

SUSE Linux Enterprise Server 15 SP6

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。SEV with Encrypted State (SEV-ES) 更进一步，能够加密虚拟机的 CPU 寄存器内容。这些技术提高了系统安全性，非常适合云计算等多租户环境。它们可以防范各种跨 VM 和基于超级管理程序的攻击。举例来说，某个恶意 VM 即使避开了超级管理程序强制实施的限制，能够读取任意内存，它仍无法从 SEV 或 SEV-ES VM 窃取敏感数据。

本文旨在提供有关 SEV 和 SEV-ES 的工作原理以及如何启用和配置这些功能的基本知识。文中还涉及了与非加密虚拟化相比使用 SEV 和 SEV-ES 的某些限制。

出版日期：2024 年 12 月 12 日

目录

- 1 SEV 简介 3
- 2 VM 主机要求 3
- 3 VM 要求 4
- 4 VM 配置 4
- 5 VM 安装 7

6	VM 证明	7
7	SEV 与 KubeVirt	9
8	当前限制	10
9	更多信息	11
10	法律声明	11
11	GNU Free Documentation License	11

1 SEV 简介

对磁盘上存储的计算机数据进行加密这项功能已得到广泛部署，但 RAM 中存储的数据并未加密。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，在有許多租户共享物理资源的云计算环境中更是如此。想象一下某个恶意租户的虚拟机利用超级管理程序 Bug 逃离了沙箱并在内存中搜索敏感数据的情景。

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。SEV 可以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。

当虚拟机正在处理敏感数据时，它可以存在于 CPU 寄存器以及内存中。如果处理出于某种原因（例如需要提供中断或与其他进程共享时间）而停止，虚拟机的 CPU 寄存器内容将会保存到超级管理程序内存中。超级管理程序可以读取此内存，即使启用了 SEV 也是如此。SEV-ES 可以防范这种情况，它会在虚拟机的处理停止时对所有 CPU 寄存器内容进行加密。SEV-ES 在 SEV 的基础上构建而成，能够为在多租户环境中运行的虚拟机缩小受攻击面。

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 `libvirt` 的功能中是否包含 `sev` 属性，并且该属性的值是否设置恰当：

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

此外，请确保已为 `kvm_amd` 内核模块启用 `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。可以让 `libvirt` 自动选择启用了 SEV 或 SEV-ES 的适当 UEFI 固件，也可以手动指定。目前，唯一受支持的固件为 `/usr/share/qemu/ovmf-x86_64-code.bin` 和 `/usr/share/qemu/ovmf-x86_64-4m-code.bin`。有关如何使用 UEFI 固件以及自动选择功能的更多细节，请参见《虚拟化指南》，第 10 章“Guest 安装”，第 10.3.1 节“高级 UEFI 配置”。



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-net` 设备都需要配置为禁用 iPXE 选项 ROM。iPXE 目前与 SEV 和 SEV-ES 不兼容。必须锁定对 VM 所用全部内存区域的直接内存访问 (DMA)，以防发生交换。其中包括 VM 的内存以及 QEMU 为支持 VM 运行而分配的任何内存区域，例如作为固件和变量存储区的 UEFI pflash、视频 RAM 等。

