Strecht Simulados · Guia de preparação



Guia de preparação LPIC-1 102

Tudo o que a prova cobra, organizado por domínio: conceitos-chave, comparações que confundem, pegadinhas reais, gatilhos do enunciado, questões comentadas e um plano para chegar pronto ao exame.

6 capítulos por domínio	**36** questões comentadas	**65%** nota de corte
6 provas completas no curso		

ANTES DE COMEÇAR

Como usar este guia

Este guia foi feito para ser estudado junto com as 6 provas completas do curso LPIC-1 102: o guia explica o que cai e onde estão as armadilhas; as provas treinam o ritmo e mostram o que você ainda não domina.

Quando	O que fazer
Semana 1	Faça o teste diagnóstico (página seguinte) e leia os capítulos 1 e 2. No fim da semana, faça a Prova 1 do curso no tempo do exame.
Semana 2	Leia os demais capítulos, começando pelos domínios em que você errou mais no diagnóstico. Faça as provas 2 e 3.
Semana 3	Releia os alertas de pegadinha e as tabelas de comparação. Faça as provas 4 e 5 e revise cada erro pela explicação.
Semana 4	Estude a folha de cola, faça a Prova 6 e refaça as provas abaixo de 80%. Agende o exame quando estiver acima de 80% em todas (a nota de corte é 65%).

Mapa do exame

Cada prova do curso tem 60 questões e 90 minutos, no formato do exame. Referência de aprovação: 65%.

Domínio (capítulo)	Peso	Neste guia
1. 105 Shells e Scripts	13,3%	17 conceitos · 14 pegadinhas
2. 106 Interfaces de Usuário e Desktops	6,7%	16 conceitos · 12 pegadinhas
3. 107 Tarefas Administrativas	20,0%	17 conceitos · 14 pegadinhas
4. 108 Serviços Essenciais do Sistema	20,0%	18 conceitos · 14 pegadinhas
5. 109 Fundamentos de Rede	23,3%	16 conceitos · 14 pegadinhas
6. 110 Segurança	16,7%	15 conceitos · 14 pegadinhas

Como ler os capítulos: os **tópicos-chave** são o que mais cai; a **tabela de memorização** separa o que a prova costuma confundir; os **alertas de prova** mostram as armadilhas das alternativas erradas; os **gatilhos** ligam palavras do enunciado à resposta; e o **checklist** diz se você está pronto para o domínio.

Estude um pouco todo dia, de graça

Instagram @strecht.simulados

Um post de prova por dia: questão comentada, pegadinhas e o “não confunda” de cada certificação.

Seguir no Instagram →

YouTube Strecht Simulados

Shorts diários com pegadinhas de prova e, aos sábados, um simulado comentado.

Inscrever-se no canal →

DIAGNÓSTICO

Você já sabe isso?

Responda às 12 questões sem consultar nada. As respostas, com a explicação e o capítulo para revisar, estão no fim do guia. Comece o estudo pelos capítulos em que errou.

D1 · 105 Shells e Scripts

Um script executado com ./config.sh define export APP=1. Depois que ele termina, a variável não existe no shell do usuário. Por quê?

A. O script rodou em um processo filho
B. O bash não aceita letras maiúsculas
C. A variável foi apagada pelo cron
D. O export só vale para o root

D2 · 105 Shells e Scripts

Um script recém-criado retorna Permission denied ao ser executado com ./script.sh. O que falta?

A. Permissão de execução no arquivo
B. Um alias com o nome do script
C. Uma variável PATH mais longa
D. Uma linha export no início

D3 · 105 Shells e Scripts

Qual expressão calcula a soma de A e B em um script bash?

A. TOTAL={A + B}
B. TOTAL=$((A + B))
C. TOTAL=$(A + B)
D. TOTAL=[A + B]

D4 · 106 Interfaces de Usuário e Desktops

Na variável DISPLAY=:0, o que o :0 representa?

A. A primeira placa de rede
B. A porta 0 do servidor SSH
C. O display 0 da máquina local
D. O primeiro usuário do sistema

D5 · 106 Interfaces de Usuário e Desktops

Qual protocolo é usado com frequência para acessar a tela de máquinas virtuais no KVM, como no virt-manager?

A. SNMP
B. SFTP
C. SMB
D. SPICE

D6 · 106 Interfaces de Usuário e Desktops

Qual protocolo permite que um terminal remoto obtenha a tela de login gráfica de um servidor X pela rede?

A. SMTP
B. XDMCP
C. DHCP
D. LDAP

D7 · 107 Tarefas Administrativas

Qual comando mostra a data e a hora atuais em UTC?

A. date -I
B. date -r
C. date -s
D. date -u

D8 · 107 Tarefas Administrativas

Qual comando define o fuso horário do sistema para America/Sao_Paulo com systemd?

A. localectl set-timezone America/Sao_Paulo
B. hwclock --timezone America/Sao_Paulo
C. date --zone America/Sao_Paulo
D. timedatectl set-timezone America/Sao_Paulo

D9 · 107 Tarefas Administrativas

Qual comando muda o nome de login do usuário jsilva para joao.silva?

A. usermod -l joao.silva jsilva
B. usermod -d joao.silva jsilva
C. usermod -g joao.silva jsilva
D. usermod -c joao.silva jsilva

D10 · 108 Serviços Essenciais do Sistema

Qual comando mostra as fontes de tempo usadas pelo chrony e o estado de sincronização?

A. chronyc shutdown
B. chronyc sources
C. hwclock --show
D. date --sources

D11 · 108 Serviços Essenciais do Sistema

Qual comando ativa a sincronização automática de horário via NTP em um sistema com systemd?

A. timedatectl set-ntp true
B. date --ntp true
C. timedatectl set-time true
D. hwclock --ntp true

D12 · 108 Serviços Essenciais do Sistema

Qual comando mostra qual é a impressora padrão do sistema?

A. lpstat -d
B. lpr -d
C. lpq -d
D. lprm -d

01

CAPÍTULO 1 · 13,3% DA PROVA

105 Shells e Scripts

Este domínio vale cerca de 13,3% e cobra duas coisas: ambiente do shell (arquivos de inicialização, variáveis, aliases, funções, source) e scripts bash (parâmetros especiais, testes, laços, if/case, códigos de saída, read, printf). A prova adora detalhes de sintaxe: $(( )) x $( ), = para strings x -eq para números, -z x -n, && x ||, shebang com #! na ordem certa. Também preciso saber exatamente qual arquivo é lido em shell de login (/etc/profile e depois ~/.bash_profile, ~/.bash_login ou ~/.profile) e qual em shell interativo sem login (~/.bashrc). Onde mais erro é achar que executar um script com ./ altera o shell atual: só source ou . fazem isso.

Neste capítulo
17 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Arquivos de shell de login

O bash de login lê /etc/profile e depois o primeiro que existir entre ~/.bash_profile, ~/.bash_login e ~/.profile. Ao sair de um shell de login, executa ~/.bash_logout. O /etc/profile costuma ler os .sh de /etc/profile.d/.

Arquivos de shell interativo

~/.bashrc é lido por shells interativos sem login e é o lugar de aliases e funções pessoais. Em sistemas Debian, /etc/bash.bashrc vale para todos os usuários em shells interativos.

/etc/environment

Define variáveis para todos os usuários no formato VAR=valor; é lido pelo PAM, não pelo shell, e não é um script (aceita só atribuições simples).

/etc/skel x /etc/profile.d

/etc/skel só é copiado para usuários novos. Para acrescentar variáveis ao ambiente de login de todos sem editar o /etc/profile, coloca-se um script em /etc/profile.d/.

source e .

source arquivo ou . arquivo executam os comandos no shell atual, sem exigir permissão de execução (só leitura). Executar com ./script cria um processo filho, então variáveis exportadas nele somem quando termina.

Variáveis e ambiente

Atribuição sem espaço ao redor do = e sem $ (HOJE=valor). VAR=valor comando define a variável só para aquele processo (env faz o mesmo); export altera o shell atual. set lista variáveis e funções, inclusive não exportadas; env e printenv mostram só o ambiente exportado; declare -f lista funções.

PATH, PS1 e PS2

PATH define onde procurar comandos (incluir ~/bin para executar scripts pelo nome). PS1 é o prompt principal, com sequências como \u (usuário), \h (máquina) e \w (diretório); PS2 é o prompt de continuação.

Aliases

alias cria apelidos; unalias remove (unalias -a remove todos). Um alias criado no terminal some ao abrir outro: para persistir, coloque no ~/.bashrc. unset remove variáveis e funções, não aliases.

Parâmetros especiais

$0 é o nome do script; $1, $2... os argumentos; $# a quantidade; $@ todos (com aspas, "$@" preserva argumentos com espaços); $? o código de saída do último comando. shift descarta $1 e desloca os demais (shift N desloca N).

Shebang e permissão

A primeira linha #!/bin/bash define o interpretador. Para rodar com ./script.sh é preciso o bit x; sem ele vem Permission denied (alternativa: bash script.sh).

Testes com [ ]

Arquivos: -f arquivo comum, -d diretório, -e existe, -r leitura, -x execução, -s tamanho maior que zero. Strings: -z vazia, -n não vazia, = e != para comparar. Números: -eq, -ne, -lt, -le, -gt, -ge. Aspas em "$VAR" evitam erros com valores vazios.

Aritmética e substituição de comando

$(( )) avalia expressões inteiras (10/3 dá 3; para decimais, bc ou awk). $(comando) ou crases capturam a saída; $( ) é preferível por aninhar com facilidade.

Estruturas de controle

if condição; then ...; elif ...; else ...; fi. case valor in padrão) ... ;; esac. for var in lista; do ...; done; while repete enquanto a condição é verdadeira e until enquanto é falsa. O if avalia o código de saída do comando (grep -q retorna 0 quando encontra, sem imprimir).

Códigos de saída e && / ||

Zero indica sucesso; outros valores, erros definidos pelo script (exit 3). && executa o segundo se o primeiro deu certo; || executa se falhou; ; executa sempre. Em funções, return define o status sem encerrar o script; exit termina o shell.

Funções

Escritas como nome() { comandos; } ou function nome { comandos; }. alias não define funções.

read e printf

read lê da entrada padrão: -p mostra um prompt, -s oculta a digitação (senhas), -n espera um número de caracteres, -a lê para um vetor, -r não trata barras invertidas. while read linha percorre um arquivo linha por linha. printf usa formatos como %s, %d e \n.

Depuração

bash -n verifica a sintaxe sem executar; bash -x (ou set -x) mostra cada comando antes de executar, e set +x desativa.

Macetes para memorizar

💡 Ordem do login

/etc/profile primeiro; depois o primeiro de bash_PROFILE, bash_LOGIN, PROFILE (P-L-P).

💡 Parâmetros especiais

$# = # de quantos; $? = ? deu certo; $0 = o zero é o próprio script; $@ = @ todos.

💡 Testes de string

-z = zero (vazia); -n = non-zero (não vazia).

💡 Operadores numéricos

eq igual, ne diferente, lt menor, le menor ou igual, gt maior, ge maior ou igual (less/greater, than/equal).

&& e ||

&& = E deu certo, então faz; || = OU faz isso se falhou.

Parênteses

Dois parênteses fazem conta $(( )); um parêntese roda comando $( ).

Fechamentos

Palavra ao contrário fecha: if/fi, case/esac; laços fecham com do/done.

Tabela de memorização: não confunda

Quando é...	...e quando é
~/.bash_profile Variáveis só no login (shell de login).	**~/.bashrc** Aliases e funções em cada terminal interativo sem login.
source script / . script Aplicar mudanças no shell atual (variáveis permanecem).	**./script** Executar em processo filho; o ambiente do shell atual não muda.
$(( )) Cálculo aritmético inteiro.	**$( )** Substituição de comando (captura a saída).
= / != Comparar strings.	**-eq / -gt / -ne** Comparar números.
&& Executar o segundo comando só se o primeiro der certo.	**||** Executar o segundo só se o primeiro falhar (ex.: [-d /backup] || mkdir /backup).
bash -n Verificar sintaxe sem executar.	**bash -x** Executar mostrando cada comando (rastreamento).
return Encerrar só a função com um código.	**exit** Encerrar o script/shell inteiro.

Números que caem

Item	Valor
Código de saída de sucesso	**0**
Resultado de $((10 / 3))	**3 (só inteiros)**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que a variável exportada em ./config.sh some por causa de maiúsculas, do cron ou de permissão de root.
Como não cair: O script rodou em processo filho. Para afetar o shell atual: source config.sh ou . config.sh.

⚠ **Alerta de prova:** Aplicar o ~/.bashrc com bash ~/.bashrc ou chmod +x.
Como não cair: bash abre um subshell e chmod não aplica nada. Use source ~/.bashrc.

⚠ **Alerta de prova:** Escrever TOTAL=$(A + B) para somar.
Como não cair: $( ) tentaria executar o comando A. Aritmética é $((A + B)).

⚠ **Alerta de prova:** Esperar 3.33 de echo $((10 / 3)).
Como não cair: $(( )) só trabalha com inteiros: imprime 3.

⚠ **Alerta de prova:** Comparar strings com -eq ou -gt.
Como não cair: -eq e -gt são numéricos. Strings usam = e !=.

⚠ **Alerta de prova:** Usar -n para testar variável vazia ou -s para string.
Como não cair: -z testa vazia; -n não vazia; -s testa arquivo com tamanho maior que zero.

⚠ **Alerta de prova:** Usar [-d /backup] && mkdir /backup para criar se não existir.
Como não cair: && só criaria se já existisse. O certo é [-d /backup] || mkdir /backup.

⚠ **Alerta de prova:** Usar tar ... && mail para avisar falha.
Como não cair: && roda em caso de sucesso; ; roda sempre; | envia a saída. Para falha, ||.

⚠ **Alerta de prova:** Testar quantidade de argumentos com $? ou $0.
Como não cair: $# é a quantidade; $? é o código de saída; $0 o nome do script. Ex.: if [$# -ne 2]; then.

⚠ **Alerta de prova:** Escrever HOJE='date +%F' ou $HOJE=$(date +%F).
Como não cair: Aspas simples guardam o texto literal e não se usa $ na atribuição. Correto: HOJE=$(date +%F).

⚠ **Alerta de prova:** Usar for i in seq 1 5 ou for f in ls .log.
Como não cair: Sem substituição o for percorre as palavras literais. Use $(seq 1 5) e o glob *.log.

⚠ **Alerta de prova:** Usar exit 1 dentro da função para devolver erro.
Como não cair: exit encerra o script inteiro; return 1 encerra só a função.

⚠ **Alerta de prova:** Usar unset ll para remover um alias.
Como não cair: unset remove variáveis e funções; alias se remove com unalias ll.

⚠ **Alerta de prova:** Escrever o shebang como !#/bin/bash ou #/bin/bash.
Como não cair: A ordem é #! seguido do caminho: #!/bin/bash.

