SELinux

O QUE É?

O tópico apresenta informações básicas sobre o Security-Enhanced Linux.

POR QUÊ?

Para compreender o SELinux e saber como configurá-lo no SLE Micro.

DEDICAÇÃO

A leitura leva aproximadamente 40 minutos.

Data de Publicação: 11/12/2025

Conteúdo

1 Sobre o SELinux

O SELinux foi desenvolvido como uma solução de segurança adicional do Linux que usa a estrutura de segurança do kernel Linux. O objetivo era permitir uma política de segurança mais granular que fosse além dos Controles de Acesso Discricionários (DAC, Discretionary Access Controls) padrão: as permissões de arquivo tradicionais de proprietário/grupo/globais e leitura/gravação/execução.

O SELinux usa rótulos anexados a objetos (por exemplo, arquivos e soquetes de rede) e toma decisões de acesso com base neles.

A ação padrão do SELinux é negar qualquer acesso. O SELinux apenas permite ações que foram especificamente autorizadas em sua política. Outro recurso do SELinux que reforça a segurança é que ele permite o confinamento rigoroso de processos até o ponto em que os processos não conseguem acessar arquivos de outros processos no mesmo sistema.

O SELinux foi projetado para aprimorar as soluções de segurança existentes, não para substituí-las. Por exemplo, o controle de acesso discricionário (DAC) ainda é aplicado, mesmo que o sistema use o SELinux. Se o DAC negar o acesso primeiro, o SELinux não será usado, pois o acesso já foi bloqueado por outro mecanismo.

2 Obtendo o SELinux

O SELinux é instalado por padrão durante a instalação do SLE Micro pelo YaST ou faz parte das imagens predefinidas.

Se o SELinux não está configurado no sistema, execute o seguinte comando:

```
# transactional-update setup-selinux
```

Reinicialize o sistema após a conclusão do comando. O comando instala a política do SELinux, se ela não estiver instalada, define o modo `enforcing` do SELinux e reconstrói o `initrd`.

3 Modos do SELinux

O SELinux pode ser executado em um destes três modos: `disabled`, `permissive` ou `enforcing`.

O uso do modo `disabled` significa que nenhuma regra da política do SELinux é aplicada e o sistema não está protegido. Portanto, não recomendamos o uso do modo `disabled`.

No modo `permissive`, o SELinux está ativo, a política de segurança é carregada, o sistema de arquivos é rotulado e as entradas de negação de acesso são registradas. No entanto, a política não é imposta e, portanto, nenhum acesso é, de fato, negado.

No modo `enforced`, a política de segurança é aplicada. Cada acesso que não é explicitamente permitido pela política é negado.

Para obter informações sobre como alternar entre os modos do SELinux, consulte a *Seção 3.1, "Mudando o modo do SELinux"*.

3.1 Mudando o modo do SELinux

Você pode alternar o modo do SELinux temporariamente ou permanentemente.

3.1.1 Mudando o modo do SELinux temporariamente

Para definir o SELinux como `permissive` ou `enforcing` temporariamente, use o comando **`setenforce`**.

O comando **`setenforce`** tem a seguinte sintaxe:

```
# setenforceMODE_ID
```

em que *`MODE_ID`* é *`0`* para o modo `permissive` ou *`1`* para o modo `enforced`.

Lembre-se de que você não pode desabilitar o SELinux usando o comando **`setenforce`**.

3.1.2 Mudando o modo do SELinux permanentemente

Para fazer mudanças no modo do SELinux que persistam após a reinicialização do sistema, edite o arquivo de configuração `/etc/selinux/config`. Nesse arquivo, você também pode desabilitar o SELinux no sistema. No entanto, essa ação não é recomendada. Se o SELinux estiver possivelmente causando problemas no sistema, alterne para o modo `permissive` e depure o sistema.

No arquivo `/etc/selinux/config`, mude o valor de `SELINUX` para `disabled`, `permissive` ou `enforced` da seguinte maneira:

```
SELINUX=disabled
```

As mudanças no arquivo serão aplicadas após a próxima reinicialização.

