

# Guia Rápido do Novell AppArmor (2.3.1)

Novell®

Este documento ajuda-o compreender os conceitos principais por trás do Novell® AppArmor— o conteúdo dos perfis do AppArmor. Aprenda como criar ou modificar perfis do AppArmor. Você pode criar e gerenciar os perfis do AppArmor de três maneiras diferentes. A interface mais conveniente para o AppArmor é fornecida através dos módulos do AppArmor no YaST, que podem ser usados tanto no modo gráfico quanto na interface ncurses. A mesma funcionalidade é fornecida pelas ferramentas de linha de comando do AppArmor ou editando-se os perfis num editor de texto.

## Modos do AppArmor

### reclamação/aprendizado

No modo de reclamação ou aprendizado, as violações das regras do perfil do AppArmor, tal como programas com o perfil traçado acessando arquivos não permitidos, são detectadas. As violações são permitidas, mas também registradas. Esse modo é conveniente para o desenvolvimento dos perfis e é usado pelo AppArmor para gerá-los.

### forçar

O carregamento de um perfil no modo forçado impõe a política definida no perfil, bem como gera relatórios para o syslogd das tentativas de violação da política.

## Iniciando e parando o AppArmor

Use o comando `rcapparmor` com um dos seguintes parâmetros:

### start

Carrega o módulo do kernel, monta o securityfs, analisa e carrega perfis. Perfis e limitações são aplicadas para qualquer aplicação iniciada depois que esse comando for executado. Processos em execução durante a inicialização do AppArmor continuam executando sem as limitações.

### stop

Desmonta o securityfs e invalida os perfis.

### reload

Recarrega os perfis.

### status

Se o AppArmor estiver habilitado, exibe quantos perfis estão carregados no modo reclamação ou forçado.

Use o comando `rcaeventd` para controlar o registro de eventos com o `aa-eventd`. Use as opções `start` e `stop`

para alternar o status do `aa-eventd` e verifique seu status usando `status`.

## Ferramentas de linha de comando do AppArmor

### autodep

Realiza suposições sobre os requisitos básicos do perfil do AppArmor. O `autodep` cria um perfil de rascunho para o programa ou aplicação examinada. O perfil resultante é chamado “aproximado” porque não contém, necessariamente, todas as entradas de perfil que o programa precisa para ser confinado corretamente.

### complain

Atribui um perfil do AppArmor ao modo de reclamação.

A ativação manual do modo de reclamação (usando a linha de comando) adiciona um indicador para o topo do perfil, para que `/bin/foo` torne-se `/bin/foo flags=(complain)`.

### forçar

Atribui um perfil do AppArmor para modo forçado a partir do modo de reclamação.

A ativação manual do modo forçado (usando a linha de comando) remove o indicador de modo do topo do perfil `/bin/foo flags=(complain) torne-se /bin/foo`.

### genprof

Gera ou atualiza um perfil. Quando em execução, você deve especificar um programa para o perfil. Se o programa especificado não for um caminho absoluto, o `genprof` pesquisa na variável `$PATH`. Se um perfil não existir, o `genprof` cria um usando o `autodep`.

### logprof

Administra os perfis do AppArmor. O `logprof` é uma ferramenta interativa usada para revisar a saída do modo forçado ou de aprendizado encontrada nas entradas do

syslog do AppArmor e para gerar novas entradas nos perfis do AppArmor.

não delimitado

Retorna uma lista de processos com portas TCP ou UDP abertas que não possuem perfis do AppArmor carregados.

## Métodos de criação do perfil

Perfil avulso

Usando genprof. Adequado para criar perfis de aplicações de pequeno porte.

Perfil sistêmico

Adequado para criar perfis de um grande número de programas de uma só vez e para criar perfis para aplicações que podem ser executadas “para sempre”.

Para criar o perfil sistêmico, siga as instruções:

1. Crie perfis individuais para os programas que compõem sua aplicação (autodep).
2. Coloque os perfis relevantes no modo de reclamação ou aprendizado.
3. Treine seu aplicativo.
4. Analise o log (logprof).
5. Repita os passos 3 e 4.
6. Edite os perfis.
7. Retorne para o modo forçado.
8. Recarregue todos os perfis (`rcapparmor restart`).