Como cai na prova

📝 **Como cai:** Qual arquivo de inicialização usar em um cenário (só no login, cada terminal, todos os usuários, ao sair).
Como resolver: Defina escopo (pessoal ~ x global /etc) e momento (login x interativo x saída). Login pessoal = ~/.bash_profile; interativo = ~/.bashrc; global login = /etc/profile ou /etc/profile.d; saída = ~/.bash_logout.

📝 **Como cai:** Trecho de script com sintaxe quase certa em quatro variações.
Como resolver: Confira cada detalhe: then/fi, do/done, ;; e esac, $(( )) x $( ), aspas, ausência de espaço no =, operador de string x número.

📝 **Como cai:** Qual parâmetro especial contém X ($#, $?, $0, $1, $@).
Como resolver: Associe: quantidade, código de saída, nome do script, primeiro argumento, todos os argumentos.

📝 **Como cai:** Escolher entre &&, || , ; e | para uma lógica condicional.
Como resolver: Pergunte: executar quando der certo (&&), quando falhar (||), sempre (;) ou passar a saída (|).

📝 **Como cai:** Escolha DUAS sobre source.
Como resolver: Lembre: roda no shell atual e . tem o mesmo efeito; não cria processo filho, não exige permissão de execução nem root.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
aplicar mudanças no terminal atual sem abrir outro	**source ~/.bashrc (ou .)**

variável exportada sumiu depois do script	**Processo filho; usar source**
variáveis para todos sem editar /etc/profile	**/etc/profile.d/**
VAR=valor lido pelo PAM, não pelo shell	**/etc/environment**
alias para todos os usuários em shells interativos (Debian)	**/etc/bash.bashrc**
alias some ao abrir novo terminal	**Colocar no ~/.bashrc**
executar ao sair do shell de login	**~/.bash_logout**
sem ~/.bash_profile nem ~/.bash_login	**~/.profile**
Permission denied ao rodar ./script.sh	**Falta o bit de execução**
ver cada comando antes de executar	**bash -x ou set -x**
verificar sintaxe sem executar	**bash -n**
saber se o texto aparece sem mostrar linhas	**grep -q dentro do if**
senha não deve aparecer ao digitar	**read -s**
percorrer argumentos preservando espaços	**"$@"**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- ./script roda em processo filho; source/. roda no shell atual.
- Strings com = e !=; números com -eq, -ne, -lt, -le, -gt, -ge.
- $# quantidade, $? código de saída, $0 nome, "$@" todos preservando espaços.
- Login: /etc/profile e depois ~/.bash_profile, ~/.bash_login ou ~/.profile; interativo: ~/.bashrc.
- Sem espaço ao redor do = na atribuição.

Essenciais para a prova (checklist)

- ☐ Sei a ordem de leitura dos arquivos em shell de login e em shell interativo.
- ☐ Sei quando usar /etc/profile.d, /etc/bash.bashrc, /etc/environment e /etc/skel.
- ☐ Sei a diferença entre source/. e executar com ./.
- ☐ Sei criar, persistir e remover aliases e definir funções.
- ☐ Sei o significado de $0, $1, $#, $?, $@ e o efeito do shift.
- ☐ Sei escrever testes de arquivo, de string e numéricos com [ ].
- ☐ Sei escrever if, case, for, while e until com a sintaxe correta.
- ☐ Sei usar $(( )), $( ), crases, &&, || e códigos de saída com exit e return.
- ☐ Sei usar read -p/-s e printf com formatos.

- [ ] Sei depurar com bash -n e bash -x.

Questões de revisão do capítulo

R1.1 · 105 Shells e Scripts

Qual arquivo pessoal é executado quando o usuário sai de um shell de login do bash?

A. ~/.profile
B. ~/.bash_logout
C. ~/.bashrc
D. ~/.bash_profile

R1.2 · 105 Shells e Scripts

Em um script bash, qual variável contém o número de argumentos recebidos?

A. $0
B. $#
C. $?
D. $@

R1.3 · 105 Shells e Scripts

Qual laço repete o bloco enquanto a condição for falsa, parando quando ela se tornar verdadeira?

A. Estrutura case
B. Laço while
C. Laço for
D. Laço until

R1.4 · 105 Shells e Scripts

Qual comando remove o alias ll da sessão atual?

A. unalias ll
B. unset ll
C. alias -r ll
D. export -n ll

Respostas comentadas

R1.1. B) ~/.bash_logout

Por quê: Pode limpar a tela ou arquivos temporários ao sair.

✗ A) Incorreta. Roda ao iniciar o login.
✗ C) Incorreta. Roda em shells interativos.
✗ D) Incorreta. Roda ao iniciar o login.

> **Dica de prova:** Ao sair do login: ~/.bash_logout.

R1.2. B) $#

Por quê: $1, $2... são argumentos; $# a quantidade; $@ todos; $0 o nome do script.

✗ A) Incorreta. Contém o nome do script.
✗ C) Incorreta. Contém o código de saída.
✗ D) Incorreta. Contém todos os argumentos.

> **Dica de prova:** Número de argumentos: $#.

R1.3. D) Laço until

Por quê: until é o inverso do while.

✗ A) Incorreta. Não é um laço.
✗ B) Incorreta. Executa enquanto a condição for verdadeira.
✗ C) Incorreta. Percorre uma lista.

> **Dica de prova:** Repetir até ficar verdadeiro: until.

R1.4. A) unalias ll

Por quê: unalias -a remove todos os apelidos.

✗ B) Incorreta. Remove variáveis e funções.
✗ C) Incorreta. Opção inválida.
✗ D) Incorreta. Tira variáveis do ambiente.

> **Dica de prova:** Remover alias: unalias.

02

CAPÍTULO 2 · 6,7% DA PROVA

106 Interfaces de Usuário e Desktops

É o menor domínio da prova (cerca de 6,7%), então eu foco nos pontos que se repetem: modelo cliente-servidor do X11, variável DISPLAY, ssh -X com X11Forwarding, Wayland e XWayland, protocolos de acesso remoto (VNC, RDP, SPICE, XDMCP) e recursos de acessibilidade. A prova adora inverter o X11: o servidor X roda na máquina onde está a tela, e o programa remoto é o cliente. Na acessibilidade, o erro clássico é confundir teclas de aderência, teclas lentas, teclas de repercussão e teclas do mouse. Também preciso separar gerenciador de exibição (GDM, LightDM, SDDM), gerenciador de janelas e ambiente de desktop.

Neste capítulo

16 tópicos-chave · 12 pegadinhas · 5 macetes · 12 gatilhos · 4 questões comentadas

Tópicos-chave

Modelo cliente-servidor do X11

No X11, o servidor X é quem exibe e roda na máquina local, onde está a tela; os programas são clientes. Ao abrir um programa remoto, o cliente X roda no servidor remoto e desenha na tela local.

DISPLAY

Variável que indica ao cliente X onde exibir a janela. O formato é host:display.tela; vazio antes do : indica a máquina local, então DISPLAY=:0 é o display 0 local. XAUTHORITY aponta o arquivo de autorização do X.

ssh -X e X11Forwarding

ssh -X usuario@servidor executa um programa gráfico remoto e o exibe localmente. No servidor, o sshd_config precisa de X11Forwarding yes e o xauth instalado. É mais seguro que liberar o servidor X na rede.

xhost +

Libera o servidor X para qualquer máquina, por isso é inseguro. O controle por xauth ou o encaminhamento X pelo SSH são as alternativas seguras.

Wayland

Protocolo de exibição que vem substituindo o X11; o compositor atua como servidor de exibição e gerencia a exibição.

XWayland

Mantém a compatibilidade com aplicativos feitos apenas para X11 em uma sessão Wayland.

Xorg e xorg.conf

Xorg é um servidor de exibição. A configuração tradicional fica em /etc/X11/xorg.conf; hoje o Xorg detecta quase tudo sozinho e ajustes ficam em /etc/X11/xorg.conf.d. XFree86 é uma implementação antiga do X11.

Gerenciador de exibição

Display manager como GDM, LightDM ou SDDM: mostra a tela de login gráfica, autentica e inicia a sessão gráfica do usuário.

Gerenciador de janelas x ambiente de desktop

O ambiente de desktop (GNOME, KDE Plasma, Xfce, Cinnamon) reúne gerenciador de janelas, painéis e aplicativos. O gerenciador de janelas sozinho não inclui navegador nem escritório.

XDMCP

Protocolo que permite a um terminal remoto obter a tela de login gráfica de um servidor X pela rede. Não é criptografado e deve ser usado com cuidado.

VNC, RDP e SPICE

VNC é comum para ver a mesma tela do usuário remotamente. RDP é o protocolo do cliente de área de trabalho remota nativo do Windows; no Linux, o xrdp oferece RDP. SPICE (e VNC) são comuns para consoles de VMs no KVM, como no virt-manager.

Teclas de aderência (sticky keys)

Mantêm Ctrl, Shift e Alt ativos até a próxima tecla, para quem não consegue pressionar duas teclas ao mesmo tempo.

Teclas lentas e de repercussão

Teclas lentas (slow keys) só aceitam teclas mantidas pressionadas por um tempo. Teclas de repercussão (bounce keys) ignoram repetições rápidas da mesma tecla. Ambas reduzem acionamentos acidentais, por exemplo por tremores.

Teclas do mouse

Mouse keys permitem mover o cursor usando o teclado numérico, para quem não consegue usar um mouse.

Leitor de tela e linha braille

O Orca é o leitor de tela comum em desktops Linux e lê o conteúdo em voz alta. Linhas braille têm celas táteis e funcionam junto com leitores de tela.

Baixa visão e teclado virtual

Alto contraste, fontes grandes e lupa de tela ajudam pessoas com baixa visão. O teclado virtual na tela permite digitar clicando, para quem não usa o teclado físico.

Macetes para memorizar

💡 Servidor X

Servidor X = onde estão os seus olhos (a tela). Cliente X = onde está o programa.

💡 DISPLAY

host:display.tela; sem host = esta máquina, então :0 é a primeira tela local.

💡 Acessibilidade de teclado

ADERÊNCIA gruda o Ctrl; LENTA exige segurar; REPERCUSSÃO ignora o quique repetido; MOUSE anda pelo teclado numérico.

💡 Protocolos remotos

VNC vê a tela, RDP fala com Windows, SPICE abre VM, XDMCP traz o login do X (sem cripto).

💡 Hierarquia gráfica

Display manager faz login -> ambiente de desktop (painéis + apps) -> gerenciador de janelas cuida das janelas.

Tabela de memorização: não confunda

Quando é...	...e quando é
Servidor X Roda na máquina local, onde está a tela, e exibe as janelas.	**Cliente X** É o programa; em acesso remoto, roda no servidor remoto onde está o programa.
DISPLAY Indica onde exibir a janela (host:display.tela).	**XAUTHORITY** Indica o arquivo de autorização do X.

Teclas de aderência Não consegue pressionar Ctrl e C ao mesmo tempo: mantém modificadores ativos.	**Teclas lentas** Aciona teclas sem querer: só aceita teclas mantidas pressionadas por um tempo.
Teclas de repercussão Ignora repetições rápidas da mesma tecla pressionada várias vezes sem querer.	**Teclas de repetição** Controla a repetição de caracteres.
VNC Acesso remoto vendo a mesma tela do usuário.	**RDP** Cliente de área de trabalho remota nativo do Windows acessando o Linux (xrdp).
Wayland Protocolo de exibição que substitui o X11, com o compositor como servidor.	**XWayland** Camada que roda apps X11 dentro de uma sessão Wayland.

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que o servidor X roda no servidor remoto, onde está o programa.
Como não cair: No X11 o servidor é quem exibe: fica na máquina local. No servidor remoto roda o cliente X.

⚠ **Alerta de prova:** Pensar que :0 em DISPLAY=:0 é a porta 0, a primeira placa de rede ou o primeiro usuário.
Como não cair: É o display 0 da máquina local; o formato é host:display.tela e host vazio = local.

⚠ **Alerta de prova:** Escolher XAUTHORITY, TERM ou HOSTNAME para dizer onde exibir a janela.
Como não cair: Onde exibir é DISPLAY. XAUTHORITY é o arquivo de autorização e TERM o tipo de terminal.

⚠ **Alerta de prova:** Achar que o ssh -X sem janelas se resolve com PasswordAuthentication ou PermitRootLogin.
Como não cair: A diretiva é X11Forwarding yes no sshd_config do servidor, com xauth instalado.

⚠ **Alerta de prova:** Usar ssh -L, -N ou -q para exibir programa gráfico remoto.
Como não cair: -X é encaminhamento X11. -L encaminha portas locais, -N não executa comandos e -q reduz mensagens.

⚠ **Alerta de prova:** Pensar que xhost + só bloqueia usuário, desliga o X ou apaga preferências.
Como não cair: xhost + libera o servidor X a qualquer máquina; por isso é inseguro.

⚠ **Alerta de prova:** Confundir XWayland com xargs, xinetd ou xdg-open pelo prefixo x.
Como não cair: xargs monta argumentos, xinetd é superservidor de rede, xdg-open abre arquivos. Compatibilidade X11 no Wayland é XWayland.

⚠ **Alerta de prova:** Marcar SPICE ou XDMCP como o protocolo que substitui o X11.
Como não cair: Quem substitui o X11 é o Wayland. SPICE é acesso a VMs e XDMCP é login remoto no X.

⚠ **Alerta de prova:** Escolher systemd, CUPS ou Xorg como ambiente de desktop.
Como não cair: Ambientes de desktop: GNOME, KDE Plasma, Xfce, Cinnamon. Xorg é servidor de exibição; systemd gerencia serviços; CUPS é impressão.

⚠ **Alerta de prova:** Confundir gerenciador de exibição com gerenciador de volumes, pacotes ou impressão.
Como não cair: GDM, LightDM e SDDM são gerenciadores de exibição: tela de login gráfica e início da sessão.

⚠ **Alerta de prova:** Usar teclas de aderência para quem pressiona a mesma tecla várias vezes sem querer.
Como não cair: Aderência mantém modificadores. Repetições rápidas acidentais = teclas de repercussão; pressão prolongada exigida = teclas lentas.

⚠ **Alerta de prova:** Marcar /etc/xdg/autostart ou /etc/xinetd.conf como configuração do servidor X.
Como não cair: A configuração tradicional do Xorg é /etc/X11/xorg.conf (ajustes em /etc/X11/xorg.conf.d).

Como cai na prova

📝 **Como cai:** Cenário de acessibilidade descrevendo a dificuldade de uma pessoa (tremor, uma mão, baixa visão, cegueira).
Como resolver: Mapeie a dificuldade ao recurso: modificadores = aderência; acionar sem querer = lentas; repetição rápida = repercussão; baixa visão = alto contraste e lupa; cegueira = leitor de tela e linha braille.

📝 **Como cai:** Pergunta sobre onde roda o servidor X ou o cliente X em acesso remoto.
Como resolver: Inverta a intuição: o servidor X fica na máquina com a tela (local); o programa remoto é cliente.

📝 **Como cai:** Qual protocolo para acesso gráfico remoto em um contexto específico (VM, Windows, login X, suporte).
Como resolver: Leia o contexto: VM = SPICE; Windows nativo = RDP; tela de login X = XDMCP; mesma tela do usuário = VNC. Descarte SNMP, SMB, LDAP, SMTP, DHCP.