Nota: Rotulando novamente o sistema após alternar do modo `disabled`

Se você desabilitar e, mais tarde, habilitar o SELinux no sistema, certifique-se de rotular novamente o sistema. Quando o SELinux está desabilitado, e você faz mudanças no sistema de arquivos, as mudanças não são mais refletidas no contexto (por exemplo, novos arquivos não têm nenhum contexto). Portanto, você precisa rotular novamente o sistema usando o comando **`restorecon`**, o parâmetro de boot `autorelabel` ou criando um arquivo que acionará o novo rótulo na próxima inicialização. Para criar o arquivo, execute o seguinte comando:

```
# touch /etc/selinux/.autorelabel
```

Após a reinicialização, o arquivo `/etc/selinux/.autorelabel` é substituído por outro arquivo de flag `/etc/selinux/.relabelled`, para evitar que o novo rótulo seja aplicado às reinicializações subsequentes.

3.1.3 Verificando o modo do SELinux ativo

Para verificar o modo, execute o seguinte comando:

```
# getenforce
```

O comando deve retornar `permissive` ou `enforced`, dependendo do *`MODE_ID`* inserido.

3.2 Verificando se o SELinux está funcionando

Se você está fazendo mudanças na configuração, pode ser útil alternar para o modo permissivo. Durante esse período, os usuários podem rotular os arquivos incorretamente e, portanto, causar problemas ao reverter para o modo de imposição.

Para retornar o sistema ao estado seguro, execute as seguintes etapas:

1. Redefina o contexto de segurança:

```
> sudo restorecon -R /
```

2. Alterne para o modo de imposição definindo o `SELINUX=enforcing` em `/etc/selinux/config`.

3. Reinicialize o sistema e efetue login novamente.

4. Execute o comando **`sestatus -v`**. Ele deve retornar uma saída semelhante a esta:

```
> sudosestatus -v
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     requested(insecure)
Max kernel policy version:      33

Process contexts:
Current context:                unconfined_u:unconfined_r:unconfined_t:s0-
s0:c0.c1023
Init context:                   system_u:system_r:init_t:s0
/usr/sbin/sshd                  system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal:           unconfined_u:object_r:user_tty_device_t:s0
/etc/passwd                     system_u:object_r:passwd_file_t:s0
/etc/shadow                     system_u:object_r:shadow_t:s0
/bin/bash                       system_u:object_r:shell_exec_t:s0 \
                                -> system_u:object_r:shell_exec_t:s0
/bin/login                      system_u:object_r:login_exec_t:s0
/bin/sh                         system_u:object_r:bin_t:s0 \
                                -> system_u:object_r:shell_exec_t:s0
/sbin/agetty                    system_u:object_r:bin_t:s0 \
                                -> system_u:object_r:getty_exec_t:s0
/sbin/init                      system_u:object_r:bin_t:s0 -> \
                                system_u:object_r:init_exec_t:s0
/usr/sbin/sshd                  system_u:object_r:sshd_t:s0
```

5. Se o sistema não estiver funcionando apropriadamente, consulte os arquivos de registro em `/var/log/audit/audit.log`. Para obter mais detalhes, consulte SELinux troubleshooting (https://documentation.suse.com/smart-supported.html).

4 Contexto de segurança do SELinux

O contexto de segurança é um conjunto de informações atribuídas a um arquivo ou processo. Ele consiste em usuário, função, tipo, nível e categoria do SELinux. Essas informações são usadas para tomar decisões de controle de acesso.

CAMPOS DE CONTEXTO DO SELINUX

Usuário do SELinux

Uma identidade definida na política que é autorizada para um conjunto específico de funções e para uma faixa de *níveis* específica. Cada usuário do Linux é mapeado para apenas um usuário do SELinux. No entanto, um usuário do SELinux pode ter várias funções.

O SELinux não usa a lista de contas de usuário mantida pelo Linux no `/etc/passwd`, mas usa o próprio banco de dados e mapeamento. Por convenção, o nome da identidade recebe o sufixo `_u`, por exemplo: `user_u`.

Quando uma nova conta do Linux é criada e o usuário do SELinux não é atribuído à conta, o usuário do SELinux padrão é usado. Normalmente, o valor padrão é `unconfined_u`. Para ver um procedimento sobre como mudar o valor padrão, consulte a *Seção 7.5.2, "O comando* **`semanage login`**".

role

Define um conjunto de permissões que um usuário pode receber. A função atribuída a um usuário define os *tipos* que ele pode acessar. Por convenção, o nome da função recebe o sufixo `_r`, por exemplo: `system_r`.

type

O tipo transmite informações sobre como arquivos e processos específicos podem interagir. Um processo consiste em arquivos com um tipo concreto do SELinux e não pode acessar arquivos de outro tipo. Por convenção, o nome do tipo recebe o sufixo `_t`, por exemplo: `var_t`.

level

Um atributo opcional que especifica a faixa de níveis de permissão na segurança multinível.

category

Um atributo opcional que permite adicionar categorias a processos, arquivos e usuários. Um usuário pode acessar arquivos que tenham a mesma categoria.

