



SUSE Linux Enterprise Desktop 15 SP4

Guia de Administração

Guia de Administração

SUSE Linux Enterprise Desktop 15 SP4


Esse guia aborda as tarefas de administração do sistema, como manutenção, monitoramento e personalização de um sistema instalado inicialmente.

Data de Publicação: setembro 29, 2024

<https://documentation.suse.com> 

Copyright © 2006-2024 SUSE LLC e colaboradores. Todos os direitos reservados.

Permissão concedida para copiar, distribuir e/ou modificar este documento sob os termos da Licença GNU de Documentação Livre, Versão 1.2 ou (por sua opção) versão 1.3; com a Seção Invariante sendo estas informações de copyright e a licença. Uma cópia da versão 1.2 da licença está incluída na seção intitulada “GNU Free Documentation License” (Licença GNU de Documentação Livre).

Para ver as marcas registradas da SUSE, visite <https://www.suse.com/company/legal/> . Todas as marcas comerciais de terceiros pertencem a seus respectivos proprietários. Os símbolos de marca registrada (®, ™ etc.) indicam as marcas registradas da SUSE e de suas afiliadas. Os asteriscos (*) indicam marcas registradas de terceiros.

Todas as informações deste manual foram compiladas com a maior atenção possível aos detalhes. Entretanto, isso não garante uma precisão absoluta. A SUSE LLC, suas afiliadas, os autores ou tradutores não serão responsáveis por possíveis erros nem pelas consequências resultantes de tais erros.

Conteúdo

Prefácio **xxi**

- 1 Documentação disponível **xxi**
- 2 Melhorando a documentação **xxi**
- 3 Convenções da documentação **xxii**
- 4 Suporte **xxiv**
 - Declaração de suporte do SUSE Linux Enterprise Desktop **xxiv** • Prévias de tecnologia **xxv**

I TAREFAS COMUNS **1**

1 Bash e scripts Bash **2**

- 1.1 O que é “o shell”? **2**
 - Arquivos de configuração do Bash **2** • Estrutura de diretórios **5**
- 1.2 Gravando scripts shell **9**
- 1.3 Redirecionando eventos de comando **11**
- 1.4 Usando aliases **12**
- 1.5 Usando variáveis no Bash **12**
 - Usando variáveis de argumento **13** • Usando substituição de variável **14**
- 1.6 Agrupando e combinando comandos **15**
- 1.7 Trabalhando com construções de fluxo comuns **16**
 - Comando de controle if **16** • Criando loops com o comando **for** **17**
- 1.8 Mais informações **17**

2 Conceitos básicos sobre o **sudo** **18**

- 2.1 Uso básico do **sudo** **18**
 - Executando um único comando **18** • Iniciando um shell **19**

- 2.2 Configurando o **sudo** 20
 - Editando os arquivos de configuração 20 • Sintaxe de configuração básica do sudoers 21 • Regras básicas do sudoers 22
- 2.3 Casos de uso do **sudo** 24
 - Usando o **sudo** sem senha de root 24 • Usando o **sudo** com aplicativos X.Org 26
- 2.4 Mais informações 26
- 3 Usando o YaST 27**
- 3.1 Visão geral da interface do YaST 27
- 3.2 Combinações de teclas úteis 27
- 4 YaST em modo de texto 29**
- 4.1 Navegação em módulos 30
- 4.2 Combinações de teclas avançadas 31
- 4.3 Restrição de combinações de teclas 32
- 4.4 Opções de linha de comando do YaST 33
 - Instalando pacotes da linha de comando 33 • Trabalhando com módulos individuais 33 • Parâmetros de linha de comando dos módulos do YaST 34
- 5 Mudando as configurações de idioma e país com o YaST 58**
- 5.1 Mudando o idioma do sistema 58
 - Modificando idiomas do sistema com o YaST 59 • Trocando o idioma padrão do sistema 61 • Alternando idiomas de aplicativos X padrão e do GNOME 62
- 5.2 Mudando as configurações de país e horário 62
- 6 Gerenciando usuários com o YaST 66**
- 6.1 Caixa de diálogo Administração de Usuário e Grupo 66

6.2	Gerenciando contas de usuário	68
6.3	Opções adicionais para contas dos usuários	70
	Login automático e login sem senha	70 • Assegurando o uso obrigatório de políticas de senha
	Gerenciando cotas	71
6.4	Mudando as configurações padrão para usuários locais	74
6.5	Atribuindo usuários a grupos	75
6.6	Gerenciando grupos	75
6.7	Mudando o método de autenticação do usuário	77
6.8	Usuários do sistema padrão	78
7	Atualização online do YaST	81
7.1	Caixa de diálogo de atualização online	82
7.2	Instalando patches	83
7.3	Vendo os patches recolhidos	84
7.4	Atualização online automática	85
8	Instalando ou removendo software	88
8.1	Definição de termos	88
8.2	Registrando um sistema instalado	90
	Registrando no YaST	90 • Registrando no SUSEConnect
8.3	Usando o gerenciador de software do YaST	90
	Pesquisando software	91 • Instalando e removendo pacotes ou padrões
	Atualizando pacotes	94 • Dependências de pacotes
	Lidando com as recomendações de pacotes	98
8.4	Gerenciando repositórios de software e serviços	98
	Adicionando repositórios de software	99 • Gerenciando as propriedades do repositório
	Gerenciando chaves de repositório	102
8.5	Atualizador de pacotes do GNOME	103
8.6	Atualizando pacotes com o <i>GNOME Software</i>	105

9 Gerenciando software com ferramentas de linha de comando 107

9.1 Usando o zypper 107

Uso geral 107 • Usando os subcomandos do Zypper 109 • Instalando e removendo software com o Zypper 109 • Atualizando software com o zypper 114 • Identificando processos e serviços que usam arquivos apagados 120 • Gerenciando repositórios com o Zypper 122 • Consultando repositórios e pacotes com o Zypper 124 • Mostrando as informações de ciclo de vida 126 • Configurando o Zypper 127 • Solução de problemas 127 • Recurso de rollback do Zypper no sistema de arquivos Btrfs 128 • Mais informações 128

9.2 RPM: gerenciador de pacotes 128

Verificando a autenticidade do pacote 129 • Gerenciando pacotes: instalar, atualizar e desinstalar 129 • Pacotes RPM Delta 131 • RPMconsultas 131 • Instalando e compilando pacotes de fontes 134 • Compilando pacotes RPM com build 136 • Ferramentas para arquivos e banco de dados RPM 137

10 Recuperação de sistema e gerenciamento de instantâneos com o Snapper 138

10.1 Configuração padrão 139

Configurações padrão 140 • Tipos de instantâneos 140 • Diretórios que são excluídos dos instantâneos 141 • Personalizando a configuração 142

10.2 Usando o Snapper para desfazer mudanças 146

Desfazendo mudanças do YaST e do Zypper 147 • Usando o Snapper para restaurar arquivos 152

10.3 Rollback do sistema por inicialização de instantâneos 154

Instantâneos após rollback 156 • Acessando e identificando entradas de boot de instantâneos 157 • Limitações 158

- 10.4 Habilitando o Snapper em diretórios pessoais dos usuários **160**
Instalando o pam_snapper e criando usuários **160** • Removendo
usuários **161** • Habilitando manualmente os instantâneos em diretórios
pessoais **161**
- 10.5 Criando e modificando as configurações do Snapper **162**
Gerenciando configurações existentes **163**
- 10.6 Criando e gerenciando instantâneos manualmente **167**
Metadados de instantâneos **167** • Criando
instantâneos **169** • Modificando os metadados do
instantâneo **170** • Apagando instantâneos **171**
- 10.7 Limpeza automática de instantâneos **172**
Limpando instantâneos numerados **173** • Limpando instantâneos
de linha do tempo **175** • Limpando pares de instantâneos
que não são diferentes **176** • Limpando instantâneos criados
manualmente **177** • Adicionando suporte a cotas de disco **177**
- 10.8 Mostrando o espaço em disco exclusivo usado pelos instantâneos **179**
- 10.9 Perguntas frequentes **181**
- 11 Kernel Live Patching com KLP **182****
- 11.1 Vantagens do Kernel Live Patching **182**
- 11.2 Visão geral do Kernel Live Patching **182**
Escopo do Kernel Live Patching **184** • Limitações do Kernel Live
Patching **184**
- 11.3 Ativando o Kernel Live Patching por meio do YaST **184**
- 11.4 Ativando o Kernel Live Patching pela linha de comando **185**
- 11.5 Executando o Kernel Live Patching **186**
Verificando a data de vencimento do patch ativo **187**
- 11.6 Solucionando problemas do Kernel Live Patching **187**
Downgrade manual do patch **187**

12 Aplicação de patches ativos no espaço do usuário 189

- 12.1 Sobre a aplicação de patches ativos no espaço do usuário 189
Pré-requisitos 189 • Usando o libpulp 189

- 12.2 Mais informações 191

13 Atualizações transacionais 192

- 13.1 Limitações da prévia de tecnologia 193
- 13.2 Habilitar `transactional-update` 195
- 13.3 Gerenciando as atualizações automáticas 195
- 13.4 Comando **`transactional-update`** 195
- 13.5 Solução de problemas 198

14 Sessões gráficas remotas com VNC 199

- 14.1 Cliente **`vncviewer`** 199
Conexão por meio da CLI do `vncviewer` 199 • Conexão por meio da GUI do `vncviewer` 200 • Notificação de conexões não criptografadas 200
- 14.2 Remmina: o cliente de área de trabalho remota 200
Instalação 201 • Janela principal 201 • Adicionando sessões remotas 201 • Iniciando sessões remotas 203 • Editando, copiando e apagando sessões gravadas 204 • Executando sessões remotas da linha de comando 204
- 14.3 Configurando sessões únicas no servidor VNC 205
Configurações disponíveis 207 • Iniciando uma sessão VNC única 207 • Configurando sessões VNC únicas 207
- 14.4 Configurando sessões persistentes do servidor VNC 208
Sessão VNC iniciada usando `vncserver` 209 • Sessão VNC iniciada usando `vncmanager` 211
- 14.5 Configurando a criptografia no servidor VNC 214

15 Cópia de arquivo com RSync 217

- 15.1 Visão geral conceitual 217
- 15.2 Sintaxe básica 217
- 15.3 Copiando arquivos e diretórios localmente 218
- 15.4 Copiando arquivos e diretórios remotamente 219
- 15.5 Configurando e usando um servidor Rsync 219
- 15.6 Mais informações 222

II INICIALIZANDO UM SISTEMA LINUX 224

16 Introdução ao processo de boot 225

- 16.1 Terminologia 225
- 16.2 Processo de boot do Linux 226
 - Fase de inicialização e do carregador de boot 226 • Fase do kernel 228 • Fase do init no initramfs 231 • Fase do systemd 233

17 UEFI (Unified Extensible Firmware Interface) 234

- 17.1 Boot seguro 234
 - Implementação no SUSE Linux Enterprise Desktop 235 • MOK (Chave do Proprietário da Máquina) 238 • Inicializando um kernel personalizado 238 • Usando drivers que não são de caixa de entrada 240 • Recursos e limitações 241
- 17.2 Mais informações 242

18 Carregador de boot GRUB 2 243

- 18.1 Principais diferenças entre o GRUB legado e o GRUB 2 243
- 18.2 Estrutura do arquivo de configuração 244
 - Arquivo /boot/grub2/grub.cfg 245 • Arquivo /etc/default/grub 245 • Scripts em /etc/grub.d 248 • Mapeamento entre unidades BIOS e dispositivos Linux 250 • Editando as entradas de menu durante o

- procedimento de boot 250 • Definindo uma senha de boot 252 • Acesso autorizado às entradas do menu de boot 253
- 18.3 Configurando o carregador de boot com o YaST 254
 - Local do carregador de boot e opções de código de boot 255 • Ajustando a ordem dos discos 257 • Configurando as opções avançadas 257
- 18.4 Comandos úteis do GRUB 2 261
- 18.5 Mais informações 262
- 19 Daemon systemd 263**
 - 19.1 Conceito do systemd 263
 - Arquivo unit 264
 - 19.2 Uso básico 265
 - Gerenciando serviços em um sistema em execução 265 • Habilitando/Desabilitando serviços permanentemente 267
 - 19.3 Inicialização do sistema e gerenciamento de destino 269
 - Comparação entre destinos e níveis de execução 269 • Depurando a inicialização do sistema 273 • Compatibilidade com o System V 276
 - 19.4 Gerenciando serviços com o YaST 277
 - 19.5 Personalizando systemd 278
 - Personalizando os arquivos unit 278 • Criando arquivos drop-in 279 • Convertendo serviços xinetd em systemd 280 • Criando destinos personalizados 281
 - 19.6 Uso avançado 282
 - Limpando diretórios temporários 282 • Registro do sistema 283 • Instantâneos 283 • Carregando módulos do kernel 284 • Executando ações antes de carregar um serviço 284 • Grupos de controle (cgroups) do kernel 285 • Terminando os serviços (enviando sinais) 286 • Notas importantes sobre o serviço D-Bus 287 • Depurando serviços 288