📝 **Como cai:** Escolha DUAS: ambientes de desktop ou recursos para baixa visão.
Como resolver: Elimine o que é outro tipo de componente (Xorg, systemd, CUPS) ou recurso de teclado/mouse quando o problema é visual.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
aplicativo X11 em sessão Wayland	**XWayland**
compositor atua como servidor de exibição	**Wayland**
variável que diz ao cliente X onde exibir	**DISPLAY**
ssh -X não abre janelas	**X11Forwarding yes no sshd_config (e xauth no servidor)**
tela de login gráfica pela rede de um servidor X	**XDMCP (sem criptografia)**
console de VM no KVM/virt-manager	**SPICE (ou VNC)**
cliente de área de trabalho remota do Windows	**RDP (xrdp no Linux)**
ver a mesma tela do usuário remotamente	**VNC**
GDM, LightDM, SDDM	**Gerenciador de exibição**
não consegue pressionar Ctrl e C juntos	**Teclas de aderência**
mover o cursor pelo teclado numérico	**Teclas do mouse**
ler a tela em voz alta / celas táteis	**Leitor de tela (Orca) / linha braille**

🎯 Se você lembrar de só uma coisa deste capítulo...

- No X11, o servidor X roda na máquina local, onde está a tela.
- ssh -X precisa de X11Forwarding yes e xauth no servidor.
- xhost + libera o X para qualquer máquina: inseguro.
- XDMCP não é criptografado.
- XWayland mantém apps X11 funcionando no Wayland.

Essenciais para a prova (checklist)

- ☐ Sei explicar quem é servidor e quem é cliente no X11.
- ☐ Sei interpretar DISPLAY=:0 e para que serve XAUTHORITY.
- ☐ Sei habilitar e usar o encaminhamento X pelo SSH.
- ☐ Sei por que xhost + é inseguro.
- ☐ Sei diferenciar Wayland, XWayland, Xorg e onde fica o xorg.conf.
- ☐ Sei associar VNC, RDP, SPICE e XDMCP a seus cenários.
- ☐ Sei diferenciar gerenciador de exibição, gerenciador de janelas e ambiente de desktop.
- ☐ Sei associar cada recurso de acessibilidade (aderência, lentas, repercussão, teclas do mouse, leitor de tela, braille, lupa, alto contraste, teclado virtual) à necessidade.

Questões de revisão do capítulo

R2.1 · 106 Interfaces de Usuário e Desktops

Qual recurso de acessibilidade lê em voz alta o conteúdo da tela para usuários com deficiência visual?

A. Software de leitura de tela
B. Teclas de aderência
C. Tema de alto contraste
D. Teclas de repetição lenta

R2.2 · 106 Interfaces de Usuário e Desktops

Um técnico precisa acessar remotamente a área de trabalho gráfica de um Linux, vendo a mesma tela do usuário. Qual protocolo é comum para isso?

A. VNC
B. NTP
C. SMTP
D. DHCP

R2.3 · 106 Interfaces de Usuário e Desktops

Uma pessoa com dificuldade motora não consegue pressionar Ctrl e C ao mesmo tempo. Qual recurso de acessibilidade ajuda?

A. Teclas de aderência
B. Lupa de tela
C. Teclas lentas
D. Teclas de repetição

R2.4 · 106 Interfaces de Usuário e Desktops

Um usuário pressiona a mesma tecla várias vezes sem querer por causa de tremores. Qual recurso ignora repetições rápidas da mesma tecla?

A. Teclas do mouse
B. Teclas de aderência
C. Teclas de repercussão
D. Leitura de tela

Respostas comentadas

R2.1. A) Software de leitura de tela

Por quê: O Orca é o leitor de tela comum em desktops Linux; há também lupa, teclado virtual e braille.

✗ B) Incorreta. Ajudam a usar atalhos com uma mão.
✗ C) Incorreta. Melhora a visibilidade, sem fala.
✗ D) Incorreta. Evitam repetições acidentais.

> **Dica de prova:** Fala do conteúdo da tela: leitor de tela.

R2.2. A) VNC

Por quê: VNC, RDP, SPICE e XDMCP são usados para acesso gráfico remoto.

✗ B) Incorreta. Sincroniza relógios.
✗ C) Incorreta. Envia e-mails.
✗ D) Incorreta. Distribui endereços IP.

> **Dica de prova:** Área de trabalho remota: VNC ou RDP.

R2.3. A) Teclas de aderência

Por quê: Sticky keys mantêm Ctrl, Shift e Alt ativos até a próxima tecla.

✗ B) Incorreta. Amplia a imagem.
✗ C) Incorreta. Exigem pressionar a tecla por mais tempo.
✗ D) Incorreta. Controlam a repetição de caracteres.

> **Dica de prova:** Atalhos com uma tecla por vez: teclas de aderência.

R2.4. C) Teclas de repercussão

Por quê: Bounce keys, slow keys e sticky keys fazem parte das opções de teclado acessível.

✗ A) Incorreta. Movem o ponteiro.
✗ B) Incorreta. Mantêm modificadores ativos.
✗ D) Incorreta. Lê o conteúdo em voz.

> **Dica de prova:** Repetições acidentais: teclas de repercussão.

03

CAPÍTULO 3 · 20,0% DA PROVA

107 Tarefas Administrativas

Este domínio pesa cerca de 20% e reúne três blocos: contas e grupos (useradd, usermod, userdel, groupadd, groupmod, gpasswd, chage, passwd e os arquivos /etc/passwd, /etc/shadow, /etc/group, /etc/gshadow), agendamento (cron, at, batch, anacron e timers do systemd) e localização (locale, LANG, LC_*, iconv, fuso horário). A prova cobra muito a letra exata da opção: usermod -aG x -G, usermod -l x -d x -c, chage -M x -W x -E x -I, passwd -l x -e x -S. Também cai a leitura de linhas de crontab e dos campos do /etc/passwd e /etc/group. Onde mais erro é na lógica de cron.allow/cron.deny e na precedência LC_ALL > LC_* > LANG.

Neste capítulo
17 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

/etc/passwd

Campos: login, senha, UID, GID, comentário, home e shell. O x no segundo campo indica que a senha está no /etc/shadow. O passwd é legível por todos; o shadow só pelo root.

/etc/shadow e bloqueio

Guarda os hashes das senhas locais. Um ! no início do hash indica conta bloqueada, inserido por passwd -l ou usermod -L (desbloqueio com -u ou -U).

/etc/group e /etc/gshadow

/etc/group tem nome, senha (x), GID e lista de membros secundários. /etc/gshadow guarda as senhas criptografadas e os administradores dos grupos, como o shadow complementa o passwd.

useradd

-m cria o home copiando /etc/skel; -u define o UID; -e define a data de expiração da conta; -r cria conta de sistema; -d define o home, -g o grupo primário, -c o comentário, -f dias de inatividade, -k o diretório modelo. Altera /etc/passwd e /etc/shadow (e pode alterar /etc/group e /etc/gshadow).

Padrões de criação de contas

/etc/default/useradd guarda os padrões do useradd (shell, diretório base), vistos ou alterados com useradd -D. /etc/login.defs define faixas de UID (UID_MIN, geralmente 1000) e a validade máxima padrão das senhas para contas novas. /etc/skel contém os modelos como .bashrc e .profile.

usermod

-aG acrescenta grupos secundários (só -G substitui a lista); -l muda o login; -d muda o home e -m move o conteúdo; -s muda o shell (chsh também); -g muda o grupo primário; -c o comentário; -L/-U bloqueiam e desbloqueiam.

userdel e grupos

userdel -r apaga a conta, o home e o spool de e-mail; sem -r o home fica. groupadd cria, groupmod altera (-n renomeia, -g muda o GID) e groupdel remove grupos. gpasswd -a adiciona e -d remove membros. newgrp inicia um shell com outro grupo efetivo.

chage e passwd

chage -l mostra a validade; -M validade máxima; -m mínimo; -W dias de aviso; -I inatividade após expirar; -E expiração da conta; -d 0 força troca. passwd -l bloqueia, -u desbloqueia, -e força troca no próximo login, -d remove a senha e -S mostra o estado.

Consultas de identidade e consistência

id mostra UID, GID e grupos (id -u só o UID, id -un o nome); groups mostra os grupos. getent passwd consulta todas as fontes do nsswitch, inclusive LDAP. pwck verifica /etc/passwd e /etc/shadow e grpck verifica group e gshadow. vipw e vigr editam com bloqueio (-s edita os shadow).

UID 0 e contas de serviço

UID 0 identifica o superusuário: qualquer conta com UID 0 tem poderes de root. Contas de serviço usam /sbin/nologin ou /bin/false para impedir login interativo.

Crontab

Campos: minuto, hora, dia do mês, mês, dia da semana (0 ou 7 é domingo) e comando. */N significa a cada N unidades. Atalhos: @reboot, @hourly, @daily, @weekly, @monthly, @yearly. crontab -l lista, -e edita, -r remove, -u usuario permite ao root gerenciar outro usuário. MAILTO define quem recebe a saída (vazio desativa).

Crontabs do sistema

/etc/crontab e arquivos de /etc/cron.d têm um sexto campo com o usuário. Pacotes colocam tarefas em /etc/cron.d. Scripts sem horário vão em /etc/cron.hourly, daily, weekly ou monthly. Crontabs dos usuários ficam em /var/spool/cron (no Debian, /var/spool/cron/crontabs).

cron.allow e cron.deny

Se cron.allow existe, só os listados usam o crontab. Se não existe, cron.deny lista os bloqueados. A mesma lógica vale para at.allow e at.deny: sem at.allow e com at.deny vazio, todos podem usar o at; sem os dois arquivos, só o root.

at, batch e anacron

at agenda tarefas únicas (at 23:00, at now + 1 hour, at -f arquivo 18:00); atq e atrm listam e removem (= at -l e at -d). batch executa quando a carga do sistema baixar. anacron executa tarefas periódicas atrasadas em máquinas desligadas; o /etc/anacrontab tem período em dias, atraso em minutos, identificador e comando.

Timers do systemd

backup.timer ativa por padrão backup.service (a diretiva Unit= aponta outra). OnCalendar define horários de calendário; OnBootSec e OnUnitActiveSec definem intervalos. systemctl list-timers mostra a próxima e a última execução. systemd-run --on-active=30m cria um temporizador transitório.

Locale

Formato idioma_TERRITÓRIO.codificação (pt_BR.UTF-8). Precedência: LC_ALL, depois LC_*, depois LANG. LC_TIME controla datas, LC_NUMERIC números, LC_MONETARY moeda, LC_COLLATE ordenação. LANG=C (ou LC_ALL=C) deixa mensagens e ordenação previsíveis. locale mostra o atual, locale -a lista os disponíveis e localectl set-locale define o do sistema.

Codificação e fuso

UTF-8 codifica Unicode com tamanho variável e é compatível com ASCII nos primeiros 128 caracteres; iconv -f origem -t destino converte codificações. O fuso fica em /etc/localtime (link para /usr/share/zoneinfo), definido com timedatectl set-timezone Região/Cidade; tzselect ajuda a achar o nome. date -u mostra UTC e date +%F ou +%Y-%m-%d o formato ISO.

Macetes para memorizar

Campos do crontab

Minha Hora Dia Mês Semana: m h dom mon dow.

/etc/passwd

Login, senha(x), UID, GID, comentário, home, shell: sete campos, o último é o shell.

chage

M = Máximo, m = mínimo, W = Warning (aviso), I = Inativo, E = Expira a conta, l = lista.

usermod -aG

Sem o A de Adicionar, o G Golpeia a lista inteira.

allow x deny

Allow manda primeiro: se existe, só ele fala; senão, o deny diz quem fica de fora.

Precedência de locale

ALL > LC_* > LANG: o ALL atropela todos.

at

atq = queue (lista), atrm = remove, batch = quando o sistema descansar.

Tabela de memorização: não confunda

Quando é...	...e quando é
usermod -aG Acrescentar grupo secundário mantendo os outros.	**usermod -G** Substituir toda a lista de grupos secundários.
chage -M Validade máxima da senha em dias (ex.: expira a cada 90 dias).	**chage -E** Data de expiração da conta inteira.
chage -W Dias de aviso antes de a senha expirar.	**chage -I** Dias de inatividade após a senha expirar.
cron.allow Se existe, só os listados podem usar o crontab.	**cron.deny** Só vale quando cron.allow não existe; lista os bloqueados.
at Tarefa única em um horário (batch: quando a carga baixar).	**crontab / anacron** Tarefa repetida; anacron recupera execuções perdidas em máquina desligada.
/etc/crontab e /etc/cron.d Têm sexto campo com o usuário que executa.	**crontab do usuário** Sem campo de usuário; roda como o próprio dono.
LC_ALL Sobrepõe todas as configurações de localização.	**LANG** Valor padrão, usado quando LC_ALL e LC_* não estão definidos.

Números que caem

Item	Valor
UID do superusuário	**0**
Primeiro UID de usuário comum (UID_MIN)	**Geralmente 1000**
Domingo no campo dia da semana do crontab	**0 ou 7**
Campos do /etc/passwd	**7**
Campos do /etc/group	**4 (nome, senha, GID, membros)**
Compatibilidade UTF-8 com ASCII	**Primeiros 128 caracteres**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Usar usermod -G docker ana para adicionar ao grupo docker.
Como não cair: Sem -a, -G substitui a lista de grupos secundários. O certo é usermod -aG docker ana (ou gpasswd -a ana docker).

⚠ **Alerta de prova:** Usar usermod -d novo_home sem -m esperando mover os arquivos.
Como não cair: -d só altera o caminho; -m move o conteúdo antigo: usermod -d /home/novo -m usuario.

⚠ **Alerta de prova:** Usar usermod -d ou -c para renomear o login.
Como não cair: Renomear login é usermod -l novo antigo; -d é home e -c é comentário.

⚠ **Alerta de prova:** Usar chage -M 7 para avisar 7 dias antes.
Como não cair: Aviso é -W; -M é validade máxima, -E expiração da conta, -I inatividade.

⚠ **Alerta de prova:** Bloquear com passwd -d ou ver validade com passwd -l.
Como não cair: passwd -d remove a senha; passwd -l bloqueia; validade é chage -l.

⚠ **Alerta de prova:** Achar que userdel temp apaga o home.
Como não cair: Sem -r o diretório pessoal permanece; userdel -r apaga home e spool de e-mail.

⚠ **Alerta de prova:** Ler o x do /etc/passwd como conta bloqueada ou sem senha.
Como não cair: x indica que a senha está no /etc/shadow; bloqueio é ! no início do hash no shadow.

⚠ **Alerta de prova:** Com só estagiario no cron.deny e sem cron.allow, achar que ninguém ou só ele usa o cron.
Como não cair: Sem cron.allow, o deny lista os bloqueados: só estagiario fica sem acesso.

