

Autenticação com o PAM

O QUE É?

O artigo descreve o conceito, a estrutura de configuração e o uso de ferramentas para configurar o PAM.

POR QUÊ?

Para saber como configurar um módulo PAM e o seu sistema para usar as chaves U2F.

DEDICAÇÃO

A leitura do artigo leva aproximadamente 20 minutos.

REQUISITOS

Para configurar a autenticação usando as chaves U2F, você precisa

- ter o YubiKeys ou Security Keys.

Data de Publicação: 11/12/2025

Conteúdo

- 1 Introdução ao PAM 3
- 2 Estrutura de configuração do PAM 3
- 3 Configuração de módulos PAM 9
- 4 Configurando o PAM com **pam-config** 10
- 5 Configurando manualmente o PAM 11
- 6 Configurando o SLE Micro para exigir chaves U2F para login local 11

7 Informações legais 14

A Licença GFDL (GNU Free Documentation License) 14

1 Introdução ao PAM

Os programadores e administradores do sistema muitas vezes desejam restringir o acesso a certas partes do sistema ou limitar o uso de certas funções de um aplicativo. Sem o PAM, os aplicativos devem ser adaptados toda vez que é introduzido um novo mecanismo de autenticação, como LDAP, Samba ou Kerberos. No entanto, esse processo é demorado e sujeito a erros. Uma forma de evitar essas desvantagens é separar os aplicativos do mecanismo de autenticação e delegar a autenticação a módulos gerenciados centralmente. Sempre que um esquema de autenticação passa a ser necessário, basta adaptar ou gravar um *módulo PAM* adequado para ser usado pelo programa em questão.

O conceito do PAM consiste em:

- *Módulos PAM*, que são um conjunto de bibliotecas compartilhadas para um mecanismo de autenticação específico.
- Uma *pilha de módulos* com um ou mais módulos PAM.
- Um *serviço* compatível com PAM, que precisa de autenticação usando uma pilha de módulos ou módulos PAM. Normalmente, um serviço é um nome familiar do aplicativo correspondente, como `login` ou `su`. O nome do serviço `other` é uma palavra reservada para regras padrão.
- *Argumentos de módulo*, com os quais a execução de um único módulo PAM pode ser influenciada.
- Um mecanismo que avalia cada *resultado* de uma única execução de módulo PAM. Um valor positivo executa o próximo módulo PAM. A forma como um valor negativo é tratado depende da configuração: “sem influência, prosseguir” até “terminar imediatamente”, e qualquer opção intermediária é válida.

2 Estrutura de configuração do PAM

O PAM no SLE Micro é fornecido com a chamada configuração baseada em diretório. O conjunto de arquivos de configuração é armazenado em `/etc/pam.d`. Cada serviço (ou programa) que depende do mecanismo PAM tem seu próprio arquivo de configuração nesse diretório. Por exemplo, o serviço para `sshd` pode estar em `/etc/pam.d/sshd`.



Nota: Configuração baseada em arquivo (`/etc/pam.conf`) não usada no SLE Micro

A configuração de cada serviço também pode ser armazenada em `/etc/pam.conf`. No entanto, por motivos de manutenção e usabilidade, esse esquema de configuração não é usado no SLE Micro.

Os arquivos em `/etc/pam.d/` definem os módulos PAM usados para autenticação. Cada arquivo consiste em linhas, que definem um serviço, e cada linha consiste em, no máximo, quatro componentes:

```
TYPE  
CONTROL  
MODULE_PATH  
MODULE_ARGS
```

Os componentes têm o seguinte significado:

TYPE

Declara o tipo de serviço. Os módulos PAM são processados como pilhas. Tipos diferentes de módulos têm finalidades distintas. Por exemplo, um módulo verifica a senha, outro verifica o local de onde o sistema é acessado e outro ainda lê as configurações específicas do usuário. O PAM tem conhecimento sobre quatro tipos diferentes de módulos:

auth

Verificar a autenticidade do usuário, normalmente ao consultar uma senha. No entanto, isso também pode ser feito com um cartão com chip ou por meio de biometria (por exemplo, impressões digitais ou escaneamento da íris).

account

Os módulos desse tipo verificam se o usuário tem uma permissão geral para usar o serviço solicitado. A título de exemplo, essa verificação deve ser realizada para assegurar que ninguém possa efetuar login com o nome de usuário de uma conta que já expirou.

password

O objetivo desse tipo de módulo é permitir a mudança de um token de autenticação. Normalmente, trata-se de uma senha.

session

Os módulos desse tipo são responsáveis pelo gerenciamento e configuração de sessões de usuários. Eles são iniciados antes e depois da autenticação para registrar as tentativas de login e configurar o ambiente específico do usuário.

