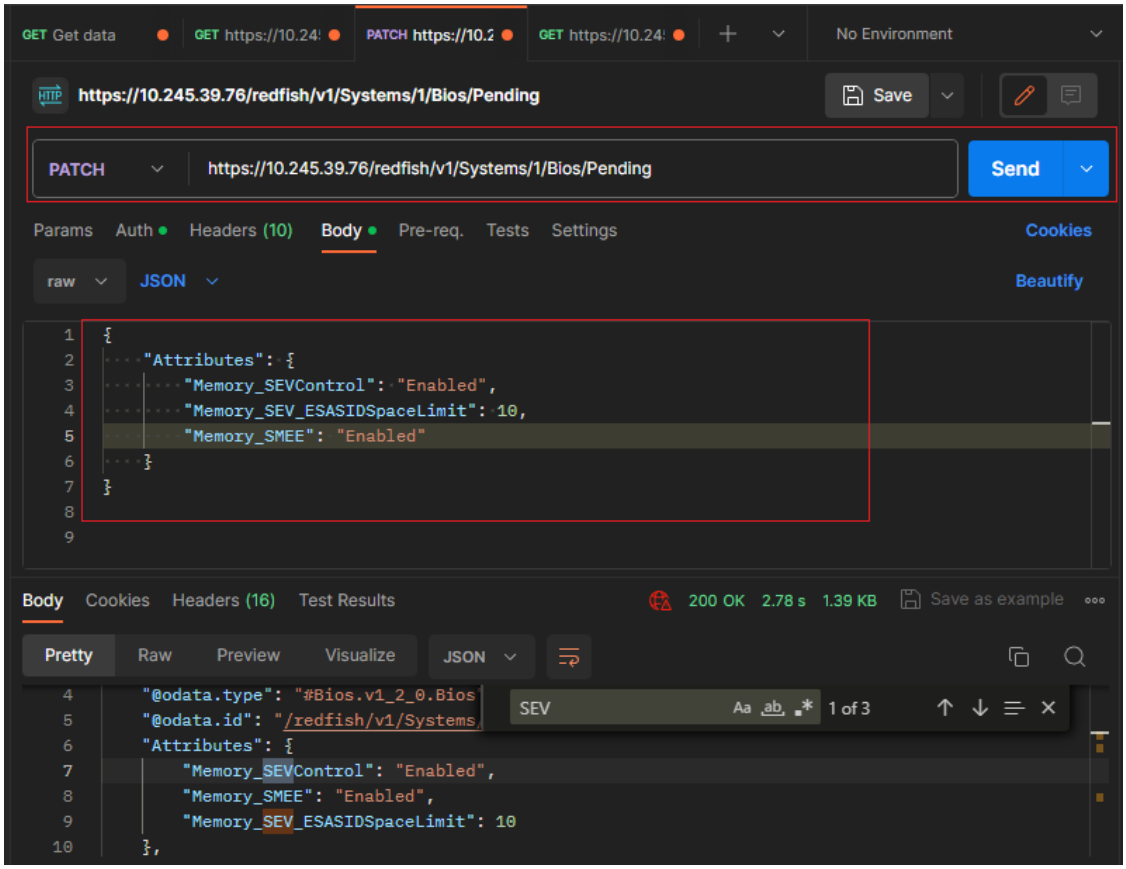

Figure 6. Configure AMD SEV-ES via Redfish on SR655 V3

3. Reboot host to make SEV-ES configuration take effect.

Configure AMD SEV-ES using OneCLI

Lenovo XClarity Essentials OneCLI is a collection of several command-line applications, which can be used to configure the server, collect service data for the server, update firmware and device drivers, and perform power-management functions on the server. We can use OneCLI to configure AMD SEV-ES on Lenovo ThinkSystem servers.

OneCLI can be downloaded from the following page on the the Lenovo support site:
https://datacentersupport.lenovo.com/us/en/solutions/ht116433

The following steps describe the process to configure AMD SEV-ES via OneCLI on ThinkSystem servers with AMD EPYC processors:

Tip: The commands for ThinkSystem SR635 and SR655 are different to the other AMD-based servers.

1. Run the following OneCLI command to check the status of SME as shown in the following figure:

```
onecli config show Memory.SMEE --imm <USERID>:<PASSWORD>@<IP>
```

```
D:\OneCLI4>onecli config show Memory.SMEE --imm USERID:PASSW0RD!!@10.245.39.76

Lenovo XClarity Essentials OneCLI lxce_onecli02d-4.0.0
(C) Lenovo 2013-2022 All Rights Reserved

OneCLI License Agreement and OneCLI Legal Information can be found at the following location:
    "D:\OneCLI4\Lic"

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

Start to connect BMC at 10.245.39.76 to apply config show
Invoking SHOW command ...
Connected to BMC at IP address 10.245.39.76 by REDFISH
Memory.SMEE=Disabled
Succeed.
```