Veja abaixo um exemplo de contexto do SELinux:

```
allow user_t bin_t:file {read execute gettattr};
```

Esta regra de exemplo especifica que o usuário com o tipo de contexto `user_t` (esse usuário é chamado de objeto de origem) tem permissão para acessar objetos do *arquivo* de classe com o tipo de contexto `bin_t` (o destino), usando as permissões `read`, `execute` e `getattr`.

5 Visão geral da política do SELinux

A política é o principal componente do SELinux. A política do SELinux define regras que especificam quais objetos podem acessar quais arquivos, diretórios, portas e processos em um sistema. Para fazer isso, um contexto de segurança é definido para todos eles.

Uma política do SELinux contém um grande número de regras. Para torná-las mais gerenciáveis, as políticas costumam ser divididas em módulos. Isso permite que o administrador ative ou desative a proteção para diferentes partes do sistema.

Ao compilar a política para seu sistema, você pode trabalhar com uma política modular ou monolítica, em que uma política extensa é usada para proteger tudo no sistema. É altamente recomendável usar uma política modular em vez de uma monolítica. As políticas modulares são muito mais fáceis de gerenciar.

O SLE Micro já vem com a política `targeted` do SELinux.

5.1 Trabalhando com módulos do SELinux

Como administrador, você pode ativar ou desativar módulos. Isso poderá ser útil se você quiser desabilitar apenas uma parte da política do SELinux e não quiser executar um serviço específico sem a proteção do SELinux.

Para ver todos os módulos de política do SELinux em uso, execute o comando:

```
semodule -l
```

Após obter o nome do módulo que deseja desativar, execute o comando:

```
> sudo semodule -d MODULENAME
```

Para ativar o módulo de política, execute o comando:

```
> sudo semodule -e MODULENAME
```

5.2 Criando políticas para contêineres

O SLE Micro é fornecido com uma política que, por padrão, não permite que os contêineres acessem arquivos que não façam parte dos dados dos contêineres. Por outro lado, todo o acesso à rede é permitido. Normalmente, os contêineres são criados com montagens de vinculação e devem ser capazes de acessar outros diretórios, como `/home` ou `/var`. Talvez você queira ter a opção de permitir o acesso a esses diretórios ou, ao contrário, restringir o acesso de determinadas portas ao contêiner, mesmo que o SELinux seja usado no sistema. Nesse caso, você precisa criar novas regras de política que habilitem ou desabilitem o acesso. Para essa finalidade, o SLE Micro oferece a ferramenta Udica.

O procedimento a seguir descreve como criar uma política personalizada para seus contêineres:

1. Verifique se o SELinux está no modo de imposição. Para obter informações detalhadas, consulte a *Seção 3.1, "Mudando o modo do SELinux"*.

2. Inicie um contêiner usando os seguintes parâmetros:

   ```
   # podman run -v /home:/home:rw -v /var/:/var/:rw -p 21:21 -it sle15 bash
   ```

   O contêiner é executado com a política padrão que não permite acesso aos pontos de montagem, mas não restringe outras portas.

3. Você pode sair do contêiner.

4. Obtenha o ID do contêiner:

   ```
   # podman ps -a

   CONTAINER ID  IMAGE
               COMMAND     CREATED        STATUS            PORTS               NAMES
   e59f9d0f86f2  registry.opensuse.org/devel/bci/tumbleweed/containerfile/opensuse/
   bci/ruby:latest  /bin/bash   8 minutes ago  Up 8 seconds ago  0.0.0.0:21->21/tcp
    zen_ramanujan
   ```

5. Crie um arquivo JSON que o Udica usará para criar uma política personalizada para o contêiner:

   ```
   # podman inspect e59f9d0f86f2 >OUTPUT_JSON_FILE
   ```

   Por exemplo, substitua *`OUTPUT_JSON_FILE`* por `container.json`.