## Modo de aprendizagem

Quando estiver usando o genprof, logprof ou YaST no modo de aprendizagem, você possui diversas maneiras de proceder:

Permitir

Concede acesso.

Negar

Impede o acesso.

Glob

Modifica o caminho do diretório para incluir todos arquivos no diretório sugerido.

Glob com ext

Modifica o caminho do diretório original enquanto pega a extensão do arquivo. Isso permite que o programa acesse todos arquivos nos diretórios sugeridos que acabam com a extensão especificada.

Editar

Permite a edição da linha em destaque. A nova linha (editada) aparece na parte inferior da lista. Essa opção é chamada *Novo* nas ferramentas de linha de comando do logprof e genprof.

Cancelar

Cancela o logprof ou YaST, descartando todas mudanças de regras inseridas até o momento e deixando todos perfis sem modificações.

Concluir

Fecha o logprof ou YaST, salvando todas regras modificadas inseridas até o momento e modificando todos perfis.

## Perfil de exemplo

```
#include<tunables/global>

@{HOME} = /home/*/ /root/ # variável

/usr/bin/foo {
    #include <abstractions/base>
    network inet tcp,
    capability setgid,

    /bin/mount                ux,
    /dev/{,u}random           r,
    /etc/ld.so.cache          r,
    /etc/foo/*                 r,
    /lib/ld-*.so*              mr,
    /lib/lib*.so*              mr,
    /proc/[0-9]**             r,
    /usr/lib/**                mr,
    /tmp/                      r,
    /tmp/foo.pid               wr,
    /tmp/foo.*                 lrw,
    /@{HOME}/.foo_file         rw,
    /@{HOME}/.foo_lock         kw,

    link /etc/sysconfig/foo -> /etc/foo.conf,
    deny /etc/shadow           w,
    owner /home/*/**           rw,

    /usr/bin/foobar            cx,
    /bin/**                     px -> bin_generic

    # comentário no perfil local do foo, o foobar

    foobar {
        /bin/bash               rmix,
        /bin/cat                 rmix,
        /bin/more                rmix,
        /var/log/foobar*         rwl,
        /etc/foobar              r,
    }
}
```

## Estrutura de um perfil

Perfis são simples arquivos de texto no diretório `/etc/apparmor.d`. Eles consistem de algumas partes: `#include`, entradas de capacidade, regras e “hats”.

### #include

Esta é a seção de um perfil do AppArmor que faz referência a um arquivo de inclusão, o qual faz o intermédio com as permissões de acesso aos programas. Usando uma inclusão (`include`), você pode conceder aos programas o acesso a diretórios ou arquivos que também são requeridos por outros programas. O uso de `includes` pode reduzir o tamanho de um perfil. É uma boa prática selecionar `includes` quando sugerido.

Para ajudá-lo a criar o perfil de suas aplicações, o AppArmor fornece três classes de `#includes`: abstrações, blocos de programas e ajustáveis.

Abstrações são `#includes` agrupados por tarefas comuns de uma aplicação. Essas tarefas incluem acesso a mecanismos de autenticação, acesso a rotinas de nomes de serviço, requisitos gráficos comuns e sistema de cálculos (por exemplos, `base`, `consoles`, `kerberosclient`, `perl`, `user-mail`, `user-tmp`, `authentication`, `bash`, `nameservice`).

Os blocos de programas são controles de acessos para programas específicos que um administrador de sistema pode desejar controlar baseado em políticas locais. Cada bloco é usado por um único programa.

Os ajustáveis são definições de variáveis globais. Quando usados em um perfil, essas variáveis são expandidas para um valor que pode ser alterado sem alterar o perfil completo. Consequentemente, seus perfis tornam-se portáteis para ambientes diferentes.