CONTROL

Indica o comportamento de um módulo PAM. Cada módulo pode ter os seguintes flags de controle:

required

Um módulo com esse flag precisa ser processado com êxito para que a autenticação possa prosseguir. Após a falha de um módulo com o flag required, todos os outros módulos com o mesmo flag serão processados antes que o usuário receba uma mensagem sobre a falha da tentativa de autenticação.

requisite

Os módulos com esse flag também devem ser processados com êxito, de forma muito semelhante a um módulo com o flag required. Contudo, em caso de falha, um módulo com esse flag dá um retorno imediato ao usuário e os módulos restantes deixam de ser processados. Em caso de êxito, os outros módulos serão processados na sequência, assim como qualquer módulo com o flag required. O flag requisite pode ser usado como um filtro básico para verificar a existência de determinadas condições essenciais para a autenticação correta.

sufficient

Após o processamento bem-sucedido de um módulo com esse flag, o aplicativo que fez a solicitação receberá imediatamente uma mensagem sobre o êxito, e o processamento de outros módulos será interrompido, exceto quando houver falhas anteriores em um módulo com o flag required. A falha de um módulo com o flag sufficient não causa consequências diretas, com os módulos subsequentes sendo processados na sua respectiva ordem.

optional

A falha ou êxito de um módulo com esse flag não traz consequências diretas. Isso pode ser útil no caso de módulos cujo único propósito é exibir uma mensagem (por exemplo, informar ao usuário sobre a chegada de e-mails) sem executar nenhuma ação adicional.

include

Quando esse flag é dado, o arquivo especificado como argumento é inserido nesse lugar.

MODULE_PATH

Contém o nome de arquivo completo de um módulo PAM. Ele não precisará ser especificado explicitamente se o módulo estiver localizado no diretório padrão /lib/security (para todas as plataformas de 64 bits suportadas pelo SLE Micro, o diretório é /lib64/security).

MODULE_ARGS

Contém uma lista de opções separadas por espaço para influenciar o comportamento de um módulo PAM, como debug (habilita a depuração) ou nullok (permite o uso de senhas vazias).

Além disso, há arquivos de configuração global para módulos PAM em /etc/security, que definem o comportamento exato desses módulos (alguns exemplos são pam_env.conf e time.conf). Cada aplicativo que usa um módulo PAM chama um conjunto de funções do PAM que, em seguida, processa as informações nos arquivos de configuração e retorna o resultado para o aplicativo que fez a solicitação.

Para simplificar a criação e a manutenção dos módulos PAM, foram introduzidos arquivos de configuração padrão comuns para os módulos dos tipos auth, account, password e session. Eles são recuperados da configuração do PAM de cada aplicativo. As atualizações nos módulos de configuração global do PAM em common-* são propagadas para todos os arquivos de configuração do PAM, sem exigir que o administrador atualize cada um desses arquivos.

Os arquivos de configuração global do PAM são mantidos usando a ferramenta pam-config. Essa ferramenta adiciona automaticamente novos módulos à configuração, muda a configuração daqueles existentes ou apaga módulos (ou opções) das configurações. A intervenção manual na manutenção das configurações do PAM é minimizada ou não é mais necessária.

2.1 Um exemplo de configuração do PAM

Para demonstrar um exemplo de caso de uso real da configuração do PAM, a configuração do sshd foi usada nesta seção:

EXEMPLO 1: **CONFIGURAÇÃO DO PAM PARA SSHD (/etc/pam.d/sshd)**

```
##PAM-1.0 ①
```

```

auth    requisite      pam_nologin.so          ②
auth    include        common-auth             ③
account requisite    pam_nologin.so          ②
account include      common-account           ③
password include    common-password          ③
session required     pam_loginuid.so         ④
session include      common-session           ③
session optional     pam_lastlog.so   silent nouupdate showfailed ⑤

```

- ① Declara a versão desse arquivo de configuração para o PAM 1.0. Isso é apenas uma convenção, mas pode ser usado no futuro para verificar a versão.
- ② Verifica se `/etc/nologin` existe. Em caso afirmativo, nenhum outro usuário `root` poderá efetuar login.
- ③ Refere-se aos arquivos de configuração de quatro tipos de módulo: `common-auth`, `common-account`, `common-password` e `common-session`. Esses quatro arquivos abrigam a configuração padrão de cada tipo de módulo.
- ④ Define o atributo de processo do UID de login para o processo que foi autenticado.
- ⑤ Exibe informações sobre o último login de um usuário.

Ao incluir os arquivos de configuração em vez de adicionar cada módulo separadamente à respectiva configuração do PAM, você obtém automaticamente uma configuração do PAM atualizada quando um administrador muda os padrões.

O primeiro arquivo de inclusões (`common-auth`) chama os módulos do tipo `auth`: `pam_env.so`, `pam_gnome_keyring.so` e `pam_unix.so`. Consulte o [Exemplo 2, “Configuração padrão da seção auth \(common-auth\)”.](#) Lembre-se de que os módulos podem ser diferentes de acordo com a sua instalação.

EXEMPLO 2: CONFIGURAÇÃO PADRÃO DA SEÇÃO auth (common-auth)

```

auth required pam_env.so          ①
auth optional pam_gnome_keyring.so ②
auth required pam_unix.so try_first_pass ③

```

- ① O `pam_env.so` carrega o `/etc/security/pam_env.conf` para definir as variáveis de ambiente conforme especificado nesse arquivo. Ele pode ser usado para definir o valor correto da variável `DISPLAY`, pois o módulo `pam_env` reconhece o local de onde o login está sendo efetuado.
- ② O `pam_gnome_keyring.so` compara o login e a senha do usuário com o chaveiro do GNOME.

- ③ O pam_unix verifica compara o login e a senha do usuário com /etc/passwd e /etc/shadow.