⚠ **Alerta de prova:** Escrever 15 * * * * para rodar a cada 15 minutos.
Como não cair: 15 no primeiro campo é o minuto 15 de cada hora. A cada 15 minutos é */15 * * * *.

⚠ **Alerta de prova:** Ler 30 2 * * 1 como dia 1 do mês.
Como não cair: O 1 está no quinto campo (dia da semana): é às 2h30 de toda segunda-feira.

⚠ **Alerta de prova:** Usar crontab -e joao ou crontab -l joao como root.
Como não cair: Outro usuário exige -u: crontab -u joao -l.

⚠ **Alerta de prova:** Usar localectl set-timezone para o fuso.
Como não cair: localectl trata locale e teclado; fuso é timedatectl set-timezone.

⚠ **Alerta de prova:** Escolher TZ, LANGUAGE ou LC_CTYPE como a variável que sobrepõe todas.
Como não cair: LC_ALL tem precedência sobre LC_* e LANG; TZ é fuso e LANGUAGE ordena idiomas de mensagens.

⚠ **Alerta de prova:** Usar tr, file ou locale para converter ISO-8859-1 em UTF-8.
Como não cair: Conversão de codificação é iconv -f ISO-8859-1 -t UTF-8.

Como cai na prova

📝 **Como cai:** Qual comando faz X com usuário/grupo, com quatro opções do mesmo comando (usermod -l/-d/-g/-c; chage -M/-W/-E/-I).
Como resolver: Traduza a ação para a letra: login, home, grupo, comentário, shell, aviso, validade, expiração. Desconfie de -G sem -a e de -d sem -m.

📝 **Como cai:** Interpretar uma linha de crontab ou escolher a linha que roda em determinada frequência.
Como resolver: Escreva mentalmente os cinco campos na ordem m h dom mon dow e posicione cada valor. Lembre que */N é passo e número fixo é instante.

📝 **Como cai:** Cenário com cron.allow/cron.deny ou at.allow/at.deny.
Como resolver: Primeiro pergunte se o allow existe. Se sim, só os listados. Se não, o deny bloqueia os listados; deny vazio libera todos.

📝 **Como cai:** Interpretar campos de /etc/passwd, /etc/group, /etc/shadow ou /etc/anacrontab.
Como resolver: Lembre a ordem dos campos e o significado de x e de ! no início do hash.

📝 **Como cai:** Escolher entre cron, at, batch, anacron e timer do systemd para um cenário.
Como resolver: Única = at; carga baixa = batch; repetida = cron; máquina desligada = anacron; systemd = timer com OnCalendar ou systemd-run.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
rodar uma única vez hoje às 23h	**at 23:00**
quando a carga do sistema estiver baixa	**batch**
notebook desligado à noite perde tarefas diárias	**anacron (/etc/anacrontab)**
pacote instala tarefa agendada sem editar /etc/crontab	**/etc/cron.d/**
rodar uma vez por dia sem escrever horário	**/etc/cron.daily/**
executar script sempre que o sistema iniciar	**@reboot no crontab**
para quem vai o e-mail com a saída do cron	**MAILTO**
tarefa única em 30 minutos com systemd	**systemd-run --on-active=30m**
horário de calendário em timer	**OnCalendar**
modelos copiados para o home de novos usuários	**/etc/skel**
faixas de UID para contas comuns e de sistema	**/etc/login.defs**
conta de serviço sem login interativo	**/sbin/nologin ou /bin/false**
entrada do usuário mesmo vinda do LDAP	**getent passwd usuario**
saída de comandos em inglês e ordenação previsível	**LANG=C (ou LC_ALL=C)**

🎯 Se você lembrar de só uma coisa deste capítulo...

- usermod -aG acrescenta; -G sozinho substitui.
- Se cron.allow existe, só os listados usam o cron.
- LC_ALL sobrepõe LC_* e LANG.
- userdel sem -r mantém o home.
- /etc/crontab e /etc/cron.d têm o campo de usuário.

Essenciais para a prova (checklist)

- ☐ Sei os campos de /etc/passwd, /etc/shadow, /etc/group e o significado de x e !.
- ☐ Sei criar usuário com home, UID, expiração e entender /etc/skel, /etc/default/useradd e /etc/login.defs.
- ☐ Sei usar usermod -aG, -l, -d -m, -s e userdel -r.
- ☐ Sei gerenciar grupos com groupadd, groupmod -n, gpasswd -a/-d e newgrp.
- ☐ Sei usar chage (-l, -M, -W, -E, -I) e passwd (-l, -u, -e, -S).
- ☐ Sei ler e escrever linhas de crontab, inclusive */N e @reboot.
- ☐ Sei a lógica de cron.allow/cron.deny e at.allow/at.deny.
- ☐ Sei usar at, atq, atrm, batch e o formato do /etc/anacrontab.
- ☐ Sei criar e listar timers do systemd (OnCalendar, list-timers, systemd-run).
- ☐ Sei a precedência de locale, usar locale, locale -a, localectl, iconv e definir o fuso.

Questões de revisão do capítulo

R3.1 · 107 Tarefas Administrativas

No /etc/group, o que aparece no quarto campo da linha dev:x:1005:ana,joao?

A. O diretório padrão do grupo
B. A senha do grupo em texto claro
C. Os membros secundários do grupo
D. O shell padrão do grupo

R3.2 · 107 Tarefas Administrativas

Um comando deve rodar uma única vez, hoje às 23h. Qual ferramenta é a mais adequada?

A. watch -n 23
B. crontab -e
C. at 23:00
D. anacron -n

R3.3 · 107 Tarefas Administrativas

Qual comando cria um novo grupo chamado auditoria?

A. useradd auditoria
B. groupadd auditoria
C. groupmod auditoria
D. newgrp auditoria

R3.4 · 107 Tarefas Administrativas

No /etc/shadow, a senha de uma conta começa com !. O que isso indica?

A. A senha está em texto claro
B. A senha nunca expira
C. A conta está bloqueada
D. A conta é do administrador

Respostas comentadas

R3.1. C) Os membros secundários do grupo

Por quê: Campos: nome, senha (x), GID e lista de membros.

✗ A) Incorreta. Não existe esse campo.
✗ B) Incorreta. O x indica senha em outro arquivo.
✗ D) Incorreta. Não existe esse campo.

> **Dica de prova:** Quarto campo do group: membros.

R3.2. C) at 23:00

Por quê: at agenda tarefas únicas; atq lista e atrm remove.

✗ A) Incorreta. Repete um comando em intervalos.
✗ B) Incorreta. Agenda execuções repetidas.
✗ D) Incorreta. Executa tarefas periódicas atrasadas.

> **Dica de prova:** Execução única: at.

R3.3. B) groupadd auditoria

Por quê: groupadd cria, groupmod altera e groupdel remove grupos.

✗ A) Incorreta. Cria um usuário.

✗ C) Incorreta. Altera grupos existentes.

✗ D) Incorreta. Troca o grupo da sessão.

> **Dica de prova:** Criar grupo: groupadd.

R3.4. C) A conta está bloqueada

Por quê: passwd -l e usermod -L inserem o ! no início do hash.

✗ A) Incorreta. Não é o significado.

✗ B) Incorreta. Não é o significado.

✗ D) Incorreta. Não é o significado.

> **Dica de prova:** ! no shadow: conta bloqueada.

04

CAPÍTULO 4 · 20,0% DA PROVA

108 Serviços Essenciais do Sistema

Aqui eu preciso dominar quatro blocos: hora do sistema (date, hwclock, timedatectl, chrony, ntpd), registro (journald, rsyslog, logrotate, logger), MTA local (aliases, ~/.forward, mailq, mail) e impressão com CUPS (lpr, lp, lpq, lprm, lpstat, lpadmin). É um dos domínios mais pesados da prova, com cerca de 20% das questões. Quase tudo cai como 'qual comando faz X' com quatro opções do mesmo comando, então o que derruba é trocar a letra da opção: lpstat -d x lpstat -p x lpstat -t, journalctl -u x -k x -f, hwclock --systohc x --hctosys. Também caem caminhos de arquivos (/etc/cups/cupsd.conf, /etc/logrotate.d, /var/log/auth.log x /var/log/secure) e a ordem das prioridades do syslog. Meu ponto fraco costuma ser a família lp*: preciso saber qual imprime, qual lista, qual remove e qual mostra estado.

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

hwclock --systohc e --hctosys

hwclock lê e ajusta o relógio de hardware (RTC). --systohc grava a hora do sistema no RTC; --hctosys copia a hora do RTC para o sistema. hwclock --show mostra a hora guardada no RTC.

/etc/adjtime

Registra se o relógio de hardware está em UTC ou em hora local e guarda ajustes do RTC. Em servidores Linux, o recomendado é manter o RTC em UTC. Não confundir com /etc/localtime (fuso do sistema) nem /etc/timezone (nome do fuso).

timedatectl

Mostra e ajusta hora, fuso e NTP em sistemas com systemd. timedatectl status (ou sem argumentos) mostra horário de sistema, horário do RTC e se o NTP está ativo; set-ntp true ativa a sincronização; set-timezone define o fuso; list-timezones lista os fusos do banco em /usr/share/zoneinfo; set-time espera uma data e hora.

chrony e chronyc

O chronyd sincroniza o relógio; a configuração fica em /etc/chrony.conf ou /etc/chrony/chrony.conf, com fontes definidas pelas diretivas server e pool (ex.: pool 2.pool.ntp.org iburst). chronyc sources lista as fontes, chronyc tracking mostra o desvio (offset) e a referência, e chronyc makestep força a correção imediata em vez do ajuste gradual.

ntpd e ntpq -p

O ntpd lê os servidores de tempo em /etc/ntp.conf. ntpq -p lista os pares consultados e o estado de sincronização (equivale ao chronyc sources). ntpd -p é opção de arquivo de PID, não lista pares.

NTP: porta e stratum

O NTP usa 123/UDP. O stratum indica a distância até a referência: stratum 0 são relógios de referência e cada nível acima soma um. Clientes NTP no Linux: chronyd, ntpd e systemd-timesyncd (cliente SNTP simples do systemd).

systemd-journald e journalctl

O journald coleta as mensagens do sistema; com systemd, ele costuma atender o socket /dev/log. journalctl -u filtra por unidade, -f acompanha em tempo real, -k mostra só o kernel, -r inverte a ordem, --since/--until filtram por tempo, --list-boots lista inicializações (usadas com -b) e --disk-usage mostra o espaço ocupado.

journald.conf

Em /etc/systemd/journald.conf: Storage aceita volatile, persistent, auto e none (persistent grava em disco em /var/log/journal). SystemMaxUse limita o espaço do journal persistente e RuntimeMaxUse o journal em memória (/run/log/journal). ForwardToSyslog=yes repassa as mensagens a um syslog tradicional como o rsyslog.

Limpeza do journal

journalctl --vacuum-size (ex.: =500M) e --vacuum-time limpam arquivos arquivados antigos; SystemMaxUse limita de forma permanente. --rotate só gira os arquivos atuais e --flush grava o journal volátil em disco.

rsyslog

Configuração principal em /etc/rsyslog.conf e regras extras em arquivos .conf de /etc/rsyslog.d. O seletor é facility.prioridade e a prioridade inclui as mais graves (mail.err = mail com erro ou pior). Para log remoto, @ envia por UDP e @@ por TCP; o syslog tradicional recebe em 514/UDP. Em distribuições modernas, o journald coleta e o rsyslog grava os arquivos em /var/log; os dois coexistem.

Prioridades do syslog

Da mais grave para a menos grave: emerg, alert, crit, err, warning, notice, info, debug. As facilities local0 a local7 são livres para uso.

Arquivos de log por distribuição

Debian: autenticação em /var/log/auth.log e log geral em /var/log/syslog. Família Red Hat: autenticação em /var/log/secure e log geral em /var/log/messages; há também /var/log/maillog e /var/log/cron.

logrotate

Gira, compacta e apaga logs antigos; costuma rodar diariamente por cron ou timer do systemd. Opções globais em /etc/logrotate.conf, que inclui as regras por pacote de /etc/logrotate.d/. rotate N mantém N cópias, compress compacta, e o bloco postrotate ... endscript recarrega o serviço após girar. logrotate -f força a rotação e -d só simula.

logger e systemd-cat

logger grava mensagens no syslog/journal a partir de scripts: -t define a etiqueta (filtrável com journalctl -t), -p define facility.prioridade (ex.: local0.info), -f lê de um arquivo e -n define servidor remoto. systemd-cat -t conecta a saída de um comando ao journal.

MTA e e-mail local

Postfix, Exim e Sendmail são MTAs; todos oferecem o comando sendmail por compatibilidade com programas. /etc/aliases redireciona e-mails locais e newaliases gera o banco usado pelo MTA; ~/.forward redireciona o e-mail do próprio usuário. mailq (equivale a sendmail -bp) mostra a fila; mail -s envia e, sem argumentos, lê a caixa em /var/spool/mail (ou /var/mail).

Comandos de impressão lp*

lpr imprime (-P escolhe a impressora, -# define cópias); lp é o estilo System V (-d destino, -n cópias). lpq mostra a fila, lprm ou cancel removem trabalhos. lpstat -d mostra a padrão, -p o estado das impressoras, -t o resumo completo, -o só os trabalhos, -a quem aceita e -r se o servidor roda.

lpadmin e lpoptions

lpadmin gerencia impressoras do CUPS: -p configura, -x remove, -d define a padrão do sistema, -u define permissões de uso. lpoptions -d define a padrão do próprio usuário, gravada em ~/.cups/lpoptions.

Arquivos e portas do CUPS

Configuração do servidor em /etc/cups/cupsd.conf; impressoras em /etc/cups/printers.conf (gerado pelo CUPS, não editar com o serviço rodando); spool em /var/spool/cups; logs em /var/log/cups. A interface web fica na porta 631/TCP. PPD descreve os recursos de um modelo; impressoras de rede usam URIs como ipp://, socket://, lpd:// e usb://.

Macetes para memorizar

hwclock

Lê da esquerda para a direita: SYS-to-HC grava no hardware; HC-to-SYS traz do hardware.

Prioridades do syslog

Emergência Alerta CRÍTICA, ERRo Avisa, Nota INFOrma, DEBUGa: emerg, alert, crit, err, warning, notice, info, debug.

rsyslog remoto

Um @ é leve como o UDP; @@ é duplo, com confirmação, como o TCP.

Família lp*

lpR = Roda a impressão, lpQ = Queue (fila), lpRM = ReMove, lpSTAT = STATus, lpADMIN = administra.

lpstat

-d = default (padrão), -p = printers (estado), -t = total (tudo), -o = output (trabalhos).

journalctl

-u = unit, -f = follow, -k = kernel, -b = boot, -r = reverse.

logrotate

post = depois: postrotate roda depois de girar; -f = force, -d = debug (só simula).

