Troubleshooting 2 – “SSH caiu no Servidor Linux”

Ambientação

Este laboratório foi desenvolvido para simular uma falha crítica em um servidor Linux Ubuntu: a interrupção do serviço SSH, impedindo o acesso remoto essencial para operações diárias. Para reproduzir essa condição, foi introduzida intencionalmente uma configuração inválida no arquivo /etc/ssh/sshd_config, causando a falha do serviço ao ser reiniciado. O objetivo principal é duplo:

- Diagnosticar e resolver a falha seguindo boas práticas de suporte técnico;
- Realizar uma análise complementar com olhar de segurança da informação, verificando possíveis sinais de ataque e oportunidades de hardening pós-incidente.

Processo do troubleshooting

O primeiro passo foi confirmar a indisponibilidade do serviço por meio de uma tentativa de conexão SSH externa, que falhou imediatamente. Em seguida, acessei o servidor localmente (via console) e executei o comando ***sudo systemctl status ssh***, que retornou o estado ***“inactive (dead)”*** e indicou genericamente que o serviço não havia iniciado.

Para identificar a causa raiz, consultei os logs específicos do serviço com o comando ***sudo journalctl -u ssh --no-pager -n 20***

A análise revelou um erro de sintaxe na linha 133 do arquivo de configuração (/etc/ssh/sshd_config), referente à opção inválida **EssaConfigNaoExiste**.

Como prática recomendada, validei a configuração antes de qualquer reinício com o comando ***sudo sshd -t***

Esse utilitário testa a sintaxe do arquivo sem interromper o serviço atual, confirmando exatamente o mesmo erro encontrado nos logs — o que permitiu diagnosticar o problema com precisão e segurança.

Análise com perspectiva de segurança

Mesmo tratando-se de uma falha de configuração autoinfligida, é fundamental descartar atividades maliciosas que possam ter contribuído ou explorado a indisponibilidade.

Verifiquei tentativas de brute force no arquivo de autenticação com o comando ***sudo grep -i "failed password" /var/log/auth.log | tail -10*** e nenhum padrão suspeito foi identificado, conforme esperado em um ambiente controlado.

Consultei o histórico de logins recentes com ***sudo last***, confirmando que todos os acessos foram legítimos e realizados durante os testes.

Por fim, executei uma auditoria de segurança com a ferramenta Lynis, amplamente utilizada em ambientes corporativos para avaliação de postura de segurança. A auditoria gerou recomendações críticas para o hardening do servidor, destacando três ações prioritárias:

- Desativar o login root via SSH, reduzindo o risco de acesso privilegiado direto;
- Alterar a porta padrão do SSH (22), dificultando varreduras automatizadas;
- Instalar e configurar o fail2ban, capaz de bloquear IPs após múltiplas tentativas de login falhas.