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/> ①
  </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 ❷ type='sev'>
<cbitmappos>47</cbitmappos> ❸
<reducedPhysBits>1</reducedPhysBits> ❹
<policy>0x0033</policy> ❺
<dhCert>AAAABBBB=CCCCDDDD</dhCert> ❻
<session>AAAABBBB=EEEEFFFFFF</session> ❼
</launchSecurity>
<devices>
<interface type='bridge'>
<source bridge='br0' />
<model type='virtio' />
<rom enabled='no' /> ❽
</interface>
...
</devices>
...
</domain>

```

- ❶ 使用 `memoryBacking` 元素及其子元素 `locking` 来放宽 `libvirt` 对 VM 的 `cgroup` 施加的内存限制。如果不这样做，当 QEMU 尝试锁定 VM 的内存区域以及用于支持 VM 操作的其他区域时，VM 创建将会失败。如需详细了解 SEV VM 的 VM 内存配置要求，请访问 https://libvirt.org/kbase/launch_security_sev.html#memory。
- ❷ `launchSecurity type='sev'` 元素及其内容用于启用 VM 内存内容加密。
- ❸ 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。必要元素 `cbitmappos` 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。`cbitmappos` 的值与超级管理程序相关，可从域功能中的 `sev` 元素获取。

- ④ 启用内存加密后，我们会丢失物理地址空间的某些位。必要元素 `reducedPhysBits` 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。
- ⑤ 必要元素 `policy` 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。
- ⑥ 可选元素 `dhCert` 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。
- ⑦ 可选元素 `session` 提供 Guest 所有者的 base64 编码会话 Blob（如 SEV API 规范中所定义）。请参见 SEV 规范中针对会话 Blob 格式的 LAUNCH_START 部分。
- ⑧ 除了 `launchSecurity` 设置以外，SEV 加密的 VM 的所有 virtio-net 设备上都必须禁用 iPXE 选项 ROM。目前，iPXE 与 SEV 加密的 VM 不兼容。

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

5 VM 安装

`virt-install` 支持安装 SEV 和 SEV-ES 虚拟机。除了标准安装参数以外，还需要为 `virt-install` 提供用于满足 VM 要求的选项以及 `--launchSecurity` 选项。

下面的示例会启动通过 SEV-ES 提供保护的 SLES 15 SP4 虚拟机的网络安装。

```
virt-install --name sles15sp4-sev-es --location
http://192.168.0.1/install/sles15sp4/x86_64 --disk size=20 --
network=bridge=br0,model=virtio,rom.bar=off ❶ --vcpus 4 --memory 4096
--noautoconsole --events on_reboot=destroy --machine q35 --memptune
hard_limit=4563402 --launchSecurity sev,policy=0x07 ❷ --boot firmware=efi ❸
--vnc --serial pty
```

- ❶ iPXE 选项 ROM 与 SEV 加密的 VM 不兼容，必须在所有 virtio-net 设备上将其禁用。libvirt 支持使用 rom 元素的 enabled 或 bar 属性禁用选项 ROM，而 virt-install 仅支持使用 bar 属性来禁用选项 ROM。
- ❷ launchSecurity 选项指定 SEV 固件要强制实施的类型和策略。策略设置详见表 1 “Guest 策略定义”。
- ❸ boot 选项可用于指定许多与引导相关的设置，包括虚拟机使用的固件。指定 efi 固件类型表示允许 libvirt 的固件自动选择功能为虚拟机选择支持 SEV 的适当固件。

6 VM 证明

VM 证明是校验可信软件组件是否在可信计算平台上正确实例化的过程。该过程通常涉及启动处于暂停状态的 VM，检索已实例化软件组件的启动度量，校验该度量，然后提供磁盘口令或其他密钥来解锁 VM 并恢复已暂停的引导过程。启动度量包括 VM 所有者提供的加密项目，其中的加密信任根是 AMD SEV 平台。启动度量经过校验后，VM 所有者就可以确认其软件组件未受到侵害并在可信平台上运行。

整个证明过程相当复杂，并且很可能会发生错误。必须小心确保该过程本身是安全的。例如，安全证明过程不能直接在运行 VM 的超级管理程序上执行，因为其目标是证明超级管理程序不存在恶意行为，并且不会污染 VM。

SLES 15 SP4 中提供了该证明所需的所有信息和 API，而 SLES 15 SP5 则引入了一个名为 **virt-qemu-sev-validate** 的简单实用程序，可用于满足多种证明用例的需要。例如，用于质量保证的自动化测试，以及不受大型商业管理堆栈管理的小规模 libvirt+KVM 部署。

virt-qemu-sev-vailidate 包含在 libvirt-client-qemu 软件包中，支持脱机和联机证明模式。**virt-qemu-sev-validate** 要求以命令行参数的形式为证明提供输入。如果在可信计算机上调用该实用程序，则可以信任 **virt-qemu-sev-validate** 的结果，因为不会从不可信的来源检索任何信息。联机模式不太安全，尤其是直接在运行 VM 的超级管理程序上执行时。

无论采用哪种模式，libvirt+KVM VM 的证明过程首先都会创建 VM 或来宾拥有者 (GO) 证书和会话 Blob，每次启动 VM 时，该证书和会话 Blob 都是唯一的。可以使用 sevctl 软件包中提供的 **sevctl** 实用程序创建该证书和 Blob。以下示例说明如何使用 **sevctl session** 命令创建所有与预启动 SEV 相关的项目。NAME 参数是可选的，用于为项目文件名指定前缀。使用 VM 名称作为前缀可便于稍后将项目与 VM 进行匹配。平台 Diffie-Hellman (DH) 证书的路径和所需的 SEV 策略是必需参数。

