

Laboratório de Redes de Computadores e Sistemas Operacionais

Linux: Adicionando Usuários

Fabricio Breve

Introdução

- Administradores precisam ter um entendimento completo de como funcionam contas Linux
- Contas usadas com pouca frequência ou com senhas fáceis são os principais alvos de hackers
- Mesmo que você use ferramentas automatizadas para criação de contas é importante compreender as modificações que essas ferramentas estão realizando

O arquivo `/etc/passwd`

- Representa uma lista de usuários reconhecidos pelo sistema. O sistema consulta este arquivo no momento do login para verificar UID e senha
- Cada linha no arquivo indica um usuário e contém sete campos:
 - Nome de login
 - Senha criptografada (a menos que um arquivo de senha-sombra seja utilizado)
 - Número UID
 - Número GID-padrão
 - Informações GECOS: nome completo, empresa, ramal, telefone residencial
 - Diretório inicial
 - Shell de login

Exemplo de arquivo /etc/passwd

```
[root@localhost etc]# cat passwd |more
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpm:x:37:37:/:/var/lib/rpm:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
```

--Mais--

O arquivo `/etc/passwd`

- A medida que o hardware dos computadores se tornou mais rápido, ficou cada vez mais perigoso deixar senhas criptografadas às claras
 - O Linux permite que as senhas sejam armazenadas separadamente em um arquivo-sombra que não é visto por todos
 - Este é o padrão de várias distribuições, incluindo o Red Hat
- Para compartilhar o arquivo de senhas entre vários sistemas normalmente utiliza-se NIS ou LDAP

Nome de login

- Precisam ser exclusivos e não ter mais de 32 caracteres
 - Qualquer caractere exceto dois pontos (:)
 - Versões antigas do UNIX são limitadas a 8 caracteres alfanuméricos
 - Usando NIS também há um limite de 8 caracteres
 - É altamente recomendável seguir as restrições para evitar possíveis conflitos
 - Nomes de login diferenciam maiúsculas e minúsculas, mas programas de e-mail não
 - É prática comum utilizar apenas caracteres minúsculos
 - Evite nomes aleatórios e cognomes

Nome de login

- É útil estabelecer um esquema fixo para atribuição de nomes
 - Exemplos: nomes, sobrenomes, combinações de ambos
 - Qualquer esquema fixo poderá eventualmente gerar nomes repetidos e/ou muito longos, portanto será necessário abrir exceções
 - Aliases de e-mail podem ser definidos em **/etc/aliases**

Senha criptografada

- A maioria dos sistemas armazena as senhas no arquivo-sombra **/etc/shadow**
 - Nota: estaremos nos referindo sempre a **/etc/passwd**, mas assuma **/etc/shadow** caso seu sistema use arquivo-sombra
- As senhas são armazenadas criptografadas, você terá de usar o comando **passwd** para configurá-la ou copiar a senha criptografada de outra conta (a menos que você consiga executar algoritmos de criptografia em sua cabeça)
- Se você editar **/etc/passwd** manualmente para criar uma conta deixe a senha como * até configurá-la
 - Jamais deixe o campo senha vazio, isso permitiria que qualquer pessoa acessasse essa conta sem digitar senha

Senha criptografada

- A maioria das distribuições Linux utiliza DES como padrão de criptografia
 - Senhas não criptografadas tem no máximo 8 caracteres, senhas mais longas são aceitas, porém os caracteres adicionais são ignorados
- Alguns sistemas utilizam o padrão MD5 (inclusive Red Hat)
 - Não é criptograficamente melhor que o DES
 - Permite senhas de tamanho arbitrário
 - Senhas maiores são mais seguras se efetivamente usadas
 - Vários sistemas permitem MD5 como opcional

Número UID

- São inteiros de 32 bits não sinalizados, que podem representar valores de 0 a 4.294.967.296
 - Por questões de interoperabilidade com sistemas antigos procure limitar sua instalação a 32.767
- Usuário root tem UID 0 por padrão
 - Muitos sistemas definem pseudo-usuários bin, deamon, etc...
 - É costumeiro colocá-los no início do arquivo **passwd** e atribuir a eles valores baixos

