SUSE

SUSE Linux Enterprise Server 15 SP3

AMD 安全加密虚拟化 (AMD-SEV) 指南

AMD 的安全加密虚拟化 (SEV) 可让您加密虚拟机的内存。这是 Linux 内置的基于内核的虚拟机 (KVM) 超级管理程序的新功能。其目的是为了提高系统安全性，尤其在使用永久性内存的情况下。

本文旨在提供 SEV 的工作原理以及如何启用和配置 SEV 的基本知识。文中还涉及了与非加密虚拟化相比使用 SEV 的一些限制。

出版日期：2024 年 9 月 29 日

目录

1 SEV 简介

对磁盘上储存的计算机数据进行加密这项功能已得到广泛部署，但 RAM 中储存的数据并未加密。这可能会导致这些数据暴露给通过软件或硬件嗅探入侵主机系统的攻击者。新的永久性内存技术让此问题变得更加严重：用户可从系统上取下 NVDIMM（非易失性内存模块）实体且其上的数据将保持不变，就像硬盘或 SSD 上的数据一样。如果未加密，储存的任何信息（如敏感数据、口令或机密密钥）都可能轻易泄露。

AMD 的 SEV（安全加密虚拟化）技术通过独有的密钥以透明方式加密每个 VM 的内存，可以保护 Linux KVM 虚拟机。SEV 还可计算出内存内容的签名，该签名可发送给 VM 的所有者，作为固件已正确加密内存的证明。SEV 特别适用于云计算环境，在此环境中，VM 托管在远程服务器上，并不在 VM 所有者的控制之下。这样可减少需要置于超级管理程序及其主机系统管理员控制之下的可信 VM 的数量。

在 SUSE Linux Enterprise 12 SP4 及以上版本和即将推出的 SUSE Linux Enterprise 15 维护版本中，内核、QEMU 和 `libvirt` 支持使用 SEV 创建和管理 VM。

2 VM 主机要求

VM 主机硬件必须支持 AMD 的 SEV 技术。要检测主机硬件是否支持 SEV，请检查 `sev` 属性是否包含在 `libvirt` 的功能中，并且其值是否设置恰当：

```
<domainCapabilities>
   ...
   <features>
   ...
   <sev supported='yes'/>
   ...
   </sev>
   </features>
</domainCapabilities>
```

此外，请确保 `kvm_amd` 内核模块已启用 `sev` 参数：

```
/sys/module/kvm_amd/parameters/sev = 1
```

3 VM 要求

VM 必须为新型 `Q35` 计算机类型且必须使用 UEFI 固件。

注意：Q35 中无 IDE 支持

Q35 计算机类型没有 IDE 控制器，不支持 IDE 磁盘。

所有 `virtio` 设备都需要配置 `iommu='on'` 属性（在其 `<driver>` 配置中）。此外，必须锁定对 VM 使用的所有内存区域的直接内存访问 (DMA)，以防发生交换。

4 VM 配置

例 1： 示例配置文件

例如，配置了 4 GB 内存的 SEV 加密 VM 将包含以下 XML 配置：

```
<domain type='kvm'>
    <memory unit='KiB'>4194304</memory>
    <currentMemory unit='KiB'>4194304</currentMemory>
    <memoryBacking>
    <locked/>
    </memoryBacking>
    <os>
    <type arch='x86_64' machine='pc-q35-2.11'>hvm</type>
    <loader readonly='yes' type='pflash'>/usr/share/qemu/ovmf-x86_64-ms-4m-
code.bin</loader>
    <nvram>/var/lib/libvirt/qemu/nvram/sles15-sev-guest_VARS.fd</nvram>
    <boot dev='hd'/>
    </os>
    <launchSecurity ❶ type='sev'>
    <cbitpos>47</cbitpos> ❷
    <reducedPhysBits>1</reducedPhysBits> ❸
    <policy>0x0033</policy> ❹
    </launchSecurity>
    <devices>
```

```
    <disk type='file' device='disk'>
    <driver iommu='on' name='qemu' type='raw'/>
    <target dev='vda' bus='virtio'/>
    <source file='/vmimages/sev-guest-disk.raw'/>
    </disk>
    <rng model='virtio'>
    <driver iommu='on'/>
    ...
    </rng>
    <memballoon model='virtio'>
    <driver iommu='on' /> ❺
    ...
    </memballoon>
    <video>
    <model type='qxl' ram='65536' vram='65536' vgamem='16384' heads='1'
primary='yes'/>
    </video>
    ...
    </devices>
    ...
    </domain>
```

