

Localização de arquivos no sistema

Pesquisa de arquivos

Um administrador de sistema precisa de ferramentas para procurar arquivos que correspondam a determinados critérios no sistema de arquivos.

Esta seção aborda dois comandos para pesquisar arquivos na hierarquia do sistema de arquivos:

- O comando `locate` procura um índice pré-gerado de nomes de arquivos ou caminhos de arquivos e retorna os resultados instantaneamente.
- O comando `find` faz uma busca em tempo real por arquivos, analisando a hierarquia do sistema de arquivos.

Localização de arquivos por nome

1. O comando `locate` pesquisa arquivos com base no nome ou caminho para o arquivo.
2. O comando é rápido porque procura essas informações no banco de dados `mlocate`.
3. No entanto, esse banco de dados não é atualizado em tempo real e exige atualizações frequentes para obter resultados precisos.
4. Esse recurso também significa que o comando `locate` não pesquisa arquivos que foram criados desde a última atualização do banco de dados.

O banco de dados de `locate` é atualizado automaticamente todos os dias. No entanto, o usuário `root` pode usar o comando `updatedb` para forçar uma atualização imediata.

```
[root@host ~]#updatedb
```

O comando `locate` restringe os resultados para usuários sem privilégios.

Para ver o nome do arquivo resultante, o usuário deve ter permissão de pesquisa no diretório em que o arquivo reside

Por exemplo, localize os arquivos que o usuário `developer` pode ler e que correspondem à palavra-chave `passwd` no nome ou no caminho:

```
[developer@host ~]$ locate passwd
/etc/passwd
/etc/passwd-
/etc/pam.d/passwd
...output omitted...
```

O seguinte exemplo mostra o nome do arquivo ou o caminho para uma correspondência parcial com a consulta de pesquisa:

```
[root@host ~]# locate image
/etc/selinux/targeted/contexts/virtual\_image_context
/usr/bin/grub2-mkimage
/usr/lib/sysimage...output omitted...
```

A opção `-i` do comando `locate` realiza uma pesquisa que não diferencia maiúsculas e minúsculas. Essa opção retorna todas as combinações possíveis de letras maiúsculas e minúsculas correspondentes:

```
[developer@host ~]$ locate -i messages...output omitted...
/usr/share/locale/zza/LC_MESSAGES
/usr/share/makedumpfile/eppic_scripts/ap_messages_3_10_to_4_8.c
/usr/share/vim/vim82/ftplugin/msmessages.vim
...output omitted...
```

A opção `-n` do comando `locate` limita o número de resultados da pesquisa retornados. O seguinte exemplo limita os resultados da pesquisa retornados pelo comando `locate` às cinco primeiras ocorrências:

```
[developer@host ~]$locate -n 5 passwd
/etc/passwd
/etc/passwd-
/etc/pam.d/passwd
...output omitted...
```

Pesquisa de arquivos em tempo real

- O comando `find` localiza os arquivos, pesquisando em tempo real na hierarquia de sistema de arquivos.
- O comando `find` também pesquisa arquivos com base em critérios diferentes do nome do arquivo, como as permissões do arquivo, o tipo de arquivo, seu tamanho ou sua hora de modificação.
- O comando `find` examina os arquivos do sistema de arquivos com a conta de usuário que executou a pesquisa.
- O usuário que executa o comando `find` deve ter permissão de leitura e execução em um diretório para examinar o respectivo conteúdo.
- O primeiro argumento do comando `find` é o diretório a ser pesquisado.
- Se o comando `find` omite o argumento do diretório, ele começa a pesquisa no diretório atual e procurará correspondências em todos os subdiretórios.

Para pesquisar arquivos por nome de arquivo

Use a opção `-name FILENAME` do comando `find` para retornar o caminho dos arquivos que correspondem exatamente a `FILENAME`.

Por exemplo, para pesquisar os arquivos `sshd_config` a partir do diretório root `/`, execute o seguinte comando:

```
[root@host ~]#find / -name sshd_config
/etc/ssh/sshd_config
```

Nota

No comando `find`, a palavra completa `options` usa um único traço para `options`, ao contrário de um traço duplo para a maioria dos outros comandos do Linux.

Caracteres curinga

- Estão disponíveis para pesquisa por nome de arquivo e retornarão todos os resultados que forem correspondências parciais.
- Com caracteres curinga, é essencial colocar o nome do arquivo a ser procurado entre aspas para evitar que o terminal interprete o caractere curinga incorretamente.