### Variáveis locais

Variáveis locais são definidas no cabeçalho de um perfil. Use variáveis locais para criar atalhos para caminhos, por exemplo, para fornecer a base para um caminho com raiz alterada (`chroot`):

```
@{CHROOT_BASE}=/tmp/foo
/sbin/syslog-ng {
...
# aplicativos com raiz alterada
@{CHROOT_BASE}/var/lib/*/dev/log w,
@{CHROOT_BASE}/var/log/** w,
...
}
```

### Apelidos

Regras de apelidos fornecem uma forma alternativa de reescrever o caminho para usar variáveis e são processadas após a resolução das variáveis:

```
alias /home/ -> /mnt/users/
```

## Controle de acesso à rede

O AppArmor fornece mediação no acesso à rede baseado no domínio e tipo de rede:

```
/bin/ping {
network inet dgram,
network inet raw,
...
}
```

O exemplo habilitaria o acesso da rede IPv4 ao datagrama e tipos não genéricos para o comando `ping`. Para mais detalhes sobre a regra de sintaxe de rede, consulte Parte “Confining Privileges with Novell AppArmor” (↑*Guia de Segurança*).

## Entradas de capacidade (POSIX.1e)

As declarações de capacidades são simplesmente a palavra “capability” seguida pelo nome da capacidade POSIX.1e, como definido na página `man capabilities(7)`.

## Regras: opções gerais de arquivos e diretórios

Opção	Arquivo
leitura	r
escrita	w
associação	l
bloquear arquivo	k
anexar ao arquivo (mutuamente exclusivo com w)	a

## Regras: pares de associação

O modo de associação concede permissão para criar associações para arquivos arbitrários, desde que a associação tenha um subconjunto de permissões concedidas pelo alvo (teste do subconjunto de permissões). Especificando a origem e o destino, a regra do par de associação proporciona maior controle sobre como as associações fortes são criadas. Regras do par de associação, por padrão, não reforçam o teste do conjunto de permissões que os padrões que as regras do par requerem. Para forçar a regra para requerer o teste, a palavra-chave `subset` é usada. As seguintes regras são equivalentes:

```
/link l,
link subset /link -> /**,
```

## Regras: regras de negação

O AppArmor fornece regras de negação que são regras padrões, mas com a palavra `deny` como prefixo. Elas são usadas para lembrar rejeições conhecidas, e rejeitando-as para não encher os arquivos de log. Para mais

informações, veja Parte “Confining Privileges with Novell AppArmor” (↑*Guia de Segurança*).

## Regras: regras condicionais proprietárias

As regras de arquivos podem ser ampliadas para que elas possam ser condicionais ao usuário ser dono do arquivo usando a palavra-chave `owner` como prefixo na regra. Regras condicionais proprietárias acumulam bem como as regras regulares de arquivos e são consideradas um subconjunto de regras regulares de arquivos. Se uma regra regular sobrepõe-se com um regra de arquivo condicional proprietária, a permissão resultante será a da regra regular do arquivos.

## Regras: definindo permissões de execução

Para executáveis que podem ser chamados a partir de programas confinados, a ferramenta de criação de perfis lhe pergunta pelo modo apropriado, o qual também é refletido diretamente no próprio perfil:

<i>Opção</i>	<i>Arquivo</i>	<i>Descrição</i>
Herdar	<code>ix</code>	Fica no mesmo perfil (do pai).
Perfil	<code>px</code>	Requer que um perfil separado exista para executar o programa. Use <code>Px</code> para fazer uso do ambiente "scrubbing".
Perfil local	<code>cx</code>	Requer que o perfil local exista para o programa executado. Use <code>Cx</code> para fazer uso do ambiente "scrubbing".
Sem restrições	<code>ux</code>	Executa o programa sem um perfil. Evite executar programas em modos irrestritos ou não confinados por razões de segurança. Use <code>Ux</code> para fazer uso do ambiente "scrubbing".
Permitir mapeamento executável	<code>m</code>	permita <code>PROT_EXEC</code> com chamadas a <code>mmap(2)</code>

### ATENÇÃO: Executando no modo ux

Evite executar programas no modo `ux` o máximo possível. Um programa rodando no modo `ux` não é somente desprotegido pelo AppArmor mas seus processos filhos herdam certas variáveis de ambiente dele que podem influenciar o comportamento dos filhos e criar possíveis riscos de segurança.

Para mais informações sobre os diferentes modos de execução de arquivos, consulte a página `man apparmor.d(5)`. Para mais informações sobre o ambiente de "scrubbing" do `setgid` e `setuid`, consulte a página `man ld.so(8)`.