A pilha inteira de módulos auth é processada antes que o sshd receba qualquer retorno se o login foi bem-sucedido. Todos os módulos da pilha que têm o flag de controle required devem ser processados com êxito antes que o sshd receba uma mensagem sobre o resultado positivo. Se um dos módulos não for bem-sucedido, a pilha de módulos inteira ainda será processada, e somente depois disso é que o sshd será notificado sobre o resultado negativo.

Quando todos os módulos do tipo auth tiverem sido processados com êxito, outra declaração de inclusão será processada, neste caso, aquela no *Exemplo 3, “Configuração padrão da seção account (common-account)”*. O common-account contém apenas um módulo: pam_unix. Se pam_unix retornar o resultado de que o usuário existe, o sshd receberá uma mensagem de êxito, e a próxima pilha de módulos (password) será processada, conforme mostrado em .

EXEMPLO 3: CONFIGURAÇÃO PADRÃO DA SEÇÃO account (common-account)

```
account required pam_unix.so try_first_pass
```

Mais uma vez, a configuração do PAM de sshd envolve apenas uma declaração de inclusão referente à configuração padrão para os módulos password localizados em common-password. Esses módulos devem ser concluídos com êxito (flags de controle requisitee required) sempre que o aplicativo solicita a mudança de um token de autenticação.

A mudança de uma senha ou de outro token de autenticação requer uma verificação de segurança. Isso é feito com o módulo pam_cracklib. O módulo pam_unix usado posteriormente transfere as senhas antigas e novas do pam_cracklib, portanto, o usuário não precisa se autenticar novamente após mudar a senha. Esse procedimento também torna impossível contornar as verificações realizadas pelo pam_cracklib. Sempre que o tipo account ou auth for configurado para reclamar sobre senhas expiradas, os módulos password também deverão ser usados.

Na etapa final, os módulos do tipo session (incluídos no arquivo common-session) são chamados para definir a sessão de acordo com as configurações do usuário em questão. O módulo pam_limits carrega o arquivo /etc/security/limits.conf, que pode definir limites para o uso de determinados recursos do sistema. O módulo pam_unix é processado novamente. O módulo pam_umask pode ser usado para definir a máscara de criação do modo de arquivo. Como esse módulo tem o flag optional, uma falha dele não afeta a conclusão bem-sucedida de toda a pilha de módulos da sessão. Os módulos session são chamados uma segunda vez quando o usuário efetua logout.

3 Configuração de módulos PAM

Alguns módulos PAM são configuráveis. Os arquivos de configuração estão localizados em `/etc/security`. Esta seção descreve resumidamente os arquivos de configuração relevantes ao exemplo do sshd: `pam_env.conf` e `limits.conf`.

3.1 pam_env.conf

O `pam_env.conf` pode ser usado para definir um ambiente padronizado para os usuários, que será definido sempre que o módulo `pam_env` for chamado. Com ele, predefina variáveis de ambiente usando a seguinte sintaxe:

```
VARIABLE [DEFAULT=VALUE] [OVERRIDE=VALUE]
```

VARIABLE

Nome da variável de ambiente a ser definida.

[DEFAULT=<value>]

VALUE padrão que o administrador deseja definir.

[OVERRIDE=<value>]

Os valores que podem ser consultados e definidos por `pam_env`, anulando o valor padrão.

Um exemplo típico de como o módulo `pam_env` pode ser usado é na adaptação da variável `DISPLAY`, que é mudada sempre que um login remoto é efetuado. Você pode ver isso no [Exemplo 4, “pam_env.conf”](#).

EXEMPLO 4: PAM_ENV.CONF

```
REMOTEHOST DEFAULT=localhost OVERRIDE=@{PAM_RHOST}
DISPLAY     DEFAULT=${REMOTEHOST}:0.0 OVERRIDE=${DISPLAY}
```

A primeira linha define o valor da variável `REMOTEHOST` como `localhost`, que é usado sempre que `pam_env` não consegue determinar nenhum outro valor. A variável `DISPLAY`, por sua vez, contém o valor de `REMOTEHOST`. Encontre mais informações nos comentários em `/etc/security/pam_env.conf`.

3.2 limits.conf

Os limites do sistema podem ser definidos por usuário ou grupo em `limits.conf`, que é lido pelo módulo `pam_limits`. O arquivo permite definir limites fixos, que não podem ser excedidos, e limites flexíveis, que podem ser excedidos temporariamente. Para obter mais informações sobre a sintaxe e as opções, consulte os comentários em `/etc/security/limits.conf`.

4 Configurando o PAM com pam-config

A ferramenta `pam-config` ajuda você a configurar os arquivos de configuração global do PAM (`/etc/pam.d/common-*`) e várias configurações de aplicativo selecionadas. Para obter uma lista dos módulos suportados, use o comando `pam-config --list-modules`. Use o comando `pam-config` para manter os arquivos de configuração do PAM. Adicione novos módulos às configurações do PAM, apague outros módulos ou modifique as opções desses módulos. Ao mudar os arquivos de configuração global do PAM, nenhum ajuste manual da configuração do PAM para aplicativos individuais é necessário.