- 19.7 Unidades do temporizador do `systemd` 289
 - Tipos de temporizador do `systemd` 289 • Temporizadores e unidades de serviço do `systemd` 290 • Exemplo prático 290 • Gerenciando temporizadores do `systemd` 292
- 19.8 Mais informações 292

III SISTEMA 293

20 Aplicativos de 32 bits e 64 bits em um ambiente de sistema de 64 bits 294

- 20.1 Suporte em tempo de execução 294
- 20.2 Especificações do kernel 295

21 `journalctl`: Consultar o diário do `systemd` 296

- 21.1 Tornando o diário persistente 296
- 21.2 `journalctl`: Switches úteis 297
- 21.3 Filtrando a saída do diário 298
 - Filtrando com base em um número de boot 298 • Filtrando com base no intervalo de tempo 299 • Filtrando com base nos campos 299
- 21.4 Investigando erros do `systemd` 300
- 21.5 Configuração do `journald` 301
 - Mudando o limite de tamanho do diário 302 • Encaminhando o diário para `/dev/ttyX` 302 • Encaminhando o diário para o recurso do `syslog` 302
- 21.6 Usando o YaST para filtrar o diário do `systemd` 303
- 21.7 Vendo registros no GNOME 303

22 `update-alternatives`: Gerenciando várias versões de comandos e arquivos 304

- 22.1 Visão Geral 304
- 22.2 Casos de uso 306
- 22.3 Obtendo uma visão geral das alternativas 306

22.4	Vendo detalhes das alternativas específicas	306
22.5	Definindo a versão padrão das alternativas	307
22.6	Instalando alternativas personalizadas	308
22.7	Definindo alternativas dependentes	310
23	Rede básica	312
23.1	Endereços IP e roteamento	315
	Endereços IP	315 • Máscaras de rede e roteamento
23.2	IPv6: a Internet de última geração	318
	Vantagens	319 • Estrutura e tipos de endereços
	Coexistência de IPv4 e IPv6	325 • Configurando o IPv6
	Mais informações	326
23.3	Resolução de nome	327
23.4	Configurando uma conexão de rede com o YaST	328
	Configurando a placa de rede com o YaST	329
23.5	NetworkManager	341
	NetworkManager e wicked	342 • Funcionalidade e arquivos de configuração do NetworkManager
	Controlando e bloqueando recursos do NetworkManager	343
23.6	Configurando uma conexão de rede manualmente	344
	Configuração de rede com wicked	344 • Arquivos de configuração
	Testando a configuração	363 • Arquivos unit e scripts de inicialização
		368
23.7	Configurando dispositivos de ligação	369
	Hotplug de portas de ligação	372
23.8	Configurando dispositivos de equipe para agrupamento de rede	373
	Caso de uso: equilíbrio de carga com agrupamento de rede	377 • Caso de uso: failover com agrupamento de rede
	Caso de uso: VLAN em dispositivo de agrupamento	378 • Caso de uso: VLAN em dispositivo de agrupamento
		379
24	Operação da impressora	382
24.1	O workflow do CUPS	383

- 24.2 Métodos e protocolos de conexão de impressoras 384
- 24.3 Instalando o software 384
- 24.4 Impressoras de rede 385
- 24.5 Configurando o CUPS com ferramentas de linha de comando 386
- 24.6 Imprimindo pela linha de comando 388
- 24.7 Recursos especiais no SUSE Linux Enterprise Desktop 388
 - CUPS e firewall 388 • Procurando impressoras de rede 389 • Arquivos PPD em vários pacotes 390
- 24.8 Solução de problemas 390
 - Impressoras sem suporte de linguagem de impressora padrão 390 • Nenhum arquivo PPD adequado disponível para impressora PostScript 391 • Conexões da impressora de rede 392 • Defeitos na impressão sem mensagem de erro 394 • Filas desabilitadas 394 • Navegação do CUPS: apagando serviços de impressão 395 • Serviços de impressão com defeito e erros de transferência de dados 395 • Depurando o CUPS 396 • Mais informações 396

25 Interface gráfica do usuário 397

- 25.1 Sistema X Window 397
- 25.2 Instalando e configurando fontes 398
 - Mostrando as fontes instaladas 399 • Vendo fontes 400 • Consultando fontes 400 • Instalando fontes 401 • Configurando a aparência das fontes 401
- 25.3 Configuração do GNOME para administradores 411
 - Sistema dconf 411 • Configuração de todo o sistema 411 • Mais informações 412
- 25.4 Alternando entre as GPUs Intel e NVIDIA Optimus com o SUSE Prime 412
 - Pré-requisitos 413 • Instalando e usando o SUSE Prime 413 • Instalando drivers NVIDIA 414

26	Acessando sistemas de arquivos com o FUSE	415
26.1	Configurando o FUSE	415
26.2	Montando uma partição NTFS	415
26.3	Mais informações	416
27	Instalando várias versões do kernel	417
27.1	Habilitando e configurando suporte multiversão	417
	Apagando kernels não usados automaticamente 418 • Caso de uso: Apagando um kernel antigo apenas depois da reinicialização 419 • Caso de uso: Mantendo kernels mais antigos como fallback 420 • Caso de uso: Mantendo uma versão específica do kernel 420	
27.2	Instalando/Removendo várias versões do kernel com o YaST	421
27.3	Instalando/Removendo várias versões do kernel com o Zypper	422
28	Gerenciando módulos do kernel	424
28.1	Listando módulos carregados com lsmod e modinfo	424
28.2	Adicionando e removendo módulos do kernel	425
	Carregando módulos do kernel automaticamente na inicialização 425 • Adicionando módulos do kernel à lista negra com modprobe 426	
29	Gerenciamento dinâmico de dispositivos do kernel com udev	428
29.1	Diretório /dev	428
29.2	Kernel uevents e udev	428
29.3	Drivers, módulos do kernel e dispositivos	429
29.4	Inicialização e configuração do dispositivo inicial	430
29.5	Monitorando o daemon udev em execução	430

- 29.6 Influenciando o gerenciamento de eventos de dispositivo do kernel com as regras do udev 431
 - Usando operadores nas regras do udev 434 • Usando substituições nas regras do udev 434 • Usando as chaves de correspondência do udev 435 • Usando as chaves de atribuição do udev 437
- 29.7 Nomeação persistente de dispositivos 438
- 29.8 Arquivos usados pelo udev 439
- 29.9 Mais informações 440

30 Recursos especiais do sistema 441

- 30.1 Informações sobre pacotes de software especiais 441
 - Pacote bash e /etc/profile 441 • Pacote cron 442 • Parando mensagens de status do Cron 443 • Arquivos de registro: pacote logrotate 443 • Comando **locate** 443 • Comando **ulimit** 444 • Comando **free** 445 • Páginas de manual e de informações 445 • Selecionando páginas de manual usando o comando **man** 446 • Configurações para GNU Emacs 446
- 30.2 Consoles virtuais 447
- 30.3 Mapeamento de teclado 447
- 30.4 Configurações de idioma e específicas de país 448
 - Configurações de idioma de todo o sistema 449 • Alguns exemplos 450 • Configurações de idioma em ~/.i18n 451 • Configurações de suporte de idioma 452 • Mais informações 452

31 Usando o NetworkManager 453

- 31.1 Casos de uso do NetworkManager 453
- 31.2 Habilitando ou desabilitando o NetworkManager 454
- 31.3 Configurando conexões de rede 454
 - Gerenciando conexões de rede com fio 456 • Gerenciando conexões de rede wireless 457 • Habilitando detecção de portal cativo

- wireless 457 • Configurando a placa Wi-Fi/Bluetooth como ponto de acesso 458 • NetworkManager e VPN 458
- 31.4 NetworkManager e segurança 460
 - Conexões de usuário e sistema 461 • Armazenando senhas e credenciais 461 • Zonas do firewall 461
- 31.5 Perguntas frequentes 462
- 31.6 Solução de problemas 464
- 31.7 Mais informações 465
- IV CONFIGURAÇÃO DE HARDWARE 466**
- 32 Configurando o layout do teclado do sistema 467**
- 33 Configurando placas de som 468**
- 34 Configurando uma impressora 471**
 - 34.1 Configurando impressoras 471
 - Adicionando drivers com o YaST 473 • Editando a configuração da impressora local 474
 - 34.2 Configurando a impressão pela rede com o YaST 475
 - Usando CUPS 475 • Usando servidores de impressão diferentes do CUPS 476
 - 34.3 Compartilhando impressoras pela rede 476
- 35 Configurando um scanner 478**
 - 35.1 Configurando um dispositivo multifuncional HP 478
 - 35.2 Compartilhando um scanner pela rede 479
 - 35.3 Digitalizando pela rede 479
- 36 Gerenciamento de energia 480**
 - 36.1 Funções de economia de energia 480

36.2 Advanced Configuration and Power Interface (ACPI) 481
Controlando o desempenho da CPU 482 • Solução de problemas 482

36.3 Inatividade do disco rígido 484

36.4 Solução de problemas 486
A frequência da CPU não funciona 486

37 Memória persistente 487

37.1 Introdução 487

37.2 Termos 488

37.3 Casos de uso 491
PMEM com DAX 491 • PMEM com BTT 491

37.4 Ferramentas para gerenciamento de memória persistente 492

37.5 Configurando a memória persistente 493
Vendo o armazenamento NVDIMM disponível 493 • Configurando o armazenamento como um único namespace PMEM com DAX 495 • Criando um namespace PMEM com BTT 497 • Colocando o diário do sistema de arquivos na PMEM/BTT 498

37.6 Mais informações 499

V SERVIÇOS 500

38 Gerenciamento de serviços com o YaST 501

39 Sincronização de horário com NTP 503

39.1 Configurando um cliente NTP com YaST 504
Início do daemon do NTP 504 • Tipo de fonte de configuração 505 • Configurar servidores de horário 505

39.2 Configurando manualmente o NTP na rede 506

39.3 Configurar o chronyd em tempo de execução usando o **chronyc** 507

39.4 Sincronização de horário dinâmica em tempo de execução 508

- 39.5 Configurando um relógio de referência local 508
- 39.6 Sincronização do relógio com uma Referência de Horário Externa (ETR, External Time Reference) 509

VI SOLUÇÃO DE PROBLEMAS 511

40 Ajuda e documentação 512

- 40.1 Diretório da documentação 512
 - Manuais do SUSE 513 • Documentação do pacote 513
- 40.2 Páginas de manual 514
- 40.3 Páginas de informações 516
- 40.4 Recursos online 516

41 Reunindo informações do sistema para suporte 518

- 41.1 Exibindo informações atuais do sistema 518
- 41.2 Coletando informações do sistema com o supportconfig 519
 - Criando um número de solicitação de serviço 519 • Destinos de upload 520 • Criando um arquivo supportconfig com o YaST 520 • Criando um arquivo supportconfig da linha de comando 523 • Compreendendo a saída do **supportconfig** 524 • Opções comuns do supportconfig 525 • Visão geral do conteúdo do arquivo 526
- 41.3 Enviando informações ao suporte técnico global 529
- 41.4 Analisando as informações do sistema 531
 - Ferramenta de linha de comando SCA 532 • Aplicação SCA 533 • Desenvolvendo padrões de análise personalizados 545
- 41.5 Coletando informações durante a instalação 545
- 41.6 Suporte aos módulos do kernel 546
 - Informações técnicas 547 • Trabalhando com módulos não suportados 547
- 41.7 Mais informações 548

42 Problemas comuns e suas soluções 550

42.1 Localizando e reunindo informações 550

42.2 Problemas de boot 553

Falha ao carregar o carregador de boot GRUB 2 553 • Não é exibido nenhum prompt nem tela de login 554 • Não há login gráfico 555 • Não é possível montar a partição Btrfs raiz 555 • Forçar verificação de partições raiz 555 • Desabilitar a troca (swap) para habilitar a inicialização 556 • O GRUB 2 falha durante a reinicialização em um sistema de boot duplo 556

42.3 Problemas de login 556

Falha nas combinações de nome de usuário e senha válidas 557 • Nome de usuário e senha válidos que não são aceitos 558 • Falha de login na partição pessoal criptografada 560 • A área de trabalho do GNOME tem problemas 561

42.4 Problemas de rede 562

Problemas no NetworkManager 566

42.5 Problemas de dados 566

Gerenciando imagens de partição 567 • Usando o sistema de recuperação 567

A Rede de exemplo 575

B GNU licenses 576

Prefácio

1 Documentação disponível

Documentação online

A documentação online deste produto está disponível em <https://documentation.suse.com/#sled>. Procure ou faça download da documentação em vários formatos.