## Regras: caminhos e globbing

O AppArmor suporta manipulação explícita de diretórios. Use uma `/` final para qualquer caminho que precisa ser explicitamente distinguido:

```
/algum/exemplo/aleatório/* r
    Habilita o acesso para leitura aos arquivos no diretório
    /algum/exemplo/aleatório.
/algum/exemplo/aleatório/ r
    Permite acesso de leitura somente para o diretório.
/algum/**/ r
    Concede acesso de leitura para quaisquer diretórios em
    /algum.
/algum/exemplo/aleatório/** r
    Concede acesso de leitura aos arquivos e diretórios em
    /algum/exemplo/aleatório.
/algum/exemplo/aleatório/**[^/] r
    Concede acesso a leitura aos arquivos em /algum/
    exemplo/aleatório. Exclua diretórios explicitamente
    ([^/]).
```

Para poupar o usuário de especificar caminhos semelhantes novamente, o AppArmor suporta globbing básico:

<i>Glob</i>	<i>Descrição</i>
<code>*</code>	Substituto para qualquer número de caracteres, exceto <code>/</code> .
<code>**</code>	Substituto para qualquer número de caracteres, incluindo <code>/</code> .
<code>?</code>	Substituto para qualquer caractere único, exceto <code>/</code> .
<code>[ abc ]</code>	Substituto para o caractere único <code>a</code> , <code>b</code> ou <code>c</code> .
<code>[ a-c ]</code>	Substituto para o caractere único <code>a</code> , <code>b</code> ou <code>c</code> .
<code>{ ab,cd }</code>	Expande para uma regra corresponder a <code>ab</code> e outra para corresponder a <code>cd</code> .
<code>[ ^a ]</code>	Substituto para qualquer caractere, exceto <code>a</code> .

## Regras: regras de auditoria

O AppArmor fornece ao usuário a habilidade de auditar determinadas regras para que quando elas forem comparadas, uma mensagem de auditoria apareça no log do audit. Para habilitar as mensagens de auditoria para uma dada regra, a palavra-chave `audit` é prefixada à regra:

```
audit /etc/foo/* rw,
```

## Regras: ajustando capacidades

Normalmente, o AppArmor só restringe controles nativos existentes do Linux e não concede privilégios adicionais. A

única exceção a essa regra é a regra `set capability`. Por razões de segurança, as regras `set capability` não serão herdadas. Uma vez que o programa deixar o perfil, ele perderá todos privilégios elevados. O ajuste de uma capacidade também implica em adicionar uma regra de capacidade permitindo aquela capacidade. Como essa regra concede privilégios de root a processos, deve ser usada com extremo cuidado e somente em casos excepcionais.

```
set capability cap_chown,
```

## Hats

Um perfil do AppArmor representa uma política de segurança para uma instância de programa individual ou processo. Isso é aplicado a um programa executável, mas se uma porção do programa precisa de diferentes permissões de acesso, o programa pode “trocar hats” para usar um diferente contexto de segurança, diferente do acesso do programa principal. Isso é conhecido como um hat ou subperfil.

Um perfil pode ter um número arbitrário de hats, mas há somente dois níveis: um hat não pode ter outros hats.

A funcionalidade `ChangeHat` do AppArmor pode ser usada por aplicações para acessar hats durante a execução. Atualmente, os pacotes `apache2-mod_apparmor` e `tomcat_apparmor` utilizam o `ChangeHat` para fornecer um confinamento de subprocessos para o servidor web Apache e o contentor servlet Tomcat.

## Confinando usuários com o pam\_apparmor

O módulo `pam_apparmor` PAM permite que aplicações confinem usuários autenticados no subperfil baseado nos nomes dos grupos, nomes de usuários ou perfil padrão. Para realizar isso, o `pam_apparmor` precisa ser registrado como um módulo de seção PAM.

Detalhes sobre como configurar o `pam_apparmor` podem ser encontrados em `/usr/share/doc/packages/pam_apparmor/README`. Um HOWTO da configuração do controle de acesso baseado em permissões (RBAC) com `pam_apparmor` está disponível em [http://developer.novell.com/wiki/index.php/Apparmor\\_RBAC\\_in\\_version\\_2.3](http://developer.novell.com/wiki/index.php/Apparmor_RBAC_in_version_2.3).