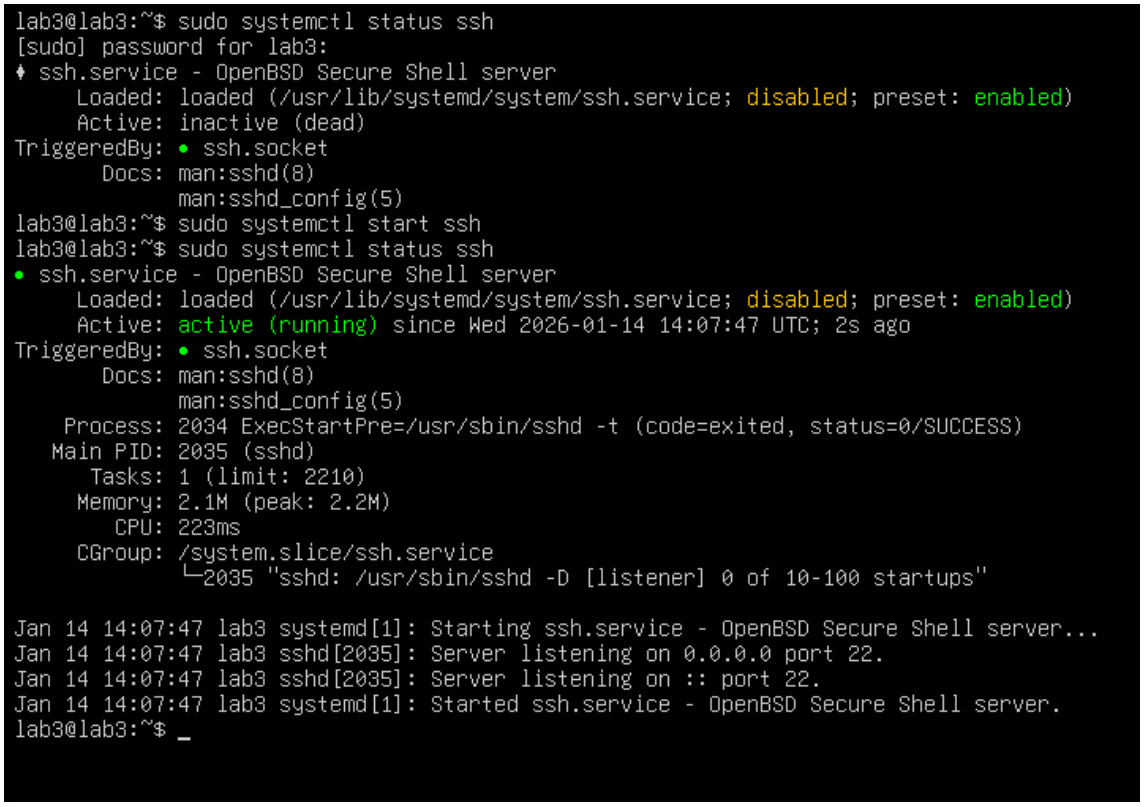
Essas medidas não apenas previnem ataques comuns, mas também demonstram maturidade na gestão de servidores expostos à rede.