Encontre a documentação online de outros produtos em <https://documentation.suse.com/>.



Nota: Atualizações mais recentes

Normalmente, as atualizações mais recentes estão disponíveis na versão em inglês da documentação.

Notas de versão

Para ver as notas de versão, visite <https://www.suse.com/releasesnotes/>.

Em seu sistema

Para uso offline, encontre a documentação no sistema instalada em `/usr/share/doc`. Muitos comandos também estão descritos em detalhes nas respectivas *páginas de manual*. Para vê-los, execute `man`, seguido do nome de um comando específico. Se o comando `man` não estiver instalado no sistema, instale-o com `sudo zypper install man`.

2 Melhorando a documentação


Seus comentários e suas contribuições para esta documentação são bem-vindos. Os seguintes canais para fornecer feedback estão disponíveis:

Solicitações de serviço e suporte

Para conhecer os serviços e as opções de suporte disponíveis para o seu produto, consulte <https://www.suse.com/support/>.

Para abrir uma solicitação de serviço, você precisa de uma assinatura do SUSE registrada no SUSE Customer Center. Vá para <https://scc.suse.com/support/requests>, efetue login e clique em *Criar Novo*.

Relatórios de bugs

Relate os problemas com a documentação em <https://bugzilla.suse.com/> . Para simplificar esse processo, você pode usar os links *Report Documentation Bug* (Relatar Bug na Documentação) ao lado dos cabeçalhos na versão HTML deste documento. Isso pré-seleciona o produto e a categoria certos no Bugzilla e adiciona um link à seção atual. Você pode começar a digitar o relatório do bug imediatamente. Uma conta do Bugzilla é necessária.


Contribuições

Para contribuir com esta documentação, use os links *Edit Source* (Editar Fonte) ao lado dos cabeçalhos na versão HTML deste documento. Eles levarão você até o código-fonte no GitHub, onde é possível abrir uma solicitação pull. Uma conta do GitHub é necessária.



Nota: *Edit Source* (Editar Fonte) disponível apenas para inglês

Os links *Edit Source* (Editar Fonte) estão disponíveis apenas para a versão em inglês de cada documento. Para todos os outros idiomas, use os links *Report Documentation Bug* (Relatar Bug na Documentação).

Para obter mais informações sobre o ambiente da documentação usado para este documento, consulte o README do repositório em <https://github.com/SUSE/doc-sle/blob/main/README.adoc> .

E-mail

É possível também relatar erros e enviar comentários sobre a documentação para doc-team@suse.com. Inclua o título do documento, a versão do produto e a data de publicação do documento. Mencione também o número e o título da seção relevante (ou inclua o URL) e insira uma breve descrição do problema.

3 Convenções da documentação

Os seguintes avisos e convenções tipográficas são usados nesta documentação:

- /etc/passwd: nomes de diretório e arquivo
- MARCADOR: substitua MARCADOR pelo valor real

- PATH: a variável do ambiente PATH
- ls, --help: comandos, opções e parâmetros
- user: usuários ou grupos
- package name: nome de um pacote
- Alt, Alt – F1: uma tecla ou uma combinação de teclas a serem pressionadas; as teclas são mostradas em letras maiúsculas como aparecem no teclado
- *Arquivo*, *Arquivo* > *Gravar Como*: itens de menu, botões
- *Pinguins Dançarinos* (Capítulo *Pinguins*, ↑Outro Manual): É uma referência a um capítulo de outro manual.
- Comandos que devem ser executados com privilégios root. Geralmente, você também pode usar o comando sudo como prefixo nesses comandos para executá-los como usuário não privilegiado.

```
# command
> sudo command
```

- Comandos que podem ser executados por usuários sem privilégios.

```
> command
```

- Avisos



Atenção: Mensagem de aviso

Informações vitais que você deve saber antes de continuar. Avisa sobre problemas de segurança, potencial perda de dados, danos no hardware ou perigos físicos.



Importante: Aviso importante

Informações importantes que você deve saber antes de continuar.



Nota: Nota

Informações adicionais, por exemplo, sobre diferenças nas versões do software.



Dica: Aviso de dica


Informações úteis, como uma diretriz ou informação prática.

4 Suporte

Encontre a declaração de suporte do SUSE Linux Enterprise Desktop e as informações gerais sobre as prévias de tecnologia a seguir. Para obter detalhes sobre o ciclo de vida do produto, consulte *Livro “Upgrade Guide”, Capítulo 2 “Lifecycle and support”*.

Se você tiver direito a suporte, encontre os detalhes de como coletar informações para um ticket de suporte no *Capítulo 41, Reunindo informações do sistema para suporte*.

4.1 Declaração de suporte do SUSE Linux Enterprise Desktop

Para receber suporte, você precisa de uma inscrição apropriada na SUSE. Para ver as ofertas de suporte específicas que estão disponíveis para você, acesse <https://www.suse.com/support/>  e selecione seu produto.

Os níveis de suporte são definidos da seguinte forma:

L1

Determinação do problema, que significa suporte técnico designado para fornecer informações de compatibilidade, suporte ao uso, manutenção contínua, coleta de informações e solução básica de problemas usando a documentação disponível.

L2

Isolamento do problema, que significa suporte técnico designado para analisar os dados, reproduzir os problemas dos clientes, isolar as áreas problemáticas e resolver os problemas não resolvidos no Nível 1 ou preparar-se para o Nível 3.

L3

Resolução do problema, que significa suporte técnico designado para resolver os problemas com a participação da engenharia para solucionar defeitos nos produtos que foram identificados pelo Suporte de Nível 2.

Para clientes e parceiros contratados, o SUSE Linux Enterprise Desktop foi entregue com suporte L3 para todos os pacotes, com as seguintes exceções:

- prévias de tecnologia
- som, gráficos, fontes e arte
- pacotes que requerem um contrato de cliente adicional
- alguns pacotes enviados como parte do módulo *Workstation Extension* contam apenas com suporte L2
- os pacotes com nomes que terminam em `-devel` (contendo arquivos de cabeçalho e recursos de desenvolvedor semelhantes) serão suportados apenas junto com seus pacotes principais.

A SUSE apenas oferecerá suporte ao uso dos pacotes originais. Isto é, pacotes que não foram modificados nem recompilados.

4.2 Prévias de tecnologia

As Prévias de tecnologia são pacotes, pilhas ou recursos fornecidos pela SUSE como amostras de inovações futuras. As prévias estão incluídas para sua conveniência e para que você possa testar as novas tecnologias em seu ambiente. Agradecemos seus comentários! Se você testar uma prévia de tecnologia, contate seu representante SUSE e conte sobre sua experiência e seus casos de uso. Suas informações são úteis para o desenvolvimento futuro.

No entanto, as prévias de tecnologia são fornecidas com as seguintes limitações:

- As prévias de tecnologia ainda estão em desenvolvimento. Portanto, elas podem ter funcionalidades incompletas, instáveis ou, de alguma outra maneira, *inadequadas* para uso em produção.
- As prévias de tecnologia *não* contam com suporte.
- As prévias de tecnologia talvez estejam disponíveis apenas para arquiteturas de hardware específicas.

- Os detalhes e as funcionalidades das prévias de tecnologia estão sujeitos a mudanças. Consequentemente, o upgrade para as versões subsequentes de uma prévia de tecnologia pode ser impossível e exigir uma instalação nova.
- As prévias de tecnologia podem ser descartadas a qualquer momento. Por exemplo, se a SUSE descobrir que uma prévia não atende às necessidades do cliente ou do mercado ou não cumpre os padrões da empresa. A SUSE não se compromete em oferecer uma versão com suporte desse tipo de tecnologia no futuro.

Para obter uma visão geral das prévias de tecnologia fornecidas com seu produto, consulte as notas de lançamento em <https://www.suse.com/releasesnotes/> .

I Tarefas comuns

- 1 Bash e scripts Bash 2
- 2 Conceitos básicos sobre o **sudo** 18
- 3 Usando o YaST 27
- 4 YaST em modo de texto 29
- 5 Mudando as configurações de idioma e país com o YaST 58
- 6 Gerenciando usuários com o YaST 66
- 7 Atualização online do YaST 81
- 8 Instalando ou removendo software 88
- 9 Gerenciando software com ferramentas de linha de comando 107
- 10 Recuperação de sistema e gerenciamento de instantâneos com o Snapper 138
- 11 Kernel Live Patching com KLP 182
- 12 Aplicação de patches ativos no espaço do usuário 189
- 13 Atualizações transacionais 192
- 14 Sessões gráficas remotas com VNC 199
- 15 Cópia de arquivo com RSync 217

1 Bash e scripts Bash

Atualmente, muitas pessoas usam computadores com uma GUI (Graphical User Interface – Interface Gráfica do Usuário), como o GNOME. As GUIs oferecem muitos recursos, mas elas são limitadas para executar tarefas automatizadas. Os shells são um bom complemento às GUIs, e este capítulo apresenta uma visão geral de alguns aspectos deles; neste caso, o shell Bash.

1.1 O que é “o shell”?

Normalmente, o shell do Linux é o Bash (Bourne again Shell). Quando este capítulo menciona “o shell”, ele se refere ao Bash. Há mais shells disponíveis (ash, csh, ksh, zsh, etc.), cada um deles empregando recursos e características diferentes. Se você precisar de mais informações sobre outros shells, pesquise por *shell* no YaST.

1.1.1 Arquivos de configuração do Bash

Um shell pode ser acionado como:

1. **Shell de login interativo.** Esse tipo é usado para efetuar login em uma máquina, chamando o Bash com a opção `--login`, ou para efetuar login em uma máquina remota com SSH.
2. **Shell interativo “comum”.** Normalmente, este é o caso ao iniciar o xterm, o konsole, o gnome-terminal ou as ferramentas semelhantes de interface de linha de comando (CLI, Command Line Interface).
3. **Shell não interativo.** Ele é invocado para chamar um script de shell na linha de comando.

Dependendo do tipo de shell usado, outros arquivos de configuração serão lidos. As tabelas seguintes mostram os arquivos de configuração de shell de login e sem login.

TABELA 1.1: ARQUIVOS DE CONFIGURAÇÃO DO BASH PARA SHELLS DE LOGIN

Arquivo	Descrição
<u>/etc/profile</u>	Não modifique esse arquivo, senão as suas modificações poderão ser destruídas durante a próxima atualização!

Arquivo	Descrição
<u>/etc/profile.local</u>	Use esse arquivos se for estender <u>/etc/profile</u>
<u>/etc/profile.d/</u>	Contém arquivos de configuração de programas específicos para todo o sistema
<u>~/.profile</u>	Insira aqui a configuração específica de usuário para os shells de login

Observe que o shell de login também extrai os arquivos de configuração listados na *Tabela 1.2, “Arquivos de configuração do Bash para shells sem login”*.

TABELA 1.2: ARQUIVOS DE CONFIGURAÇÃO DO BASH PARA SHELLS SEM LOGIN

<u>/etc/bash.bashrc</u>	Não modifique esse arquivo, senão as suas modificações poderão ser destruídas durante a próxima atualização!
<u>/etc/bash.bashrc.local</u>	Use esse arquivo para inserir suas modificações apenas do Bash em todo o sistema
<u>~/.bashrc</u>	Insira aqui a configuração específica de usuário

Além desses, o Bash usa mais outros arquivos:

TABELA 1.3: ARQUIVOS ESPECIAIS DO BASH

Arquivo	Descrição
<u>~/.bash_history</u>	Contém uma lista de todos os comandos que você digitou
<u>~/.bash_logout</u>	Executado durante o logout
<u>~/.alias</u>	Áliases definidos pelo usuário dos comandos usados com frequência. Consulte man 1 alias para obter mais detalhes sobre como definir alias.

Shells sem login

Há shells especiais que impedem que os usuários efetuem login no sistema: /bin/false e /sbin/nologin. Os dois apresentam uma falha silenciosa quando o usuário tenta efetuar login no sistema. Isso foi planejado como uma medida de segurança para os usuários do sistema, embora os sistemas operacionais Linux modernos tenham ferramentas mais eficazes para controlar o acesso ao sistema, como PAM e AppArmor.

