LSOF - LiSt Open Files

Descrição

Como o nome indica, LSOF lida com arquivos abertos em um sistema UNIX. Um arquivo aberto pode ser um arquivo comum, um diretório, uma biblioteca, um *stream*, ou um soquete de rede.

LSOF é um excelente utilitário para gerenciamento de conexões de rede em seu sistema UNIX. De qualquer forma vários utilitários podem desempenhar funções similares, mas nenhum é tão robusto como LSOF. Com LSOF você pode listar portas abertas, identificar conexões que foram feitas no seu sistema, e determinar que recursos um processo está usando. Não somente isto, mas você também pode determinar que processos um usuário em particular tem e encontrar informações detalhadas sobre o uso de arquivos e diretórios.

Opções

Rodando o LSOF sem opções irá exibir todos os arquivos abertos pertencentes a todos os processos ativos na máquina. Isto geralmente exibe uma quantidade enorme de dados, então sugiro que você filtre sua busca usando as opções disponíveis.

Algumas opções disponíveis

lsf -p <PID>[,PID]

Ex.: `lsf -p 2119`

Esta opção lista os arquivos de processos cujo PID (Process IDentification) se encontra no conjunto especificado.

lsf -R

Esta opção faz com que seja listado também o PPID (Parent Process IDentification).

lsf -g <PGRP>[,PGRP]

Ex.: `lsf -g 0`

Esta opção lista os arquivos de processos cujo PGRP (Process Group IDentification) se encontra no conjunto especificado.

lsf -u <UID>[,UID] ou lsf <login>[,login]

Ex.: `lsf -u marcelo`

Esta opção lista os arquivos de processos cujo dono se encontra no conjunto especificado.

lsf -c <string>

Ex.: `lsf -c ht`

Esta opção lista os arquivos de processos executando comandos que começam com os caracteres especificados.

lsf +d <dir>

Ex: *lsf +d /opt/apache/*

O comando “*lsf +d <dir>*” lista todos os arquivos abertos do diretório **<dir>**, mas não realiza a busca nas subpastas (Ex.: */opt/apache/htdocs*), para isso use a opção “+D”.

lsf -i [protocolo][@nomehost|endereçohost][:serviço|porta]

Por padrão, esta opção lista informações detalhadas sobre cada conexão, como o comando ou programa envolvido, o PID, o usuário que está rodando o comando, o FD (File Descriptor), o tipo de conexão, o número do dispositivo, o protocolo da Internet e o nome do arquivo ou endereço da Internet. A opção “-i” pode ser útil quando você está querendo manter a segurança de sua máquina. Você pode determinar quais portas estão abertas e escutando para conexões externas. LSOF poderá também associar elas com um nome de programa. Com isso você pode identificar serviços desnecessários, que são um risco de segurança e desativá-los.

Portas que estão esperando por conexões tem a palavra *listen* associadas a elas. Estas são portas que estão abertas e aceitando conexões. Note que LSOF não fará distinção entre portas completamente abertas e portas que tem filtros aplicados. A palavra *established* indica que a conexão na porta dada foi realizada.

Esta opção exibe a lista de arquivos cujo endereço da internet corresponde ao especificado. Se nenhum endereço for especificado, ele exibe todos os arquivos da internet e arquivos x.25 (HP-UX).

Vários endereços (no máximo 100) podem ser especificados por meio de múltiplas opções “-i”. (Um número de porta ou um nome de serviço é considerado um endereço).

Descrição dos campos:

protocolo é um nome de protocolo – **TCP ou UDP** (não distingue maiúsculas e minúsculas);

nomehost é um nome de um host da Internet;

endereçohost é um endereço IP (IPv4) separado por ponto ‘.’ ou um endereço (IPv6) separado por dois pontos ‘:’ e entre parênteses;

serviço é um nome de um serviço contido no arquivo */etc/services* (ou uma lista deles). Ex.: **smtp**;

porta é um número de porta (ou uma lista delas).

O caractere ‘@’ é sempre necessário quando for especificar um host (*nomehost* ou *endereçohost*), e o caractere ‘:’ é sempre necessário quando for especificar uma porta ou um serviço. Se uma lista de serviços for especificada,

pode se fazer necessário à especificação do protocolo se o número da porta TCP e UDP de um serviço forem diferentes.

Serviços ou números de portas podem ser combinados em uma lista onde as entradas devem ser separadas por vírgulas e as faixas de números devem ser separadas por '-'. Não pode haver espaços em branco, e todo serviço deve pertencer a um protocolo específico. Como serviços podem conter '-', a entrada inicial de uma faixa não pode ser um serviço, entretanto pode ser um número de porta.

Abaixo alguns exemplos:

TCP:22 – Lista conexões que usam o protocolo TCP escutando ou estabelecidas na porta 22 (remota ou local).

@152.84.253.13 – Lista conexões realizadas pelo host 152.84.253.13 na máquina local.

@[3ffe:1ebc::1]:1234 – Lista conexões realizadas pelo host 3ffe:1ebc::1 na máquina local usando a porta 1234 (porta referente ao host remoto) na máquina local.

TCP@positron.cat.cbpf.br:1017 – Lista conexões que usam o protocolo TCP realizadas pelo host positron.cat.cbpf.br na máquina local usando a porta 1017 (porta referente ao host remoto).

tcp@152.84.253.13:1-10,smtp,99 – Lista conexões que usam o protocolo TCP realizadas pelo host 152.84.253.13 na máquina local usando portas (referentes ao host remoto) entre 1 e 10, ou a porta 99, ou a porta referente ao serviço smtp.

lsuf -F <.>

A opção “-F” proporciona uma excelente forma para formatar a saída do LSOF. Esta opção permite a você encaminhar a saída diretamente para programas externos, como um script Perl, um programa em C ou até mesmo programas de monitoração. Você faz isso especificando quais campos você deseja que sejam impressos.