Número UID

- Nunca crie mais de uma conta com o mesmo UID, especialmente o UID 0
 - Mais de um UID 0 abre brechas de segurança, prefira utilizar o **sudo**
- Evite reaproveitar UIDs, mesmo que sejam de contas já apagadas
 - Isso evita confusão caso arquivos identificados pelo UID sejam restaurados de backups antigos

Número UID

- Devem ser exclusivos em todas as máquinas da organização, um UID deve sempre se referir ao mesmo nome de login e a mesma pessoa em cada máquina
 - Evita problemas ao utilizar sistemas como o NFS
 - Use um banco de dados para armazenar UIDs, nomes de login e usuários caso necessário
 - Caso as máquinas sejam administradas por pessoas diferentes você também pode dividir o espaço de UIDs e atribuir uma faixa para cada máquina, assegurando assim interoperabilidade futura
 - Apesar de isso não garantir a exclusividade de nomes

Número GID padrão

- Também é um inteiro de 32 bits não sinalizado
- GID 0 reservado para o grupo root, GID 1 é o grupo bin, GID 2 é o grupo deamon, etc...
- Os grupos são definidos em **/etc/group** com o campo em **/etc/passwd** definindo o grupo padrão no momento do login
 - É relevante apenas na criação de arquivos/diretórios novos, não é usado para determinar acesso

Campo GECOS

- Comumente usado para registrar informações pessoais sobre cada usuário
- Não possui sintaxe bem definida
- Originalmente armazenava informações de login necessárias para transferir tarefas em segundo plano de sistemas UNIX para um mainframe executando o sistema operacional GECOS (General Electric Comprehensive Operating System), hoje apenas o nome permanece

Campo GECOS

- Podemos usar qualquer convenção de formatação nesse campo, porém **finger** interpreta entradas GECOS separadas por vírgula na seguinte ordem:
 - Nome completo
 - Prédio e número do escritório
 - Ramal do telefone comercial
 - Telefone residencial
- O comando **chfn** permite aos usuários modificar suas próprias informações GECOS
 - Útil para manter dados atualizados
 - Usuário pode colocar informações obscenas ou incorretas

Diretório Inicial

- Os shells de usuário mudam para seus diretórios iniciais via `cd` quando é feita a entrada no sistema
 - Se o diretório estiver faltando no momento o sistema imprimirá uma mensagem de erro
 - Tal mensagem não será vista se o login for feito em ambientes gráficos
 - O login prossegue mesmo com o diretório inicial inexistente, tal comportamento pode ser evitado se configurarmos `DEFAULT_HOME` para no em **`/etc/login.defs`**
 - Esteja ciente de que diretórios montados através de sistema de arquivos de rede podem ficar indisponíveis e m caso de problema de rede ou servidor

Shell de login

- Normalmente é um interpretador de comandos como o Bourne ou o shell C (**/bin/sh** ou **/bin/csh**), mas pode ser qualquer programa
- **bash** é o padrão e é utilizado se nenhum shell de login for especificado
- Os usuários podem alterar seus shells com o comando **chsh**, o arquivo **/etc/shells** tem uma lista de shells válidos que o usuário pode selecionar

O arquivo **/etc/shadow**

- O arquivo **/etc/shadow** é legível apenas pelo root e serve para manter senhas criptografadas seguras quanto a acesso não autorizado
- Fornece informações de contas que não estão disponíveis em **/etc/passwd**
- É padrão em alguns sistemas e opcional em outros

O arquivo **/etc/shadow**

- Quando as senhas-sombra estão em uso, os campos de senha com o estilo antigo devem conter um x
- Ao usar o arquivo-sombra, ambos **/etc/passwd** e **/etc/shadow** precisam ser mantidos, pois o segundo apenas estende o primeiro, não o substitui