6. Execute o Udica para gerar uma política de acordo com os parâmetros do contêiner:

```
# udica -jOUTPUT_JSON_FILECUSTOM_CONTAINER_POLICY
```

Por exemplo:

```
# udica -j container.json custom_policy
```

7. De acordo com as instruções fornecidas, carregue os módulos de política executando:

```
# semodule -i custom_policy.cil /usr/share/udica/templates/
{base_container.cil,net_container.cil,home_container.cil}
```

8. Execute um contêiner com o novo módulo de política usando a opção `--security-opt` da seguinte maneira:

```
# podman run --security-opt label=type:custom_policy.process -v /home:/home:rw -v /
var/:/var/:rw -p 21:21 -it sle15 bash
```

6 Boolianos do SELinux

Os boolianos do SELinux suportam uma abordagem flexível de gerenciamento de políticas. Por exemplo, eles permitem desabilitar uma política específica em um servidor e manter a mesma política ativa em outro. Em outras palavras, um booliano pode ser considerado como um switch de uma regra de política. Em vez de mudar uma política específica, você pode desativá-la. No código da política, os boolianos são chamados de *ajustáveis*. Como estão incluídos na política, eles ficam disponíveis assim que a política é carregada.

As mudanças no valor dos boolianos podem ser persistentes ou temporárias, durando até o término da sessão.

O SELinux oferece ferramentas que permitem listar e ver detalhes ou mudar o estado dos boolianos. Consulte as seções a seguir para obter detalhes.

6.1 Trabalhando com boolianos

6.1.1 Listando boolianos

Você pode usar o comando **getsebool** ou **semanage** para listar os boolianos definidos no momento. Para listar todos os boolianos definidos no momento, junto com os respectivos estados, execute o seguinte comando:

```
# getsebool -a

abrt_anon_write --> off
abrt_handle_event --> off
abrt_upload_watch_anon_write --> on
...
```

Para obter mais detalhes sobre boolianos específicos, você pode usar o comando **semanage** da seguinte maneira:

```
# semanage boolean -l

SELinux boolean                State   Default     Description

abrt_anon_write                (off  ,  off)       Allow abrt to anon write
abrt_handle_event              (off  ,  off)       Allow abrt to handle event
abrt_upload_watch_anon_write   (on   ,   on)       Allow abrt to upload watch anon write
```

Para saber o status de cada booliano, você pode usar o seguinte comando:

```
# getsebool BOOLEAN_NAME
```

Se preferir, use o comando **grep** na saída de **semanage boolean**:

```
# semanage boolean -l | grep BOOLEAN_NAME
```

6.1.2 Alternando boolianos

É possível usar os comandos **setsebool** e **semanage** para alternar o valor dos boolianos. Você pode mudar o status do booliano de forma persistente ou apenas temporária até o término da sessão. Para mudar o valor de um booliano temporariamente, execute o seguinte comando:

```
# setsebool BOOLEAN_NAME BOOLEAN_VALUE
```

em que *BOOLEAN_VALUE* é `on` ou `off`.

Para mudar o valor de um booliano persistentemente, execute o seguinte comando:

```
# setsebool -PBOOLEAN_NAMEBOOLEAN_VALUE
```

Se preferir, use o comando **`semanage`**:

```
# semanage boolean -m --BOOLEAN_VALUEBOOLEAN_NAME
```

em que *BOOLEAN_VALUE* é `on` ou `off`.

Um único booliano pode habilitar ou desabilitar várias regras de política. Para ver quais regras de política são habilitadas ou desabilitadas por quais boolianos, use a ferramenta **`sedispol`**, que pode analisar o arquivo de política:

```
# sedispol /etc/selinux/targeted/policy/policy.32
```

Como as regras de política geralmente são enormes, recomendamos configurar um arquivo de saída selecionando `f` e especificando um nome de arquivo. Após especificar o nome de arquivo, pressione `6`. Em seguida, você pode inspecionar o arquivo.

7 Ferramentas para gerenciar o SELinux

O SLE Micro oferece a você ferramentas para gerenciar o SELinux em seu sistema. Se as ferramentas descritas abaixo não estiverem instaladas em seu sistema, instale-as executando:

```
# transactional-update pkg install policycoreutils-python-utils
```

Após a instalação bem-sucedida, reinicialize o sistema.