Tabela de memorização: não confunda

Quando é...	...e quando é
hwclock --systohc O relógio do sistema está certo e quero gravar no hardware (sistema -> RTC).	**hwclock --hctosys** Quero carregar no sistema a hora do relógio de hardware (RTC -> sistema).
chronyc tracking Pergunta sobre desvio/offset e a fonte de referência atual.	**chronyc sources** Pergunta sobre listar as fontes de tempo usadas e seu estado (equivalente ao ntpq -p no ntpd).
@ no rsyslog Envio de log remoto por UDP.	**@@ no rsyslog** Envio de log remoto por TCP.
SystemMaxUse= Limitar o journal persistente em disco (/var/log/journal).	**RuntimeMaxUse=** Limitar o journal volátil em memória (/run/log/journal).
lpadmin -d Definir a impressora padrão do sistema inteiro.	**lpoptions -d** Usuário define a sua própria impressora padrão (~/.cups/lpoptions).

/etc/aliases + newaliases O administrador redireciona e-mail de um usuário/alias, como postmaster, para outro.	**~/.forward** O próprio usuário redireciona seus e-mails sem mexer no /etc/aliases.
/var/log/auth.log e /var/log/syslog (Debian) Enunciado cita Debian: autenticação e log geral.	**/var/log/secure e /var/log/messages (Red Hat)** Enunciado cita família Red Hat: autenticação e log geral.

Números que caem

Item	Valor
Porta do NTP	**123/UDP**
Porta do syslog remoto tradicional	**514/UDP (rsyslog também aceita TCP)**
Porta da interface web do CUPS	**631/TCP**
Porta do LPD	**515**
Porta de impressão direta	**9100**
Stratum de relógio de referência	**0 (cada nível acima soma um)**
Facilities livres do syslog	**local0 a local7**
MTA local escutando só em	**127.0.0.1:25**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que lpstat -P financeiro arquivo imprime na fila financeiro.
Como não cair: Quem imprime é lpr (-P escolhe a impressora) ou lp (-d destino). lpstat só mostra estado; lpq mostra a fila; lprm remove.

⚠ **Alerta de prova:** Usar lp -P para escolher a impressora no estilo System V.
Como não cair: -P é do lpr. No lp o destino é -d: lp -d financeiro nota.pdf.

⚠ **Alerta de prova:** Usar lpr -P 3 para imprimir 3 cópias.
Como não cair: -P escolhe a impressora chamada 3. Cópias no lpr são -# 3; no lp, -n 3.

⚠ **Alerta de prova:** Marcar *.* @10.0.0.5:514 para log remoto por TCP.
Como não cair: Um @ é UDP; dois @@ é TCP. # no início seria comentário.

⚠ **Alerta de prova:** Achar que journalctl -k nginx ou -f nginx filtra o serviço nginx.
Como não cair: Filtro por unidade é -u. -k mostra só o kernel, -f acompanha tudo e -r inverte a ordem.

⚠ **Alerta de prova:** Usar journalctl --until 1 hour ago para ver a última hora.
Como não cair: --until mostra até uma hora atrás, ou seja, o oposto. A última hora é --since 1 hour ago.

⚠ **Alerta de prova:** Escolher Storage=volatile para gravar o journal em disco.
Como não cair: volatile mantém só em memória e none descarta. Disco persistente é Storage=persistent.

⚠ **Alerta de prova:** Usar journalctl --disk-usage=500M ou --rotate para reduzir o journal.
Como não cair: --disk-usage só mostra o uso e --rotate só gira. Reduzir é --vacuum-size=500M (ou --vacuum-time).

⚠ **Alerta de prova:** Marcar NTP como 123/TCP.
Como não cair: NTP é 123/UDP. 514/UDP é syslog e 53/UDP é DNS.

⚠ **Alerta de prova:** Usar prerotate ou firstaction para recarregar o serviço depois da rotação.
Como não cair: Depois de girar é postrotate ... endscript; prerotate e firstaction rodam antes, e compress não usa bloco.

⚠ **Alerta de prova:** Escolher logrotate -d para forçar a rotação.
Como não cair: -d só simula (teste de regras); forçar é -f. -s define o arquivo de estado e -v mostra detalhes.

⚠ **Alerta de prova:** Usar logger -p backup para etiquetar a mensagem.
Como não cair: -p espera facility.prioridade (ex.: local0.info). Etiqueta é -t; -f lê de arquivo e -n define servidor.

⚠ **Alerta de prova:** Achar que chronyc tracking ou sources corrige o relógio atrasado.
Como não cair: tracking e sources só mostram. Correção imediata é chronyc makestep; normalmente o chrony ajusta aos poucos para não saltar o horário.

⚠ **Alerta de prova:** Marcar mail.* para pegar só erros de e-mail.
Como não cair: mail.* pega todas as prioridades; *.err pega erros de todas as facilities; mail.none exclui. Só erros de mail é mail.err.

Como cai na prova

📝 **Como cai:** Qual comando faz X? com quatro variações da mesma ferramenta (lpstat -d/-p/-t/-o, journalctl -u/-k/-f/-r).
Como resolver: Identifique a ação pedida (listar, filtrar, remover, definir padrão) e associe à letra da opção. Elimine as que mostram em vez de alterar, ou o contrário.

📝 **Como cai:** Onde fica o arquivo de configuração de Y? (cupsd.conf, printers.conf, rsyslog.conf, logrotate.conf, ntp.conf, adjtime).
Como resolver: Configuração vive em /etc; spool em /var/spool; logs em /var/log. Descarte caminhos inventados como /etc/ntp.servers, /var/spool/cups.conf ou /usr/lib/cups/main.conf.

📝 **Como cai:** Linha de configuração para completar: rsyslog (seletor ou destino remoto), journald.conf, regra do logrotate ou diretiva do chrony.
Como resolver: Lembre a sintaxe exata: facility.prioridade, @ x @@, Storage=persistent, SystemMaxUse=, rotate N + compress, postrotate ... endscript, pool/server no chrony.

📝 **Como cai:** Cenário com distribuição específica (Debian x Red Hat) pedindo onde está a autenticação ou o log geral.
Como resolver: Debian: auth.log e syslog. Red Hat: secure e messages. Leia a distribuição no enunciado antes de escolher.

📝 **Como cai:** Escolha DUAS: programas de uma categoria (MTAs, clientes NTP).
Como resolver: Separe por função: Postfix/Exim/Sendmail são MTA; chronyd/ntpd/timesyncd são NTP; rsyslog é log; CUPS é impressão; sshd é SSH.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
girar, compactar e apagar logs antigos	**logrotate (/etc/logrotate.conf e /etc/logrotate.d/)**
gravar mensagem no log a partir de um script	**logger (ou systemd-cat para o journal)**
desvio/offset do relógio no chrony	**chronyc tracking**
relógio atrasado, corrigir imediatamente no chrony	**chronyc makestep**
RTC em UTC ou hora local	**/etc/adjtime**
ativar sincronização NTP com systemd	**timedatectl set-ntp true**

cliente SNTP simples do systemd	**systemd-timesyncd**
socket local para enviar mensagens ao log	**/dev/log**
postmaster deve ir para admin	**/etc/aliases e depois newaliases**
mensagens aguardando envio na fila do MTA	**mailq (= sendmail -bp)**
MTA escutando só em 127.0.0.1:25	**Evitar virar relay aberto**
comando sendmail em sistema com Postfix ou Exim	**Compatibilidade com programas**
interface web de administração do CUPS	**Porta 631/TCP**
arquivo que descreve os recursos de um modelo de impressora	**PPD**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- Ordem das prioridades: emerg, alert, crit, err, warning, notice, info, debug; mail.err inclui as mais graves.
- @ = UDP e @@ = TCP no rsyslog.
- lpr imprime, lpq mostra a fila, lprm/cancel removem, lpstat mostra estado, lpadmin administra.
- Depois de editar /etc/aliases, rodar newaliases.
- hwclock --systohc grava no hardware; --hctosys lê do hardware.

Essenciais para a prova (checklist)

- ☐ Sei usar hwclock --show, --systohc e --hctosys e para que serve /etc/adjtime.
- ☐ Sei os subcomandos do timedatectl: status, set-ntp, set-timezone, list-timezones.
- ☐ Sei diferenciar chronyc sources, tracking e makestep e onde fica a configuração do chrony e do ntpd.
- ☐ Sei filtrar o journal por unidade, tempo, boot e kernel e acompanhar em tempo real.
- ☐ Sei as opções Storage, SystemMaxUse, RuntimeMaxUse e ForwardToSyslog do journald.conf.
- ☐ Sei escrever seletores do rsyslog e enviar log remoto por UDP e por TCP.
- ☐ Sei montar uma regra de logrotate com rotate, compress e postrotate e forçar a rotação.
- ☐ Sei redirecionar e-mail com /etc/aliases + newaliases e com ~/.forward, e ver a fila com mailq.
- ☐ Sei imprimir, listar, cancelar e definir impressora padrão com lpr, lp, lpq, lprm, cancel, lpstat, lpadmin e lpoptions.
- ☐ Sei os arquivos do CUPS: cupsd.conf, printers.conf, /var/spool/cups e a porta 631.

Questões de revisão do capítulo

R4.1 · 108 Serviços Essenciais do Sistema

Arquivos de log crescem sem controle. Qual ferramenta roda periodicamente para girar, compactar e apagar logs antigos?

A. logger
B. logrotate
C. journald
D. lastlog

R4.2 · 108 Serviços Essenciais do Sistema

No rsyslog, qual linha envia todas as mensagens para o servidor 10.0.0.5 por TCP?

A. *.* :10.0.0.5:514
B. *.* @10.0.0.5:514
C. *.* #10.0.0.5:514
D. *.* @@10.0.0.5:514

R4.3 · 108 Serviços Essenciais do Sistema

Em qual arquivo o ntpd lê os servidores de tempo a consultar?

A. /etc/ntp.servers
B. /etc/adjtime
C. /etc/timezone
D. /etc/ntp.conf

R4.4 · 108 Serviços Essenciais do Sistema

Qual é a relação comum entre o systemd-journald e o rsyslog em distribuições modernas?

A. Os dois não podem estar instalados
B. O journald coleta; o rsyslog grava
C. O rsyslog substitui o kernel
D. O journald só funciona sem rede

Respostas comentadas

R4.1. B) logrotate

Por quê: O logrotate usa /etc/logrotate.conf e /etc/logrotate.d.

✗ A) Incorreta. Grava mensagens no log.

✗ C) Incorreta. Coleta mensagens do sistema.

✗ D) Incorreta. Mostra os últimos logins.

> **Dica de prova:** Girar logs: logrotate.

R4.2. D) *.* @@10.0.0.5:514

Por quê: No rsyslog, @ envia por UDP e @@ por TCP.

✗ A) Incorreta. Sintaxe inválida.

✗ B) Incorreta. Um @ indica UDP.

✗ C) Incorreta. Seria um comentário.

> **Dica de prova:** Log remoto por TCP: @@.

R4.3. D) /etc/ntp.conf

Por quê: O chrony usa /etc/chrony.conf ou /etc/chrony/chrony.conf.

✗ A) Incorreta. Não é padrão.

✗ B) Incorreta. Guarda ajustes do RTC.

✗ C) Incorreta. Guarda o fuso.

> **Dica de prova:** Configuração do ntpd: /etc/ntp.conf.

R4.4. B) O journald coleta; o rsyslog grava

Por quê: O rsyslog pode ler o journal e gerar arquivos em /var/log.

✗ A) Incorreta. Podem coexistir.

✗ C) Incorreta. Não é a relação.

✗ D) Incorreta. Não é a relação.

> **Dica de prova:** journald e rsyslog: coexistem.

05

CAPÍTULO 5 · 23,3% DA PROVA

109 Fundamentos de Rede

É o domínio de maior peso da prova (cerca de 23,3%), então aqui não posso deixar ponto fraco. Preciso dominar endereçamento IPv4 (máscaras, sub-redes, broadcast, faixas privadas, link-local), IPv6 (128 bits, abreviação, fe80::, ::1, /64, SLAAC, multicast), portas bem conhecidas, a família de comandos ip (addr, route, link, neigh), ss/netstat, nmcli, e a resolução de nomes (/etc/hosts, /etc/resolv.conf, /etc/nsswitch.conf, dig, host, getent, resolvectl). A prova mistura subcomando certo com objeto errado (ip route del x ip addr del) e cobra cálculo rápido de sub-rede. Meu erro mais comum é esquecer que dig e host consultam só o DNS, enquanto getent segue o nsswitch.

Neste capítulo
16 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Sub-redes IPv4

Hosts utilizáveis = 2^(32-prefixo) - 2 (rede e broadcast). /30 tem 4 endereços e 2 hosts; /28 tem 16 endereços e 14 hosts; /26 tem 64 e 62 hosts; /24 tem 254; /16 tem 65534. Cada bit a mais no prefixo dobra o número de sub-redes: /24 dividida em /26 gera quatro sub-redes.

Endereço de rede e broadcast

Em /26 o último octeto avança em blocos de 64, então 192.168.10.77/26 está na rede 192.168.10.64 (broadcast 192.168.10.127). Em /28 os blocos são de 16: 192.168.1.0/28 tem broadcast 192.168.1.15 e a próxima rede é .16.

Máscaras

Cada 255 representa 8 bits de rede: /8 = 255.0.0.0, /16 = 255.255.0.0, /24 = 255.255.255.0 e /25 = 255.255.255.128.

Faixas especiais IPv4

Privadas (RFC 1918): 10.0.0.0/8 (classe A), 172.16.0.0/12 e 192.168.0.0/16; 172.32.x.x fica fora. 169.254.0.0/16 é link-local, usada quando não há DHCP. Loopback é 127.0.0.0/8 e multicast 224.0.0.0/4.

IPv6: formato e abreviação

IPv6 tem 128 bits, escritos em 8 grupos hexadecimais. Zeros à esquerda podem sair e :: substitui uma única sequência de grupos zerados: 2001:0db8:0:0:0:0:0:1 vira 2001:db8::1. O :: só pode aparecer uma vez.

IPv6: tipos de endereço

fe80::/10 é link-local (enlace local); ::1 é loopback; ff00::/8 é multicast; globais costumam começar com 2 ou 3. IPv6 não tem broadcast: usa unicast, multicast e anycast. Sub-redes de LAN usam /64 (64 bits de prefixo e 64 de interface); /128 identifica um único host.

SLAAC e NDP

Com SLAAC, o host obtém endereço global sem DHCPv6, combinando o prefixo anunciado pelo roteador com um identificador de interface. O IPv6 não usa ARP: a descoberta de vizinhos (NDP) cumpre esse papel.

TCP x UDP e protocolos de apoio

TCP é orientado a conexão e confiável, com handshake SYN, SYN-ACK, ACK; UDP envia datagramas sem confirmação. Ambos usam portas. ping usa ICMP (ping6 usa ICMPv6) e ARP descobre o MAC de um IPv4 na rede local.

Portas

Bem conhecidas: 0 a 1023 (só root escuta abaixo de 1024 por padrão); registradas 1024 a 49151; dinâmicas 49152 a 65535. O arquivo /etc/services associa nomes de serviços a portas e protocolos (ex.: ssh 22/tcp, domain 53/udp).