Figure 7. Check SME via OneCLI command on SR655 V3

2. Run the following OneCLI command to enable the SMEE as shown in the following figure:

```
onecli config set Memory.SMEE Enabled --imm <USERID>:<PASSWORD>@<IP>
```

```
D:\OneCLI4>onecli config set Memory.SMEE Enabled --imm USERID:PASSW0RD!!@10.245.39.76

Lenovo XClarity Essentials OneCLI lxce_onecli02d-4.0.0
(C) Lenovo 2013-2022 All Rights Reserved

OneCLI License Agreement and OneCLI Legal Information can be found at the following location:
    "D:\OneCLI4\Lic"

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

Start to connect BMC at 10.245.39.76 to apply config set
Invoking SET command ...
Connected to BMC at IP address 10.245.39.76 by REDFISH
memory.smee=Enabled
Changes completed successfully, but these changes will not take effect until next restart the system.
Succeed.
```

Figure 8. Enable SMEE via OneCLI command on SR655 V3

3. Reboot host to make SMEE configuration take effect.
4. Run the following OneCLI command to check the SEV Control as shown in the following figure:

```
onecli config show Memory.SEVControl --imm <USERID>:<PASSWORD>@<IP>
```

```
D:\OneCLI4>onecli config show Memory.SEVControl --imm USERID:PASSW0RD!!@10.245.39.76

Lenovo XClarity Essentials OneCLI lxce_onecli02d-4.0.0
(C) Lenovo 2013-2022 All Rights Reserved

OneCLI License Agreement and OneCLI Legal Information can be found at the following location:
    "D:\OneCLI4\Lic"

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

Start to connect BMC at 10.245.39.76 to apply config show
Invoking SHOW command ...
Connected to BMC at IP address 10.245.39.76 by REDFISH
Memory.SEVControl=Disabled
Succeed.
```

Figure 9. Check SEV Control via OneCLI command on SR655 V3

5. Run the following OneCLI command to enable the SEV Control as shown in the following figure:

```
onecli config set Memory.SEVControl Enabled --imm <USERID>:<PASSWORD>@<IP>
```

```
D:\OneCLI4>onecli config set Memory.SEVControl Enabled --imm USERID:PASSW0RD!!@10.245.39.76

Lenovo XClarity Essentials OneCLI lxce_onecli02d-4.0.0
(C) Lenovo 2013-2022 All Rights Reserved

OneCLI License Agreement and OneCLI Legal Information can be found at the following location:
    "D:\OneCLI4\Lic"

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

Start to connect BMC at 10.245.39.76 to apply config set
Invoking SET command ...
Connected to BMC at IP address 10.245.39.76 by REDFISH
memory.sevcontrol=Enabled
Changes completed successfully, but these changes will not take effect until next restart the system.
Succeed.
```

Figure 10. Enable SEV Control via OneCLI command on SR655 V3

6. Reboot host to make SEV Control configuration take effect.
7. Run the following OneCLI command to check the SEV-ES ASID Space Limit as shown in the following figure:

```
onecli config show Memory.SEV-ESASIDSpaceLimit -imm <USERID>:<PASSWORD>@<IP>
```

```
D:\OneCLI4>onecli config show Memory.SEV-ESASIDSpaceLimit --imm USERID:PASSW0RD!!@10.245.39.27

Lenovo XClarity Essentials OneCLI lxce_onecli02d-4.0.0
(C) Lenovo 2013-2022 All Rights Reserved

OneCLI License Agreement and OneCLI Legal Information can be found at the following location:
    "D:\OneCLI4\Lic"

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

Start to connect BMC at 10.245.39.27 to apply config show
Invoking SHOW command ...
Connected to BMC at IP address 10.245.39.27 by IPMI
Memory.SEV-ESASIDSpaceLimit=1
Succeed.
```

Figure 11. Check SEV-ES ASID Space Limit via OneCLI command on SR655 V3

8. Run the following OneCLI command to configure the SEV-ES ASID Space Limit as shown in the following figure:

```
onecli config set Memory.SEV-ESASIDSpaceLimit number -imm <USERID>:<PASSWORD>@<
IP>
```

```
D:\OneCLI4>onecli config set Memory.SEV-ESASIDSpaceLimit 10 --imm USERID:PASSW0RD!!@10.245.39.27

Lenovo XClarity Essentials OneCLI lxce_onecli02d-4.0.0
(C) Lenovo 2013-2022 All Rights Reserved

OneCLI License Agreement and OneCLI Legal Information can be found at the following location:
    "D:\OneCLI4\Lic"

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

Start to connect BMC at 10.245.39.27 to apply config set
Invoking SET command ...
Connected to BMC at IP address 10.245.39.27 by IPMI
memory.sev-esasidspacelimit=10
Changes completed successfully, but these changes will not take effect until next restart the system.
Succeed.
```

Figure 12. Configure SEV-ES ASID Space Limit via OneCLI command on SR655 V3

9. Reboot host to make SEV Control configuration take effect.

Enabling SEV-ES in UEFI on the SR635 and SR655

There are three ways to enable Secure Memory Encryption (SME) and SEV-ES in UEFI on the SR635 and SR655:

- Configure AMD SEV-ES in System Setup (SR655 and SR635)
- Configure AMD SEV-ES via Redfish REST API (SR655 and SR635)
- Configure AMD SEV-ES via OneCLI (SR655 and SR635)

Configure AMD SEV-ES in System Setup (SR655 and SR635)

The following steps describe the process to configure SMEE and SEV-ES via System Setup on a ThinkSystem server.