Um caso de uso simples para `pam-config` envolve o seguinte:

1. Gerar automaticamente uma nova configuração do PAM no estilo unix. Deixe o `pam-config` criar a configuração mais simples possível, que você poderá estender posteriormente. O comando `pam-config --create` cria uma configuração de autenticação Unix simples. Os arquivos de configuração preexistentes não mantidos pelo `pam-config` são sobregravados, mas as cópias de backup são mantidas como `*.pam-config-backup`.
2. Adicionar um novo método de autenticação. A adição de um novo método de autenticação (por exemplo, LDAP) à pilha de módulos PAM se resume a um comando `pam-config --add --ldap` simples. O LDAP é adicionado sempre que apropriado a todos os arquivos de configuração `common-* - pc` do PAM.
3. Adicionar depuração para fins de teste. Para garantir que o novo procedimento de autenticação funcione conforme planejado, ative a depuração para todas as operações relacionadas ao PAM. O `pam-config --add --ldap-debug` ativa a depuração para operações do PAM relacionadas ao LDAP.
4. Consultar sua configuração. Antes de finalmente aplicar a nova configuração do PAM, verifique se ela contém todas as opções que você deseja adicionar. O comando `pam-config --query --MODULE` lista o tipo e as opções para o módulo PAM consultado.

5. **Remover as opções de depuração.** Por fim, remova a opção de depuração de sua configuração quando você estiver totalmente satisfeito com o desempenho dela. O comando `pam-config --delete --ldap-debug` desativa a depuração para autenticação LDAP. Caso você tenha opções de depuração adicionadas para outros módulos, use comandos semelhantes para desativá-las.

Para obter mais informações sobre o comando `pam-config` e as opções disponíveis, consulte a página de manual [`pam-config\(8\)`](#).

5 Configurando manualmente o PAM

Se você preferir criar ou manter manualmente os arquivos de configuração do PAM, desabilite `pam-config` para esses arquivos.

Quando você cria os arquivos de configuração do PAM do zero usando o comando `pam-config --create`, ele cria links simbólicos dos arquivos `common-*` para os arquivos `common-*-.pc`. `pam-config` modifica apenas os arquivos de configuração `common-*-.pc`. A remoção desses links simbólicos desabilita efetivamente o `pam-config`, porque o `pam-config` opera apenas com base em arquivos `common-*-.pc`, e esses arquivos não entram em vigor sem os links simbólicos.



Atenção: Incluir `pam_systemd.so` na configuração

Se você estiver criando sua própria configuração do PAM, inclua o `pam_systemd.so` configurado como `session optional`. Se o `pam_systemd.so` não for incluído, poderá haver problemas com os limites de tarefas do `systemd`. Para obter detalhes, consulte a página de manual de `pam_systemd.so`.

6 Configurando o SLE Micro para exigir chaves U2F para login local

Para reforçar a segurança durante o login local no SLE Micro, você pode configurar a autenticação de dois fatores usando a estrutura `pam-u2f` e o recurso U2F no YubiKeys e Security Keys.

Para configurar o U2F no sistema SLE Micro, você precisa associar sua chave à sua conta no SLE Micro. Depois disso, configure seu sistema para usar a chave. O procedimento está descrito nas seções a seguir.

6.1 Associando a chave U2F à sua conta

Para associar a chave U2F à sua conta, faça o seguinte:

1. Efetue login na sua máquina.
2. Insira a chave U2F.
3. Crie um diretório para a configuração da chave U2F:

```
> sudo mkdir -p ~/.config/Yubico
```

4. Execute o comando `pamu2fcfg` que gera as linhas de configuração:

```
> sudo pamu2fcfg > ~/.config/Yubico/u2f_keys
```

5. Quando o dispositivo começar a piscar, toque no contato de metal para confirmar a associação.

Recomendamos o uso de um dispositivo U2F de backup, que você pode configurar executando os seguintes comandos:

1. Execute:

```
> sudo pamu2fcfg -n >> ~/.config/Yubico/u2f_keys
```

2. Quando o dispositivo começar a piscar, toque no contato de metal para confirmar a associação.

Você pode mover o arquivo de saída do local padrão para um diretório que exija a permissão de `sudo` para modificar o arquivo para reforçar a segurança. Por exemplo, mova-o para o diretório `/etc`. Para isso, siga as etapas:

1. Crie um diretório em `/etc`:

```
> sudo mkdir /etc/Yubico
```

2. Mova o arquivo criado:

```
> sudo mv ~/.config/Yubico/u2f_keys /etc/Yubico/u2f_keys
```



Nota: Colocando u2f_keys em um local não padrão

Se você mover o arquivo de saída para um diretório diferente do padrão (`$HOME/.config/Yubico/u2f_keys`), será necessário adicionar o caminho ao arquivo `/etc/pam.d/login` conforme descrito na [Seção 6.2, "Atualizando a configuração do PAM"](#).

6.2 Atualizando a configuração do PAM

Após criar a configuração de chaves U2F, você precisará ajustar a configuração do PAM no sistema.

1. Abra o arquivo `/etc/pam.d/login`.

2. Adicione a linha `auth required pam_u2f.so` ao arquivo da seguinte maneira:

```
 #%PAM-1.0
auth      include    common-auth
auth      required  pam_u2f.so
account   include    common-account
password  include    common-password
session   optional   pam_keyinit.so revoke
session   include    common-session
#session  optional   pam_xauth.so
```

3. Se você colocou o arquivo `u2f_keys` em um local diferente de `$HOME/.config/Yubico/u2f_keys`, precisa usar a opção `authfile` no arquivo `/etc/pam.d/login` do PAM da seguinte maneira:

```
 #%PAM-1.0
auth      requisite pam_nologin.so
auth      include    common-auth
auth      required  pam_u2f.so authfile=<PATH_TO_u2f_keys>
...
```

em que `<PATH_TO_u2f_keys>` é o caminho absoluto para o arquivo `u2f_keys`.