Comandos ip (iproute2)

O iproute2 substitui ifconfig e route. ip addr show/add/del trata endereços; ip route show/add/del/get trata rotas (ip route show default mostra o gateway, ip route get simula a decisão de roteamento); ip link set eth0 up/down ativa interfaces e ip -s link mostra contadores; ip neigh show mostra a tabela de vizinhos (legado: arp -n). ip -4 e ip -6 filtram a família. Tudo o que é feito com ip se perde ao reiniciar.

ss e netstat

ss substitui o netstat, mas os dois aparecem na prova. Opções do ss: -t TCP, -u UDP, -x Unix, -a todos, -l escuta, -n numérico, -p processo, -s resumo; aceita filtros de estado (ss -t state established). netstat -rn mostra a tabela de roteamento numérica (como route -n).

NetworkManager e nmcli

nmcli general status mostra o estado geral; nmcli device status mostra os dispositivos; nmcli connection show lista as conexões; nmcli connection up/down ativa e desativa perfis; nmcli con modify grava IP fixo de forma persistente (depois aplicar com connection up); nmcli networking on/off liga e desliga toda a rede.

Configuração persistente por distribuição

Debian com ifupdown: /etc/network/interfaces, aplicado com ifup/ifdown. Ubuntu com netplan: YAML em /etc/netplan, aplicado com netplan apply. systemd-networkd: arquivos .network em /etc/systemd/network/. Nome estático da máquina em /etc/hostname, definido com hostnamectl set-hostname.

Resolução de nomes

/etc/hosts tem o formato IP nome apelidos e vale na hora. /etc/resolv.conf lista nameserver, search/domain (completam nomes curtos) e options. /etc/nsswitch.conf define a ordem: hosts: files dns consulta primeiro o /etc/hosts. Com systemd-resolved, o resolv.conf aponta para 127.0.0.53 e resolvectl status mostra os servidores DNS reais por interface.

dig, host e getent

dig e host consultam só servidores DNS; getent hosts segue o nsswitch, como as aplicações. No dig: @servidor escolhe o servidor, tipos como A, AAAA, MX, NS, CNAME, PTR e TXT, -x faz reversa, +short resume, +trace mostra a delegação desde a raiz. host -t MX consulta um tipo e host IP faz reversa.

Diagnóstico

ping -c N envia N pacotes (sem -c continua até interromper); ping -6 testa IPv6. traceroute e tracepath mostram os roteadores no caminho; tracepath também descobre o MTU sem root. nc -zv host porta testa se a porta aceita TCP e nc -l porta abre uma porta em escuta. hostname -I lista rapidamente os IPs.

Macetes para memorizar

Hosts por prefixo

2 elevado aos bits de host, menos 2: /30=2, /29=6, /28=14, /27=30, /26=62, /25=126, /24=254.

Bloco de sub-rede

Bloco = 256 menos o último octeto da máscara (/26 -> 64; /28 -> 16). Rede = múltiplo do bloco; broadcast = próximo múltiplo menos 1.

Portas clássicas

21 FTP, 22 SSH, 25 SMTP, 53 DNS, 67/68 DHCP, 80 HTTP, 110 POP3, 123 NTP, 143 IMAP, 443 HTTPS; seguras: 993 IMAPS, 995 POP3S.

Objetos do ip

addr = endereço, route = caminho, link = cabo/interface, neigh = vizinho (MAC).

Opções do ss

ss -tulnp: T de TCP, U de UDP, L de listen, N de numérico, P de processo.

dig x getent

dig pergunta só ao DNS; getent pergunta a quem o nsswitch mandar.

IPv6

fe80 = fica no enlace; ff = fala com muitos (multicast); ::1 = eu mesmo; /64 = LAN.

Tabela de memorização: não confunda

Quando é...	...e quando é
dig / host Consultar diretamente o servidor DNS (ignora /etc/hosts).	**getent hosts** Resolver como as aplicações, seguindo /etc/nsswitch.conf (/etc/hosts e DNS).
/etc/resolv.conf Quais servidores DNS consultar (nameserver, search).	**/etc/nsswitch.conf** Em que ordem consultar as fontes (files, dns).
ip addr add/del Alteração temporária de endereço, perdida ao reiniciar.	**nmcli con modify** IP fixo persistente em uma conexão do NetworkManager.
dig +short +short mostra só a resposta (o IP).	**dig +trace** +trace mostra toda a cadeia de delegação desde os servidores raiz.
traceroute Mostrar os roteadores até o destino.	**tracepath** Mostrar os saltos e também descobrir o MTU, sem exigir root.
ss -tlnp Portas TCP em escuta com os processos.	**ss -uan** Todos os sockets UDP em formato numérico.
169.254.0.0/16 Link-local: máquina sem resposta do DHCP.	**10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16** Faixas privadas da RFC 1918.

Números que caem

Item	Valor
Tamanho do IPv6	**128 bits (8 grupos hexadecimais)**
Tamanho do IPv4 / MAC / identificador de interface IPv6	**32 / 48 / 64 bits**
Prefixo típico de LAN IPv6	**/64**

Hosts em /30, /28, /26, /24, /16	**2, 14, 62, 254, 65534**
Portas bem conhecidas / registradas / dinâmicas	**0-1023 / 1024-49151 / 49152-65535**
DHCP IPv4	**Servidor 67/UDP, cliente 68/UDP**
DNS	**53 UDP e TCP**
SMTP / submissão	**25 / 587 ou 465**
POP3 / IMAP / POP3S / IMAPS	**110 / 143 / 995 / 993**
Outras portas	**21 FTP, 22 SSH, 69 TFTP, 80 HTTP, 161 SNMP, 389 LDAP, 443 HTTPS**
Faixas privadas IPv4	**10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16**
Link-local / loopback / multicast IPv4	**169.254.0.0/16 / 127.0.0.0/8 / 224.0.0.0/4**
Resolvedor local do systemd-resolved	**127.0.0.53**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Contar 4 hosts em uma /30 ou 64 em uma /26.
Como não cair: Tire rede e broadcast: /30 = 2 hosts; /26 = 62; /16 = 65534.

⚠ **Alerta de prova:** Marcar 172.32.10.5 como privado porque começa com 172.
Como não cair: A faixa privada é 172.16.0.0/12, que vai só até 172.31.x.x.

⚠ **Alerta de prova:** Abreviar como 2001::db8::1.
Como não cair: O :: só pode aparecer uma vez. Forma correta: 2001:db8::1.

⚠ **Alerta de prova:** Achar que o IPv6 usa broadcast ou ARP.
Como não cair: IPv6 usa multicast (e unicast/anycast) e a descoberta de vizinhos (NDP) no lugar do ARP.

⚠ **Alerta de prova:** Usar ip route del para remover um endereço ou ip addr add default via para gateway.
Como não cair: Endereço = ip addr; rota/gateway = ip route; interface = ip link; vizinho = ip neigh.

⚠ **Alerta de prova:** Achar que o dig acha um nome que está só no /etc/hosts.
Como não cair: dig, host e nslookup consultam só o DNS. Para seguir o nsswitch, use getent hosts.

⚠ **Alerta de prova:** Com hosts: files dns, pensar que o DNS vence ou que há conflito.
Como não cair: A ordem da linha hosts define a prioridade: o /etc/hosts vem primeiro e é usado.

⚠ **Alerta de prova:** Confundir search do resolv.conf com o servidor DNS primário.
Como não cair: search completa nomes curtos; o servidor é definido por nameserver.

⚠ **Alerta de prova:** Achar que ping pelo IP funciona e pelo nome não por causa de cabo ou gateway.
Como não cair: Se o IP responde, a rede está ok: o problema é resolução de nomes (resolv.conf, nsswitch, DNS).

⚠ **Alerta de prova:** Ler Network is unreachable como porta TCP fechada ou falha de DNS.
Como não cair: Significa que não há rota para a rede de destino; verifique com ip route. O ping nem usa TCP.

⚠ **Alerta de prova:** Usar ping -t 4 ou -i 4 para enviar 4 pacotes.
Como não cair: -c define a quantidade; -i é intervalo, -s tamanho dos dados e -t o TTL.

⚠ **Alerta de prova:** Usar ss -u state established.
Como não cair: UDP não tem estado established; ss -t state established mostra conexões TCP estabelecidas.

⚠ **Alerta de prova:** Usar nc -z para abrir uma porta em escuta.
Como não cair: -z faz varredura sem dados; escutar é nc -l 9000 (algumas versões exigem nc -l -p 9000).

⚠ **Alerta de prova:** Usar ifconfig ou ip addr add para IP fixo persistente.
Como não cair: Ambos são temporários (ifconfig ainda é legado). Persistente no NetworkManager é nmcli con modify.

Como cai na prova

📝 **Como cai:** Cálculo de sub-rede: hosts utilizáveis, broadcast, endereço de rede ou número de sub-redes.
Como resolver: Calcule bits de host (32 - prefixo), faça 2^n e tire 2 para hosts. Para rede/broadcast, ache o bloco e o múltiplo que contém o IP. As erradas costumam ser o valor de um prefixo vizinho ou o total sem tirar rede e broadcast.

📝 **Como cai:** Comando ip com quatro objetos diferentes (addr, route, link, neigh) para a mesma ação.
Como resolver: Pergunte-se o que está sendo alterado: endereço, rota/gateway, interface ou vizinho. A ação (add/del/show/set) costuma ser igual em todas as opções.

📝 **Como cai:** Cenário de diagnóstico: ping pelo IP ok e pelo nome não; Network is unreachable; nome no /etc/hosts que o dig não encontra.
Como resolver: Separe as camadas: se o IP responde, o problema é nome; unreachable é rota; dig ignora /etc/hosts.

📝 **Como cai:** Escolha DUAS com portas ou pares serviço/porta.
Como resolver: Use a tabela de portas clássicas e cheque o protocolo: DHCP 67/68 UDP, DNS 53 UDP e TCP, POP3 110, IMAP 143.

📝 **Como cai:** Qual arquivo/comando persiste a configuração em uma distribuição (ifupdown, netplan, networkd, NetworkManager).
Como resolver: Ligue a ferramenta ao local: /etc/network/interfaces + ifup; /etc/netplan + netplan apply; /etc/systemd/network; nmcli con modify + connection up.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
endereço 169.254.x.x sem resposta do DHCP	**Link-local**
fe80::	**IPv6 de enlace local (fe80::/10)**
endereço global IPv6 sem DHCPv6, por anúncios do roteador	**SLAAC**
127.0.0.53 no resolv.conf	**Resolvedor local do systemd-resolved (resolvectl status)**
resolver seguindo /etc/hosts e DNS como as aplicações	**getent hosts**
caminho de delegação desde os servidores raiz	**dig +trace**
consulta reversa de IP	**dig -x IP (ou host IP)**
qual rota e interface serão usadas para um destino	**ip route get**
tabela de vizinhos com IP e MAC	**ip neigh show (legado arp -n)**
estatísticas de pacotes e erros por interface	**ip -s link**
rastrear caminho e descobrir MTU sem root	**tracepath**

testar se a porta 443 aceita conexões TCP	**nc -zv servidor 443**
aplicar YAML de rede no Ubuntu	**netplan apply**
associar nomes de serviços às portas	**/etc/services**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- Hosts utilizáveis = total de endereços - 2.
- dig e host consultam só DNS; getent segue o nsswitch.
- Mudanças com ip addr/route são temporárias.
- O :: aparece uma única vez em um endereço IPv6.
- hosts: files dns = /etc/hosts vence o DNS.

Essenciais para a prova (checklist)

- ☐ Sei calcular hosts, rede, broadcast e número de sub-redes para prefixos de /16 a /30.
- ☐ Sei as faixas privadas, link-local, loopback e multicast do IPv4.
- ☐ Sei abreviar IPv6 e reconhecer fe80::, ::1, ff00:: e /64.
- ☐ Sei as portas de FTP, SSH, SMTP, DNS, DHCP, HTTP, POP3, IMAP, NTP, HTTPS e versões seguras.
- ☐ Sei usar ip addr, ip route (show default, get, add, del), ip link e ip neigh.
- ☐ Sei listar sockets com ss e netstat usando as opções -t, -u, -l, -n, -p, -a.
- ☐ Sei listar, ativar e configurar IP fixo com nmcli.
- ☐ Sei onde fica a configuração persistente em ifupdown, netplan e systemd-networkd.
- ☐ Sei o papel de /etc/hosts, /etc/resolv.conf e /etc/nsswitch.conf e a diferença entre dig e getent.
- ☐ Sei usar ping -c, traceroute, tracepath e nc para diagnóstico.

Questões de revisão do capítulo

R5.1 · 109 Fundamentos de Rede

Qual comando legado mostra a tabela de roteamento em formato numérico?

A. netstat -s
B. netstat -rn
C. netstat -i
D. netstat -tl

R5.2 · 109 Fundamentos de Rede

Qual comando mostra rapidamente todos os endereços IP atribuídos à máquina?

A. hostname -d
B. hostname -s
C. hostname -I
D. hostname -f

R5.3 · 109 Fundamentos de Rede

Qual comando define de forma persistente um IP fixo em uma conexão do NetworkManager?

A. nmcli con modify lan ipv4.addresses
B. ifconfig lan 10.0.0.5 netmask 255.255.255.0
C. ip addr add 10.0.0.5/24 dev lan
D. hostnamectl set-ip 10.0.0.5/24

R5.4 · 109 Fundamentos de Rede

Como um host IPv6 costuma obter um endereço global automaticamente, sem servidor DHCPv6, a partir de anúncios do roteador?

A. Por tradução de endereços (NAT)
B. Por mensagens ARP de broadcast
C. Por autoconfiguração sem estado (SLAAC)
D. Por consultas reversas no DNS

Respostas comentadas

R5.1. B) netstat -rn

Por quê: netstat e route são do net-tools; o iproute2 usa ip route.

✗ A) Incorreta. Mostra estatísticas por protocolo.
✗ C) Incorreta. Mostra estatísticas das interfaces.
✗ D) Incorreta. Mostra portas TCP em escuta.

> **Dica de prova:** Rotas no netstat: -rn.

R5.2. C) hostname -I

Por quê: hostname -I lista endereços sem detalhes; ip addr mostra tudo.

✗ A) Incorreta. Mostra o domínio.
✗ B) Incorreta. Mostra o nome curto.
✗ D) Incorreta. Mostra o nome completo.

> **Dica de prova:** IPs da máquina: hostname -I.

R5.3. A) nmcli con modify lan ipv4.addresses

Por quê: Após modificar, use nmcli connection up para aplicar.

✗ B) Incorreta. É temporário e legado.

✗ C) Incorreta. É temporário.

✗ D) Incorreta. Subcomando inexistente.

> **Dica de prova:** IP persistente no NetworkManager: nmcli connection modify.

R5.4. C) Por autoconfiguração sem estado (SLAAC)

Por quê: O SLAAC combina o prefixo anunciado com um identificador de interface.

✗ A) Incorreta. Não atribui endereços.

✗ B) Incorreta. O IPv6 não usa ARP.

✗ D) Incorreta. Não atribui endereços.