```
# sevctl session --name test-sev /data/sev/pdh.cert 7
```

sevctl session 命令会生成四个文件：tick.bin、take.bin、godh.b64 和 session.b64。如果使用可选的 NAME 参数，则文件将以指定的值作为前缀。传输完整性密钥 (tik.bin) 和传输加密密钥 (tek.bin) 用于证明过程的校验阶段。在启动 VM 之前，来宾拥有者 Diffie-Hellman 密钥 (godh.b64) 和会话 Blob (session.b64) 将复制到 VM XML 配置中。有关更多细节，请参见 VM 配置部分中 launchSecurity 元素的 dhCert 和 session 子元素。

创建 VM 会话项目并更新 VM XML 配置后，可以在暂停状态下启动 VM，例如：

```
# virsh -c qemu+ssh://USER_NAME@HOST_NAME/system create --paused /path/to/vm.xml
```

在暂停状态下创建 VM 可以从超级管理程序检索启动度量，并将其与使用可信输入在可信主机上计算的度量进行比较。如果这些度量相同，则 VM 拥有者可以确信 VM 已在超级管理程序上正确实例化，并且可以安全地启动执行。以下命令演示如何使用 **virsh domlaunchsecinfo** 命令从宿主超级管理程序检索已暂停 VM 的启动度量和其他 SEV 相关信息。

```
# virsh -c qemu+ssh://username@hostname/system domlaunchsecinfo sevtest
sev-measurement: VZjxMSlu+UuYkWHN2mAxDVVYXRmL3wqTu84kwk+5QS
+40Mii7hs6cMAMXNpmmys/
sev-api-major : 1
```



```
sev-api-minor : 51
sev-build-id  : 3
sev-policy    : 7
```

然后，可以将检索到的启动度量提供给 **virt-qemu-sev-validate**，以校验 VM 是否已安全实例化。以下示例演示度量的完整脱机证明。

```
# virt-qemu-sev-validate --api-major 1 --api-minor 51 --build-id 3 --policy 7 \
--firmware /usr/share/qemu/ovmf-x86_64-4m.bin --tik sevtest_tik.bin --tek
sevtest_tek.bin --num-cpus 4 \
--cpu-family 25 --cpu-model 1 --cpu-stepping 1 \
--measurement QJ0oDpFmWj+bGZzFoMPbAxTuC6QD44W5w88x/hQM8toVsB75ci7V1YDfYoI9GtK
```

还可以在联机模式下使用 **virt-qemu-sev-validate**，在此模式下，将从宿主超级管理程序检索执行 VM 证明所需的信息。以下示例演示 VM 的联机证明，在此模式下，仅指定了宿主超级管理程序 URI、VM 名称以及关联的 TIK 和 TEK。**virt-qemu-sev-validate** 从宿主超级管理程序检索其余的信息，包括度量本身：

```
# virt-qemu-sev-validate --tik sevtest_tik.bin --tek sevtest_tek.bin \
--connect qemu+ssh://USER_NAME@HOST_NAME/system --domain sevtest
```

校验 VM 启动度量后，VM 所有者可以选择在 VM 中注入机密并继续执行 VM。注入机密的示例是提供一个密钥来解锁已加密的根磁盘。