O arquivo `/etc/shadow`

- Cada linha de `/etc/shadow` representa um usuário (assim como `/etc/passwd`) e contém vários campos separados por dois pontos (:)
 - Nome de login
 - Senha criptografada
 - Data da última mudança de senha
 - Número máximo de dias entre mudanças de senha
 - Número de dias antecipados para alertar os usuários sobre a expiração de suas senhas
 - Número de dias após a expiração da senha que a conta será desabilitada
 - Data de expiração da conta
 - Um campo reservado para uso futuro (atualmente vazio)
- Nome de login e senha são os únicos campos obrigatórios
- Datas são especificadas contando o número de dias desde 01/01/1970

O arquivo `/etc/shadow`

- O nome de login deve ser o mesmo que consta em `/etc/passwd`
- A senha criptografada tem o mesmo conceito que já descrevemos anteriormente
- O campo de última mudança de senha indica o momento no qual a senha foi modificada pela última vez
- O quarto campo configura o número de dias que deve ocorrer entre mudanças de senhas
 - Quando o usuário muda a senha ele só poderá mudá-la novamente após o número especificado de dias
 - Esse recurso parece inútil e até perigoso caso a segurança seja comprometida, portanto o ideal é configurar esse campo para 0
- O quinto campo configura o número máximo de dias permitido entre mudanças de senha
 - Esse recurso permite ao administrador forçar a expiração de senhas
 - O verdadeiro tempo de expiração é a soma desse campo com o sétimo campo (período de tolerância)

O arquivo `/etc/shadow`

- O sexto campo configura o número de dias antes da expiração da senha que o programa de **login** deve começar a alertar o usuário sobre a expiração
- O sétimo campo especifica o número máximo de dias que se pode esperar após o limite de existência de uma senha antes de tratar o login como expirado (tolerância)
- O oitavo campo especifica o dia (a partir de 01/01/1970) no qual uma conta irá expirar
 - Se deixado em branco a conta nunca expira
- O nono campo é reservado para uso futuro

O arquivo `/etc/shadow`

- Exemplo:

`fbreve:inNo.VRsC1Wn:11508:0:180:14::12417:`

– O usuário `fbreve` alterou sua senha pela última vez em 4 de julho de 2001. A senha tem de ser modificada novamente em 180 dias. Os alertas começarão quando faltarem 14 dias para a expiração. A conta expira em 31 de dezembro de 2003.

O arquivo `/etc/group`

- Contém os nomes dos grupos UNIX e uma lista dos membros de cada grupo.

```
[root@localhost etc]# cat group | more
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
tty:x:5:
disk:x:6:root
lp:x:7:daemon,lp
mem:x:8:
kmem:x:9:
wheel:x:10:root
mail:x:12:mail
news:x:13:news
uucp:x:14:uucp
man:x:15:
games:x:20:
gopher:x:30:
dip:x:40:
ftp:x:50:
lock:x:54:
nobody:x:99:
users:x:100:
dbus:x:81:
--Mais--
```

O arquivo `/etc/group`

- Cada linha representa um grupo e contém quatro campos:
 - Nome do grupo
 - Senha criptografada (vestigial e raramente usada)
 - Número GID
 - Lista de membros, separados por vírgula (atenção para não adicionar espaços)
- Os campos são separados por dois pontos (:)

O arquivo `/etc/group`

- Os nomes de grupos devem ser limitados a 8 caracteres para fins de compatibilidade
- Usar uma senha o grupo permite que o usuário entre no grupo através do comando **newgrp**, mas isso raramente é usado
 - A maioria das instalações coloca asteriscos nos campos de senha
 - Debian, RedHat e SuSe colocam um o caractere 'x' no campo de senha
 - Porém é seguro deixar o campo em branco
 - O comando **newgrp** não mudará para um grupo a menos que o usuário já se encontre listado como membro do grupo