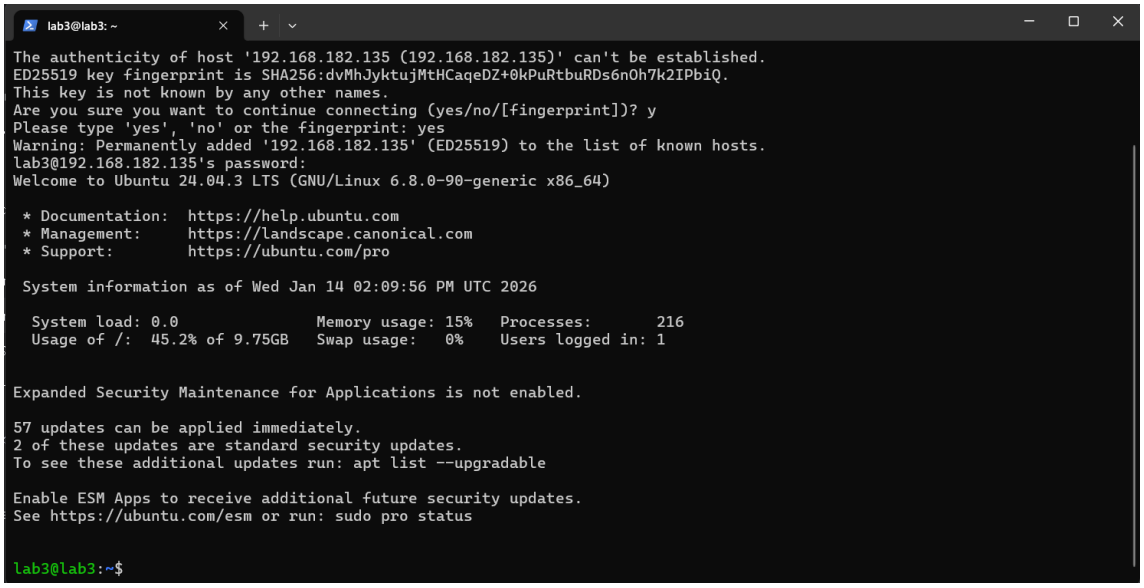
Resolução do problema

A correção foi simples e direta, editei o arquivo **/etc/ssh/sshd_config** e removi a linha 133 contendo a opção inválida. Em seguida, validei novamente a sintaxe com ***sudo sshd -t*** — ausência de mensagens de erro confirmou que a configuração estava correta.

Após reiniciar o serviço com ***sudo systemctl restart ssh***, realizei uma nova tentativa de conexão remota, que foi bem-sucedida. O serviço SSH foi restaurado, e as recomendações de segurança foram documentadas para implementação futura.

Prints do passo a passo





```
 GNU nano 7.2                                                /etc/ssh/sshd_config
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via KbdInteractiveAuthentication may bypass
# the setting of "PermitRootLogin prohibit-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and KbdInteractiveAuthentication to 'no'.
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem       sftp    /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server

EstaConfigNaoExiste yes


lab3@lab3:~$
```

```
lab3@lab3:~$ sudo systemctl restart ssh
Job for ssh.service failed because the control process exited with error code.
See "systemctl status ssh.service" and "journalctl -xeu ssh.service" for details.
lab3@lab3:~$ sudo systemctl status ssh
× ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
     Active: failed (Result: exit-code) since Wed 2026-01-14 14:13:51 UTC; 16s ago
   Duration: 6min 2.675s
TriggeredBy: × ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 2154 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=255/EXCEPTION)
        CPU: 11ms

Jan 14 14:13:51 lab3 systemd[1]: ssh.service: Control process exited, code=exited, status=255/EXCEPTION
Jan 14 14:13:51 lab3 systemd[1]: ssh.service: Failed with result 'exit-code'.
Jan 14 14:13:51 lab3 systemd[1]: Failed to start ssh.service - OpenBSD Secure Shell server.
Jan 14 14:13:51 lab3 systemd[1]: ssh.service: Scheduled restart job, restart counter is at 5.
Jan 14 14:13:51 lab3 systemd[1]: ssh.service: Start request repeated too quickly.
Jan 14 14:13:51 lab3 systemd[1]: ssh.service: Failed with result 'exit-code'.
Jan 14 14:13:51 lab3 systemd[1]: Failed to start ssh.service - OpenBSD Secure Shell server.
lab3@lab3:~$
```