1. In System Setup, navigate to the System Configuration and Boot Management page.
2. Enable SME by going to **System Settings > Memory** and set SMEE to **Enabled** as shown in the following figure.

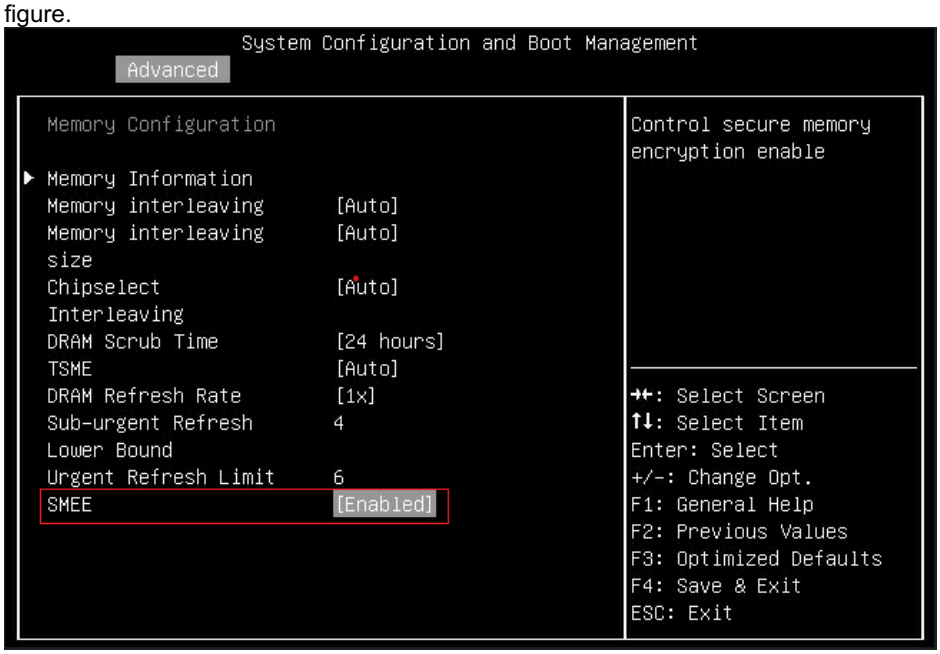

Figure 13. Enable SMEE via UEFI Settings on SR655

3. Enable AMD SEV-ES and configure SEV-ES ASID Space Limit Control via UEFI settings. Select **Advanced > CPU Configuration > AMD SEV-ES**, enable “AMD SEV-ES” and configure “SEV-ES ASID Space Limit” as shown in the following figure:

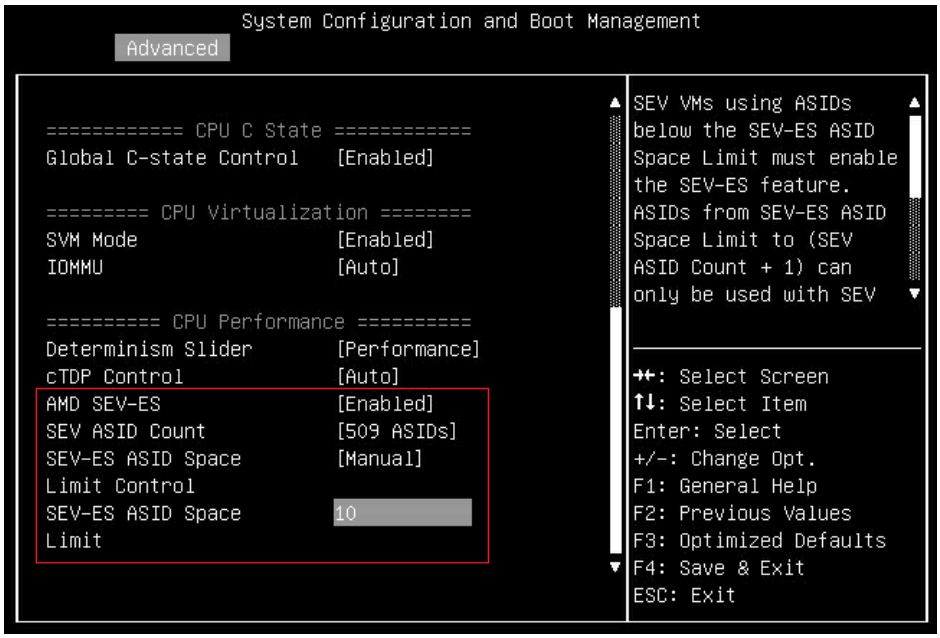

Figure 14. Configure SEV-ES ASID Space Limit via UEFI Settings on SR655

4. Press F4 to Save & Exit.
5. Reboot host to make configuration take effect.

Configure AMD SEV-ES via Redfish REST API (SR655 and SR635)

Redfish is a next-generation systems management interface standard, which enables scalable, secure, and open server management. It is a new interface that uses RESTful interface semantics to access data that is defined in model format to perform out-of-band systems management. We can use Redfish REST API to configure AMD SEV-ES on Lenovo ThinkSystem servers.

