Inetd - Internet Daemon

O número de serviços oferecido por um servidor pode ser grande, mas muitos serviços são solicitados de forma esporádica. Se todos os *daemons* responsáveis por serviços fossem lançados automaticamente na inicialização (*boot*), eles ficariam usando memória e CPU desnecessariamente. Para evitar esse problema, muitos serviços ficam a cargo de um processo especial chamado *Internet Daemon*, ou `inetd`.

Configuração

Tradicionalmente, o arquivo de configuração `/etc/inetd.conf` indica quais os serviços sob a responsabilidade do *Internet Daemon*. Esse *daemon* "ouve" as portas dos serviços que gerencia e, no caso de uma chamada, lança o processo servidor necessário para atendê-la. O arquivo de configuração básico do *Internet Daemon* tem a seguinte forma:

```
# service type    proto           user    program to launch

ftp       stream  tcp     nowait  root    /usr/sbin/in.ftpd -l -a
telnet    stream  tcp     nowait  root    /usr/sbin/in.telnetd
gopher    stream  tcp     nowait  root    /usr/sbin/gn
shell     stream  tcp     nowait  root    /usr/sbin/in.rshd
login     stream  tcp     nowait  root    /usr/sbin/in.rlogind
talk      dgram   udp     wait    root    /usr/sbin/in.talkd
```

TCP-Wrappers

Um grande problema em relação aos serviços providos à Internet é que qualquer host externo pode acessar um serviço, se este estiver disponível, e o controle de acesso ao serviço fica sob a responsabilidade do próprio daemon que responde por ele. Isso põe em risco a segurança do sistema.

Para resolver esse problema, o *Internet Daemon* geralmente é usado em conjunto com o sistema chamado *TCP-Wrappers*, permitindo a definição de políticas de acesso de forma integrada para todos os serviços oferecidos através do `inetd`. Quando o `inetd` está sendo usado com *TCP-Wrappers*, seu arquivo de configuração assume uma forma um pouco diferente:

```
#service type    proto           user    program to launch

ftp       stream  tcp     nowait  root    /usr/sbin/tcpd in.ftpd -l -a
telnet    stream  tcp     nowait  root    /usr/sbin/tcpd in.telnetd
gopher    stream  tcp     nowait  root    /usr/sbin/tcpd gn
shell     stream  tcp     nowait  root    /usr/sbin/tcpd in.rshd
login     stream  tcp     nowait  root    /usr/sbin/tcpd in.rlogind
talk      dgram   udp     wait    root    /usr/sbin/tcpd in.talkd
```

Como podemos ver, todas as chamadas são interceptadas pelo programa `tcpd`. Este programa verifica as permissões de acesso descritas nos arquivos `/etc/hosts.allow` e `/etc/hosts.deny` (localizados no mesmo computador que está executando o *daemon* `inetd`), para autorizar ou recusar o acesso a cada serviço. A estrutura de um arquivo `/etc/hosts.allow` típico é a seguinte:

```
# daemons    hosts
```

```
in.fingerd : localhost
in.telnetd : ALL
in.ftpd    : *.pucpr.br
```

O procedimento de consulta desses arquivos para cada pedido de conexão é o seguinte:

```
se o pedido de conexão constar em /etc/hosts.allow então
  autorizar o acesso
senão
  se o pedido de conexão constar em /etc/hosts.deny então
    negar o acesso
  senão
    autorizar o acesso
  fim se
fim se
```

Esse procedimento de avaliação de regras permite definir dois grandes tipos de políticas:

- **Mostly Open**:
  - `hosts.allow`: fica vazio.
  - `hosts.deny` : contém regras de bloqueio específicas.
- **Mostly Closed**:
  - `hosts.deny` : bloqueia todos os serviços (regra `ALL:ALL`).
  - `hosts.allow`: contém regras de autorização específicas.

As possibilidades de regras de acesso oferecidas pelo sistema *TCP-Wrappers* são muitas. Para maiores detalhes consulte a página de manual.