> **Dica de prova:** IPv6 automático: SLAAC.

06

CAPÍTULO 6 · 16,7% DA PROVA

110 Segurança

Este domínio vale cerca de 16,7% e se divide em administração de segurança (sudo, su, auditoria de logins, find por permissões, lsof, limites, nologin, serviços sem uso), SSH (chaves, authorized_keys x known_hosts, túneis -L/-R/-D, sshd_config) e GnuPG (gerar, listar, importar, exportar, cifrar, assinar, verificar, revogar). As questões são quase sempre 'qual opção faz X' e as erradas são opções vizinhas do mesmo comando. Onde mais erro: lado do cliente x lado do servidor no SSH (known_hosts fica no cliente, authorized_keys no servidor), direção dos túneis e a sintaxe do sudoers (% para grupo, NOPASSWD).

Neste capítulo

15 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

sudo

Permite menor privilégio e auditoria por usuário (registra quem executou o quê) e pede a senha do próprio usuário. sudo -l lista o que o usuário pode executar; -i abre shell de login como root; -s shell sem login; -u usuario executa como outro usuário (sem -u, root); -k invalida e -v renova a credencial em cache; -e edita arquivos como outro usuário.

sudoers

Formato: quem máquinas=(como_quem) comandos; % indica grupo (%admin ALL=(ALL) ALL). NOPASSWD dispensa senha: backup ALL=(root) NOPASSWD: /usr/bin/rsync. Edite com visudo (trava e valida sintaxe); visudo -c só verifica; regras extras ficam em /etc/sudoers.d/, editadas com visudo -f.

su x su -

su - simula um login completo e carrega o ambiente do usuário de destino; su mantém boa parte do ambiente atual. O su - continua pedindo a senha.

Auditoria de logins

last lê /var/log/wtmp e lista logins com data e origem; last reboot mostra reinicializações (pseudousuário reboot). lastb lê /var/log/btmp e mostra tentativas falhas, exigindo privilégios. who lista sessões, w mostra também carga e comando atual, who -b mostra a última inicialização (uptime -s também).

find para auditoria

find / -nouser e -nogroup encontram arquivos órfãos após remover contas. find / -perm -o+w -type f procura arquivos que qualquer usuário pode alterar.

lsof

Mostra arquivos, sockets e dispositivos abertos. -u usuário filtra por usuário; -i filtra conexões de rede (lsof -i :80 mostra quem usa a porta 80); -p espera PID; -c filtra pelo nome do comando; -d pelo descritor. ss -tlnp e fuser 80/tcp também ajudam.

Limites de recursos

ulimit -a mostra os limites do shell atual (como arquivos abertos). Limites persistentes por usuário ficam em /etc/security/limits.conf, aplicados no login pelo módulo pam_limits.

/etc/nologin e reforço do host

Quando /etc/nologin existe, impede o login de usuários comuns e mostra seu conteúdo; só o root entra. Desativar serviços sem uso (systemctl disable --now, remoção de pacotes) reduz a superfície de ataque. nmap faz varredura de portas, apenas com autorização.

Ativação por socket

Unidades .socket do systemd substituem o antigo superservidor inetd/xinetd, iniciando o serviço só quando chega uma conexão.

Chaves SSH do usuário

ssh-keygen -t ed25519 gera o par; ssh-copy-id usuario@servidor acrescenta a pública ao ~/.ssh/authorized_keys remoto. ssh-keygen -l -f mostra a impressão digital, -p troca a frase secreta (sem mudar o par), -y gera a pública a partir da privada, -R remove um host do known_hosts. ssh-agent guarda chaves em memória e ssh-add as carrega, pedindo a senha uma vez.

Arquivos do SSH

~/.ssh/authorized_keys fica no servidor; ~/.ssh/known_hosts fica no cliente e guarda as chaves dos servidores conhecidos; ~/.ssh/config cria atalhos com blocos Host, HostName, Port, User e IdentityFile. As chaves do próprio servidor ficam em /etc/ssh/ssh_host_*. Permissões: ~/.ssh 700 e chave privada 600.

sshd_config

PermitRootLogin no impede login direto do root; PasswordAuthentication no aceita só chaves; Port define a porta e ListenAddress o endereço. sshd -t testa a configuração antes de reiniciar, e após mudar é preciso recarregar o serviço.

Túneis SSH

-L porta_local:destino:porta encaminha porta local (ex.: ssh -L 8080:interno:80 usuario@bastion); -R abre a porta no servidor e envia ao lado do cliente; -D cria proxy SOCKS dinâmico; -N não abre shell (útil para túneis) e -f envia para segundo plano. -i indica a chave privada, -l o login, -p a porta.

GnuPG: chaves

gpg --gen-key (ou --full-generate-key) cria o par em ~/.gnupg (permissões restritas, como 700). --list-keys lista públicas e --list-secret-keys privadas. --import adiciona chave recebida; --export -a exporta a pública em texto (--armor); --send-keys publica em servidor de chaves e --recv-keys baixa. Gere logo um certificado de revogação (gpg --gen-revoke) para invalidar a chave se ela for perdida.

GnuPG: cifrar e assinar

gpg -e -r destinatario cifra com a chave pública do destinatário; gpg -c (--symmetric) cifra com senha; gpg -d (--decrypt) decifra com a chave privada. --sign assina com a privada; --clearsign mantém o texto legível com a assinatura; --detach-sign gera assinatura separada; --verify confere com a pública.

Macetes para memorizar

💡 Lados do SSH

authorized_keys = quem pode ENTRAR (servidor); known_hosts = quem eu CONHEÇO (cliente).

💡 Túneis

L = Local (abre porta aqui), R = Remote (abre porta lá), D = Dinâmico (SOCKS), N = No shell.

sudoers

% = grupo; # = comentário; NOPASSWD: antes do comando para dispensar senha.

Chaves GnuPG

Cifra com a PÚBLICA de quem recebe; assina com a sua PRIVADA; verifica com a pública de quem assinou.

gpg letras

-e encrypt, -d decrypt, -c senha (symmetric), -s sign, -a armor (texto), -k list-keys.

last/lastb

lastb = last Bad (falhas, btmp); last = wtmp (sucesso).

Permissões SSH

Diretório 700, privada 600: só o dono enxerga.

Tabela de memorização: não confunda

Quando é...	...e quando é
~/.ssh/authorized_keys No servidor: chaves públicas autorizadas a entrar na conta.	**~/.ssh/known_hosts** No cliente: chaves dos servidores já conhecidos (aviso de identificação alterada).
ssh -L Acessar pela porta local um serviço do lado remoto/interno.	**ssh -R** Expor um serviço local em uma porta do servidor remoto.
last Logins bem-sucedidos (wtmp) e reinicializações.	**lastb** Tentativas de login que falharam (btmp, exige privilégios).
gpg -e -r Cifrar com a chave pública de um destinatário.	**gpg -c** Cifrar com senha, sem par de chaves (simétrico).
gpg --clearsign Assinatura junto ao texto legível.	**gpg --detach-sign** Assinatura em arquivo separado.
sudo -i Abrir shell de login como root.	**sudo -l** Listar o que o usuário pode executar com sudo.
su - Carregar o ambiente de login completo do usuário de destino.	**su** Trocar de usuário mantendo boa parte do ambiente atual.

Números que caem

Item	Valor
Permissão do diretório ~/.ssh	**700**

Permissão da chave privada SSH	**600**
Permissão restrita do ~/.gnupg	**700**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que o sudo dispensa a senha do usuário ou dá acesso total a todos.
Como não cair: O sudo pede a senha do próprio usuário, permite controle fino e registra quem executou o quê.

⚠ **Alerta de prova:** Usar @admin ou admin para dar permissão ao grupo admin no sudoers.
Como não cair: Grupo se indica com %: %admin ALL=(ALL) ALL. # seria comentário e sem % é usuário.

⚠ **Alerta de prova:** Achar que backup ALL=(ALL) /usr/bin/rsync dispensa senha.
Como não cair: Sem NOPASSWD: a senha é exigida. backup NOPASSWD=(root) ALL é sintaxe inválida.

⚠ **Alerta de prova:** Usar sudo -e ou nano para editar o sudoers.
Como não cair: visudo trava e valida a sintaxe antes de salvar; sudo -e edita arquivos comuns.

⚠ **Alerta de prova:** Procurar a chave anterior do servidor em authorized_keys.
Como não cair: authorized_keys fica no servidor. A chave do servidor fica no known_hosts do cliente; remova com ssh-keygen -R servidor após confirmar a mudança.

⚠ **Alerta de prova:** Usar ssh-keygen ou ssh-keyscan para instalar a chave no servidor.
Como não cair: ssh-keygen gera localmente e ssh-keyscan coleta chaves de hosts. Instalar é ssh-copy-id.

⚠ **Alerta de prova:** Usar ssh -l ou -p para indicar a chave privada.
Como não cair: -i indica a chave; -l é o login, -p a porta e -o opções.

⚠ **Alerta de prova:** Trocar -L por -R ou -D no túnel.
Como não cair: -L = porta local; -R = porta aberta no servidor remoto; -D = proxy SOCKS; -X = X11.

⚠ **Alerta de prova:** Usar ssh -v, -A ou -t para criar só o túnel sem shell.
Como não cair: -N não executa comando remoto. -v detalha, -A encaminha o agente e -t força terminal.

⚠ **Alerta de prova:** Desativar senha com PubkeyAuthentication no.
Como não cair: Isso desativaria as chaves. Para aceitar só chaves: PasswordAuthentication no.

⚠ **Alerta de prova:** Usar chmod 755 ou 644 no ~/.ssh.
Como não cair: O diretório deve ser 700 (644 tira a execução do diretório) e a chave privada 600.

⚠ **Alerta de prova:** Exportar com --export-secret-keys para enviar a outras pessoas.
Como não cair: Isso exporta a privada. Para compartilhar: gpg --export -a (só a pública).

⚠ **Alerta de prova:** Usar gpg -e para cifrar só com senha ou -s para cifrar.
Como não cair: -c é simétrico (senha); -e usa chave pública; -s assina.

⚠ **Alerta de prova:** Usar lsof -p www-data ou lsof -d 80.
Como não cair: -p espera PID e -d descritor. Usuário é -u; porta de rede é -i :80.

Como cai na prova

📝 **Como cai:** Qual opção do sudo, ssh, ssh-keygen, gpg ou lsof faz X, com quatro opções vizinhas.
Como resolver: Traduza a ação para a letra (listar, executar como, chave privada, túnel local, impressão digital, cifrar, assinar) e elimine as opções que fazem outra coisa no mesmo comando.

📝 **Como cai:** Linha do sudoers para conceder um privilégio específico.
Como resolver: Cheque: usuário ou %grupo, ALL=(como_quem), NOPASSWD: se não pode pedir senha e caminho completo do comando.

📝 **Como cai:** Cenário de SSH perguntando em qual arquivo ou lado algo fica.
Como resolver: Pergunte se é servidor (authorized_keys, sshd_config, ssh_host_*) ou cliente (known_hosts, ~/.ssh/config, ssh_config).

📝 **Como cai:** Escolha DUAS: medidas de reforço do SSH ou comandos para o agente.
Como resolver: Boas práticas: PermitRootLogin no e chaves no lugar de senhas; descarte compartilhar chaves, senhas vazias e chaves 644. Agente: ssh-agent + ssh-add.

📝 **Como cai:** Qual operação GnuPG usa qual chave (cifrar, decifrar, assinar, verificar).
Como resolver: Cifrar e verificar usam a pública; decifrar e assinar usam a privada.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em

aviso de identificação do servidor mudou	**~/.ssh/known_hosts no cliente; ssh-keygen -R após confirmar**
não digitar a frase da chave a cada conexão	**ssh-agent e ssh-add**
atalho ssh prod com host, porta e usuário	**~/.ssh/config (Host, HostName, Port, User)**
checar o sshd_config antes de reiniciar	**sshd -t**
regras extras do sudo sem editar o arquivo principal	**/etc/sudoers.d/ com visudo -f**
verificar a sintaxe do sudoers sem editar	**visudo -c**
arquivos sem dono válido após remover contas	**find / -nouser (e -nogroup)**
impedir login de usuários comuns com mensagem	**/etc/nologin**
limite persistente de arquivos abertos por usuário	**/etc/security/limits.conf (pam_limits)**
substituto do inetd/xinetd	**Unidades .socket do systemd**
qual processo usa a porta 80	**lsof -i :80**
tentativas de login falhas	**lastb (/var/log/btmp)**
invalidar a chave GnuPG perdida	**Certificado de revogação (gpg --gen-revoke)**
assinatura junto ao texto legível	**gpg --clearsign**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- authorized_keys no servidor; known_hosts no cliente.
- % indica grupo no sudoers; sempre editar com visudo.
- ssh -L local, -R remoto, -D SOCKS, -N sem shell.
- Gerar certificado de revogação logo após criar a chave GnuPG.
- lastb mostra falhas (btmp); last mostra sucessos e reboots (wtmp).

Essenciais para a prova (checklist)

- ☐ Sei usar sudo -l, -i, -u, -k, -v e escrever linhas do sudoers com % e NOPASSWD.
- ☐ Sei editar e validar o sudoers com visudo, visudo -c e /etc/sudoers.d.
- ☐ Sei a diferença entre su e su -.
- ☐ Sei auditar com last, last reboot, lastb, who, w e who -b.
- ☐ Sei usar find -nouser, find -perm -o+w e lsof -u / -i.
- ☐ Sei onde configurar limites (ulimit, limits.conf) e o efeito do /etc/nologin.

- ☐ Sei gerar, copiar, listar a impressão digital e trocar a frase de chaves SSH.
- ☐ Sei os arquivos do SSH no cliente e no servidor e as permissões 700/600.
- ☐ Sei montar túneis -L, -R, -D com -N e as diretivas PermitRootLogin, PasswordAuthentication e Port.
- ☐ Sei gerar, importar, exportar, publicar e revogar chaves GnuPG e cifrar, decifrar, assinar e verificar arquivos.

Questões de revisão do capítulo

R6.1 · 110 Segurança

Em qual arquivo do servidor ficam as chaves públicas autorizadas a entrar em uma conta por SSH?

A. ~/.ssh/authorized_keys
B. ~/.ssh/known_hosts
C. ~/.ssh/id_ed25519
D. /etc/ssh/ssh_config

R6.2 · 110 Segurança

Qual comando mostra quais comandos o usuário atual pode executar com sudo?

A. sudo -i
B. sudo -k
C. sudo -v
D. sudo -l

R6.3 · 110 Segurança

Qual comando mostra os limites de recursos do shell atual, como número de arquivos abertos?

A. umask -a
B. limits -a
C. ulimit -a
D. ulimit -n 0

R6.4 · 110 Segurança

Qual linha do sudoers permite que o usuário backup execute /usr/bin/rsync como root sem digitar senha?

A. backup ALL=(ALL) /usr/bin/rsync
B. backup ALL=(root) NOPASSWD: /usr/bin/rsync
C. %backup ALL=(root) /usr/bin/rsync
D. backup NOPASSWD=(root) ALL

Respostas comentadas

R6.1. A) ~/.ssh/authorized_keys

Por quê: authorized_keys fica no servidor; known_hosts fica no cliente.