Lenovo provides some Python and PowerShell sample scripts to use Redfish. These are available as open source code on Lenovo's Github page, https://github.com/lenovo/.

- Lenovo Python Redfish Scripts: https://github.com/lenovo/python-redfish-lenovo
- Lenovo PowerShell Redfish Scripts: https://github.com/lenovo/powershell-redfish-lenovo

Since Redfish is a REST API, standard REST clients can be used to interact with the service. Postman is an easy-to-use HTTP REST client tool. The tool is available from https://www.getpostman.com/.

The following steps describe the process to configure AMD SEV-ES via Redfish REST API with Postman tool on ThinkSystem servers with AMD EPYC processors:

1. Use the GET method to retrieve properties in BIOS resource for Redfish service with Postman as shown in the following figure.

   ```
   https://<BMC_IPADDR>/redfish/v1/Systems/Self/Bios
   ```

   The following figure shows the result on the SR655:

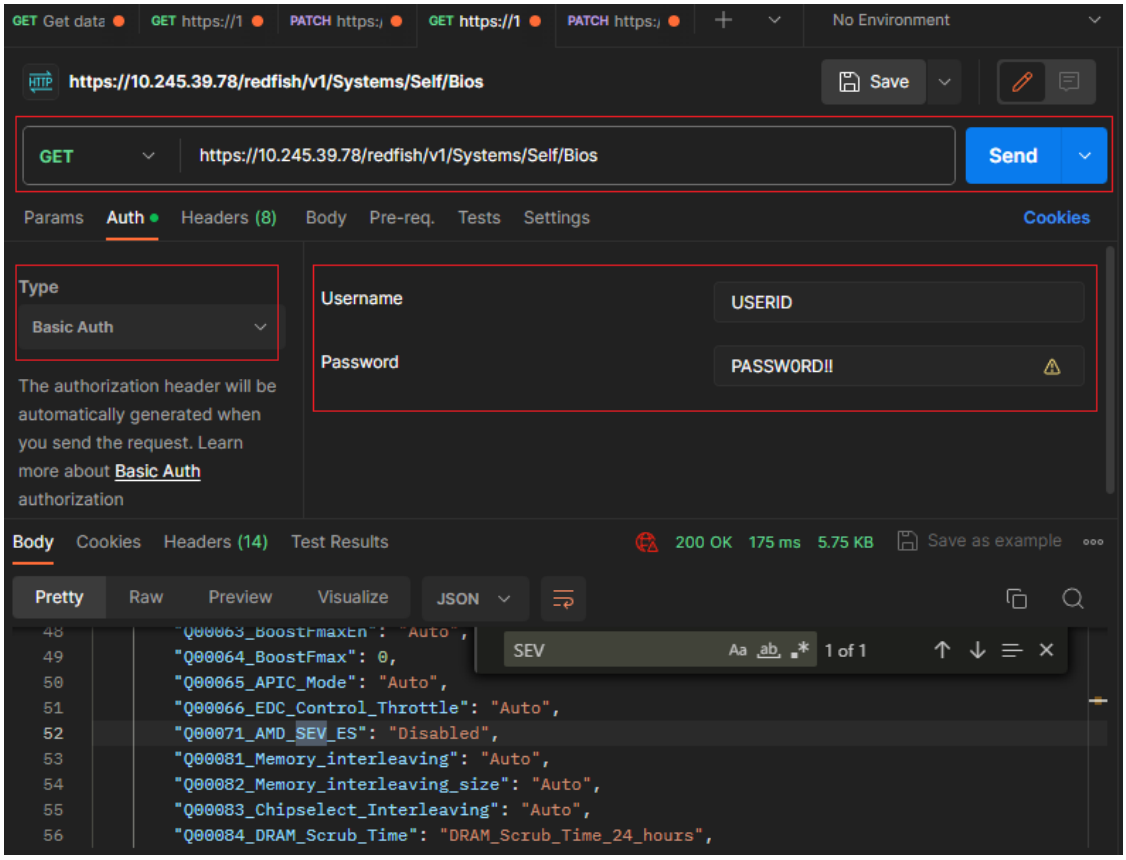

Figure 15. Get BIOS properties via Redfish on SR655

2. Use the PATCH method to update AMD SEV-ES properties in BIOS resource for Redfish service with Postman as shown in the following figure.

```
https://<BMC_IPADDR>/redfish/v1/Systems/Self/Bios/SD
```