O padrão do SUSE Linux Enterprise Desktop é atribuir /bin/bash a usuários humanos, e /bin/false ou /sbin/nologin a usuários de sistema. O usuário nobody tem o /bin/bash por razões de histórico, já que se trata de um usuário com privilégios mínimos que costumava ser o padrão para usuários de sistema. No entanto, o pouco de segurança obtida com o uso de nobody se perde quando vários usuários de sistema o utilizam. Talvez seja possível mudá-lo para /sbin/nologin. A forma mais rápida de fazer esse teste é mudá-lo e verificar se ele corrompe quaisquer serviços ou aplicativos.

Use o seguinte comando para listar os shells que são atribuídos a todos os usuários, tanto de sistema quanto humanos, em /etc/passwd. A saída varia de acordo com os serviços e os usuários no sistema:

```
> sort -t: -k 7 /etc/passwd | awk -F: '{print $1"\t" $7}' | column -t
tux                /bin/bash
nobody             /bin/bash
root               /bin/bash
avahi              /bin/false
chrony             /bin/false
dhcpd              /bin/false
dnsmasq            /bin/false
ftpsecure          /bin/false
lightdm            /bin/false
mysql              /bin/false
postfix            /bin/false
rtkit              /bin/false
sshd               /bin/false
tftp               /bin/false
unbound            /bin/false
bin                /sbin/nologin
daemon             /sbin/nologin
ftp                /sbin/nologin
lp                 /sbin/nologin
mail               /sbin/nologin
man                /sbin/nologin
nscd               /sbin/nologin
polkitd            /sbin/nologin
```

```

pulse           /sbin/nologin
qemu           /sbin/nologin
radvd          /sbin/nologin
rpc            /sbin/nologin
statd          /sbin/nologin
svn            /sbin/nologin
systemd-coredump /sbin/nologin
systemd-network /sbin/nologin
systemd-timesync /sbin/nologin
usbmux         /sbin/nologin
vnc            /sbin/nologin
wwwrun         /sbin/nologin
messagebus     /usr/bin/false
scard          /usr/sbin/nologin

```

1.1.2 Estrutura de diretórios

A tabela a seguir fornece uma breve visão geral dos mais importantes diretórios de nível superior encontrados em um sistema Linux. Informações mais detalhadas sobre os diretórios e subdiretórios importantes são encontradas na lista a seguir.

TABELA 1.4: VISÃO GERAL DE UMA ÁRVORE DE DIRETÓRIO PADRÃO

Diretório	Conteúdo
<u>/</u>	Diretório raiz: o ponto de partida da árvore do diretório.
<u>/bin</u>	Arquivos binários essenciais, como comandos necessários pelo administrador do sistema e por usuários comuns. Geralmente contém os shells, como o Bash.
<u>/boot</u>	Arquivos estáticos do carregador de boot.
<u>/dev</u>	Arquivos necessários para acessar dispositivos específicos de host.
<u>/etc</u>	Arquivos de configuração do sistema específicos de host.
<u>/home</u>	Contém os diretórios pessoais de todos os usuários que possuem conta no sistema. Porém, o diretório pessoal do <u>root</u> não está em <u>/home</u> , mas sim em <u>/root</u> .
<u>/lib</u>	Bibliotecas compartilhadas e módulos de kernel essenciais.

Diretório	Conteúdo
<u>/media</u>	Pontos de montagem de mídia removível.
<u>/mnt</u>	Ponto de montagem para montar temporariamente um sistema de arquivos.
<u>/opt</u>	Pacotes de aplicativos complementares.
<u>/root</u>	Diretório pessoal do superusuário <u>root</u> .
<u>/sbin</u>	Binários essenciais do sistema.
<u>/srv</u>	Dados de serviços fornecidos pelo sistema.
<u>/tmp</u>	Arquivos temporários.
<u>/usr</u>	Hierarquia secundária com dados apenas leitura.
<u>/var</u>	Dados variáveis, como arquivos de registro.
<u>/windows</u>	Disponível apenas se você tiver o Microsoft Windows* e o Linux instalados no sistema. Contém os dados do Windows.

A lista a seguir fornece informações mais detalhadas e alguns exemplos de arquivos e subdiretórios encontrados nos diretórios:

/bin

Contém comandos básicos do shell que podem ser usados pelo root e por outros usuários. Esses comandos incluem ls, mkdir, cp, mv, rm e rmdir. O /bin também contém o Bash, o shell padrão do SUSE Linux Enterprise Desktop.

/boot

Contém dados necessários para inicializar, como o carregador de boot, o kernel e outros dados usados para que o kernel possa executar programas em modo de usuário.

/dev

Contém arquivos de dispositivos que representam componentes de hardware.

/etc

Contém arquivos de configuração local que controlam a operação de programas como o Sistema X Window. O subdiretório /etc/init.d contém scripts init LSB que podem ser executados durante o processo de boot.

/home/NOMEDEUSUÁRIO

Contém os dados privados de todos os usuários que possuem uma conta no sistema. Os arquivos localizados aqui apenas podem ser modificados por seu proprietário ou pelo administrador do sistema. Por padrão, o diretório de e-mail e a configuração de área de trabalho pessoal estão localizados aqui, na forma de arquivos e diretórios ocultos, como .gconf/ e .config.



Nota: Diretório pessoal em um ambiente de rede

Se você estiver trabalhando em um ambiente de rede, seu diretório pessoal poderá ser mapeado para um diretório no sistema de arquivos diferente de /home.

/lib

Contém as bibliotecas compartilhadas essenciais necessárias para inicializar o sistema e executar os comandos no sistema de arquivos raiz. O equivalente no Windows para as bibliotecas compartilhadas são os arquivos DLL.

/media

Contém pontos de montagem para mídia removível, como CD-ROMs, discos flash e câmeras digitais (se usarem USB). /media geralmente mantém qualquer tipo de unidade, exceto o disco rígido do sistema. Quando o meio removível for inserido ou conectado ao sistema e estiver montado, você poderá acessá-lo deste local.

/mnt

O diretório fornece um ponto de montagem para um sistema de arquivos montado temporariamente. O root pode montar sistemas de arquivos aqui.

/opt

Reservado para a instalação de software de terceiros. Software opcional e pacotes de programas complementares maiores são encontrados aqui.

/root

Diretório pessoal do usuário root. Os dados pessoais do root estão localizados aqui.

/run

Um diretório tmpfs usado pelo systemd e por vários componentes. /var/run é um link simbólico para /run.

/sbin

Como indicado pelo s, esse diretório contém utilitários do superusuário. /sbin contém os binários essenciais para boot, restauração e recuperação do sistema, além dos binários em /bin.

/srv

Contém dados de serviços fornecidos pelo sistema, como FTP e HTTP.

/tmp

Esse diretório é usado por programas que exigem o armazenamento temporário dos arquivos.



Importante: Limpando o /tmp no momento da inicialização

Os dados armazenados em /tmp poderão não existir após uma reinicialização do sistema. Isso depende, por exemplo, das configurações feitas em /etc/tmpfiles.d/tmp.conf.

/usr

O /usr não tem relação com os usuários, mas se trata do acrônimo de Unix system resources (recursos do sistema Unix). Os dados em /usr são estáticos e apenas leitura, podendo ser compartilhados entre vários hosts compatíveis com FHS (Filesystem Hierarchy Standard – Padrão da Hierarquia do Sistema de Arquivos). Este diretório contém todos os programas de aplicativo, incluindo as áreas de trabalho gráficas, como o GNOME, e estabelece uma hierarquia secundária no sistema de arquivos. /usr contém vários subdiretórios como /usr/bin, /usr/sbin, /usr/local e /usr/share/doc.

/usr/bin

Contém programas geralmente acessíveis.

/usr/bin

Contém programas reservados ao administrador do sistema, como as funções de reparo.

/usr/local

Nesse diretório, o administrador do sistema pode instalar extensões locais e independentes de distribuição.

/usr/share/doc

Contém vários arquivos de documentação e as notas de versão do sistema. No subdiretório manual, você encontra uma versão online deste manual. Se houver mais de um idioma instalado, esse diretório poderá conter versões dos manuais em idiomas diferentes.

Em packages, você encontra a documentação incluída nos pacotes de software instalados no sistema. Para cada pacote, é criado um subdiretório /usr/share/doc/packages/NOME_DO_PACOTE, geralmente contendo arquivos README do pacote e, às vezes, exemplos, arquivos de configuração ou scripts adicionais.

Se houver HOWTOs instalados no sistema, /usr/share/doc também conterá o subdiretório howto, com documentação adicional sobre muitas tarefas relacionadas a configuração e operação do software Linux.

/var

Ao passo que /usr contém dados estáticos apenas leitura, /var destina-se aos dados gravados durante a operação do sistema, portanto variáveis, como arquivos de registro ou de spool. Para obter uma visão geral dos arquivos de registro mais importantes que estão em /var/log/, consulte a *Tabela 42.1, "Arquivos de registro"*.

/windows

Disponível apenas se você tiver o Microsoft Windows e o Linux instalados no sistema. Contém os dados do Windows disponíveis na partição do Windows do sistema. A sua capacidade de editar dados nesse diretório depende do sistema de arquivos usado pelas partições do Windows. No caso do FAT32, você pode abrir e editar os arquivos desse diretório. Para NTFS, o SUSE Linux Enterprise Desktop também oferece suporte a acesso de gravação. No entanto, o driver para o sistema de arquivos NTFS-3g possui funcionalidade limitada.

1.2 Gravando scripts shell

Os scripts shell são um modo conveniente para executar uma ampla gama de tarefas: coleta de dados, pesquisa por uma palavra ou frase em um texto e muitas outras coisas úteis. O exemplo seguinte mostra um pequeno script shell que imprime um texto:

EXEMPLO 1.1: UM SCRIPT SHELL QUE IMPRIME UM TEXTO

```
#!/bin/sh ❶  
# Output the following line: ❷
```

```
echo "Hello World" ③
```

- ① A primeira linha começa com os caracteres *Shebang* (`#!`) que indica que este arquivo é um script. O interpretador especificado após o *Shebang* executa o script. Neste caso, o interpretador especificado é `/bin/sh`.
- ② A segunda linha é um comentário que começa com o sinal de hash. É recomendável comentar linhas difíceis. Com o comentário apropriado, você pode se lembrar da finalidade e da função da linha. Além disso, outros leitores poderão entender seu script. O comentário é considerado uma boa prática na comunidade de desenvolvimento.
- ③ A terceira linha usa o comando interno `echo` para imprimir o texto correspondente.

Antes que você possa executar esse script, há alguns pré-requisitos:

1. Todo script deve conter uma linha Shebang (como no exemplo acima). Se a linha estiver ausente, você precisará chamar o interpretador manualmente.
2. Grave o script no lugar desejado. Contudo, convém gravá-lo em um diretório onde o shell possa encontrá-lo. O caminho de pesquisa em um shell é determinado pela variável de ambiente `PATH`. Um usuário normal geralmente não tem acesso de gravação em `/usr/bin`. Por essa razão, recomenda-se gravar seus scripts no diretório `~/bin/` dos usuários. O exemplo acima leva o nome `hello.sh`.
3. O script requer permissões de executável. Defina as permissões com o seguinte comando:

```
> chmod +x ~/bin/hello.sh
```

Se você atendeu a todos os pré-requisitos acima, poderá executar o script das seguintes maneiras:

1. **Como caminho absoluto.** O script pode ser executado em um caminho absoluto. No nosso caso, ele é `~/bin/hello.sh`.
2. **Em todos os lugares.** Se a variável de ambiente `PATH` incluir o diretório no qual o script está localizado, você poderá executar o script usando o comando `hello.sh`.

1.3 Redirecionando eventos de comando

Cada comando pode usar três canais, seja para entrada ou para saída:

- **Saída padrão.** Esse é o canal de saída padrão. Sempre que um comando imprime algo, ele usa o canal de saída padrão.
- **Entrada padrão.** Se um comando precisar da entrada dos usuários ou de outros comandos, ele usará esse canal.
- **Erro padrão.** Os comandos usam esse canal para gerar relatórios de erros.