No seguinte exemplo, comece no diretório `/`, pesquise os arquivos que terminam com a extensão `.txt`:

```
[root@host ~]#find / -name '*.txt'...output omitted...
/usr/share/libgpg-error/errorref.txt
/usr/share/licenses/audit-libs/lGPL-2.1.txt
/usr/share/licenses/pam/gpl-2.0.txt
...output omitted...
```

Para procurar arquivos no diretório `/etc/` que contêm a string `pass`, execute o seguinte comando:

```
[root@host ~]#find /etc -name '*pass*'
/etc/passwd-
/etc/passwd
/etc/security/opasswd
...output omitted...
```

Para executar uma pesquisa que não diferencia minúsculas de maiúsculas de um nome de arquivo

- use a opção `-iname` do comando `find`, seguida pelo nome de arquivo a pesquisar.
- Para pesquisar arquivos que correspondam à string `messages`, sem diferenciar maiúsculas de minúsculas, em seus nomes no diretório root `/`, execute o seguinte comando:

```
[root@host ~]#find / -iname '*messages*'
/sys/power/pm_debug_messages
/usr/lib/locale/C.utf8/LC_MESSAGES
/usr/lib/locale/C.utf8/LC_MESSAGES/SYS_LC_MESSAGES
...output omitted...
```

Pesquisar arquivos com base na propriedade ou permissão

O comando `find` pesquisa arquivos com base na propriedade ou nas permissões.

As opções `-user` e `-group` do comando `find` pesquisam por um nome de usuário e grupo ou por ID de usuário e ID de grupo.

Para procurar arquivos no diretório `/home/developer` que o usuário `developer` possui:

```
[developer@host ~]$find -user developer
.
./bash_logout
./bash_profile
...output omitted...
```

Para pesquisar arquivos no diretório `/home/developer` que o grupo `developer` possui:

```
[developer@host ~]$find -group developer
.
./bash_logout
```

```
./bash_profile  
...output omitted...
```

Para procurar arquivos no diretório `/home/developer` que a ID de usuário `1000` possui:

```
[developer@host ~]$find -uid 1000  
.  
./bash_logout  
./bash_profile  
...output omitted...
```

As opções `-user` e `-group` do comando `find` pesquisam arquivos em que o proprietário do arquivo e o proprietário do grupo sejam diferentes.

O exemplo a seguir lista os arquivos que o usuário `root` possui e com o grupo `mail`:

```
[root@host ~]#find / -user root -group mail  
/var/spool/mail  
...output omitted...
```

A opção `-perm` do comando `find` é usada para procurar arquivos com um conjunto específico de permissões.

Os valores octais definem as permissões com:

- `4` leitura,
- `2` gravação
- `1` execução.

As permissões são precedidas por um sinal `/` ou `-` para controlar os resultados da pesquisa.

A permissão octal precedida pelo sinal `/` :

- corresponde a arquivos em que pelo menos uma permissão foi definida para o usuário, grupo ou outro para esse conjunto de permissões.
- Um arquivo com as permissões `r--r--r--` não corresponde à permissão `/222`, mas corresponde à permissão `rw-r--r--`.

Um sinal `-` antes da permissão significa que todas as três partes das permissões devem corresponder.

No exemplo anterior, os arquivos com as permissões `rw-rw-` correspondem. Você também pode usar a opção `-perm` do comando `find` com o método simbólico para permissões.

Por exemplo, os comandos a seguir correspondem a qualquer arquivo no diretório `/home` para o qual o usuário tenha permissões de leitura, gravação e execução, os membros do grupo tenham permissões de leitura e gravação, e outros tenham acesso somente leitura.

Ambos os comandos são equivalentes; o primeiro usa o método octal para permissões, enquanto o segundo usa os métodos simbólicos.

```
[root@host ~]#find /home -perm 764...output omitted...
[root@host ~]#find /home -perm u=rwx,g=rw,o=r...output omitted...
```

A opção `-ls` do comando `find` é prática ao pesquisar arquivos por permissões, pois fornece informações para os arquivos que incluem suas permissões.

```
[root@host ~]#find /home -perm 764 -ls
26207447    0-rwxrw-r--    1 user   user    0 May 10 04:29 /home/user/file1
```

Para pesquisar arquivos para os quais o usuário tem pelo menos permissões de gravação e execução, o grupo tem pelo menos permissão de gravação, e

outros têm pelo menos permissão de leitura, execute o seguinte comando:

```
[root@host ~]#find /home -perm -324
...output omitted...
[root@host ~]#find /home -perm -u=wx,g=w,o=r
...output omitted...
```

Para pesquisar arquivos aos quais o usuário tem permissões de leitura, o grupo tem pelo menos permissões de leitura, ou outros têm pelo menos permissão de gravação, execute o seguinte comando:

```
[root@host ~]#find /home -perm /442
...output omitted...
[root@host ~]#find /home -perm /u=r,g=r,o=w
...output omitted...
```

Quando usado com os sinais `/` ou `-`, o valor `0` funciona como um caractere curinga, porque ele significa qualquer permissão.