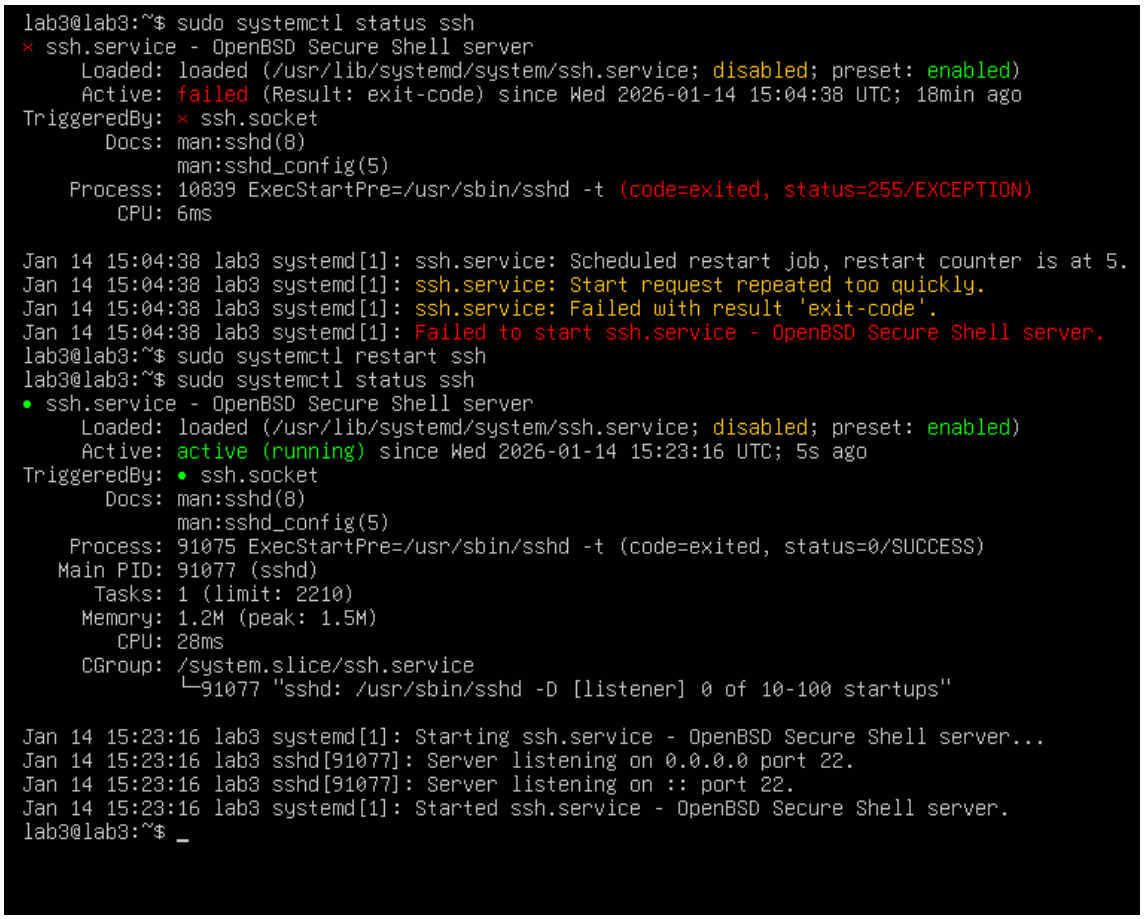
```
Windows PowerShell
O Windows PowerShell
Copyright (C) Microsoft Corporation. Todos os direitos reservados.

Instale o PowerShell mais recente para obter novos recursos e aprimoramentos! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> ssh lab3@192.168.182.135
ssh: connect to host 192.168.182.135 port 22: Connection refused
PS C:\WINDOWS\system32>
```