The following figure shows the result on the SR655:

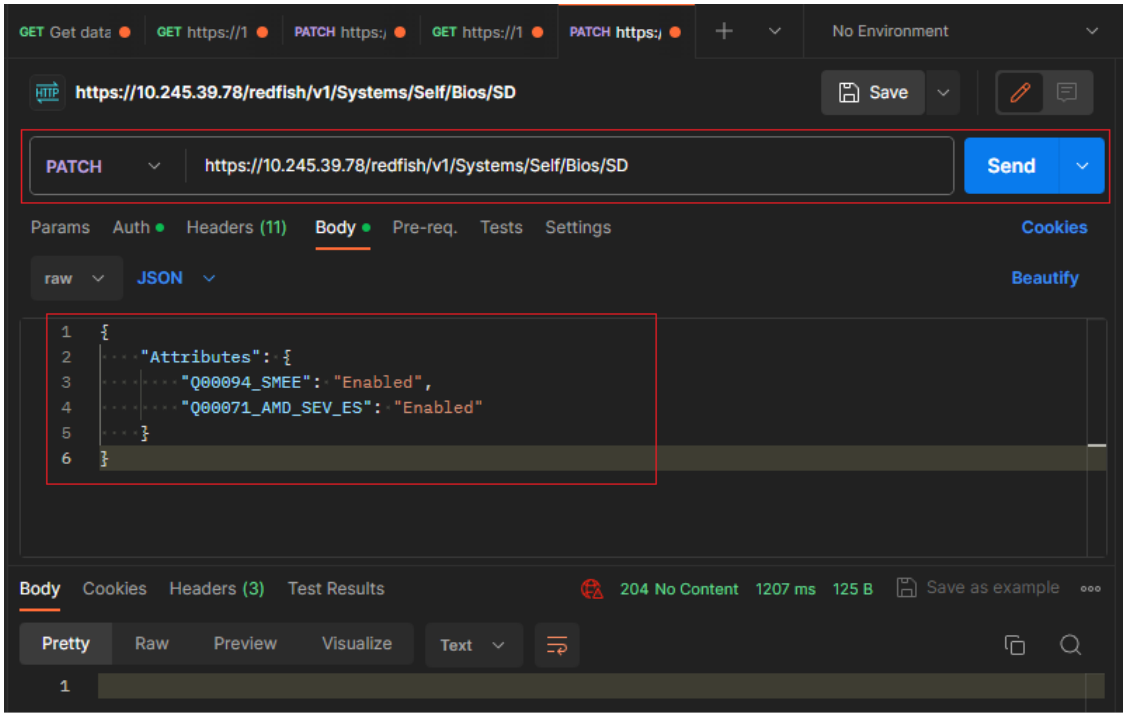

Figure 16. Configure AMD SEV-ES via Redfish on SR655

3. Reboot host to make SEV-ES configuration take effect.

Note: There are no Redfish method to check or configure the SEV-ES ASID Space Limit on the SR635 and SR655. You will need to use System Setup to perform these steps, as described in the Configure AMD SEV-ES in System Setup (SR655 and SR635) section.

Configure AMD SEV-ES via OneCLI (SR655 and SR635)

Lenovo XClarity Essentials OneCLI is a collection of several command-line applications, which can be used to configure the server, collect service data for the server, update firmware and device drivers, and perform power-management functions on the server. We can use OneCLI to configure AMD SEV-ES on Lenovo ThinkSystem servers.

OneCLI can be downloaded from the following page on the the Lenovo support site:
https://datacentersupport.lenovo.com/us/en/solutions/ht116433

The following steps describe the process to configure AMD SEV-ES via OneCLI on ThinkSystem servers with AMD EPYC processors:

Tip: The commands for ThinkSystem SR635 and SR655 are different to the other AMD-based servers.

1. Run the following OneCLI command to check the status of SME as shown in the following figure:

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

```
D:\OneCLI4>onecli config show Bios.Q00094_SMEE --bmc USERID:PASSW0RD!!@10.245.39.78

Lenovo XClarity Essentials OneCLI lxce_onecli02d-4.0.0
(C) Lenovo 2013-2022 All Rights Reserved

OneCLI License Agreement and OneCLI Legal Information can be found at the following location:
    "D:\OneCLI4\Lic"

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

Start to connect BMC at 10.245.39.78 to apply config show
Invoking SHOW command ...
Bios.Q00094_SMEE=Disabled
Succeed.
```

Figure 17. Check SME via OneCLI command on SR655

2. Run the following OneCLI command to enable the SMEE as shown in the following figure:

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

```
D:\OneCLI4>onecli config set Bios.Q00094_SMEE Enabled --bmc USERID:PASSW0RD!!@10.245.39.78

Lenovo XClarity Essentials OneCLI lxce_onecli02d-4.0.0
(C) Lenovo 2013-2022 All Rights Reserved

OneCLI License Agreement and OneCLI Legal Information can be found at the following location:
    "D:\OneCLI4\Lic"

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

Start to connect BMC at 10.245.39.78 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.
```