```
# virsh -c qemu+ssh://USER_NAME@HOST_NAME/system domsetlaunchsecstate sevtest \
--secrethdr hdr-str --secret secret-str
# virsh -c qemu+ssh://USER_NAME@HOST_NAME/system resume sevtest
```

7 SEV 与 KubeVirt

KubeVirt 从版本 0.49.0 开始支持运行 SEV Guest。该功能可通过启用 WorkloadEncryptionSEV 功能门控来激活：

```
> kubectl edit kubevirt kubevirt -n kubevirt
[...]
spec:
  configuration:
    developerConfiguration:
```

```
featureGates:
  - WorkloadEncryptionSEV
[...]
```

要运行 SEV 加密的 Guest，必须在虚拟机规范中的 `launchSecurity` 域元素下包含 `sev: {}` 项。此外，您需要配置 `firmware/bootloader` 参数，以便在将 `secureBoot` 标志设置为 `disabled` 的情况下使用 `efi` 选项。相应的 YAML 代码段如下所示：

```
[...]
spec:
  domain:
    firmware:
      bootloader:
        efi:
          secureBoot: false
    launchSecurity:
      sev: {}
[...]
```

8 当前限制

SUSE 不建议在第一代 AMD EPYC™ 7000 系列处理器（代号 Naples）上将 SEV 和 SEV-ES 功能与 SUSE Linux 产品搭配使用。建议至少使用第二代 7002 系列处理器（代号 Rome）。此外，SEV 和 SEV-ES VM 还存在以下限制。

- 在 SEV 加密的 VM 内运行的 Guest 操作系统必须包含 SEV 支持。SUSE Linux Enterprise Server 12 SP4 及更高版本以及所有 SUSE Linux Enterprise Server 15 版本都支持 SEV。
- 目前不支持涉及保存及恢复实例内存和状态的任何操作。这意味着 SEV 加密的 VM 无法从快照恢复，也无法保存/恢复或实时迁移。加密的 VM 可照常在其他主机上关闭和重新启动。
- SEV 加密的 VM 无法包含可直接访问的主机设备（即 PCI 直通）。
- SEV 加密的 VM 与安全引导不兼容。包含安全引导支持的 UEFI 固件不适用于 SEV 或 SEV-ES VM。
- SEV-ES VM 无法使用 `reboot`、`shutdown -r now` 等命令重引导。必须通过关闭 VM 然后再次启动来进行重引导。此限制不适用于 SEV VM，仅适用于 SEV-ES VM。

日后，当硬件、固件和特定软件层具有新功能时，将会解除这些限制。

9 更多信息

- <https://developer.amd.com/sev> — AMD-SEV 登录页
- AMD SEV-KM API Specification (PDF) (https://www.amd.com/system/files/TechDocs/55766_SEV-KM_API_Specification.pdf)
- AMD SEV GitHub repository containing examples and tools (<https://github.com/AMDESE/AMDSEV/>)
- libvirt SEV configuration settings (<https://libvirt.org/formatdomain.html#sev>)
- [libvirt](https://libvirt.org/kbase/launch_security_sev.html) knowledge base article on AMD SEV (https://libvirt.org/kbase/launch_security_sev.html)

10 法律声明

版权所有 © 2006– 2024 SUSE LLC 和贡献者。保留所有权利。

根据 GNU 自由文档许可证 (GNU Free Documentation License) 版本 1.2 或 (根据您的选择) 版本 1.3 中的条款，在此授予您复制、分发和/或修改本文档的权限；本版权声明和许可证附带不可变部分。许可版本 1.2 的副本包含在题为“GNU Free Documentation License”的部分。有关 SUSE 商标，请参见 <https://www.suse.com/company/legal/>。所有其他第三方商标分别为相应所有者的财产。商标符号 (®、™ 等) 代表 SUSE 及其关联公司的商标。星号 (*) 代表第三方商标。

本指南力求涵盖所有细节，但这不能确保本指南准确无误。SUSE LLC 及其关联公司、作者和译者对于可能出现的错误或由此造成的后果皆不承担责任。

GNU Free Documentation License

Copyright (C) 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non-commercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

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 subunit 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 <https://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.