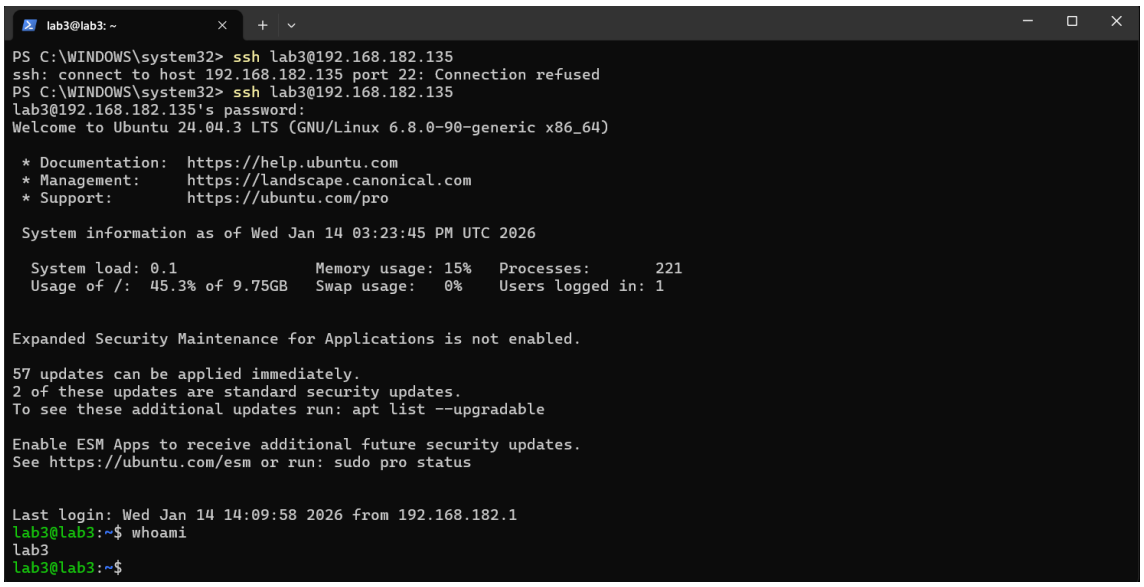
```
    - Checking LVM volumes                                    [ FOUND ]
  - Query swap partitions (fstab)                             [ OK ]
  - Testing swap partitions                                   [ OK ]
  - Testing /proc mount (hidepid)                             [ SUGGESTION ]
  - Checking for old files in /tmp                            [ OK ]
  - Checking /tmp sticky bit                                  [ OK ]
  - Checking /var/tmp sticky bit                              [ OK ]
  - ACL support root file system                              [ ENABLED ]
  - Mount options of /                                        [ OK ]
  - Mount options of /boot                                    [ DEFAULT ]
  - Mount options of /dev                                     [ PARTIALLY HARDENED ]
  - Mount options of /dev/shm                                 [ PARTIALLY HARDENED ]
  - Mount options of /run                                     [ HARDENED ]
  - Total without nodev:5 noexec:7 nosuid:3 ro or noexec (W^X): 7 of total 22
  - Disable kernel support of some filesystems

[+] USB Devices
------------------------------------
  - Checking usb-storage driver (modprobe config)             [ NOT DISABLED ]
  - Checking USB devices authorization                        [ ENABLED ]
  - Checking USBGuard                                         [ NOT FOUND ]

[+] Storage
------------------------------------
  - Checking firewire ohci driver (modprobe config)           [ DISABLED ]

[+] NFS
------------------------------------
  - Check running NFS daemon                                  [ NOT FOUND ]

[+] Name services
------------------------------------
  - Checking search domains                                   [ FOUND ]
  - Checking /etc/resolv.conf options                         [ FOUND ]
  - Searching DNS domain name                                 [ UNKNOWN ]
  - Checking /etc/hosts
    - Duplicate entries in hosts file                         [ NONE ]
    - Presence of configured hostname in /etc/hosts           [ FOUND ]
    - Hostname mapped to localhost                            [ NOT FOUND ]
    - Localhost mapping to IP address                         [ OK ]

[+] Ports and packages
------------------------------------
  - Searching package managers
    - Searching dpkg package manager                          [ FOUND ]
      - Querying package manager
    - Query unpurged packages                                 [ NONE ]
  - Checking security repository in sources.list.d directory  [ OK ]
  - Checking APT package database                             [ OK ]
```

```
-- Boot cbdf95aea39545d89c1db11e7af80bf5 --
Jan 14 14:07:47 lab3 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jan 14 14:07:47 lab3 sshd[2035]: Server listening on 0.0.0.0 port 22.
Jan 14 14:07:47 lab3 sshd[2035]: Server listening on :: port 22.
Jan 14 14:07:47 lab3 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Jan 14 14:09:56 lab3 sshd[2055]: Accepted password for lab3 from 192.168.182.1 port 23969 ssh2
Jan 14 14:09:56 lab3 sshd[2055]: pam_unix(sshd:session): session opened for user lab3(uid=1000) by lab3(uid=0)
Jan 14 14:13:50 lab3 sshd[2035]: Received signal 15; terminating.
Jan 14 14:13:50 lab3 systemd[1]: Stopping ssh.service - OpenBSD Secure Shell server...
Jan 14 14:13:50 lab3 systemd[1]: ssh.service: Deactivated successfully.
Jan 14 14:13:50 lab3 systemd[1]: Stopped ssh.service - OpenBSD Secure Shell server.
Jan 14 14:13:50 lab3 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jan 14 14:13:50 lab3 sshd[2146]: /etc/ssh/sshd_config: line 133: Bad configuration option: EstaConfigNaoExiste