7 Informações legais

Copyright © 2006-2025 SUSE LLC e colaboradores. Todos os direitos reservados.

Permissão concedida para copiar, distribuir e/ou modificar este documento sob os termos da Licença GNU de Documentação Livre, Versão 1.2 ou (por sua opção) versão 1.3; com a Seção Invariante sendo estas informações de copyright e a licença. Uma cópia da versão 1.2 da licença está incluída na seção intitulada “GNU Free Documentation License” (Licença GNU de Documentação Livre).

Para ver as marcas registradas da SUSE, visite <https://www.suse.com/company/legal/>. Todas as marcas comerciais de terceiros pertencem a seus respectivos proprietários. Os símbolos de marca registrada (®, ™ etc.) indicam marcas registradas da SUSE e de suas afiliadas. Os asteriscos (*) indicam marcas registradas de terceiros.

Todas as informações deste manual foram compiladas com a maior atenção possível aos detalhes. Entretanto, isso não garante uma precisão absoluta. A SUSE LLC, suas afiliadas, os autores ou tradutores não serão responsáveis por possíveis erros nem pelas consequências resultantes de tais erros.

A Licença GFDL (GNU Free Documentation License)

Copyright (C) 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 EUA. Qualquer pessoa está autorizada a reproduzir e distribuir cópias literais deste documento de licença, mas não a mudar seu conteúdo.

0. PREÂMBULO

A finalidade desta Licença é tornar um manual, um livro ou outro documento funcional e útil “livre”, no sentido de garantir a todos a liberdade efetiva para copiá-lo e redistribuí-lo, com ou sem modificações, para fins comerciais ou não. Em segundo lugar, esta Licença preserva ao autor e ao editor o direito de obter créditos pelo seu trabalho, não sendo considerados responsáveis pelas modificações feitas por outras pessoas.

Esta Licença é um tipo de “copyleft”, significando que trabalhos derivados do documento também devem ser livres no mesmo sentido. Ela complementa a Licença Pública Geral GNU, que é uma licença de copyleft criada para software livre.

Criamos esta Licença para usá-la em manuais de software livre, pois o software livre precisa de documentação livre: um programa livre deve incluir manuais que ofereçam a mesma liberdade que o software. Contudo, essa Licença não está limitada a manuais de software, pois pode ser usada para qualquer trabalho de texto, independentemente do assunto ou do fato de ser publicado como manual impresso. Esta licença é recomendável principalmente para trabalhos cuja finalidade seja instrução ou referência.

1. APlicabilidade e DEFINIções

Esta Licença se aplica a qualquer manual ou outro trabalho, em qualquer meio, que contenha um aviso incluído pelo detentor dos direitos autorais indicando que ele pode ser distribuído segundo os termos desta Licença. Esse aviso concede uma licença em nível mundial, isenta do pagamento de royalties e de duração ilimitada, para usar o trabalho sob as condições aqui previstas. O “Documento” a seguir refere-se a tal manual ou trabalho. Qualquer membro do público pode ser um licenciado e é tratado como “você”. Você aceitará a licença se copiar, modificar ou distribuir o trabalho de um modo que necessite de permissão de acordo com a lei de direitos autorais.

Uma “Versão Modificada” do Documento significa qualquer trabalho que contenha o Documento ou parte dele, que pode ser sua cópia fiel ou com modificações e/ou traduzido para outro idioma.

Uma “Seção Secundária” é um apêndice nomeado ou uma seção de introdução do Documento, que trata exclusivamente da relação dos editores ou autores do Documento com seu assunto geral (ou questões relacionadas), e não contém nada que possa estar diretamente ligado ao assunto geral. (Portanto, se o documento for parcialmente um livro de matemática, uma seção secundária não poderá explicar nada de matemática.) Tal relação pode ser uma conexão histórica com o assunto ou com temas relacionados, ou tratar de questões legais, comerciais, filosóficas, éticas ou políticas com relação a eles.

As “Seções Invariáveis” são determinadas Seções Secundárias cujos títulos são designados como sendo referentes a essas Seções Invariáveis, no aviso que indica que o Documento foi lançado sob esta Licença. Se uma seção não se encaixar na definição acima de secundária, não poderá ser designada como invariável. O documento pode não conter Seções Invariáveis. Se o documento não identificar seções invariáveis, isso significa que não há nenhuma.

Os “Textos de Capa” são pequenos trechos de texto, como Textos de Folha de Rosto ou de Contracapa, incluídos no aviso que indica que o Documento foi lançado sob esta licença. O Texto de Folha de Rosto pode ter no máximo 5 palavras, e o Texto de Contracapa pode ter no máximo 25.