7.1 Usando a opção Z

No sistema em que o SELinux está instalado e configurado, você pode usar `-Z` para comandos regulares, como **`ls`**, **`id`** ou **`ps`**. Usando essa opção, você pode exibir o contexto de segurança de arquivos ou processos. Por exemplo, com o comando **`ls`**:

```
> ls -Z /etc/shadow

        system_u:object_r:shadow_t:s0 /etc/shadow
```

7.2 O comando **chcon**

O nome do comando **chcon** significa mudança de contexto. O comando pode mudar o contexto de segurança completo de um arquivo para o valor fornecido na CLI ou pode mudar partes do contexto. Se preferir, insira um arquivo que sirva como referência.

Para mudar o contexto de segurança completo de um arquivo, a sintaxe do comando é a seguinte:

```
# chconSECURITY_CONTEXTFILENAME
```

em que:

- *SECURITY_CONTEXT* está no formato: *SELinux_USER*:*ROLE*:*TYPE*:*LEVEL*:*CATEGORY*. Por exemplo, o contexto pode ser: *system_u:object_r:httpd_config_t:s0*.
- *FILENAME* é um caminho para o arquivo cujo contexto deve ser mudado.

Para definir um contexto de segurança de acordo com um arquivo fornecido que serve como referência, execute o **chcon** da seguinte maneira:

```
# chcon --reference=REFERENCE_FILEFILENAME
```

em que:

- *REFERENCE_FILE* é um caminho para um arquivo que deve ser usado como referência.
- *FILENAME* é um caminho para o arquivo cujo contexto deve ser mudado.

Se preferir, mude apenas uma parte do contexto de segurança. A sintaxe geral do comando **chcon** é a seguinte:

```
# chconCONTEXT_OPTIONCONTEXT_PARTFILENAME
```

As opções e os argumentos têm o seguinte significado:

- dependendo da parte do contexto, *CONTEXT_OPTION* pode ser qualquer um dos seguintes:

  `-u` **resp** `--user`
  : indica que um contexto de usuário do SELinux será mudado no arquivo fornecido:

    ```
    # chcon -u system_u logind.conf
    ```

  `-r` **resp** `--role`
  : apenas a parte da função será mudada no contexto do arquivo fornecido:

    ```
    # chcon -r object_r logind.conf
    ```

`-t` resp `--type`

apenas a parte do tipo será mudada no contexto do arquivo fornecido:

```
# chcon -t etc_t logind.conf
```

`-l` resp `--range`

apenas a parte da faixa do contexto de segurança será mudada:

```
# chcon -l s0 logind.conf
```

- *`CONTEXT_PART`* é o valor específico do contexto de segurança que será definido.
- *`FILENAME`* é um caminho para o arquivo cujo contexto será mudado.

Nota: Usando **`chcon`** em links simbólicos

Por padrão, quando você muda o contexto de segurança em um link simbólico, o contexto do destino do link é mudado e o contexto do link simbólico **não** é mudado. Para forçar o **`chcon`** a mudar o contexto do link simbólico, e não o destino do link, use a opção `--no-dereference` mostrada abaixo:

```
# chcon --no-dereference -u system_u -t etc_t network.conf
```

Você pode mudar o contexto de todos os arquivos em um diretório usando a opção recursiva:

```
# chcon --recursive  system_u:object_r:httpd_config_t:s0 conf.d
```

7.3 Comandos **`getenforce`** e **`setenforce`**

O comando **`getenforce`** retorna o modo do SELinux atual: `Enforcing`, `Permissive` ou `Disabled`.

```
# getenforce

Permissive
```

O comando **`setenforce`** muda temporariamente o modo do SELinux para imposição ou permissivo. Não é possível usar esse comando para desabilitar o SELinux. Lembre-se de que a mudança permanece apenas até a próxima reinicialização. Para mudar o estado permanentemente, siga a descrição na *Seção 3.1, “Mudando o modo do SELinux”*.

```
# setenforceMODE_ID
```

em que *MODE_ID* é *0* para o modo `permissive` ou *1* para o modo `enforced`.