XInetd - Extended Internet Daemon

Versões mais recentes de UNIX substituem o inetd pelo xinetd (Extended Internet Daemon), que dispensa o uso de *TCP-Wrappers* e traz diversas vantagens:

- Limitação de conexões:
  - taxa de conexões recebidas por intervalo de tempo
  - número de conexões por host
  - número de conexões por serviço
- Controle de acesso mais sofisticado:
  - Feito pelo próprio daemon, dispensando o TCPWrappers
  - Por host, IP, domínio ou sub-rede
  - por horário
- Controle de logs:
  - limitação do tamanho de cada arquivo de log
  - Nível de logging de cada serviço pode ser configurado de forma independente
- Desvio de conexões
  - Um fluxo TCP pode ser redirecionado para outro host e/ou porta de forma transparente.
- Suporte a IPv6

O daemon `xinetd` usa os arquivos de configuração `/etc/xinetd.conf` (configuração geral) e `/etc/xinetd.d/*` (um arquivo para cada serviço). As entradas nos arquivos de configuração possuem o seguinte formato genérico:

```
service <service_name>
{
   <attribute> < = | += | -= > <value> <value> ...
```

```
   ...
}
```

Um exemplo de entrada para o serviço VNC (conexão remota gráfica) com resolução 800×600 (arquivo `/etc/xinetd.d/vnc-800`):

```
service vnc
{
   disable = no
   socket_type = stream
   wait = no
   user = nobody
   server = /usr/bin/Xvnc
   server_args = -inetd -query localhost -once -geometry 800x600 -depth 16
   nice = 5
}
```

Os principais atributos gerais associados a cada serviço são (uma lista completa está disponível na página de manual):

parâmetro	**exemplo**	**Significado**
disable	no	habilita o serviço
	yes	desabilita o serviço
socket_type	stream	socket TCP
	dgram	socket UDP
	raw	socket IP (baixo nível)
wait	yes	espera conclusão da conexão para aceitar novas conexões
	no	não espera conclusão da conexão para aceitar novas conexões
port	5900	porta a usar (caso o nome do serviço não esteja definido em /etc/services ou uma porta não-default deva ser usada)
user	nobody	usuário que executa o serviço
group	somegroup	grupo que executa o serviço
server	/usr/bin/Xvnc	processo que executa o serviço
server_args	-inetd -query localhost -once -geometry 800×600 -depth 16	parâmetros do processo servidor
log_type	SYSLOG	daemon info
FILE	/var/log/vnc	onde armazenar os logs do serviço
log_on_success	PID HOST DURATION	informação a logar caso a conexão seja aceita
log_on_failure	HOST	informação a logar caso a conexão seja recusada
redirect	server-b.domain.com 5901	redireciona os pacotes enviados a este serviço para o host e porta indicados, de forma transparente para o cliente

Atributos específicos de controle de acesso:

parâmetro	**exemplo**	**Significado**
only_from	20.0.0.17 200.10.0.0 20.10/16 server1.domain.com .domain.com	indica hosts dos quais conexões são aceitas
no_access	idem	indica hosts dos quais conexões são negadas

Atributos específicos de limitação de uso de recursos (importantes para suportar ataques de negação de serviço):

parâmetro	**exemplo**	**Significado**
`instances`	10	número máximo de instâncias simultâneas do serviço
`per_source`	3	número máximo de instâncias por host de origem
`nice`	15	prioridade do processo do serviço
`access_times`	02:00-06:00 18:00-22:00	horários em que o serviço está disponível
`cps`	10 30	número máximo de conexões por segundo (10) e período de suspensão do serviço (30 segundos) caso o limite seja alcançado
`max_load`	2	carga máxima do sistema operacional para aceitar novas conexões
`rlimit_as`	5M	limite de memória a ser usado pelo processo servidor
`rlimit_cpu`	30	limite de tempo de CPU do processo servidor, em segundos