

Exercício orientado:

Identificação de processos do sistema iniciados automaticamente

Neste exercício, você lista unidades de serviço instaladas e identificará quais serviços estão atualmente habilitados e ativos em um servidor.

Resultados

- Listar as unidades de serviço instaladas.
- Identificar os serviços ativos e habilitados no sistema.

Com o usuário `student` na máquina `workstation`, use o comando `lab` para preparar seu sistema para este exercício.

Esse comando prepara seu ambiente e garante que todos os recursos necessários estejam disponíveis.

```
[student@workstation ~]$lab start services-identify
```

Instruções

1. Use o comando `ssh` para fazer login na máquina `servera` como o usuário `student`.

```
[student@workstation ~]$ssh student@servera
[student@servera ~]$
```

2. Liste todas as unidades de serviço instaladas na máquina `servera`.

```
[student@servera ~]$systemctl list-units --type=service
UNIT                                LOAD    ACTIVE SUB    DESCI
PTION
atd.service                        loaded active running Deferr
ed execution scheduler
auditd.service                    loaded active running Securi
```

```

ty Auditing Service
  chronyd.service          loaded active running NTP cl
ient/server
  crond.service            loaded active running Comman
d Scheduler
  dbus-broker.service      loaded active running D-Bus
System Message Bus
...output omitted...

```

Pressione **q** para sair do comando.

3. Liste todas as unidades de soquete, ativas e inativas, na máquina `servera`.

```

[student@servera ~]$systemctl list-units --type=socket -
-all
UNIT                                LOAD    ACTIVE SUB    DESCRI
PTION
dbus.socket                        loaded active running D-Bus
System Message Bus Socket
dm-event.socket                   loaded active listening Device
-mapper event daemon FIFOs
lvm2-lvmpolld.socket              loaded active listening LVM2 p
oll daemon socket
...output omitted...

```

LOAD = Reflects whether the unit definition was proper
ly loaded.

ACTIVE = The high-level unit activation state, i.e. gene
ralization of SUB.

SUB = The low-level unit activation state, values dep
end on unit type.

13 loaded units listed.

To show all installed unit files use 'systemctl list-uni
t-files'.

4. Explore o status do serviço `chronyd`. Você pode usar esse serviço para a sincronização de tempo de rede (NTP, Network Time Protocol).

- a. Exiba o status do serviço `chronyd`. Anote a ID de processo dos daemons ativos.

```
[student@servera ~]$systemctl status chronyd
● chronyd.service - NTP client/server
   Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2022-03-14 05:38:15 EDT; 1h 16min ago
     Docs: man:chronyd(8)
           man:chrony.conf(5)
  Process: 728 ExecStart=/usr/sbin/chronyd $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 747 (chronyd)
    Tasks: 1 (limit: 10800)
   Memory: 3.7M
      CPU: 37ms
   CGroup: /system.slice/chronyd.service
           └─747 /usr/sbin/chronyd -F 2
```

```
Mar 14 05:38:15 servera.lab.example.com systemd[1]: Starting NTP client/server...
Mar 14 05:38:15 servera.lab.example.com chronyd[747]: chronyd version 4.1 starting (+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP +SCFILTER +SIGND +ASYNCDNS +NTS +SECHASH +IPV6 +DEBUG)
Mar 14 05:38:15 servera.lab.example.com chronyd[747]: commandkey directive is no longer supported
Mar 14 05:38:15 servera.lab.example.com chronyd[747]: generatecommandkey directive is no longer supported
Mar 14 05:38:15 servera.lab.example.com chronyd[747]: Frequency -11.870 +/- 1.025 ppm read from /var/lib/chrony/drift
Mar 14 05:38:15 servera.lab.example.com chronyd[747]: Loaded seccomp filter (level 2)
Mar 14 05:38:15 servera.lab.example.com systemd[1]: Started NTP client/server.
```

```
Mar 14 05:38:23 servera.lab.example.com chronyd[747]:  
Selected source 172.25.254.254
```

Pressione **q** para sair do comando.

- b. Confirme se o daemon `chronyd` está em execução usando sua ID de processo. No comando anterior, a saída da ID do processo associada ao serviço `chronyd` é 747. A ID do processo pode ser diferente no seu sistema.

```
[student@servera ~]$ps -p747  
PID TTY          TIME CMD  
747 ?            00:00:00 chronyd
```

5. Explore o status do serviço `sshd`. Você pode usar esse serviço para a comunicação criptografada segura entre sistemas.

- a. Determine se o serviço `sshd` está habilitado para começar no boot do sistema.

```
[student@servera ~]$systemctl is-enabled sshd  
enabled
```

- b. Determine se o serviço `sshd` está ativo, sem exibir todas as informações de status.

```
[student@servera ~]$systemctl is-active sshd  
active
```

- c. Exiba o status do serviço `sshd`.

```
[student@servera ~]$systemctl status sshd  
● sshd.service - OpenSSH server daemon  
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)  
   Active: active (running) since Mon 2022-03-14 05:38:16 EDT; 1h 19min ago  
     Docs: man:sshd(8)  
           man:sshd_config(5)
```

```

Main PID: 784 (sshd)
  Tasks: 1 (limit: 10800)
Memory: 6.7M
  CPU: 82ms
  CGroup: /system.slice/sshd.service
          └─784 "sshd: /usr/sbin/sshd -D [listene
r] 0 of 10-100 startups"

Mar 14 05:38:16 servera.lab.example.com systemd[1]: S
tarting OpenSSH server daemon...
Mar 14 05:38:16 servera.lab.example.com sshd[784]: Se
rver listening on 0.0.0.0 port 22.
Mar 14 05:38:16 servera.lab.example.com sshd[784]: Se
rver listening on :: port 22.
Mar 14 05:38:16 servera.lab.example.com systemd[1]: S
tarted OpenSSH server daemon.
Mar 14 06:51:36 servera.lab.example.com sshd[1090]: A
ccepted publickey for student from 172.25.250.9 port
53816 ssh2: RSA SHA256:M8ikhcEDm2tQ95Z0o7ZvufqEixCFct
+wowZLNzNlBT0
Mar 14 06:51:36 servera.lab.example.com sshd[1090]: p
am_unix(sshd:session): session opened for user studen
t(uid=1000) by (uid=0)

```

Pressione **q** para sair do comando.

6. Liste os estados habilitados ou os desabilitados de todas as unidades de serviço.

```

[student@servera ~]$systemctl list-unit-files --type=ser
vice
UNIT FILE                                STATE      VENDOR
PRESET
arp-ethers.service                      disabled   disable
d
atd.service                             enabled    enabled
auditd.service                          enabled    enabled
auth-rpcgss-module.service              static     -
autovt@.service                         alias      -

```

blk-availability.service	disabled	disable
d		
bluetooth.service	enabled	enabled
chrony-wait.service	disabled	disable
d		
chronyd.service	enabled	enabled
...output omitted...		

Pressione **q** para sair do comando.

7. Retorne ao sistema `workstation` como o usuário `student`.

```
[student@servera ~]$exit
logout
Connection to servera closed.
[student@workstation]$
```

Encerramento

Na máquina `workstation`, altere para o diretório pessoal do usuário `student` e use o comando `lab` para concluir este exercício. Essa etapa é importante para garantir que recursos de exercícios anteriores não afetem exercícios futuros.

```
[student@workstation ~]$lab finish services-identify
```

Isso conclui a seção.