Para redirecionar os canais, as possibilidades são as seguintes:

Comando > Arquivo

Grava a saída do comando em um arquivo, apagando um arquivo existente. Por exemplo, o comando **ls** grava sua saída no arquivo listing.txt:

```
> ls > listing.txt
```

Comando >> Arquivo

Anexa a saída do comando a um arquivo. Por exemplo, o comando **ls** anexa sua saída ao arquivo listing.txt:

```
> ls >> listing.txt
```

Comando < Arquivo

Lê o arquivo como entrada do comando em questão. Por exemplo, o comando **read** extrai o conteúdo do arquivo para a variável:

```
> read a < foo
```

Comando1 | Comando2

Redireciona a saída do comando à esquerda como entrada para o comando à direita. Por exemplo, o comando **cat** gera a saída do conteúdo do arquivo /proc/cpuinfo. Essa saída é usada por **grep** para filtrar apenas as linhas que contêm cpu:

```
> cat /proc/cpuinfo | grep cpu
```

Cada canal possui um *descriptor de arquivo*: 0 (zero) para entrada padrão, 1 para saída padrão e 2 para erro padrão. É permitido inserir esse descriptor de arquivo antes de um caractere `<` ou `>`. Por exemplo, a linha a seguir procura por um arquivo que começa com `foo`, mas suprime seus erros redirecionando-o para `/dev/null`:

```
> find / -name "foo*" 2>/dev/null
```

1.4 Usando alias

Um *alias* é uma definição de atalho de um ou mais comandos. A sintaxe de um *alias* é a seguinte:

```
alias NAME=DEFINITION
```

Por exemplo, a linha a seguir define um *alias* `lt` que gera uma listagem extensa (opção `-l`), classifica-a por horário de modificação (`-t`) e imprime-a em ordem inversa de classificação (`-r`):

```
> alias lt='ls -ltr'
```

Para ver todas as definições de *alias*, use `alias`. Remova o seu *alias* com `unalias` e o nome de *alias* correspondente.

1.5 Usando variáveis no Bash

Uma variável de shell pode ser global ou local. Variáveis globais, ou de ambiente, podem ser acessadas em todos os shells. As variáveis locais, ao contrário, são visíveis apenas no shell atual. Para ver todas as variáveis de ambiente, use o comando `printenv`. Se for preciso saber o valor de uma variável, insira o nome da variável como argumento:

```
> printenv PATH
```

Uma variável, seja ela global ou local, também pode ser visualizada com `echo`:

```
> echo $PATH
```

Para definir uma variável local, use um nome de variável, seguido pelo sinal de igual, seguido pelo valor:

```
> PROJECT="SLED"
```

Não insira espaços antes e depois do sinal de igual, senão você obterá um erro. Para definir uma variável de ambiente, use **export**:

```
> export NAME="tux"
```

Para remover uma variável, use **unset**:

```
> unset NAME
```

A tabela a seguir contém algumas variáveis de ambiente comuns que podem ser usadas nos seus scripts shell:

TABELA 1.5: VARIÁVEIS DE AMBIENTE ÚTEIS

<u>HOME</u>	diretório pessoal do usuário atual
<u>HOST</u>	nome do host atual
<u>LANG</u>	quando uma ferramenta é localizada, ela usa o idioma dessa variável de ambiente. Também é possível definir o idioma inglês como <u>C</u>
<u>PATH</u>	caminho de pesquisa do shell, uma lista de diretórios separados por dois-pontos
<u>PS1</u>	especifica o prompt normal impresso antes de cada comando
<u>PS2</u>	especifica o prompt secundário impresso quando você executa um comando em várias linhas
<u>PWD</u>	diretório de trabalho atual
<u>USUÁRIO</u>	usuário atual

1.5.1 Usando variáveis de argumento

Por exemplo, se você tiver o script **foo.sh**, poderá executá-lo desta maneira:

```
> foo.sh "Tux Penguin" 2000
```

Para acessar todos os argumentos que são passados ao seu script, você precisa de parâmetros de posição. Isto é, `$1` para o primeiro argumento, `$2` para o segundo e assim sucessivamente. É possível usar até nove parâmetros. Para obter o nome do script, use `$0`.

O script `foo.sh` a seguir imprime todos os argumentos de 1 a 4:

```
#!/bin/sh
echo \"$1\" \"$2\" \"$3\" \"$4\"
```

Se você executar esse script com os argumentos acima, obterá:

```
"Tux Penguin" "2000" "" ""
```

1.5.2 Usando substituição de variável

As substituições de variáveis aplicam um padrão ao conteúdo de uma variável, seja da esquerda ou da esquerda. A lista a seguir contém as formas de sintaxe possíveis:

`${VAR#padrão}`

remove a correspondência mais curta possível da esquerda:

```
> file=/home/tux/book/book.tar.bz2
> echo ${file#*/}
home/tux/book/book.tar.bz2
```

`${VAR##padrão}`

remove a correspondência mais longa possível da esquerda:

```
> file=/home/tux/book/book.tar.bz2
> echo ${file##*/}
book.tar.bz2
```

`${VAR%padrão}`

remove a correspondência mais curta possível da direita:

```
> file=/home/tux/book/book.tar.bz2
> echo ${file%.*}
/home/tux/book/book.tar
```

`${VAR%%padrão}`

remove a correspondência mais longa possível da direita:

```
> file=/home/tux/book/book.tar.bz2
```

```
> echo ${file%.*}  
/home/tux/book/book
```

\${VAR/padrão_1/padrão_2}

substitui o conteúdo de VAR do PADRÃO_1 pelo do PADRÃO_2:

```
> file=/home/tux/book/book.tar.bz2  
> echo ${file/tux/wilber}  
/home/wilber/book/book.tar.bz2
```

1.6 Agrupando e combinando comandos

Os shells permitem concatenar e agrupar comandos para uma execução condicional. Cada comando retorna um código de saída que determina o sucesso ou a falha de sua operação. Se o código for 0 (zero), significa que o comando obteve sucesso. Todos os outros códigos significam erro específico do comando.

A lista a seguir mostra como os comandos podem ser agrupados:

Comando1 ; Comando2

executa os comandos em sequência. O código de saída não é verificado. A linha a seguir exibe o conteúdo do arquivo com cat e depois imprime suas propriedades com ls, independentemente dos códigos de erro:

```
> cat filelist.txt ; ls -l filelist.txt
```

Comando1 && Comando2

executa o comando à direita quando o comando à esquerda for bem-sucedido (E lógico). A linha a seguir exibe o conteúdo do arquivo e imprime suas propriedades apenas quando o comando anterior obtiver sucesso (compare com a entrada anterior nesta lista):

```
> cat filelist.txt && ls -l filelist.txt
```

Comando1 || Comando2

executa o comando à direita quando o comando da esquerda falhar (OU lógico). A linha a seguir cria um diretório em /home/wilber/bar apenas quando a criação do diretório em /home/tux/foo falhar:

```
> mkdir /home/tux/foo || mkdir /home/wilber/bar
```

```
nome_da_função(){ ... }
```

cria uma função shell. Você pode usar os parâmetros de posição para acessar seus argumentos. A linha a seguir define a função `hello` para imprimir uma mensagem curta:

```
> hello() { echo "Hello $1"; }
```

Você pode chamar essa função assim:

```
> hello Tux
```

que imprimirá:

```
Hello Tux
```

1.7 Trabalhando com construções de fluxo comuns

Para controlar o fluxo do seu script, um shell possui as construções `while`, `if`, `for` e `case`.

1.7.1 Comando de controle if

O comando `if` é usado para verificar expressões. Por exemplo, o código a seguir testa se o usuário atual é Tux:

```
if test $USER = "tux"; then
    echo "Hello Tux."
else
    echo "You are not Tux."
fi
```

A expressão de teste pode ser tão complexa ou simples quanto possível. a expressão a seguir verifica se o arquivo `foo.txt` existe:

```
if test -e /tmp/foo.txt ; then
    echo "Found foo.txt"
fi
```

A expressão de teste também pode ser abreviada entre colchetes:

```
if [ -e /tmp/foo.txt ] ; then
    echo "Found foo.txt"
fi
```

Outras expressões úteis estão disponíveis em <https://bash.cyberciti.biz/guide/If..else..fi>.

1.7.2 Criando loops com o comando **for**

O loop **for** permite executar comandos para uma lista de entradas. Por exemplo, o código a seguir imprime algumas informações sobre arquivos PNG no diretório atual:

```
for i in *.png; do
  ls -l $i
done
```

1.8 Mais informações

Informações importantes sobre o Bash são fornecidas nas páginas de manual **man bash**. Mais informações sobre este tópico estão disponíveis na lista a seguir:

- <http://tldp.org/LDP/Bash-Beginners-Guide/html/index.html> — Bash Guide for Beginners (Guia do Bash para Iniciantes)
- <http://tldp.org/HOWTO/Bash-Prog-Intro-HOWTO.html> — BASH Programming - Introduction HOW-TO (COMO FAZER Programação de Bash: Introdução)
- <http://tldp.org/LDP/abs/html/index.html> — Advanced Bash-Scripting Guide (Guia Avançado de Criação de Scripts Bash)
- <http://www.grymoire.com/Unix/Sh.html> — Sh - the Bourne Shell (Sh: o Bourne Shell)

2 Conceitos básicos sobre o **sudo**

A execução de determinados comandos exige privilégios de `root`. No entanto, por questões de segurança e para evitar erros, não é recomendável efetuar login como `root`. Uma abordagem mais segura é efetuar login como usuário comum e, em seguida, utilizar o **sudo** para executar comandos com privilégios elevados.

No SUSE Linux Enterprise Desktop, o **sudo** é configurado para funcionar de modo parecido com o **su**. No entanto, o **sudo** oferece um mecanismo flexível que permite aos usuários executar comandos com privilégios de qualquer outro usuário. Isso pode ser usado para atribuir funções com privilégios específicos a determinados usuários e grupos. Por exemplo, é possível permitir que os membros do grupo `users` executem um comando com os privilégios do usuário `wilber`. É possível restringir ainda mais o acesso ao comando quando você não permite nenhuma opção de comando. Enquanto o `su` sempre requer senha de `root` para autenticação com PAM, o **sudo** pode ser configurado para autenticar com suas próprias credenciais. Isso significa que os usuários não precisam compartilhar a senha de `root`, o que reforça a segurança.

2.1 Uso básico do **sudo**

O capítulo a seguir apresenta uma introdução ao uso básico do **sudo**.

2.1.1 Executando um único comando

Como usuário comum, você pode executar qualquer comando como `root` inserindo **sudo** antes do comando. Isso solicitará que você forneça a senha de `root`. Se a autenticação for bem-sucedida, o comando será executado como `root`:

```
> id -un❶
tux
> sudo id -un
root's password:❷
root
> id -un
tux❸
> sudo id -un
❹
root
```

- ❶ O comando `id -un` imprime o nome de login do usuário atual.

- ② A senha não aparece ao ser digitada, nem como texto sem criptografia nem como caracteres de mascaramento.
- ③ Apenas os comandos que começam com **sudo** são executados com privilégios elevados.
- ④ Os privilégios elevados são mantidos por um determinado período, portanto, você não precisa inserir a senha de root novamente.



Dica: Redirecionamento de E/S

Ao usar o **sudo**, o redirecionamento de E/S não funciona:

```
> sudo echo s > /proc/sysrq-trigger
bash: /proc/sysrq-trigger: Permission denied
> sudo cat < /proc/l/maps
bash: /proc/l/maps: Permission denied
```

No exemplo acima, apenas os comandos **echo** e **cat** são executados com privilégios elevados. O redirecionamento é realizado pelo shell do usuário com os privilégios do usuário. Para realizar o redirecionamento com privilégios elevados, inicie um shell conforme explicado na [Seção 2.1.2, “Iniciando um shell”](#) ou use o utilitário **dd**:

```
echo s | sudo dd of=/proc/sysrq-trigger
sudo dd if=/proc/l/maps | cat
```

2.1.2 Iniciando um shell

Nem sempre é prático usar o **sudo** toda vez para executar um comando com privilégios elevados. Embora você possa usar o comando **sudo bash**, é recomendável usar um dos mecanismos incorporados para iniciar um shell:

sudo -s (<comando>)

Inicia um shell especificado pela variável de ambiente **SHELL** ou o shell padrão do usuário de destino. Se um comando for especificado, ele será passado para o shell (com a opção **-c**). Do contrário, o shell será executado no modo interativo.

```
tux:~ > sudo -s
root's password:
root:/home/tux # exit
tux:~ >
```

`sudo -i (<comando>)`

Semelhante ao `-s`, mas inicia o shell como um shell de login. Isso significa que os arquivos de inicialização do shell (`.profile` etc.) são processados, e o diretório de trabalho atual é definido como o diretório pessoal do usuário de destino.

```
tux:~ > sudo -i
root's password:
root:~ # exit
tux:~ >
```



Dica: Variáveis de ambiente

Por padrão, o `sudo` não propaga as variáveis de ambiente. É possível mudar esse comportamento com a opção `env_reset` (consulte *Opções e flags úteis*).

2.2 Configurando o `sudo`

O `sudo` oferece uma ampla variedade de opções configuráveis.



Nota: Comando `sudo` bloqueado

Se você se bloqueou por engano fora do `sudo`, use `su -` e a senha de `root` para iniciar um shell de root. Para corrigir o erro, execute `visudo`.