7.4 O script **fixfiles**

O script permite que você execute as seguintes tarefas com o contexto de segurança:

- verificar se o contexto está correto
- mudar qualquer rótulo de contexto de arquivo incorreto
- renomear seu sistema se você adicionar uma nova política

Veja a seguir a sintaxe do script:

```
# fixfiles [OPTIONS] ARGUMENT
```

em que:

- *OPTIONS* pode ser o seguinte:

  `-l` *LOGFILE*
  : grava a saída no arquivo fornecido

  `-o` *OUTPUT_FILE*
  : grava no arquivo de saída fornecido os nomes de todos os arquivos cujo contexto seja diferente do padrão

  `-F`
  : força a redefinição do contexto

- *ARGUMENT* pode ser um dos seguintes:

  `check`
  : mostra o contexto do arquivo anterior e atual de um rótulo incorreto sem realizar nenhuma mudança

  `relabel`
  : reclassifica contextos de arquivo incorretos de acordo com a política carregada no momento

  `restore`
  : restaura contextos de arquivo incorretos aos valores padrão

verify
: lista todos os arquivos com rótulos de contexto de arquivo incorretos sem realizar nenhuma mudança

7.5 O comando **semanage**

O comando **semanage** pode ser usado para configurar partes da política sem a necessidade de recompilar a política de fontes. O comando permite executar as seguintes tarefas:

- gerenciar boolianos usando o argumento `boolean`. Para obter detalhes sobre boolianos, consulte a *Seção 6.1, "Trabalhando com boolianos"*.
- ajustar o contexto dos arquivos usando o argumento `fcontext`
- gerenciar mapeamentos de usuários usando o argumento `login`
- gerenciar usuários do SELinux usando o argumento `user`
- gerenciar módulos de política do SELinux usando o argumento `module`

A sintaxe geral do comando tem a seguinte aparência:

```
# semanageARGUMENTOPTIONS [OBJECT_NAME]
```

em que:

- *ARGUMENT* é um dos seguintes: **login**, **user**, **fcontext**, **boolean** e **module**.
- *OPTIONS* depende do *ARGUMENT* especificado. As opções comuns estão descritas em *Opções comuns*.
- *OBJECT_NAME*, dependendo do *ARGUMENT* especificado, pode ser um nome de login, de módulo ou de arquivo ou um usuário do SELinux.

OPÇÕES COMUNS

`-a`, `--add`
: adiciona um objeto fornecido

`-h`, `--help`
: imprime o comando de ajuda

--extract
: exibe os comandos que foram usados para mudar o sistema (boolianos, contexto de arquivo etc.).

`-l`, `--list`
: lista todos os objetos

`-m`, `--modify`
: modifica o objeto fornecido

`-n`, `--noheading`
: modifica a saída da operação de listagem omitindo os cabeçalhos.

`-s`, `--seuser`
: especifica o usuário do SELinux.

Outras opções são específicas de determinados comandos **`semanage`** e estão descritas nas seções correspondentes.

7.5.1 O comando `semanage fcontext`

Usando o comando **`semanage fcontext`**, você pode executar as seguintes tarefas:

- consultar definições de contexto de arquivo
- adicionar contextos a arquivos
- adicionar suas próprias regras

As mudanças feitas no contexto do arquivo usando o comando **`semanage fcontext`** não exigem modificações ou recompilação da política.

Além das opções comuns descritas em *Opções comuns*, o comando **`semanage fcontext`** usa as seguintes opções:

`-e`, `--equal`
: a opção permite usar o contexto do caminho fornecido para rotular arquivos em um diretório diferente (o caminho de destino especificado). Por exemplo, para atribuir o mesmo contexto que `/home` tem a um diretório pessoal alternativo `/export/home`. Se você usar essa opção, precisará inserir o caminho de origem e de destino:

```
# semanage fcontext -a -e /home /export/home
```

`-f`, `--ftype`
: especifique um tipo de arquivo. Use um dos seguintes valores:

  - `a`: todos os arquivos, que também é o valor padrão
  - `b`: um dispositivo de blocos
  - `c`: um dispositivo de caracteres
  - `d`: um diretório
  - `f`: arquivos regulares
  - `l`: um link simbólico
  - `p`: um named pipe
  - `s`: um soquete

7.5.2 O comando **`semanage login`**

O **`semanage login`** permite executar as seguintes tarefas:

- Mapear usuários do Linux em um determinado usuário do SELinux. Por exemplo, para mapear o usuário do Linux *tux* em `sysadm_u`, execute o comando:

  ```
  # semanage login -a -s sysadm_u tux
  ```