O arquivo `/etc/group`

- Grupos também devem ser mantidos consistentes entre diversas máquinas
- Grupos em `/etc/group` e `/etc/passwd` também devem ser consistentes
 - Se um grupo aparecer em `passwd` e não aparecer em `group`, `passwd` fica com o argumento
 - Associações concedidas no momento do login são uma união dos grupos em `group` e `passwd`
- Para evitar conflitos o ideal é começar a criar grupos a partir do GID 100

O arquivo `/etc/group`

- A tradição no UNIX sempre foi adicionar novos usuários ao grupo que representa sua categoria genérica como “estudantes” ou “financeiro”
 - Tal convenção aumenta a probabilidade arquivos serem compartilhados inadvertidamente
 - Para evitar esse problema é recomendável criar um grupo exclusivo para cada usuário
 - Usualmente o mesmo nome para grupo e usuário
 - O arquivo pessoal do usuário contém somente ele, para permitir compartilhamento de arquivos grupos específicos podem ser criados para essa finalidade.
 - O **useradd** do Red Hat cria grupos pessoais por padrão.

Adicionando usuários

- Antes de criar conta para um novo usuário em uma instituição corporativa, educacional ou governamental é muito importante que o usuário assine e date uma cópia do acordo de usuário local e políticas a serem observadas.
 - Se você não esses documentos, faça-os
 - Isso é interesse do administrador e não do usuário
 - Evite liberar a conta antes de ter a papelada pronta e assinada

Adicionando usuários

- Para acrescentar um novo usuário
 - É necessário:
 - Editar os arquivos **passwd** e **shadow** para definir a conta do usuário
 - Configurar uma senha inicial
 - Criar e aplicar os comandos **chown** e **chmod** ao diretório inicial do usuário
 - Para o usuário:
 - Copiar arquivos de inicialização padrão para o diretório inicial do usuário
 - Configurar o diretório inicial de correio do usuário e estabelecer nomes alternativos
 - Para você:
 - Adicionar o usuário ao arquivo `/etc/group`
 - Configurar quotas de disco
 - Verificar se a conta está configurada corretamente
 - Adicionar as informações de contato de usuário e estado da conta ao seu banco de dados

Editando os arquivos **passwd** e **shadow**

- Para editar de maneira segura o **passwd**, execute **vipw** para chamar um editor de texto em uma cópia dele.
 - Isso funciona como um bloqueio para que apenas uma pessoa edite o arquivo de cada vez e impede que usuários troquem suas senhas durante a edição
 - Exemplo: criando a conta fbreve em **passwd** adicionando a linha:
 - fbreve: *:103:103:Fabricio Breve:/home/fbreve:/bin/bash

Configurando uma senha inicial

- O root pode modificar a senha de qualquer usuário com o comando **passwd**:
 - # **passwd** *usuário*
 - A senha deverá ser digitada duas vezes para fim de confirmação
 - Se você usar uma senha muito fácil **passwd** reclamará
 - RedHat e SuSE comparam a senha digitada com um dicionário para aumentar a segurança
 - Jamais deixe uma conta nova sem senha

Criando o diretório inicial do usuário

- Qualquer diretório criado como root pertence a root, de modo que temos que mudar seu proprietário através de **chown**
- A seqüência abaixo criaria o diretório do nosso usuário de exemplo:

```
#mkdir /home/fbreve  
#chown fbreve.fbreve /home/fbreve  
#chmod 700 /home/fbreve
```

Copiando arquivos de inicialização padrão

- Podemos personalizar alguns comandos e utilitários colocando arquivos de configuração no diretório inicial de um usuário.
 - Esses arquivos começam com um ponto e finalizam com as letras **rc**
 - O ponto faz com que esses arquivos não sejam listado por **ls**, a menos que a opção **-a** seja usada
 - Alguns arquivos com configurações padrão são oferecidos pelo fornecedor em **/etc/skel**

Editando o arquivo `/etc/group`

- Já colocamos o usuário novo no grupo 100 em **passwd**, porém devemos fazer essa alteração também em **group** para manter a consistência
- A edição no Red Hat pode ser feita com **vigr**
- Nesse caso adicionaríamos:
fbreve: x: 103: fbreve