Uma cópia “Transparente” do Documento significa uma cópia que pode ser lida por computador, representada em um formato cuja especificação esteja disponível ao público em geral, que seja adequada para a imediata revisão do documento usando editores de texto genéricos ou (para imagens compostas de pixels) programas gráficos genéricos ou (para desenhos) algum editor de desenho amplamente disponível, e que seja adequado para inclusão em formatadores de texto ou para a conversão automática em diversos formatos adequados para entrada em formatadores de texto. Uma cópia feita em outro formato de arquivo Transparente cuja marcação, ou ausência desta, foi manipulada para impedir ou desencorajar modificação subsequente pelos leitores não é Transparente. Um formato de imagem não é Transparente se usado em lugar de qualquer quantidade substancial de texto. Uma cópia que não é “Transparente” é chamada “Opaca”.

Exemplos de formatos apropriados para cópias Transparentes incluem ASCII simples sem marcação, formato de entrada Texinfo, LaTeX, SGML ou XML usando um DTD publicamente disponível, e HTML padrão simples, PostScript ou PDF projetados para modificação manual. Exemplos de formatos de imagem transparentes são PNG, XCF e JPG. Formatos Opacos incluem formatos proprietários que podem ser lidos e editados somente por processadores de texto proprietários, SGML ou XML para os quais o DTD e/ou ferramentas de processamento não são amplamente disponibilizadas, e HTML, PostScript ou PDF gerados automaticamente com finalidade apenas de saída por alguns processadores de texto.

A “Página de Título” significa, para um livro impresso, a própria página do título, além das páginas subsequentes necessárias para conter, de forma legível, o material que esta Licença requer que apareça na página de título. Para trabalhos em formatos que não tenham uma página de título assim, a “Página de Título” significa o texto próximo à ocorrência mais proeminente do título do trabalho, precedendo o início do corpo do texto.

Uma seção “Intitulada XYZ” significa uma subunidade nomeada do Documento cujo título seja precisamente XYZ ou contenha XYZ entre parênteses após o texto que traduz XYZ para outro idioma. (Aqui, XYZ representa o nome de uma seção específica mencionada abaixo, como “Agradecimentos”, “Dedicatória”, “Apoio” ou “Histórico”.) “Preservar o Título” de tal seção quando você modifica o Documento significa que ela continua sendo uma seção “Intitulada XYZ” de acordo com essa definição.

O Documento pode incluir Isenções de Responsabilidade quanto a Garantia próximas ao aviso que indica que esta Licença se aplica a este Documento. As Isenções de Responsabilidade de Garantia são consideradas incluídas por referência nesta Licença, mas apenas no que diz respeito à isenção de garantias: qualquer outra implicação que essas Isenções de Responsabilidade de Garantia possam ter será anulada e não terá efeito no significado desta Licença.

2. CÓPIAS LITERAIS

Você pode copiar e distribuir o Documento em qualquer meio, comercialmente ou não, desde que esta Licença, as informações de copyright e as informações de licença afirmado que esta Licença se aplica ao Documento sejam reproduzidas em todas as cópias, e que você não inclua outras condições, quaisquer que sejam, às condições desta Licença. Você não pode usar de medidas técnicas para obstruir ou controlar a leitura ou cópia futura das cópias que você fizer ou distribuir. Contudo, você pode aceitar remuneração em troca das cópias. Se você distribuir um número suficientemente grande de cópias, deverá também respeitar as condições na seção 3. Você também pode emprestar cópias, sob as mesmas condições mencionadas acima, além de exibi-las publicamente.

3. COPIANDO EM QUANTIDADE

Se você publicar cópias impressas (ou cópias em uma mídia que normalmente tem capas impressas) do Documento, em número superior a 100, e o aviso de licença do Documento exigir Textos de Capa, deverá encadernar as cópias em capas que contenham, de forma clara e legível, todos estes Textos de Capa: Textos de Folha de Rosto na folha de rosto e Textos de Contracapa na contracapa. As duas capas também devem identificar, de forma clara e legível, você como o editor das cópias. A capa frontal deve apresentar o título completo com todas as palavras deste igualmente proeminentes e visíveis. Você pode adicionar outros materiais nas capas. Cópias com mudanças limitadas às capas, desde que preservando o título do Documento e satisfazendo a essas condições, podem ser tratadas como cópias literais em outros aspectos.

Se os textos necessários a qualquer uma das capas forem muito volumosos para serem incluídos de forma legível, você deverá colocar os primeiros listados (quanto couberem razoavelmente) na própria capa, e continuar o restante nas páginas adjacentes.

Se você publicar ou distribuir cópias Opacas do Documento em número superior a 100, deverá incluir uma cópia Transparente legível por computador juntamente com cada cópia Opaca, ou informar em, ou juntamente com, cada cópia Opaca um endereço de rede do qual o público geral possa acessar e obter, usando protocolos de rede públicos padrão, uma cópia Transparente completa do Documento, livre de material adicionado. Se você decidir pela segunda opção, deverá seguir etapas razoavelmente prudentes, quando começar a distribuir as cópias Opacas em quantidade, para garantir que essa cópia transparente permaneça acessível no local indicado por pelo menos um ano após a última vez que você distribuir uma cópia Opaca (diretamente ou através de seus agentes ou distribuidores) dessa edição ao público.

É solicitado, mas não exigido, que você contate os autores do Documento muito antes de redistribuir qualquer número grande de cópias, para dar-lhes a oportunidade de lhe fornecer uma versão atualizada do Documento.