- Mapear um grupo de usuários do Linux em um determinado usuário do SELinux. Por exemplo, para mapear usuários do grupo *writers* em `user_u`, execute o comando:

  ```
  # semanage login -a -s user_u %writers
  ```

  O grupo é listado na saída de **`semanage login -l`**, prefixado com o caractere %. Lembre-se de que o grupo de usuários deve ser o principal, pois o mapeamento de usuários do SELinux em grupos Suplementares pode resultar em mapeamentos incompatíveis.

  ```
  # semanage login -m -s staff_u %writers
  ```

- Mapear usuários do Linux em uma faixa de segurança MLS/MCS específica do SELinux.

- Modificar o mapeamento já criado. Para isso, basta substituir a opção `-a` por `-m` nos comandos anteriores.
- Definir o usuário padrão do SELinux para novos usuários do Linux. O usuário padrão do SELinux costuma ser `unconfined_u`. Para mudar o valor para `staff_u`, execute o comando:

```
# semanage login -m -s staff_u __default__
```

7.5.3 O comando `semanage boolean`

O comando **`semanage boolean`** é usado para controlar os boolianos na política do SELinux.

A sinopse do comando tem a seguinte aparência:

```
semanage boolean [-h] [-n]  [ --extract |
       --deleteall | --list [-C] | --modify ( --on | --off | -1 | -0 ) boolean ]
```

Além das opções comuns, você pode usar as seguintes opções específicas do comando **`semanage boolean`**:

--list -C
: Para exibir uma lista de modificações locais em boolianos.

-m --on | -1
: Para ativar o booliano fornecido.

-m --off | -0
: Para desativar o booliano fornecido.

-D, --deleteall
: Para apagar todas as modificações locais em boolianos.

O uso mais comum do comando é ativar ou desativar um booliano específico. Por exemplo, para ativar o booliano `authlogin_yubikey`, execute:

```
# semanage boolean -m on authlogin_yubikey
```

7.5.4 O comando `semanage user`

O comando **`semanage user`** controla o mapeamento entre o usuário do SELinux e as funções e os níveis MLS/MCS.

Além das opções comuns descritas em *Opções comuns*, o comando **`semanage use`** usa as seguintes opções:

-R [ROLES], --roles [ROLES]
: Uma lista de funções do SELinux. Você pode colocar várias funções entre aspas duplas e separá-las com espaços ou usar `-R` várias vezes.

Usando esse comando, você pode executar as seguintes tarefas:

- Listar o mapeamento de usuários do SELinux em funções executando:

```
# semanage user -l
```

- Mudar as funções atribuídas ao usuário `user_u` do SELinux:

```
# semanage user -m -R "system_r unconfined_r user_r"
```

- Atribuir para `admin_u` a função `staff_r` e a uma categoria `s0`:

```
# semanage user -a -R "staff_r -r s0 admin_u
```

- Criar um novo usuário do SELinux, por exemplo, `admin_u` com a função `staff_r`. Você também precisa definir o prefixo de rótulo para esse usuário usando `-P`:

```
# semanage user -a -R "staff_r" -P admin admin_u
```

7.5.5 O comando `semanage module`

O comando **`semanage module`** pode instalar, remover, desabilitar ou habilitar módulos de política do SELinux.

Além das opções comuns descritas em *Opções comuns*, o comando **`semanage fcontext`** usa as seguintes opções:

`-d`, `--disable`
: Para desabilitar o módulo de política do SELinux fornecido:

```
# semanage module --disable MODULE_NAME
```

`-e`, `--enable`
: Para habilitar o módulo de política do SELinux fornecido:

```
# semanage module --enable MODULE_NAME
```

7.6 O comando **sestatus**

O **sestatus** obtém o status de um sistema em que o SELinux está sendo executado.

A sintaxe genérica do comando é a seguinte:

```
sestatus [OPTION]
```

Quando executado sem opções e argumentos, o comando gera as seguintes informações:

```
# sestatus

SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     requested (insecure)
Max kernel policy version:      33
```

O comando pode ter as seguintes opções:

-b

Exibe o status dos boolianos no sistema.

-v

Exibe o contexto de segurança dos arquivos e processos listados no arquivo `/etc/sestatus.conf`.

8 Informações legais

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 afirmando 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 (quantos 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 “Apoio”.

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.