Configurando cotas de disco

- Se a instação possui um sistema de quotas ela poderá ser editada com **edquota**
 - **edquota** pode ser usado iterativamente ou no modo protótipo, que apenas copia as características de uma conta padrão para uma nova conta
- # **edquota** -p *proto-usuário novo-usuário*

Verificando o novo login

- Para verificar uma nova conta você deve sair do sistema e entrar com a nova conta
 - Use o comando **pwd** para verificar se o diretório inicial está correto
 - Use **ls -la** para verificar se os proprietários de arquivos de inicialização estão corretos
- Você deverá informar seus usuários de seus a respeito de seus nomes de logins e senha iniciais
 - Evite fazê-lo por e-mail, seu e-mail poderá ser interceptado e o sistema ser invadido antes que o usuário tenha chance de recebê-lo
 - Você pode solicitar que seu usuário troque a senha imediatamente após o primeiro login
 - Você pode forçá-lo a isso especificando uma data de expiração próxima

Registrando situação do usuário e informações para contato

- Em ambientes pequenos e informais é relativamente fácil controlar quem está usando o sistema e o motivo para tal
- Mas se você gerencia uma grande e mutável base de usuários deve se preocupar em encontrar uma maneira formal de controlar essas contas
 - Uma sugestão é manter um banco de dados com informações sobre cada usuário e suas respectivas contas
 - É importante ter informações completas para contato caso seja necessário, inclusive em casos de problemas de comportamento

Eliminando Usuários

- Quando um usuário deixa uma empresa, a conta deste usuário e seus respectivos arquivos devem ser eliminados do sistema.
- O equivalente automatizado de **useradd** é **userdel**
- Você pode querer fazer a remoção manualmente verificando os seguintes itens:
 - Configurar a cota de disco deste usuário em zero, caso o sistema de cotas esteja sendo utilizado
 - Eliminar o usuário de todos os bancos de dados e listas telefônicas de usuários
 - Eliminar o usuário do arquivo **aliases** ou adicionar um endereço de encaminhamento
 - Eliminar o arquivo **crontab** do usuário e quaisquer tarefas pendentes
 - Extinguir qualquer processo do usuário que ainda esteja em execução
 - Eliminar quaisquer arquivos temporários de propriedade deste usuário em **/var/tmp** ou **/tmp**)
 - Eliminar o usuário dos arquivos **passwd**, **shadow** e **group**
 - Eliminar o diretório inicial do usuário
 - Eliminar o spool de e-mail do usuário

Eliminando Usuários

- Antes de eliminar o diretório inicial do usuário, certifique-se de realocar quaisquer arquivos que ainda sejam úteis
 - Como nem sempre sabemos quais são esses arquivos é sempre bom fazer um backup
- Ao eliminar o usuário pode ser interessante ver se o UID dele ainda tem propriedade sobre arquivos do sistema
 - Para localizar arquivos órfãos use **find** com o argumento **-nouser**

Utilitários para gerenciamento de contas

- O comando **useradd** adiciona usuários ao arquivo **passwd** (e ao arquivo **shadow** se aplicável)
 - Fornece interface dirigida por linhas de comando fácil de ser executada manualmente
 - **userdel** elimina usuários do sistema
 - Por padrão não remove o diretório do usuário, para remover utilize **-r**
 - Mesmo na opção mais agressiva só realiza as últimas 3 tarefas da lista
 - **groupadd**, **groupmod** e **groupdel** operam sobre **/etc/group**
 - **Usermod** modifica uma conta de usuário já existente
 - Mesmos flags de **useradd**

Questões

- Como é determinado o grupo padrão de um usuário? Como poderíamos modificá-lo?
- Explique as diferenças entre os seguintes valores umask: 077, 027, 022 e 755
- Qual é o objetivo do arquivo de senhas-sombra?

Referências Bibliográficas

- NEMETH, Evi.; HEIN, Trent R.; SNYDER, Garth. *Manual Completo do Linux: Guia do Administrador*. Makron Books, 2004.