4. MODIFICAÇÕES

Você pode copiar e distribuir uma Versão Modificada do Documento sob as condições das seções 2 e 3 acima, desde que forneça a Versão Modificada estritamente sob esta Licença, com a Versão Modificada no lugar do Documento, permitindo assim a distribuição e modificação da Versão Modificada a quem quer que possua uma cópia desta. Além disso, você deve executar os seguintes procedimentos na Versão Modificada:

- A. Use na Página de Título (e nas capas, se houver) um título distinto do título do Documento, e dos de versões anteriores (os quais devem, se houver algum, ser listados na seção “Histórico” do Documento). Você pode usar o mesmo título de uma versão anterior se o editor original dessa versão assim o permitir.
- B. Liste na Página de Título, como autores, uma ou mais pessoas ou entidades responsáveis pela autoria das modificações na Versão Modificada, juntamente com pelo menos cinco dos autores principais do Documento (todos seus autores principais, se houver menos que cinco), a menos que eles lhe desobriguem dessa exigência.
- C. Mencione na Página de Título o nome do editor da Versão Modificada, como seu editor.
- D. Preserve todas as informações de copyright do Documento.
- E. Adicione as informações de copyright adequadas para suas modificações ao lado das outras informações de copyright.
- F. Inclua, imediatamente após as informações de copyright, informações de licença concedendo ao público permissão para usar a Versão Modificada sob os termos desta Licença, na forma mostrada no Adendo abaixo.
- G. Preserve, nesse aviso de licença, as listas completas de Seções Invariáveis e os Textos de Capa necessários fornecidos no aviso de licença do Documento.
- H. Inclua uma cópia inalterada desta Licença.
- I. Preserve a seção intitulada “Histórico”, Preserve seu Título e adicione à seção um item mencionando pelo menos o título, o ano, os novos autores e o editor da Versão Modificada, como mostrado na Página de Título. Se não houver uma seção intitulada “Histórico” no

Documento, crie uma mencionando o título, o ano, os autores e o editor do Documento, como mostrado na Página de Título; em seguida, adicione um item que descreva a Versão Modificada, como mencionado na frase anterior.

- J. Preserve a localização de rede, se houver, indicada no Documento para acesso público a uma cópia Transparente deste e, da mesma maneira, as localizações de rede indicadas no Documento para versões anteriores nas quais ele se baseia. Essas informações podem ser incluídas na seção “Histórico”. Você pode omitir uma localização de rede para um trabalho que foi publicado pelo menos quatro anos antes do Documento em si, ou se o editor original da versão à qual a localização se refere der permissão.
- K. Para qualquer seção intitulada “Agradecimentos” ou “Dedicatória”, Preserve o Título da seção, e preserve dentro da seção toda a essência e o tom de cada um dos agradecimentos e/ou dedicatórias aos colaboradores nela mencionados.
- L. Preserve todas as Seções Invariantes do Documento, inalteradas em seu texto e títulos. Números de seção ou o equivalente não são considerados parte dos títulos das seções.
- M. Apague qualquer seção intitulada “Apoio”. Tal seção não pode ser incluída na Versão Modificada.
- N. Não modifique o título de qualquer seção existente para “Apoio” nem de forma a gerar conflito com o título de qualquer Seção Invariável.
- O. Preserve as Isenções de Responsabilidade quanto a Garantia.

Se a Versão Modificada incluir novas seções iniciais ou apêndices que sejam qualificados como Seções Secundárias, e não contiver material copiado do Documento, você poderá, a seu critério, tornar invariantes algumas dessas seções ou todas elas. Para fazer isso, adicione seus títulos à lista de Seções Invariáveis no aviso de licença da Versão Modificada. Esses títulos devem ser diferentes de outros títulos de seção.

Você pode adicionar uma seção intitulada “Apoio”, desde que ela não contenha nada além do apoio recebido para sua Versão Modificada por várias partes; por exemplo, notas do revisor ou de que o texto foi aprovado por uma organização como a definição oficial de um padrão.

Você pode adicionar uma passagem de até cinco palavras como Texto de Folha de Rosto, e uma passagem de até 25 palavras como Texto de Contracapa, ao fim da lista de Textos de Capa na Versão Modificada. Somente uma passagem de Texto de Folha de Rosto e uma de Texto de Contracapa pode ser adicionada por (ou através de arranjos feitos por) uma entidade qualquer. Se o Documento já incluir um texto de capa para a mesma capa, anteriormente incluído por

você ou por arranjo feito pela mesma entidade em cujo nome você está agindo, não será possível adicionar outro, mas sim substituir o antigo, com permissão explícita do editor anterior que o incluiu.

O(s) autor(es) e editor(es) do Documento, por esta Licença, não dá(ão) permissão para seu(s) nome(s) ser(em) usado(s) para publicidade ou defesa ou apoio implícito para qualquer Versão Modificada.

5. COMBINANDO DOCUMENTOS

Você pode combinar o documento com outros documentos publicados sob esta Licença, sob os termos definidos na seção 4 acima para versões modificadas, desde que você inclua na combinação todas as Seções Invariantes de todos os documentos originais, sem modificações, e as liste como Seções Invariantes de seu trabalho combinado, na sua nota de licença, e que você preserve todas as Notas de Garantia.