2.2.1 Editando os arquivos de configuração

O arquivo de configuração de política principal do `sudo` é `/etc/sudoers`. Já que é possível se bloquear fora do sistema se o arquivo estiver incorreto, é altamente recomendável usar o `visudo` para edição. Ele evita conflitos de edição e verifica se há erros de sintaxe antes de gravar as modificações.

Você pode definir a variável de ambiente `EDITOR` para usar outro editor no lugar do `vi`, por exemplo:

```
sudo EDITOR=/usr/bin/nano visudo
```

Lembre-se de que o arquivo `/etc/sudoers` está incluído nos pacotes de sistema, e as modificações feitas diretamente no arquivo podem danificar as atualizações. Portanto, é recomendável inserir a configuração personalizada nos arquivos no diretório `/etc/sudoers.d/`. Use o seguinte comando para criar ou editar um arquivo:

```
sudo visudo -f /etc/sudoers.d/NAME
```

O comando a seguir abre o arquivo usando um editor diferente (neste caso, `nano`):

```
sudo EDITOR=/usr/bin/nano visudo -f /etc/sudoers.d/NAME
```



Nota: Arquivos ignorados em `/etc/sudoers.d`

A diretiva `#includedir` em `/etc/sudoers` ignora os arquivos que terminam com o caractere `~` (til) ou que contêm o caractere `.` (ponto).

Para obter mais informações sobre o comando `visudo`, execute `man 8 visudo`.

2.2.2 Sintaxe de configuração básica do sudoers

Os arquivos de configuração sudoers contêm dois tipos de opções: strings e flags. Enquanto as strings podem conter qualquer valor, os flags podem ser ON ou OFF. Veja a seguir as construções de sintaxe mais importantes para os arquivos de configuração sudoers:

```
# Everything on a line after # is ignored ❶
Defaults !insults # Disable the insults flag ❷
Defaults env_keep += "DISPLAY HOME" # Add DISPLAY and HOME to env_keep
tux ALL = NOPASSWD: /usr/bin/frobnicate, PASSWD: /usr/bin/journalctl ❸
```

- ❶ Há duas exceções: `#include` e `#includedir` são comandos regulares.
- ❷ Remova o caractere `!` para definir o flag desejado como ON.
- ❸ Consulte a [Seção 2.2.3, “Regras básicas do sudoers”](#).

OPÇÕES E FLAGS ÚTEIS

`targetpw`

Esse flag controla se o usuário que faz a chamada deve digitar a senha do usuário de destino (ON) (por exemplo `root`) ou do usuário que faz a chamada (OFF).

```
Defaults targetpw # Turn targetpw flag ON
```

rootpw

Se definido, o **sudo** solicitará a senha de root. O padrão é OFF.

```
Defaults !rootpw # Turn rootpw flag OFF
```

env_reset

Se definido, o **sudo** construirá um ambiente mínimo com TERM, PATH, HOME, MAIL, SHELL, LOGNAME, USER, USERNAME e SUDO_*. Além disso, as variáveis listadas em env_keep serão importadas do ambiente de chamada. O padrão é ON.

```
Defaults env_reset # Turn env_reset flag ON
```

env_keep

Lista de variáveis de ambiente para manter quando o flag env_reset é ON.

```
# Set env_keep to contain EDITOR and PROMPT
Defaults env_keep = "EDITOR PROMPT"
Defaults env_keep += "JRE_HOME" # Add JRE_HOME
Defaults env_keep -= "JRE_HOME" # Remove JRE_HOME
```

env_delete

Lista de variáveis de ambiente para remover quando o flag env_reset é OFF.

```
# Set env_delete to contain EDITOR and PROMPT
Defaults env_delete = "EDITOR PROMPT"
Defaults env_delete += "JRE_HOME" # Add JRE_HOME
Defaults env_delete -= "JRE_HOME" # Remove JRE_HOME
```

É possível também usar o token Defaults para criar aliases para uma coleção de usuários, hosts e comandos. Além disso, é possível aplicar uma opção apenas a um conjunto específico de usuários.

Para obter informações detalhadas sobre o arquivo de configuração /etc/sudoers, consulte man 5 sudoers.

2.2.3 Regras básicas do sudoers

Cada regra segue o esquema abaixo ([] marca as partes opcionais):

#Who	Where	As whom	Tag	What
------	-------	---------	-----	------

```
User_List Host_List = [(User_List)] [NOPASSWD:|PASSWD:] Cmnd_List
```

SINTAXE DA REGRA DO SUDOERS

User_List

Um ou vários identificadores (separados por vírgula): um nome de usuário, um grupo no formato %GROUPNAME ou um ID de usuário no formato #UID. A negação pode ser especificada com o prefixo !.

Host_List

Um ou vários identificadores (separados por vírgula): um nome (completo) do host ou um endereço IP. A negação pode ser especificada com o prefixo !. ALL é a opção comum para Host_List.

NOPASSWD:|PASSWD:

Não é solicitada uma senha para o usuário ao executar comandos correspondentes a Cmnd_List após NOPASSWD:.

PASSWD é o padrão. Ele precisa ser especificado apenas quando ambos PASSWD e NOPASSWD estão na mesma linha:

```
tux ALL = PASSWD: /usr/bin/foo, NOPASSWD: /usr/bin/bar
```

Cmnd_List

Um ou vários especificadores (separados por vírgula): Um caminho para um executável, seguido de um argumento opcional permitido.

```
/usr/bin/foo      # Anything allowed
/usr/bin/foo bar  # Only "/usr/bin/foo bar" allowed
/usr/bin/foo ""   # No arguments allowed
```

É possível usar ALL como User_List, Host_List e Cmnd_List.

Uma regra que permite que o tux execute todos os comandos como root sem digitar uma senha:

```
tux ALL = NOPASSWD: ALL
```

Uma regra que permite que o tux execute systemctl restart apache2:

```
tux ALL = /usr/bin/systemctl restart apache2
```

Uma regra que permite que o tux execute wall como admin sem argumentos:

```
tux ALL = (admin) /usr/bin/wall ""
```



Atenção: Regras não seguras

Não use regras como `ALL ALL = ALL` sem `Defaults targetpw`. Do contrário, qualquer pessoa pode executar comandos como `root`.



Importante: Winbind e sudo

Ao especificar o nome do grupo no arquivo `sudoers`, use o nome do domínio NetBIOS em vez do domínio Kerberos, por exemplo:

```
%DOMAIN\GROUP_NAME ALL = (ALL) ALL
```

Ao usar o `winbindd`, lembre-se de que o formato também depende da opção `winbind separator` no arquivo `smb.conf`. O padrão é `\`. Por exemplo, se ele for mudado para `+`, o formato da conta no arquivo `sudoers` deverá ser `DOMAIN+GROUP_NAME`.

2.3 Casos de uso do **sudo**

Embora a configuração padrão funcione em cenários de uso padrão, é possível personalizá-la de forma a atender às suas necessidades específicas.

2.3.1 Usando o **sudo** sem senha de root

Por concepção, os membros do grupo `wheel` podem executar todos os comandos com o **sudo** como root. O procedimento a seguir explica como adicionar uma conta do usuário ao grupo `wheel`.

1. Adicione sua conta do usuário ao grupo `wheel`.

Se a sua conta do usuário ainda não é membro do grupo `wheel`, adicione-a usando o comando `sudo usermod -a -G wheel USERNAME`. Efetue logout e login novamente para habilitar a mudança. Verifique se a mudança foi bem-sucedida executando o comando `groups USERNAME`.

2. Autentique-se com a senha normal da conta do usuário.

Crie o arquivo `/etc/sudoers.d/userpw` usando o comando **visudo** (consulte a [Seção 2.2.1, “Editando os arquivos de configuração”](#)) e adicione o seguinte:

```
Defaults !targetpw
```

3. Selecione uma nova regra padrão.

Se os usuários tiverem que digitar as senhas novamente, remova o comentário da linha apropriada em `/etc/sudoers` e comente a regra padrão.

```
## Uncomment to allow members of group wheel to execute any command
# %wheel ALL=(ALL) ALL

## Same thing without a password
# %wheel ALL=(ALL) NOPASSWD: ALL
```

4. Torne a regra padrão mais restritiva.

Comente ou remova a regra `allow-everything` em `/etc/sudoers`:

```
ALL    ALL=(ALL) ALL    # WARNING! Only use this together with 'Defaults targetpw'!
```



Atenção: Regra perigosa em sudoers

Não ignore esta etapa. Do contrário, *qualquer* usuário poderá executar *qualquer* comando como root!

5. Teste a configuração.

Execute o **sudo** como membro e não membro do grupo `wheel`.

```
tux:~ > groups
users wheel
tux:~ > sudo id -un
tux's password:
root
wilber:~ > groups
users
wilber:~ > sudo id -un
wilber is not in the sudoers file. This incident will be reported.
```

2.3.2 Usando o **sudo** com aplicativos X.Org

Geralmente, ocorre o seguinte erro ao iniciar aplicativos gráficos com o **sudo**:

```
> sudo xterm
xterm: Xt error: Can't open display: %s
xterm: DISPLAY is not set
```

Uma solução alternativa simples é usar o **xhost** para permitir temporariamente que o usuário **root** acesse a sessão X do usuário local. Para fazer isso, execute o seguinte comando:

```
xhost si:localuser:root
```

O comando a seguir remove o acesso concedido:

```
xhost -si:localuser:root
```



Atenção: Possível problema de segurança

A execução de aplicativos gráficos com privilégios de **root** tem implicações de segurança. É recomendável habilitar o acesso de **root** para um aplicativo gráfico apenas como uma exceção. Também é recomendável revogar o acesso de **root** concedido logo após fechar o aplicativo gráfico.

2.4 Mais informações

O comando **sudo --help** oferece uma breve visão geral das opções de linha de comando disponíveis. O comando **man sudoers** fornece informações detalhadas sobre o **sudoers** e sua configuração.

3 Usando o YaST

O YaST é uma ferramenta do SUSE Linux Enterprise Desktop que estabelece uma interface gráfica com todas as tarefas essenciais de instalação e de configuração do sistema. Se você precisa atualizar pacotes, configurar uma impressora, modificar configurações de firewall, configurar um servidor FTP ou particionar um disco rígido, pode fazer tudo isso usando o YaST. Desenvolvido em Ruby, o YaST conta com uma arquitetura extensível que possibilita adicionar novas funcionalidades por meio de módulos.

Há mais informações sobre o YaST disponíveis no site oficial do projeto na Web <https://yast.opensuse.org/>.

3.1 Visão geral da interface do YaST

O YaST tem duas interfaces gráficas: uma para uso com ambientes gráficos de área de trabalho, como KDE e GNOME, e uma interface pseudográfica com base no ncurses para uso em sistemas sem um servidor X (consulte o *Capítulo 4, YaST em modo de texto*).

Na versão gráfica do YaST, todos os módulos dele são agrupados por categoria, e a barra lateral de navegação permite acessar rapidamente os módulos na categoria desejada. O campo de pesquisa na parte superior permite localizar os módulos pelos nomes. Para localizar um módulo específico, digite o nome dele no campo de pesquisa, e você verá os módulos correspondentes à string enquanto digita.

3.2 Combinações de teclas úteis

A versão gráfica do YaST suporta atalhos de teclado

Print Screen

Tirar e gravar uma captura de tela. Talvez não funcione em determinados ambientes de área de trabalho.

Shift – F4

Habilitar e desabilitar a paleta de cores otimizada para usuários com dificuldades visuais.

Shift – F7

Habilitar/Desabilitar registro de mensagens de depuração.

Shift – F8

Abra uma caixa de diálogo de arquivo para gravar os arquivos de registro em um local definido pelo usuário.

Ctrl – Shift – Alt – D

Enviar um DebugEvent. Módulos do YaST podem reagir a isso executando ações especiais de depuração. O resultado depende do módulo específico do YaST.

Ctrl – Shift – Alt – M

Iniciar e parar o gravador de macro.

Ctrl – Shift – Alt – P

Reproduzir macro.

Ctrl – Shift – Alt – S

Mostrar editor de folha de estilo.

Ctrl – Shift – Alt – T

Despejo da árvore de widget no arquivo de registro.

Ctrl – Shift – Alt – X

Abrir uma janela de terminal (xterm). Útil para processo de instalação via VNC.

Ctrl – Shift – Alt – Y

Mostrar navegador de árvore de widget.