## Criação de log e auditoria

Todos eventos do AppArmor são gravados usando a interface do sistema audit (é gravado no `/var/log/audit/audit.log`). No topo dessa infraestrutura, as notificações de eventos podem ser configuradas. Configure essa funcionalidade usando o YaST. Isso é baseado nos níveis de gravidade de acordo com `/etc/apparmor/severity`

`.db`. A frequência e o tipo de notificação (como por e-mail) podem ser configurados.

Se o `auditd` não estiver em execução, os logs do AppArmor ficam armazenados em `/var/log/messages` usando o `LOG_KERN` para facilitar.

Use o YaST para gerar relatórios no formato CSV ou HTML.

O framework audit do Linux contém um despachante que pode enviar eventos do AppArmor para qualquer aplicação via dbus. O monitor da área de trabalho do AppArmor (GNOME) é um exemplo de aplicação que reúne eventos do AppArmor via dbus. Para configurar uma aplicação para receber eventos do despachante dbus, modifique o despachante na configuração do audit em `/etc/audit/auditd.conf` para `apparmor-dbus` e reinicie o `auditd`:

```
dispatcher=/usr/bin/apparmor-dbus
```

Uma vez que o despachante dbus esteja configurado corretamente, adicione o monitor de área de trabalho do AppArmor ao painel do GNOME. Assim que um evento `REJECT` for registrado, o ícone do miniaplicativo no painel mudará de aparência e você poderá clicar no miniaplicativo para ver o número de eventos rejeitados por aplicação confinada. Para ver o log de mensagens, entre no log do audit em `/var/log/audit/audit.log`. Use o assistente de atualização de perfil do YaST para ajustar o respectivo perfil.

## Diretórios e arquivos

`/sys/kernel/security/apparmor/profiles`

Arquivo virtualizado representando o conjunto de perfis carregados no momento.

`/etc/apparmor/`

Localização dos arquivos de configuração do AppArmor.

`/etc/apparmor/profiles/extras/`

Um repositório de perfis fornecidos com o AppArmor, mas, por padrão, não estão habilitados.

`/etc/apparmor.d/`

Local dos perfis, nomeando com a convenção de substituir a `/` nos nomes dos caminhos por `.` (exceto para o `/` do root), assim os perfis são fáceis de controlar. Por exemplo, o perfil para o programa `/usr/sbin/ntpd` é nomeado como `usr.sbin.ntpd`.

`/etc/apparmor.d/abstractions/`

Local das abstrações.

`/etc/apparmor.d/program-chunks/`

Local dos blocos de programas.

`/proc/*/attr/current`

Para ver o status de confinamento de um processo e o perfil que é usado para confinar o processo. O comando `ps auxZ` obtém essa informação automaticamente.

## Para mais informações

Para aprender mais sobre o projeto AppArmor, verifique o site do projeto em <http://en.opensuse.org/AppArmor>. Encontre mais informações sobre o conceito e configuração do AppArmor em Parte “Confining Privileges with Novell AppArmor” (↑*Guia de Segurança*).

## Legal Notice

Copyright© 2006–2010 Novell, Inc. and contributors. All rights reserved.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or (at your option) version 1.3; with the Invariant Section being this copyright notice and license.

A copy of the license version 1.2 is included in the section entitled “GNU Free Documentation License”.

SUSE®, openSUSE®, the openSUSE® logo, Novell®, the Novell® logo, the N® logo, are registered trademarks of Novell, Inc. in the United States and other countries. Linux\* is a registered trademark of Linus Torvalds. All other third party trademarks are the property of their respective owners. A trademark symbol (®, ™, etc.) denotes a Novell trademark; an asterisk (\*) denotes a third-party trademark.

All information found in this book has been compiled with utmost attention to detail. However, this does not guarantee complete accuracy. Neither Novell, Inc., SUSE LINUX Products GmbH, the authors, nor the translators shall be held liable for possible errors or the consequences thereof.



# GNU Free Documentation License

Version 1.2, November 2002

Copyright (C) 2000,2001,2002 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

## 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 noncommercially. 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 in order 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.

## 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.

## VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, 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.

## 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.

## 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.

## 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”.

## 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.

## 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.

## 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.

## 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.

## 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

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

```
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.