O trabalho combinado somente precisa conter uma cópia desta Licença, e várias Seções Invariantes idênticas podem ser substituídas por uma única cópia. Se houver várias Seções Invariantes com o mesmo nome, mas com conteúdos diferentes, torne o título de cada uma dessas seções único, adicionando ao fim dele, entre parênteses, o nome do autor ou editor original da seção, se conhecido, ou então um número exclusivo. Faça o mesmo ajuste nos títulos de seção na lista de Seções Invariantes nas informações de licença do trabalho combinado.

Na combinação, você deve combinar quaisquer seções intituladas “Histórico” nos vários documentos originais, formando uma seção intitulada “Histórico”; do mesmo modo, combine quaisquer seções intituladas “Agradecimentos” e quaisquer seções intituladas “Dedicatória”. Você deve eliminar todas as seções intituladas “Apóio”.

6. COLEÇÕES DE DOCUMENTOS

Você pode fazer uma coleção consistindo do Documento e outros documentos publicados sob esta Licença, e substituir as cópias individuais desta Licença, nos vários documentos, por uma única cópia a ser incluída na coleção, desde que você siga as regras desta Licença para cópias literais de cada documento em todos os outros aspectos.

Você pode extrair um único documento dessa coleção e distribuí-lo individualmente sob esta Licença, desde que insira uma cópia desta Licença no documento extraído e siga esta Licença em todos os outros aspectos com relação à cópia literal do documento.

7. AGREGAÇÃO A TRABALHOS INDEPENDENTES

Uma compilação do Documento, ou seus derivados com outros documentos ou trabalhos separados e independentes, dentro de ou junto a um volume de uma mídia de armazenamento ou distribuição, constituirá um “agregado” se os direitos autorais resultantes da compilação não forem usados para limitar os direitos legais dos usuários dessa compilação além do que os trabalhos individuais permitem. Quando o Documento é incluído em um agregado, a Licença não se aplica a outros trabalhos no agregado que não sejam, por sua vez, derivados do Documento. Se o requisito do Texto de Capa da seção 3 for aplicável a estas cópias do Documento e, ainda, se o Documento for menor do que a metade do agregado inteiro, os Textos de Capa do Documento poderão ser colocados em capas que encerrem o Documento dentro do agregado, ou no equivalente eletrônico das capas, se o Documento estiver em formato eletrônico. Caso contrário, eles deverão aparecer como capas impressas que envolvam o agregado inteiro.

8. TRADUÇÃO

A tradução é considerada um tipo de modificação, portanto, você pode distribuir traduções do Documento em conformidade com os termos da seção 4. A substituição de Seções Invariantes por traduções requer permissão especial de seus detentores de direitos autorais, mas você pode incluir traduções de algumas ou de todas as Seções Invariantes, além das versões originais dessas Seções Invariantes. Você pode incluir uma tradução desta Licença e todos os avisos de licença no Documento, bem como qualquer Isenção de Responsabilidade quanto a Garantia, desde que também inclua a versão original em Inglês desta Licença e as versões originais dos avisos e das isenções de responsabilidade. Em caso de discordância entre a tradução e a versão original desta Licença ou informações de licença ou isenção de responsabilidade, a versão original prevalecerá. Se uma seção do Documento for intitulada “Agradecimentos”, “Dedicatória” ou “Histórico”, o requisito (seção 4) para Preservar seu Título (seção 1) normalmente exigirá a mudança do título em si.

9. REVOGAÇÃO

Você não pode copiar, modificar, sublicenciar ou distribuir o Documento, exceto como expressamente previsto por esta Licença. Qualquer outra tentativa de copiar, modificar, sublicenciar ou distribuir o Documento é anulada, e implicará a revogação automática de seus

direitos sob esta Licença. Porém, terceiros a quem você forneceu cópias ou direitos sob os termos desta Licença não terão suas licenças revogadas, desde que permaneçam em total concordância com ela.

10. REVISÕES FUTURAS DESTA LICENÇA

A Free Software Foundation pode publicar ocasionalmente novas versões revisadas da Licença de Documentação Livre GNU. As novas versões serão semelhantes à versão atual, mas poderão diferir em detalhes para atender a novos problemas ou situações. Consulte <https://www.gnu.org/copyleft/>.

A cada versão da Licença é atribuído um número de versão exclusivo. Se o Documento especificar que um número de versão específico desta Licença, “ou de qualquer versão posterior”, aplica-se a ele, você terá a opção de seguir os termos e condições da versão especificada ou de qualquer versão posterior que tenha sido publicada (não como rascunho) pela Free Software Foundation. Se o documento não especificar um número de versão desta Licença, você poderá escolher qualquer versão já publicada (não como rascunho) pela Free Software Foundation.

ADENDO: Como usar esta Licença em seus documentos

```
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".
```

Se você tiver Seções Invariantes, Textos de Capa Frontal e Textos de Contracapa, substitua a linha “with...Texts” por isto:

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

Se você tiver Seções Invariantes sem Textos de Capa ou alguma outra combinação das três, utilize essas duas alternativas para se adequar à situação.

Se seu documento contiver exemplos incomuns de código de programação, recomendamos publicar esses exemplos paralelamente, sob a licença de software livre de sua preferência como, por exemplo, a Licença Pública Geral GNU, para permitir seu uso em software livre.