❶ 元素 `launchSecurity type='sev'` ，其内容启用了 VM 内存内容加密。

❷ 启用内存加密后，如果某个内存页受保护，会使用其中一个物理地址位（也称为 C 位）进行标记。必需的 `cbitpos` 元素，提供 Guest 页表项中 C 位的位置。例如，值 `47` 表示页表项中的第 47 位将决定该页是否加密。C 位数字从主机的 CPUID 读取，因此与硬件相关。元素 `cbitpos` 的值与超级管理程序相关，可从域功能中的 `sev` 元素获取。

❸ 启用内存加密后，我们会丢失物理地址空间的某些位。必需的 `reducedPhysBits` 元素提供此物理地址位缩减。与 `cbitpos` 类似， `reducedPhysBits` 的值与处理器系列相关，可从域功能中的 `sev` 元素获取。

❹ 必需的 `policy` 元素提供必须由 SEV 固件维护的 Guest 策略。此策略由固件强制实施，用于限制在 VM 上可由超级管理程序执行的配置和操作命令。启动 VM 时提供的 Guest 策略与该 VM 绑定在一起，且在其整个生命周期都无法更改。

> ❺ 除了 `launchSecurity` 设置外，SEV 加密的 VM 还必须设置 `iommu='on'` 属性（在每个 `virtio` 设备中）。需要指定此属性才能为 QEMU 内的设备启用 DMA API。

Guest 策略是定义如下的 4 个无符号字节：

表 1： GUEST 策略定义

位	定义
0	如果设置，则不允许调试 Guest
1	如果设置，则不允许与其他 Guest 共享密钥
2	如果设置，则需要 SEV-ES
3	如果设置，则不允许将 Guest 发送到其他平台
4	如果设置，则不得将 Guest 传送到不属于该域的其他平台
5	如果设置，则不得将 Guest 传送到不支持 SEV 的其他平台
6-15	保留
16-32	不得将 Guest 传送到固件版本更低的其他平台

可选 `dhCert` 元素提供 Guest 所有者的 base64 编码 Diffie-Hellman (DH) 密钥。该密钥用于在 SEV 固件与 Guest 所有者之间协商主机密密钥。此主机密密钥之后会用于在 SEV 固件与 Guest 所有者之间建立可信通道。

可选 `session` 元素提供 Guest 所有者的 base64 编码会话 Blob，如 SEV API 规范中定义。请参见 SEV 规范中针对会话 Blob 格式的 LAUNCH_START 部分。

SEV 加密的 VM 还必须锁定其所有内存区域，以允许 DMA 并防止发生交换。必须使用 `memoryBacking` 的 `locked` 子元素指定内存的显式锁定。可通过将虚拟机配置为使用 大页 来避免进行显式内存锁定。有关在 VM 中使用大页的详细信息，请参见虚拟化最佳实践《虚拟化最佳实践》文章, 第 4.1.1 节 “将 VM 主机服务器和 VM Guest 配置为使用大页”。

如果产生的开销与非 SEV VM 所需并无不同，那么固定内存时设置正确的硬限制就重要得多。如果限制过低，VM 将被终止。

5 当前限制

- 在 SEV 加密的 VM 内运行的 Guest 操作系统必须包含 SEV 支持。目前 SUSE Linux Enterprise Server 12 SP4、SUSE Linux Enterprise Server 15 和 SUSE Linux Enterprise Server 15 SP1 都提供此支持。
- 当前不支持涉及保存及恢复实例的内存和状态的任何操作。这表示 SEV 加密的 VM 无法从快照恢复，并且无法进行实时迁移。加密的 VM 可照常在其他主机上关闭和重启动。
- SEV 加密的 VM 无法包含可直接访问的主机设备（即 PCI 直通）。

未来，当硬件、固件和各层软件具有新的功能时，将会去除这些限制。

6 更多信息

- https://developer.amd.com/sev — AMD-SEV 登录页
- https://developer.amd.com/wp-content/resources/55766.PDF — AMD SEV-KM API 规范 (PDF)
- https://github.com/AMDESE/AMDSEV/ — 包含示例和工具的 AMD SEV GitHub 储存库
- https://libvirt.org/formatdomain.html#sev — libvirt SEV 配置设置

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named sub-unit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or non-commercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- **A.** Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- **B.** List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- **C.** State on the Title page the name of the publisher of the Modified Version, as the publisher.
- **D.** Preserve all the copyright notices of the Document.
- **E.** Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- **F.** Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- **G.** Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- **H.** Include an unaltered copy of this License.
- **I.** Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- **J.** Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- **K.** For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- **L.** Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- **M.** Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- **N.** Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- **O.** Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/↗.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled “GNU
Free Documentation License”.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with...Texts.” line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.