Jan 14 14:13:50 lab3 sshd[2146]: /etc/ssh/sshd_config: terminating, 1 bad configuration options
Jan 14 14:13:50 lab3 systemd[1]: ssh.service: Control process exited, code=exited, status=255/EXCEPTION
Jan 14 14:13:50 lab3 systemd[1]: ssh.service: Failed with result 'exit-code'.
Jan 14 14:13:50 lab3 systemd[1]: Failed to start ssh.service - OpenBSD Secure Shell server.
Jan 14 14:13:50 lab3 systemd[1]: ssh.service: Scheduled restart job, restart counter is at 1.
Jan 14 14:13:50 lab3 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jan 14 14:13:50 lab3 sshd[2148]: /etc/ssh/sshd_config: line 133: Bad configuration option: EstaConfigNaoExiste
Jan 14 14:13:50 lab3 sshd[2148]: /etc/ssh/sshd_config: terminating, 1 bad configuration options
Jan 14 14:13:50 lab3 systemd[1]: ssh.service: Control process exited, code=exited, status=255/EXCEPTION
Jan 14 14:13:50 lab3 systemd[1]: ssh.service: Failed with result 'exit-code'.
Jan 14 14:13:50 lab3 systemd[1]: Failed to start ssh.service - OpenBSD Secure Shell server.
Jan 14 14:13:50 lab3 systemd[1]: ssh.service: Scheduled restart job, restart counter is at 2.
Jan 14 14:13:50 lab3 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jan 14 14:13:50 lab3 sshd[2150]: /etc/ssh/sshd_config: line 133: Bad configuration option: EstaConfigNaoExiste
Jan 14 14:13:50 lab3 sshd[2150]: /etc/ssh/sshd_config: terminating, 1 bad configuration options
Jan 14 14:13:50 lab3 systemd[1]: ssh.service: Control process exited, code=exited, status=255/EXCEPTION
Jan 14 14:13:50 lab3 systemd[1]: ssh.service: Failed with result 'exit-code'.
Jan 14 14:13:50 lab3 systemd[1]: Failed to start ssh.service - OpenBSD Secure Shell server.
Jan 14 14:13:50 lab3 systemd[1]: ssh.service: Scheduled restart job, restart counter is at 3.
Jan 14 14:13:50 lab3 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jan 14 14:13:50 lab3 sshd[2152]: /etc/ssh/sshd_config: line 133: Bad configuration option: EstaConfigNaoExiste
Jan 14 14:13:50 lab3 sshd[2152]: /etc/ssh/sshd_config: terminating, 1 bad configuration options
Jan 14 14:13:50 lab3 systemd[1]: ssh.service: Control process exited, code=exited, status=255/EXCEPTION
Jan 14 14:13:50 lab3 systemd[1]: ssh.service: Failed with result 'exit-code'.
Jan 14 14:13:50 lab3 systemd[1]: Failed to start ssh.service - OpenBSD Secure Shell server.
Jan 14 14:13:51 lab3 systemd[1]: ssh.service: Scheduled restart job, restart counter is at 4.
Jan 14 14:13:51 lab3 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jan 14 14:13:51 lab3 sshd[2154]: /etc/ssh/sshd_config: line 133: Bad configuration option: EstaConfigNaoExiste
Jan 14 14:13:51 lab3 sshd[2154]: /etc/ssh/sshd_config: terminating, 1 bad configuration options
Jan 14 14:13:51 lab3 systemd[1]: ssh.service: Control process exited, code=exited, status=255/EXCEPTION
Jan 14 14:13:51 lab3 systemd[1]: ssh.service: Failed with result 'exit-code'.
Jan 14 14:13:51 lab3 systemd[1]: Failed to start ssh.service - OpenBSD Secure Shell server.
Jan 14 14:13:51 lab3 systemd[1]: ssh.service: Scheduled restart job, restart counter is at 5.
Jan 14 14:13:51 lab3 systemd[1]: ssh.service: Start request repeated too quickly.
Jan 14 14:13:51 lab3 systemd[1]: ssh.service: Failed with result 'exit-code'.
Jan 14 14:13:51 lab3 systemd[1]: Failed to start ssh.service - OpenBSD Secure Shell server.
lines 17-65/65 (END)
```

```
lab3@lab3:~$ sudo sshd -t
/etc/ssh/sshd_config: line 133: Bad configuration option: EstaConfigNaoExiste
/etc/ssh/sshd_config: terminating, 1 bad configuration options
lab3@lab3:~$ _
```

```
lab3@lab3:~$ sudo grep "Failed Password" /var/log/auth.log | tail -10
2026-01-14T14:23:42.203554+00:00 lab3 sudo:     lab3 : TTY=tty1 ; PWD=/home/lab3 ; USER=root ; COMMAND=/usr/bin/grep 'Failed Password' /var/log/auth.log
lab3@lab3:~$ _
```