✗ B) Incorreta. Guarda chaves de servidores conhecidos.

✗ C) Incorreta. É a chave privada do usuário.

✗ D) Incorreta. Configuração do cliente.

> **Dica de prova:** Chaves autorizadas: ~/.ssh/authorized_keys.

R6.2. D) sudo -l

Por quê: sudo -l lê as regras do sudoers aplicáveis ao usuário.

✗ A) Incorreta. Abre um shell de login como root.

✗ B) Incorreta. Invalida a credencial em cache.

✗ C) Incorreta. Renova a credencial em cache.

> **Dica de prova:** Privilégios no sudo: sudo -l.

R6.3. C) ulimit -a

Por quê: ulimit consulta e ajusta limites; valores persistentes ficam em /etc/security/limits.conf.

✗ A) Incorreta. Opção inválida.

✗ B) Incorreta. Comando inexistente.

✗ D) Incorreta. Definiria o limite de arquivos.

> **Dica de prova:** Limites do shell: ulimit -a.

R6.4. B) backup ALL=(root) NOPASSWD: /usr/bin/rsync

Por quê: Restringir comandos específicos segue o menor privilégio.

✗ A) Incorreta. Exige senha para o comando.

✗ C) Incorreta. Refere-se a um grupo e exige senha.

✗ D) Incorreta. Sintaxe inválida.

> **Dica de prova:** Comando sem senha: NOPASSWD.

DIA DA PROVA

Estratégia de prova

A LPIC-1 102-500 tem 60 questões em 90 minutos, com múltipla escolha, múltipla resposta e preenchimento, e aprovação com 500 em uma escala de 200 a 800. A maioria das questões pede o comando, a opção ou o arquivo exato para uma tarefa, e as alternativas erradas são quase sempre o mesmo comando com outra letra ou um arquivo vizinho. Muitas questões vêm como cenário curto (um usuário quer, um administrador precisa) que esconde a palavra-chave da resposta. Os maiores pesos estão em Fundamentos de Rede (23,3%), Tarefas Administrativas (20%) e Serviços Essenciais (20%), seguidos de Segurança (16,7%), Shells e Scripts (13,3%) e Interfaces de Usuário (6,7%).

Como responder

✓ Distribua o estudo pelos pesos: rede, tarefas administrativas e serviços essenciais somam mais de 60% da prova.

✓ Com 90 minutos para 60 questões, você tem cerca de 1,5 minuto por questão: marque as de cálculo de sub-rede para o fim se travar.

✓ Nas questões de preenchimento, treine escrever comandos, opções e caminhos completos de memória (ex.: usermod -aG, /etc/logrotate.d/, journalctl -u).

✓ Antes de olhar as alternativas, sublinhe a ação pedida (listar, remover, definir, mostrar, forçar) e só então procure a letra da opção que faz isso.

✓ Em múltipla resposta (Escolha DUAS), elimine primeiro os itens de outra categoria (ex.: CUPS em uma lista de MTAs) e confirme as duas restantes.

✓ Leia o contexto da distribuição e da ferramenta (Debian x Red Hat, ifupdown x netplan x NetworkManager, chrony x ntpd) antes de escolher arquivo ou comando.

✓ Diferencie sempre o temporário do persistente: ip, export e alterações em memória somem; arquivos em /etc, nmcli con modify e Storage=persistent ficam.

✓ Monte tabelas de comparação pessoais (lp*, journalctl, usermod, chage, gpg, ssh) e revise-as nas provas de treino até zerar os erros por letra trocada.

Erros que derrubam candidatos

✗ Trocar a letra da opção de um comando conhecido (usermod -G sem -a, chage -M x -W, lpstat -d x -p, ssh -L x -R).

✗ Confundir lado do cliente e do servidor (servidor X no X11, known_hosts x authorized_keys).

✗ Esquecer de tirar rede e broadcast ao contar hosts de uma sub-rede.

✗ Achar que dig e host consultam o /etc/hosts.

✗ Achar que executar um script com ./ altera o shell atual.

✗ Errar a lógica de cron.allow/cron.deny ou a ordem dos campos do crontab.

✗ Inverter direções: hwclock --systohc x --hctosys, journalctl --since x --until, @ x @@ no rsyslog.

Na semana da prova

- ☐ Refaça as provas de treino focando nos domínios de maior peso e anote cada erro de letra trocada em uma lista única.
- ☐ Revise diariamente a tabela de portas, as faixas IPv4/IPv6 e faça alguns cálculos de sub-rede de /24 a /30.
- ☐ Releia os campos de /etc/passwd, /etc/group, crontab e /etc/anacrontab e a ordem das prioridades do syslog.
- ☐ Pratique em um terminal os comandos que mais confunde (ip, ss, nmcli, journalctl, chage, usermod, gpg, ssh-keygen).
- ☐ Na véspera, revise só as seções de pegadinhas e lembrar de cada capítulo e descanse.

REVISÃO FINAL

Folha de cola

Leia na véspera e na manhã da prova: os gatilhos e as pegadinhas mais importantes de cada domínio.

1. 105 Shells e Scripts

‣ aplicar mudanças no terminal atual sem abrir outro → **source ~/.bashrc (ou .)**

‣ variável exportada sumiu depois do script → **Processo filho; usar source**

‣ variáveis para todos sem editar /etc/profile → **/etc/profile.d/**

‣ VAR=valor lido pelo PAM, não pelo shell → **/etc/environment**

‣ alias para todos os usuários em shells interativos (Debian) → **/etc/bash.bashrc**

⚠ O script rodou em processo filho. Para afetar o shell atual: source config.sh ou . config.sh.

⚠ bash abre um subshell e chmod não aplica nada. Use source ~/.bashrc.

⚠ $( ) tentaria executar o comando A. Aritmética é $((A + B)).

2. 106 Interfaces de Usuário e Desktops

‣ aplicativo X11 em sessão Wayland → **XWayland**

‣ compositor atua como servidor de exibição → **Wayland**

‣ variável que diz ao cliente X onde exibir → **DISPLAY**

‣ ssh -X não abre janelas → **X11Forwarding yes no sshd_config (e xauth no servidor)**

‣ tela de login gráfica pela rede de um servidor X → **XDMCP (sem criptografia)**

⚠ No X11 o servidor é quem exibe: fica na máquina local. No servidor remoto roda o cliente X.

⚠ É o display 0 da máquina local; o formato é host:display.tela e host vazio = local.

⚠ Onde exibir é DISPLAY. XAUTHORITY é o arquivo de autorização e TERM o tipo de terminal.

3. 107 Tarefas Administrativas

‣ rodar uma única vez hoje às 23h → **at 23:00**

‣ quando a carga do sistema estiver baixa → **batch**

‣ notebook desligado à noite perde tarefas diárias → **anacron (/etc/anacrontab)**

‣ pacote instala tarefa agendada sem editar /etc/crontab → **/etc/cron.d/**

‣ rodar uma vez por dia sem escrever horário → **/etc/cron.daily/**

⚠ Sem -a, -G substitui a lista de grupos secundários. O certo é usermod -aG docker ana (ou gpasswd -a ana docker).

⚠ -d só altera o caminho; -m move o conteúdo antigo: usermod -d /home/novo -m usuario.

⚠ Renomear login é usermod -l novo antigo; -d é home e -c é comentário.

4. 108 Serviços Essenciais do Sistema

‣ girar, compactar e apagar logs antigos → **logrotate (/etc/logrotate.conf e /etc/logrotate.d/)**

‣ gravar mensagem no log a partir de um script → **logger (ou systemd-cat para o journal)**

‣ desvio/offset do relógio no chrony → **chronyc tracking**

‣ relógio atrasado, corrigir imediatamente no chrony → **chronyc makestep**

‣ RTC em UTC ou hora local → **/etc/adjtime**

⚠ Quem imprime é lpr (-P escolhe a impressora) ou lp (-d destino). lpstat só mostra estado; lpq mostra a fila; lprm remove.

⚠ -P é do lpr. No lp o destino é -d: lp -d financeiro nota.pdf.

⚠ -P escolhe a impressora chamada 3. Cópias no lpr são -# 3; no lp, -n 3.

5. 109 Fundamentos de Rede

‣ endereço 169.254.x.x sem resposta do DHCP → **Link-local**

‣ fe80:: → **IPv6 de enlace local (fe80::/10)**

‣ endereço global IPv6 sem DHCPv6, por anúncios do roteador → **SLAAC**

‣ 127.0.0.53 no resolv.conf → **Resolvedor local do systemd-resolved (resolvectl status)**

‣ resolver seguindo /etc/hosts e DNS como as aplicações → **getent hosts**

⚠ Tire rede e broadcast: /30 = 2 hosts; /26 = 62; /16 = 65534.

⚠ A faixa privada é 172.16.0.0/12, que vai só até 172.31.x.x.

⚠ O :: só pode aparecer uma vez. Forma correta: 2001:db8::1.

6. 110 Segurança

‣ aviso de identificação do servidor mudou → **~/.ssh/known_hosts no cliente; ssh-keygen -R após confirmar**

‣ não digitar a frase da chave a cada conexão → **ssh-agent e ssh-add**

‣ atalho ssh prod com host, porta e usuário → **~/.ssh/config (Host, HostName, Port, User)**

‣ checar o sshd_config antes de reiniciar → **sshd -t**

‣ regras extras do sudo sem editar o arquivo principal → **/etc/sudoers.d/ com visudo -f**

⚠ O sudo pede a senha do próprio usuário, permite controle fino e registra quem executou o quê.

⚠ Grupo se indica com %: %admin ALL=(ALL) ALL. # seria comentário e sem % é usuário.

⚠ Sem NOPASSWD: a senha é exigida. backup NOPASSWD= (root) ALL é sintaxe inválida.

GABARITO

Respostas do diagnóstico

D1. A) O script rodou em um processo filho → revise o capítulo 1

Por quê: Para alterar o shell atual, use source config.sh ou . config.sh.

✗ B) Incorreta. Aceita normalmente.
✗ C) Incorreta. O cron não participa.
✗ D) Incorreta. Vale para qualquer usuário.

> **Dica de prova:** Variável sumiu: processo filho; use source.

D2. A) Permissão de execução no arquivo → revise o capítulo 1

Por quê: Scripts precisam do bit x ou devem ser chamados como bash script.sh.

✗ B) Incorreta. Não resolve a permissão.
✗ C) Incorreta. O caminho ./ já foi indicado.
✗ D) Incorreta. Não resolve a permissão.

> **Dica de prova:** Permission denied: falta chmod +x.

D3. B) TOTAL=$((A + B)) → revise o capítulo 1

Por quê: $(( )) avalia expressões inteiras; $( ) executa comandos.

✗ A) Incorreta. Não é aritmética.
✗ C) Incorreta. Tentaria executar o comando A.
✗ D) Incorreta. Não é aritmética.

> **Dica de prova:** Aritmética no bash: $(( )).

D4. C) O display 0 da máquina local → revise o capítulo 2

Por quê: O formato é host:display.tela; vazio antes de : indica a máquina local.

✗ A) Incorreta. Não se refere à rede.
✗ B) Incorreta. Não se refere ao SSH.
✗ D) Incorreta. Não se refere a usuários.

> **Dica de prova:** DISPLAY=:0: primeiro display local.

D5. D) SPICE → revise o capítulo 2

Por quê: SPICE e VNC são comuns para consoles de VMs.

✗ A) Incorreta. Gerencia dispositivos.
✗ B) Incorreta. Transfere arquivos.
✗ C) Incorreta. Compartilha arquivos.

> **Dica de prova:** Console de VM no KVM: SPICE.

D6. B) XDMCP → revise o capítulo 2

Por quê: O XDMCP não é criptografado e deve ser usado com cuidado.

✗ A) Incorreta. Envia e-mails.

✗ C) Incorreta. Distribui endereços IP.

✗ D) Incorreta. Acessa diretórios.

> **Dica de prova:** Login gráfico remoto no X: XDMCP.

D7. D) date -u → revise o capítulo 3

Por quê: date -u usa UTC; TZ=região date mostra outro fuso.

✗ A) Incorreta. Mostra em formato ISO local.

✗ B) Incorreta. Mostra a data de um arquivo.

✗ C) Incorreta. Define a data.

> **Dica de prova:** Hora em UTC: date -u.

D8. D) timedatectl set-timezone America/Sao_Paulo → revise o capítulo 3

Por quê: Fusos seguem o formato Região/Cidade do banco tz.

✗ A) Incorreta. localectl não trata fusos.

✗ B) Incorreta. Opção inválida.

✗ C) Incorreta. Opção inválida.

> **Dica de prova:** Definir fuso: timedatectl set-timezone.

D9. A) usermod -l joao.silva jsilva → revise o capítulo 3

Por quê: usermod -l muda o login; o home pode ser movido com -d e -m.

✗ B) Incorreta. Altera o diretório pessoal.

✗ C) Incorreta. Altera o grupo primário.

✗ D) Incorreta. Altera o comentário.

> **Dica de prova:** Renomear login: usermod -l.

D10. B) chronyc sources → revise o capítulo 4

Por quê: chronyc sources e chronyc tracking mostram a sincronização; ntpq -p faz o mesmo no ntpd.

✗ A) Incorreta. Não lista fontes.

✗ C) Incorreta. Mostra o relógio de hardware.

✗ D) Incorreta. Opção inválida.

> **Dica de prova:** Fontes do chrony: chronyc sources.

D11. A) timedatectl set-ntp true → revise o capítulo 4

Por quê: Com set-ntp true, o systemd-timesyncd ou o chrony mantém o horário.

✗ B) Incorreta. Opção inválida.

✗ C) Incorreta. Espera uma data e hora.

✗ D) Incorreta. Opção inválida.

> **Dica de prova:** Ativar NTP: timedatectl set-ntp true.

D12. A) lpstat -d → revise o capítulo 4

Por quê: lpstat -d mostra a padrão; lpstat -p mostra o estado das impressoras.

✗ B) Incorreta. Opção inválida para lpr.

✗ C) Incorreta. Opção inválida para lpq.

✗ D) Incorreta. Opção inválida para lprm.

> **Dica de prova:** Impressora padrão: lpstat -d.

Agora, treine no formato real

Faça as 6 provas completas do curso LPIC-1 102: 360 questões inéditas, tempo do exame, explicação de cada alternativa e link da documentação para revisar.

Ver as 6 provas completas e o cupom do mês →

Até o dia da prova, uma revisão por dia no seu feed

Instagram @strecht.simulados

Um post de prova por dia: questão comentada, pegadinhas e o "não confunda" de cada certificação.

Seguir no Instagram →

YouTube Strecht Simulados

Shorts diários com pegadinhas de prova e, aos sábados, um simulado comentado.

Inscrever-se no canal →

Material independente de preparação, sem afiliação ou endosso de Linux Professional Institute (LPI). As questões são inéditas e não reproduzem a prova real.