Figure 18. Enable SMEE via OneCLI command on SR655

3. Reboot host to make SMEE configuration take effect.
4. Run the following OneCLI command to check the SEV Control as shown in the following figure:

```
onecli config show Bios.Q00071_AMD_SEV_ES --bmc <USERID>:<PASSWORD>@<IP>
```

```
D:\OneCLI4>onecli config show Bios.Q00071_AMD_SEV_ES  --bmc USERID:PASSW0RD!!@10.245.39.78

Lenovo XClarity Essentials OneCLI lxce_onecli02d-4.0.0
(C) Lenovo 2013-2022 All Rights Reserved

OneCLI License Agreement and OneCLI Legal Information can be found at the following location:
    "D:\OneCLI4\Lic"

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

Start to connect BMC at 10.245.39.78 to apply config show
Invoking SHOW command ...
Bios.Q00071_AMD_SEV_ES=Disabled
Succeed.
```

Figure 19. Check SEV Control via OneCLI command on SR655

5. Run the following OneCLI command to enable the SEV Control as shown in the following figure:

```
onecli config set Q00071_AMD_SEV_ES Enabled --bmc <USERID>:<PASSWORD>@<IP>
```

```
D:\OneCLI4>onecli config set Bios.Q00071_AMD_SEV_ES Enabled --bmc USERID:PASSW0RD!!@10.245.39.78

Lenovo XClarity Essentials OneCLI lxce_onecli02d-4.0.0
(C) Lenovo 2013-2022 All Rights Reserved

OneCLI License Agreement and OneCLI Legal Information can be found at the following location:
    "D:\OneCLI4\Lic"

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

Start to connect BMC at 10.245.39.78 to apply config set
Invoking SET command ...
Bios.Q00071_AMD_SEV_ES=Enabled
Changes completed successfully, but these changes will not take effect until next reboot.
Succeed.
```

Figure 20. Enable SEV Control via OneCLI command on SR655

6. Reboot host to make SEV Control configuration take effect.

Note: There are no OneCLI commands to check or configure the SEV-ES ASID Space Limit on the SR635 and SR655. You will need to use System Setup to perform these steps, as described in the Configure AMD SEV-ES in System Setup (SR655 and SR635) section.

Configuring AMD SEV-ES in vSphere

The following steps describe the process to configure and use AMD SEV-ES in VMware vSphere. In our lab, we used vSphere 7.0 U3 and a RHEL 8.5 virtual machine on a ThinkSystem SR635 server.

1. Install VMware vSphere 7.0 U3 on the server.
2. Connect to vCenter Server by using the vSphere Client.
3. Create a virtual machine and install a guest OS (e.g., RHEL 8.5) that supports AMD SEV-ES.
4. 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 Firmware is set to **EFI**, and Secure Boot is deselected, as highlighted in the figure below.