Alguns campos disponíveis

- c** nome de comando do processo
- n** nome do arquivo, comentário, endereço da Internet
- p** PID (sempre é selecionado)
- u** UID (usuário dono do processo)
- s** tamanho do arquivo
- t** tipo do arquivo
- f** descritor do arquivo

Muitas outras opções estão disponíveis, isto é bom pois boa parte do trabalho de análise será feito automaticamente.

Ex.:

```
[root@cyclone /]# lsuf -u marcelo -Fcfn
p936
cbash
fcwd
n/home/marcelo
```

frtd
n/

Descrição dos campos

(Alguns campos não possuem descrição completa, para obtê-la veja o man page do LSOF)

COMMAND – Contém os primeiros 9 caracteres do nome do comando UNIX associado com o processo.

PID – É o número de identificação do processo.

PPID – É o número de identificação do processo pai.

PGRP – É o número de identificação do grupo do processo.

USER – É o número de identificação (UID - User IDentification) ou nome (login) do usuário que é dono do processo.

FD – É o número descritor do arquivo ou:

cwd – diretório de trabalho corrente;

Lnn – Biblioteca de referência (AIX);

Itx – Biblioteca de texto compartilhada (código e dados);

Mxx – xx tipo do número hexadecimal mapeado em memória;

m86 – Arquivo mapeado combinado;

mem – Arquivo mapeado em memória;

txt – Texto do programa (código e dados);

v86 – arquivo mapeado VP/ix

FD é seguido por um desses caracteres abaixo, indicando que modo cada arquivo está aberto:

r indica acesso de leitura;

w indica acesso de escrita;

u indica acesso de leitura e escrita;

espaço se desconhecido e não possui caractere de trava;

- se desconhecido e possui caractere de trava.

O caractere de modo é seguido por um dos caracteres abaixo, indicando o tipo de trava aplicada ao arquivo:

N para uma trava NFS do Solaris de um tipo desconhecido;

r para uma trava de leitura em parte do arquivo;

R para uma trava de leitura no arquivo inteiro;

w para uma trava de escrita em parte do arquivo;

W para uma trava de escrita no arquivo inteiro;

u para uma trava de leitura e escrita de qualquer tamanho;

U para uma trava de tipo desconhecido;

x para uma trava SCO OpenServer Xenix em parte do arquivo;

X para uma trava SCO OpenServer Xenix no arquivo inteiro;

espaço se não existe uma trava.

TYPE – É o tipo de *node* associado com o arquivo: (Alguns exemplos)

IPv4 – Para um soquete IP versão 4;

DIR – Para um diretório;

LINK – Para um link simbólico;

PIPE – Para *pipes*;

REG – Para arquivos comuns (regulares);

FIFO – Para um arquivo especial FIFO;
LINK – Para um link simbólico;
unix – para um soquete de domínio UNIX;
Inet – Para um soquete de domínio da Internet.

DEVICE – contém os números do dispositivo, separados por vírgulas, para um caractere especial, bloco especial, regular, diretório ou arquivo NFS;
Ou o protocolo de controle de bloco de endereço de um DECnet (Ultrix4.2), Internet, UNIX, ou arquivo de rede x.25 (HP-UX);
Ou “memory” para uma memória de nó de arquivo de sistema sobre DEC OSF/1, Digital UNIX, ou Tru64 UNIX;
Ou um endereço de referência que identifica o arquivo;
Ou o endereço base ou nome de dispositivo de um dispositivo de soquete Linux AX.25.

SIZE – É o tamanho do arquivo

NODE – É o número do *node* de um arquivo local;
Ou o número do *node* de um arquivo NFS no servidor;
Ou o tipo de protocolo da Internet;
Ou “STR” para um *stream*;
Ou “CCITT” para um soquete HP-UX x.25;
Ou a IRQ ou *inode* de um dispositivo de soquete Linux AX.25.

NAME – É o nome do ponto de montagem e do *file system* em que o arquivo reside;
Ou o nome de um arquivo especificado na opção “names” (depois que qualquer link simbólico tenha sido resolvido);
Ou o nome de um caractere especial ou dispositivo especial de bloco;
Ou o endereço de Internet local e remoto de um arquivo de rede;
Ou o *node* local e remoto e endereços de objetos de um arquivo DECnet;
Ou o endereço ou nome de um soquete de domínio UNIX.

Algumas considerações sobre as opções

Normalmente quando a lista de opções é explicitamente passada ao LSOF, as opções são tratadas com o operador lógico **ou**.

Ex.: Passando a opção “-i” sem um endereço e a opção “-u <usuário>” ao LSOF, produz uma lista com todos os arquivos de rede **ou** arquivos pertencentes aos processos cujo dono é <usuário>.

Uma exceção é o login ou UID “^” (negado) especificado com a opção “-u”, como ele é uma exclusão, ele é aplicado sem ser usado um dos operadores lógicos **e/ou**, e é considerado antes que qualquer critério de seleção seja aplicado.

A opção “-a” pode ser usada para aplicar o operador lógico **e** entre as opções passadas ao LSOF.

Ex.: “ls -a -U -u marcelo” produz uma listagem de arquivos de soquete UNIX que pertencem aos processos do usuário marcelo somente.

Cuidado: A opção “-a” faz com que todas as opções passadas ao LSOF sejam interpretadas com o operador lógico **e**, não sendo possível que o

operador lógico **e** seja interpretado somente em pares de opções por meio da colocação da opção “-a” entre duas outras opções.