4 YaST em modo de texto

A interface pseudográfica com base no ncurses do YaST foi projetada principalmente para ajudar administradores do sistema a gerenciar sistemas sem um servidor X. A interface oferece várias vantagens em comparação com a GUI convencional. Você pode navegar pela interface do ncurses utilizando o teclado, e há atalhos de teclado para praticamente todos os elementos de interface. A interface do ncurses é leve no que diz respeito aos recursos e é executada de forma rápida mesmo em hardware de capacidade limitada. Você pode executar a versão do YaST com base no ncurses por meio de uma conexão SSH para poder administrar sistemas remotos. Lembre-se de que o tamanho mínimo suportado do emulador de terminal no qual executar o YaST é de 80 x 25 caracteres.

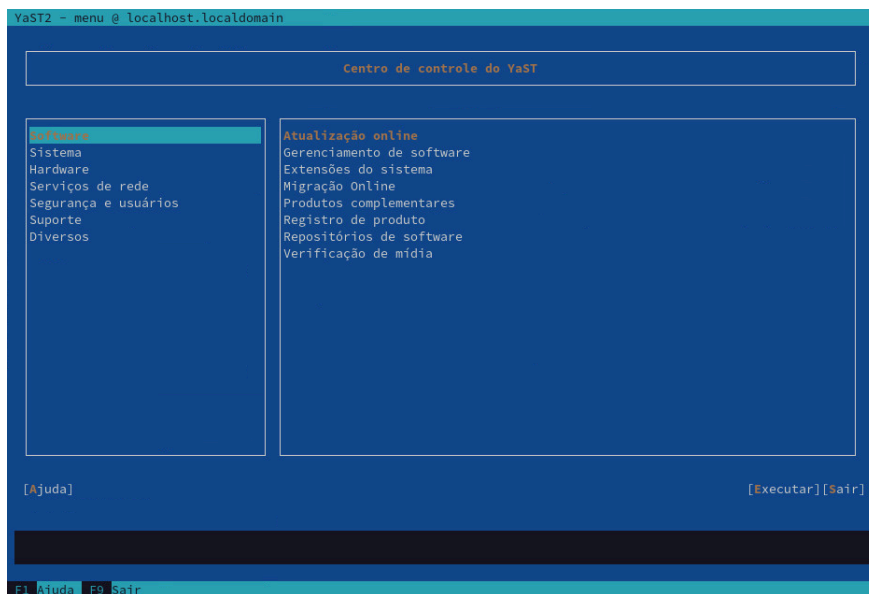


FIGURA 4.1: JANELA PRINCIPAL DO YAST EM MODO DE TEXTO

Para iniciar a versão do YaST com base no ncurses, abra o terminal e execute o comando **sudo yast2**. Use a tecla **→** ou as teclas de seta para navegar pelos elementos da interface, como itens de menu, campos e botões. É possível acessar todos os itens e botões no YaST usando as teclas de função ou os atalhos de teclado apropriados. Por exemplo, é possível cancelar a operação atual pressionando **F9** e usar a tecla **F10** para aceitar as mudanças. Cada item de menu e botão na interface com base no ncurses do YaST tem uma letra realçada no rótulo. Essa letra faz parte do atalho de teclado atribuído ao elemento da interface. Por exemplo, a letra **Q** está realçada no botão *Quit* (Sair). Isso significa que você pode ativar o botão pressionando **Alt-Q**.



Dica: Atualizando caixas de diálogo do YaST

Se uma caixa de diálogo do YaST for corrompida ou distorcida (por exemplo, ao redimensionar a janela), pressione **Ctrl** - **L** para atualizar e restaurar seu conteúdo.

4.1 Navegação em módulos

A seguinte descrição dos elementos de controle nos módulos do YaST pressupõe que todas as teclas de função e combinações de teclas **Alt** funcionam e que não estão atribuídas a funções globais diferentes. Leia a [Seção 4.3, “Restrição de combinações de teclas”](#) para obter informações sobre possíveis exceções.

Movendo entre botões e listas de seleção

Use **→|** para mover entre os botões e frames que contêm listas de seleção. Para navegar na direção oposta, use as combinações **Alt** - **→|** ou **Shift** - **→|**.

Navegando nas listas de seleção

Use as teclas de seta (**↑** e **↓**) para mover pelos elementos individuais em um frame ativo que contenha uma lista de seleção. Se as entradas individuais forem maiores do que a largura do frame, use **Shift** - **→** ou **Shift** - **←** para mover a barra de rolagem na horizontal. Se tecla de seta fizer com que a seleção seja movida para outro frame, use **Ctrl** - **E** ou **Ctrl** - **A** A no lugar dela.

Trabalhando com botões, botões de opção e caixas de seleção

Para selecionar itens com colchetes vazios (caixas de seleção) ou parênteses vazios (botões de opção), pressione **Space** ou **Enter**. Se preferir, marque os botões de opção e as caixas de seleção diretamente com **Alt** - **highlighted_letter**. Nesse caso, não é necessário confirmar com **Enter**. Se você navegar até um item com **→|**, pressione **Enter** para executar a ação selecionada ou ativar o item de menu respectivo.

Teclas de função

As teclas de função (de **F1** a **F12**) permitem o acesso rápido a vários botões. As combinações de teclas de função disponíveis (**FX**) são mostradas na linha inferior da tela do YaST. As teclas de função que são realmente mapeadas para cada botão dependem do módulo do YaST ativo, pois módulos diferentes oferecem botões diferentes (*Detalhes*, *Informações*, *Adicionar*, *Apagar*, etc). Use **F10** para *Aceitar*, *OK*, *Avançar* e *Concluir*. Pressione **F1** para acessar a ajuda do YaST.

Usando a árvore de navegação

Alguns módulos do YaST usam uma árvore de navegação na parte esquerda da janela para seleção de caixas de diálogo de configuração. Use as teclas de seta (**↑** e **↓**) para navegar na árvore. Use **Space** para abrir ou fechar itens da árvore. No modo ncurses, você deve pressionar **Enter** após uma seleção na árvore de navegação para mostrar a caixa de diálogo selecionada. Esse é um comportamento intencional que visa evitar novos desenhos demorados durante a navegação na árvore.

Selecionando um software no módulo de instalação de software

Use os filtros à esquerda para listar os pacotes que correspondem à string especificada. Os pacotes instalados estão marcados com a letra **i**. Para mudar o status de um pacote, pressione **Space** ou **Enter**. Se preferir, use o menu **Ações** para selecionar a mudança de status necessária (instalar, apagar, atualizar, proibir ou bloquear).

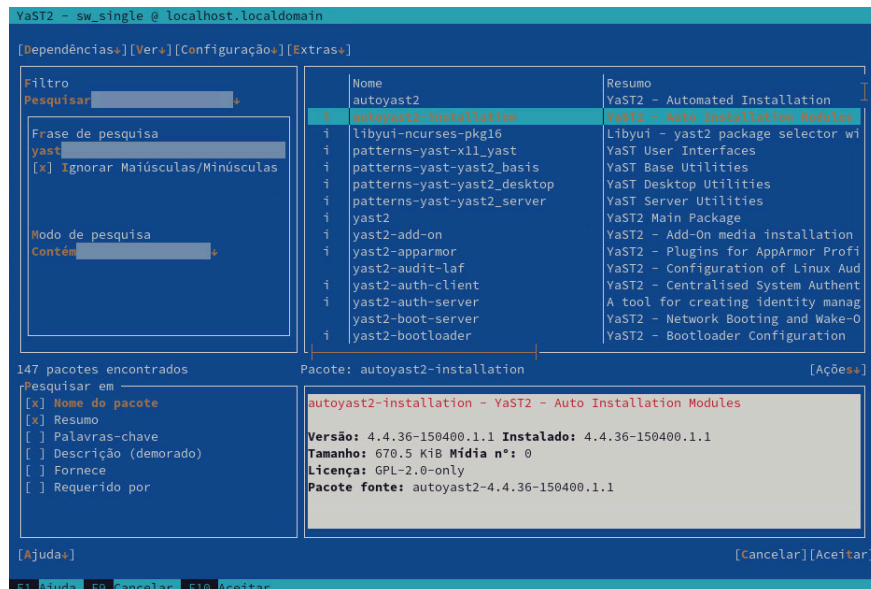


FIGURA 4.2: MÓDULO DE INSTALAÇÃO DE SOFTWARE

4.2 Combinações de teclas avançadas

A versão com base no ncurses do YaST oferece várias combinações de teclas avançadas.

Shift – F1

Listar as teclas de atalho avançadas.

Shift – F4

Mudar o esquema de cores.

Ctrl –

Sair do aplicativo.

Ctrl – L

Atualizar tela.

Ctrl – D F1

Listar as teclas de atalho avançadas.

Ctrl – D Shift – D

Despejo da caixa de diálogo no arquivo de registro como uma captura de tela.

Ctrl – D Shift – Y

Abrir YDialogSpy para ver a hierarquia do widget.

4.3 Restrição de combinações de teclas

Se o seu gerenciador de janelas usar combinações **Alt** globais, as combinações **Alt** no YaST talvez não funcionem. Teclas como **Alt** ou **Shift** também podem ser ocupadas pelas configurações do terminal.

Usando **Alt** em vez de **Esc**

Os atalhos com **Alt** podem ser executados com **Esc** em vez de **Alt**. Por exemplo, **Esc – H** substitui **Alt – H**. (Pressione **Esc** e *depois* **H**.)

Navegação para trás e para frente com **Ctrl – F** e **Ctrl – B**

Se as combinações **Alt** e **Shift** estiverem ocupadas pelo gerenciador de janelas ou pelo terminal, use as combinações **Ctrl – F** (avançar) e **Ctrl – B** (voltar) no lugar delas.

Restrição de teclas de função

As teclas de função (**F1** ... **F12**) também são usadas para funções. Algumas teclas de função podem estar ocupadas pelo terminal e talvez não estejam disponíveis para o YaST. No entanto, as combinações de teclas **Alt** e as teclas de função devem estar sempre disponíveis em um console apenas de texto.

4.4 Opções de linha de comando do YaST

Além da interface de modo de texto, o YaST oferece uma interface de linha de comando. Para obter uma lista das opções de linha de comando do YaST, use o seguinte comando:

```
> sudo yast -h
```

4.4.1 Instalando pacotes da linha de comando

Se você sabe o nome do pacote e ele é fornecido por um repositório de instalação ativo, pode usar a opção de linha de comando `-i` para instalá-lo:

```
> sudo yast -i package_name
```

ou

```
> sudo yast --install -i package_name
```

nome_do_pacote pode ser um único nome de pacote abreviado (por exemplo, `gvim`), instalado com verificação de dependência, ou o caminho completo para um pacote RPM, instalado sem verificação de dependência.

Embora o YaST ofereça uma funcionalidade básica para gerenciar o software por meio da linha de comando, considere usar o Zypper para tarefas mais avançadas de gerenciamento de pacote. Há mais informações sobre como usar o Zypper na [Seção 9.1, "Usando o zypper"](#).

4.4.2 Trabalhando com módulos individuais

Para economizar tempo, você pode iniciar os módulos individuais do YaST usando o seguinte comando:

```
> sudo yast module_name
```

Exiba uma lista de todos os módulos disponíveis no seu sistema com `yast -l` ou `yast --list`.

4.4.3 Parâmetros de linha de comando dos módulos do YaST

Para usar a funcionalidade do YaST em scripts, ele oferece suporte a linha de comando para módulos individuais. Entretanto, nem todos os módulos têm suporte para linha de comando. Para exibir as opções disponíveis de um módulo, use o seguinte comando:

```
> sudo yast module_name help
```

Se um módulo não fornecer suporte para linha de comando, ele será iniciado no modo de texto, e a seguinte mensagem aparecerá:

```
This YaST module does not support the command line interface.
```

As seções a seguir descrevem todos os módulos do YaST com suporte para linha de comando, juntamente com uma breve explicação de todos os comandos e as opções disponíveis.

4.4.3.1 Comandos comuns dos módulos do YaST

Todos os módulos do YaST suportam os seguintes comandos:

help

Lista todos os comandos suportados pelo módulo com a respectiva descrição:

```
> sudo yast lan help
```

longhelp

Igual a **help**, mas adiciona uma lista detalhada de todas as opções do comando e suas descrições:

```
> sudo yast lan longhelp
```

xmlhelp

Igual a **longhelp**, mas a saída é estruturada como um documento XML e redirecionada para um arquivo:

```
> sudo yast lan xmlhelp xmlfile=/tmp/yast_lan.xml
```

interactive

Entra no modo *interativo*. Isso permite executar os comandos do módulo sem incluir o prefixo **sudo yast** neles. Use **exit** para sair do modo interativo.

4.4.3.2 **yast add-on**

Adiciona um novo produto complementar do caminho especificado:

```
> sudo yast add-on http://server.name/directory/Lang-AddOn-CD1/
```

Você pode usar os seguintes protocolos para especificar o caminho de origem: http:// ftp:// nfs:// disk:// cd:// ou dvd://.