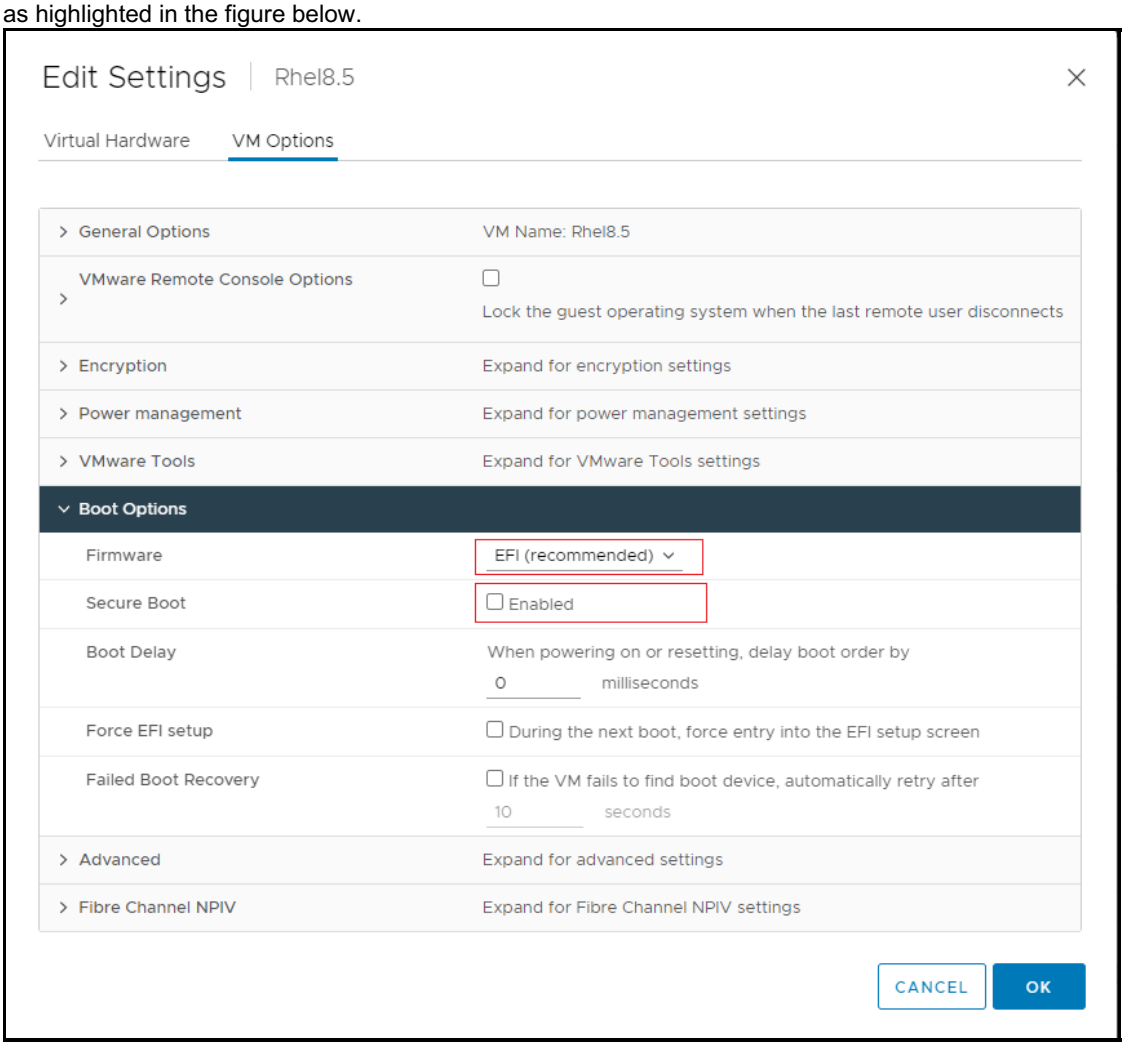

Figure 21. Configure Boot Options on vSphere client

   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 the figure below.