Para pesquisar qualquer arquivo no diretório `/home/developer` para o qual outros usuários têm pelo menos acesso de leitura na máquina `host`, execute o seguinte comando:

```
[developer@host ~]$find -perm -004
...output omitted...
[developer@host ~]$find -perm -o=r
...output omitted...
```

Para pesquisar todos os arquivos no diretório `/home/developer` em que outros têm permissão de gravação, execute o seguinte comando:

```
[developer@host ~]$find -perm -002
...output omitted...
```



```
[developer@host ~]$find -perm -o=w  
...output omitted...
```

Localizar arquivos com base no tamanho

A opção `-size` do comando `find` é seguida por um valor numérico, e a unidade procura arquivos que correspondem a um tamanho especificado.

Use a seguinte lista de unidades com a opção `-size` do comando `find`:

- Para kilobytes, use a unidade `k` com `k` sempre em letras minúsculas.
- Para megabytes, use a unidade `M` com `M` sempre em letras maiúsculas.
- Para gigabytes, use a unidade `G` com `G` sempre em letras maiúsculas.

Você pode usar os caracteres de adição `+` e subtração `-` para incluir arquivos maiores e menores do que o tamanho fornecido, respectivamente.

O exemplo a seguir mostra uma pesquisa por arquivos com um tamanho exato de 10 megabytes:

```
[developer@host ~]$find -size 10M  
...output omitted...
```

Para pesquisar os arquivos com tamanho superior a 10 gigabytes:

```
[developer@host ~]$find -size +10G...output omitted...
```

Para pesquisar os arquivos com tamanho inferior a 10 kilobytes:

```
[developer@host ~]$find -size -10k  
...output omitted...
```

Importante

A opção `-size` do comando `find` arredonda tudo para unidades únicas. Por exemplo, o comando `find -size 1M` mostra os arquivos com menos de 1 MB, porque arredonda todos os arquivos para 1 MB.

Pesquisar arquivos com base no horário de modificação

A opção `-mmin` do comando `find`, seguida pelo tempo em minutos, pesquisa todos os arquivos com conteúdo alterado há `n` minutos.

O carimbo de data e hora do arquivo é arredondado para baixo e é compatível com valores fracionários com o intervalo `+n` e `-n`.

Para pesquisar todos os arquivos com conteúdo alterado há 120 minutos:

```
[root@host ~]#find / -mmin 120
...output omitted...
```

O modificador `+` na frente dos minutos encontra todos os arquivos no diretório `/` que foram alterados há mais de `n` minutos.

Para pesquisar todos os arquivos com conteúdo alterado há mais de 200 minutos:

```
[root@host ~]#find / -mmin +200
...output omitted...
```

O modificador `-` pesquisa todos os arquivos no diretório `/` que foram alterados há menos de `n` minutos.

O exemplo a seguir lista arquivos que foram alterados há menos de 150 minutos:

```
[root@host ~]#find / -mmin -150
...output omitted...
```

Pesquisar arquivos com base no tipo de arquivo

A opção `-type` do comando `find` limita o escopo da pesquisa para um determinado tipo de arquivo. Use os seguintes sinalizadores para limitar o escopo da pesquisa:

- Para arquivos regulares, use o sinalizador `f`.
- Para diretórios, use o sinalizador `d`.
- Para softlinks, use o sinalizador `l`.
- Para dispositivos de bloco, use o sinalizador `b`.

Pesquise todos os diretórios no diretório `/etc`:

```
[root@host ~]#find /etc -type d
/etc
/etc/tmpfiles.d
/etc/systemd
/etc/systemd/system
/etc/systemd/system/getty.target.wants
...output omitted...
```

Pesquise todos os softlinks no diretório `/`:

```
[root@host ~]#find / -type l...output omitted...
```

Pesquise todos os dispositivos de bloco no diretório `/dev`:

```
[root@host ~]#find /dev -type b
/dev/vda1
/dev/vda
```

A opção `-links` do comando `find` seguida por um número procura todos os arquivos com uma determinada contagem de links físicos.

- O número precedido por um modificador `+` procura arquivos com a contagem mais alta à contagem de links físicos fornecida.
- Se o número for precedido por um modificador `-`, a pesquisa será limitada aos arquivos com uma contagem de links físicos inferior ao número fornecido.

Pesquise todos os arquivos regulares com mais de um link físico:

```
[root@host ~]#find / -type f -links +1...output omitted...
```

ad