lab3@lab3:~$ sudo systemctl status ssh
× ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
Active: failed (Result: exit-code) since Wed 2026-01-14 15:04:38 UTC; 18min ago
TriggeredBy: × ssh.socket
Docs: man:sshd(8)
man:sshd_config(5)
Process: 10839 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=255/EXCEPTION)
CPU: 6ms
Jan 14 15:04:38 lab3 systemd[1]: ssh.service: Scheduled restart job, restart counter is at 5.
Jan 14 15:04:38 lab3 systemd[1]: ssh.service: Start request repeated too quickly.
Jan 14 15:04:38 lab3 systemd[1]: ssh.service: Failed with result 'exit-code'.
Jan 14 15:04:38 lab3 systemd[1]: Failed to start ssh.service - OpenBSD Secure Shell server.
lab3@lab3:~$ sudo systemctl restart ssh
lab3@lab3:~$ sudo systemctl status ssh
• ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
Active: active (running) since Wed 2026-01-14 15:23:16 UTC; 5s ago
TriggeredBy: • ssh.socket
Docs: man:sshd(8)
man:sshd_config(5)
Process: 91075 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
Main PID: 91077 (sshd)
Tasks: 1 (limit: 2210)
Memory: 1.2M (peak: 1.5M)
CPU: 28ms
CGroup: /system.slice/ssh.service
└─91077 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
Jan 14 15:23:16 lab3 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jan 14 15:23:16 lab3 sshd[91077]: Server listening on 0.0.0.0 port 22.
Jan 14 15:23:16 lab3 sshd[91077]: Server listening on :: port 22.
Jan 14 15:23:16 lab3 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
lab3@lab3:~$


lab3@lab3: ~
PS C:\WINDOWS\system32> ssh lab3@192.168.182.135
ssh: connect to host 192.168.182.135 port 22: Connection refused
PS C:\WINDOWS\system32> ssh lab3@192.168.182.135
lab3@192.168.182.135's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-90-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
System information as of Wed Jan 14 03:23:45 PM UTC 2026
System load: 0.1 Memory usage: 15% Processes: 221
Usage of /: 45.3% of 9.75GB Swap usage: 0% Users logged in: 1
Expanded Security Maintenance for Applications is not enabled.
57 updates can be applied immediately.
2 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
Last login: Wed Jan 14 14:09:58 2026 from 192.168.182.1
lab3@lab3:~$ whoami
lab3
lab3@lab3:~$