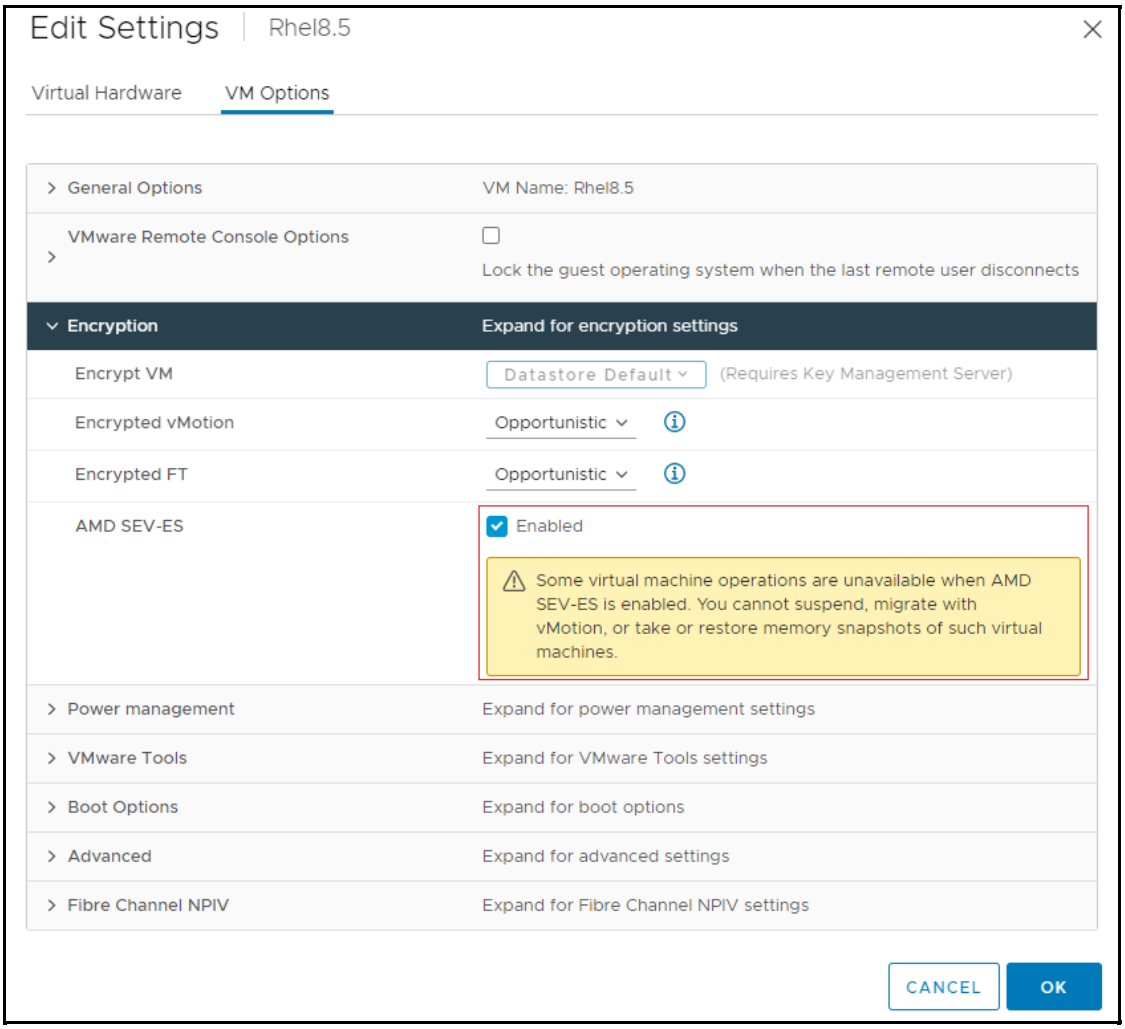

Figure 22. Enable AMD SEV-ES on vSphere client

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

a. Download and installed PowerCLI from the PowerCLI home page: https://developer.vmware.com/web/tool/vmware-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 the figure below.

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

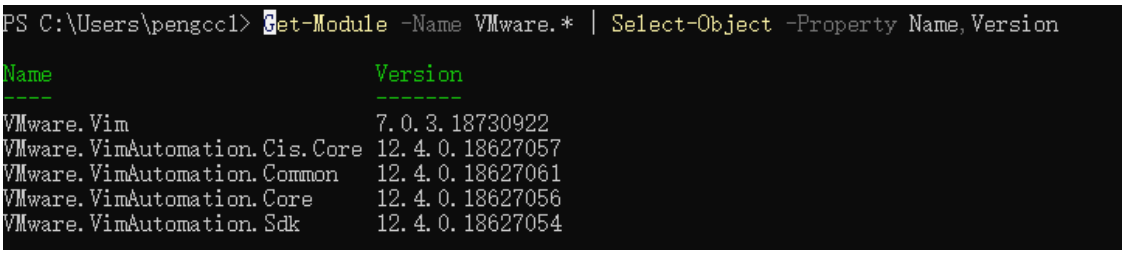

Figure 23. Check VMware Power CLI modules

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

```
Set-ExecutionPolicy RemoteSigned
```

Figure 24. Set execution policy

d. In PowerCLI console, run the following Connect-VIServer cmdlet as an administrator to the vCenter server, as shown in the figure below.

```
Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Passw
ord 'password'
```

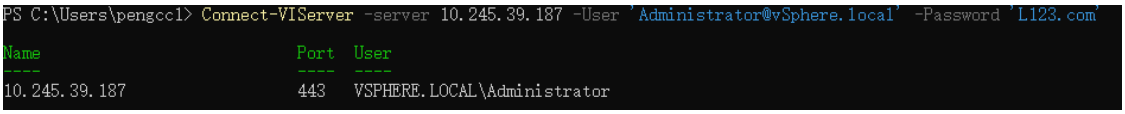

Figure 25. Connect to vCenter server

e. Add SEV-ES to the virtual machine with the following Set-VM cmdlet, as shown in the figure below.

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

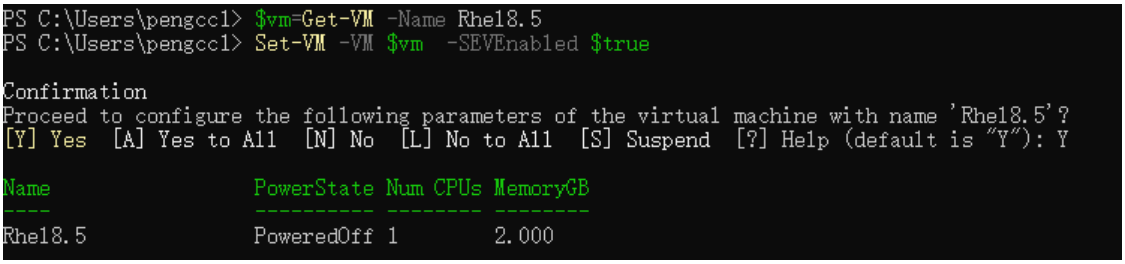

Figure 26. Enable SEV-ES via PowerCLI

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

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

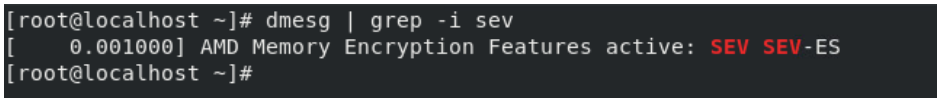

Figure 27. Check SEV-ES in RHEL 8.5

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 in 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

Related product families

Product families related to this document are the following:

- Processors
- VMware vSphere

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, LP1545, was created or updated on January 5, 2024.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/LP1545
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/LP1545.

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:

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

PowerShell is a trademark 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.