4.4.3.3 **yast audit-laf**

Exibe e configura o Linux Audit Framework. Consulte o *Livro "Security and Hardening Guide"* para obter mais detalhes. O **yast audit-laf** aceita os seguintes comandos:

set

Define uma opção:

```
> sudo yast audit-laf set log_file=/tmp/audit.log
```

Para obter uma lista completa das opções, execute **yast audit-laf set help**.

show

Exibe as configurações de uma opção:

```
> sudo yast audit-laf show disk-space
space_left: 75
space_left_action: SYSLOG
admin_space_left: 50
admin_space_left_action: SUSPEND
action_mail_acct: root
disk_full_action: SUSPEND
disk_error_action: SUSPEND
```

Para obter uma lista completa das opções, execute **yast audit-laf show help**.

4.4.3.4 **yast dhcp-server**

Gerencia o servidor DHCP e define suas configurações. O **yast dhcp-server** aceita os seguintes comandos:

disable

Desabilita o serviço do servidor DHCP.

enable

Habilita o serviço do servidor DHCP.

host

Define as configurações de hosts individuais.

interface

Especifica a interface de rede de escuta:

```
> sudo yast dhcp-server interface current
Selected Interfaces: eth0
Other Interfaces: bond0, pbu, eth1
```

Para obter uma lista completa das opções, execute **yast dhcp-server interface help**.

options

Gerencia as opções DHCP globais. Para obter uma lista completa das opções, execute **yast dhcp-server options help**.

status

Imprime o status do serviço DHCP.

subnet

Gerencia as opções de sub-rede DHCP. Para obter uma lista completa das opções, execute **yast dhcp-server subnet help**.

4.4.3.5 yast dns-server

Gerencia a configuração do servidor DNS. O **yast dns-server** aceita os seguintes comandos:

acls

Exibe as configurações de lista de controles de acesso:

```
> sudo yast dns-server acls show
ACLs:
-----
Name      Type      Value
-----
any       Predefined
localips  Predefined
localnets Predefined
none      Predefined
```

dnsrecord

Configura os registros de recursos da zona:

```
> sudo yast dnsrecord add zone=example.org query=office.example.org type=NS  
value=ns3
```

Para obter uma lista completa das opções, execute **yast dns-server dnsrecord help**.

forwarders

Define os encaminhadores DNS:

```
> sudo yast dns-server forwarders add ip=10.0.0.100  
> sudo yast dns-server forwarders show  
[...]  
Forwarder IP  
-----  
10.0.0.100
```

Para obter uma lista completa das opções, execute **yast dns-server forwarders help**.

host

Processa “A” e seu registro “PTR” relacionado de uma vez:

```
> sudo yast dns-server host show zone=example.org
```

Para obter uma lista completa das opções, execute **yast dns-server host help**.

logging

Define as configurações de registro:

```
> sudo yast dns-server logging set updates=no transfers=yes
```

Para obter uma lista completa das opções, execute **yast dns-server logging help**.

mailserver

Configura os servidores de correio eletrônico da zona:

```
> sudo yast dns-server mailserver add zone=example.org mx=mx1 priority=100
```

Para obter uma lista completa das opções, execute **yast dns-server mailserver help**.

nameserver

Configura os servidores de nomes da zona:

```
> sudo yast dns-server nameserver add zone=example.com ns=ns1
```

Para obter uma lista completa das opções, execute **yast dns-server nameserver help**.

soa

Configura o registro SOA (Start of Authority – Início de Autoridade):

```
> sudo yast dns-server soa set zone=example.org serial=2006081623 ttl=2D3H20S
```

Para obter uma lista completa das opções, execute **yast dns-server soa help**.

startup

Gerencia o serviço do servidor DNS:

```
> sudo yast dns-server startup atboot
```

Para obter uma lista completa das opções, execute **yast dns-server startup help**.

transport

Configura as regras de transporte da zona. Para obter uma lista completa das opções, execute **yast dns-server transport help**.

zones

Gerencia as zonas do DNS:

```
> sudo yast dns-server zones add name=example.org zonetype=master
```

Para obter uma lista completa das opções, execute **yast dns-server zones help**.

4.4.3.6 yast disk

Imprime as informações sobre todos os discos ou as partições. O único comando suportado é **list** seguido de uma das seguintes opções:

disks

Lista todos os discos configurados no sistema:

```
> sudo yast disk list disks
Device   | Size      | FS Type | Mount Point | Label | Model
-----+-----+-----+-----+-----+-----
/dev/sda | 119.24 GiB |         |              |       | SSD 840
/dev/sdb | 60.84 GiB  |         |              |       | WD1003FBYX-0
```

partições

Lista todas as partições no sistema:

```
> sudo yast disk list partitions
Device      | Size      | FS Type | Mount Point | Label | Model
```

-----+-----+-----+-----+-----+-----					
/dev/sda1		1.00 GiB		Ext2	/boot
/dev/sdb1		1.00 GiB		Swap	swap
/dev/sdc1		698.64 GiB		XFS	/mnt/extra
/dev/vg00/home		580.50 GiB		Ext3	/home
/dev/vg00/root		100.00 GiB		Ext3	/
[...]					

4.4.3.7 `yast ftp-server`

Define as configurações do servidor FTP. O **yast ftp-server** aceita as seguintes opções:

SSL, TLS

Controla as conexões seguras por meio de SSL e TLS. As opções de SSL são válidas apenas para `vsftpd`.

```
> sudo yast ftp-server SSL enable
> sudo yast ftp-server TLS disable
```

access

Configura as permissões de acesso:

```
> sudo yast ftp-server access authen_only
```

Para obter uma lista completa das opções, execute **yast ftp-server access help**.

anon_access

Configura as permissões de acesso de usuários anônimos:

```
> sudo yast ftp-server anon_access can_upload
```

Para obter uma lista completa das opções, execute **yast ftp-server anon_access help**.

anon_dir

Especifica o diretório dos usuários anônimos. O diretório já deve existir no servidor:

```
> sudo yast ftp-server anon_dir set_anon_dir=/srv/ftp
```

Para obter uma lista completa das opções, execute **yast ftp-server anon_dir help**.

chroot

Controla o ambiente do *change root* (chroot):

```
> sudo yast ftp-server chroot enable
```

```
> sudo yast ftp-server chroot disable
```

idle-time

Define o tempo máximo de inatividade em minutos para o servidor FTP terminar a conexão atual:

```
> sudo yast ftp-server idle-time set_idle_time=15
```

logging

Determina se as mensagens de registro devem ser gravadas em um arquivo de registro:

```
> sudo yast ftp-server logging enable  
> sudo yast ftp-server logging disable
```

max_clients

Especifica o número máximo de clientes conectados simultaneamente:

```
> sudo yast ftp-server max_clients set_max_clients=1500
```

max_clients_ip

Especifica o número máximo de clientes conectados simultaneamente por IP:

```
> sudo yast ftp-server max_clients_ip set_max_clients=20
```

max_rate_anon

Especifica a taxa máxima de transferência de dados permitida para clientes anônimos (KB/s):

```
> sudo yast ftp-server max_rate_anon set_max_rate=10000
```

max_rate_authen

Especifica a taxa máxima de transferência de dados permitida para usuários autenticados localmente (KB/s):

```
> sudo yast ftp-server max_rate_authen set_max_rate=10000
```

port_range

Especifica a faixa de portas para respostas de conexão passiva:

```
> sudo yast ftp-server port_range set_min_port=20000 set_max_port=30000
```

Para obter uma lista completa das opções, execute **yast ftp-server port_range help**.

show

Exibe as configurações do servidor FTP.

startup

Controla o método de inicialização do FTP:

```
> sudo yast ftp-server startup atboot
```

Para obter uma lista completa das opções, execute **yast ftp-server startup help**.

umask

Especifica o desmascaramento de arquivo para usuários autenticados:anônimos:

```
> sudo yast ftp-server umask set_umask=177:077
```

welcome_message

Especifica o texto a ser exibido quando alguém se conecta ao servidor FTP:

```
> sudo yast ftp-server welcome_message set_message="hello everybody"
```

4.4.3.8 yast http-server

Configura o servidor HTTP (Apache2). O **yast http-server** aceita os seguintes comandos:

configure

Define as configurações de host do servidor HTTP:

```
> sudo yast http-server configure host=main servername=www.example.com \
serveradmin=admin@example.com
```

Para obter uma lista completa das opções, execute **yast http-server configure help**.

hosts

Configura os hosts virtuais:

```
> sudo yast http-server hosts create servername=www.example.com \
serveradmin=admin@example.com documentroot=/var/www
```

Para obter uma lista completa das opções, execute **yast http-server hosts help**.

listen

Especifica as portas e os endereços de rede de escuta do servidor HTTP:

```
> sudo yast http-server listen add=81
```

```
> sudo yast http-server listen list
Listen Statements:
=====
:80
:81
> sudo yast http-server delete=80
```

Para obter uma lista completa das opções, execute **yast http-server listen help**.

mode

Habilita ou desabilita o modo do assistente:

```
> sudo yast http-server mode wizard=on
```

modules

Controla os módulos do servidor Apache2:

```
> sudo yast http-server modules enable=php5,rewrite
> sudo yast http-server modules disable=ssl
> sudo http-server modules list
[...]
Enabled rewrite
Disabled ssl
Enabled php5
[...]
```

4.4.3.9 yast kdump

Define as configurações do kdump. Para obter mais informações sobre o kdump, consulte o Livro *“System Analysis and Tuning Guide”, Capítulo 19 “Kexec and Kdump”, Seção 19.7 “Basic Kdump configuration”*. O **yast kdump** aceita os seguintes comandos:

copykernel

Copia o kernel para o diretório de dump.

customkernel

Especifica a parte string_do_kernel do nome do kernel personalizado. O esquema de nomeação é /boot/vmlinu[zx]-string_do_kernel[.gz].

```
> sudo yast kdump customkernel kernel=kdump
```

Para obter uma lista completa das opções, execute **yast kdump customkernel help**.

dumpformat

Especifica o formato (compactação) da imagem do kernel de dump. Os formatos disponíveis são: “none”, “ELF”, “compressed” ou “lzo”:

```
> sudo yast kdump dumpformat dump_format=ELF
```

dumplevel

Especifica o número do nível de dump na faixa de 0 a 31:

```
> sudo yast kdump dumplevel dump_level=24
```

dumptarget

Especifica o destino para gravação das imagens de dump:

```
> sudo kdump dumptarget target=ssh server=name_server port=22 \
dir=/var/log/dump user=user_name
```

Para obter uma lista completa das opções, execute **yast kdump dumptarget help**.

immediatereboot

Controla se o sistema deve ser reinicializado imediatamente após a gravação do núcleo no kernel do kdump:

```
> sudo yast kdump immediatereboot enable
> sudo yast kdump immediatereboot disable
```

keepolddumps

Especifica quantas imagens de dump antigas são mantidas. Especifique zero para manter todas:

```
> sudo yast kdump keepolddumps no=5
```

kernelcommandline

Especifica a linha de comando que precisa ser passada para o kernel do kdump:

```
> sudo yast kdump kernelcommandline command="ro root=LABEL=/"
```

kernelcommandlineappend

Especifica a linha de comando que você precisa *anexar* à string de linha de comando padrão:

```
> sudo yast kdump kernelcommandlineappend command="ro root=LABEL=/"
```

notificationcc

Especifica um endereço de e-mail para enviar cópias das mensagens de notificação:

```
> sudo yast kdump notificationcc email="user1@example.com user2@example.com"
```

notificationto

Especifica um endereço de e-mail para enviar mensagens de notificação:

```
> sudo yast kdump notificationto email="user1@example.com user2@example.com"
```

show

Exibe as configurações do kdump:

```
> sudo yast kdump show
Kdump is disabled
Dump Level: 31
Dump Format: compressed
Dump Target Settings
target: file
file directory: /var/crash
Kdump immediate reboots: Enabled
Numbers of old dumps: 5
```

smtppass

Especifica o arquivo com a senha SMTP em texto puro usada para enviar mensagens de notificação:

```
> sudo yast kdump smtppass pass=/path/to/file
```

smtpserver

Especifica o nome de host do servidor SMTP usado para enviar mensagens de notificação:

```
> sudo yast kdump smtpserver server=smtp.server.com
```

smtpuser

Especifica o nome de usuário SMTP usado para enviar mensagens de notificação:

```
> sudo yast kdump smtpuser user=smtp_user
```

startup

Habilita ou desabilita as opções de inicialização:

```
> sudo yast kdump startup enable alloc_mem=128,256
> sudo yast kdump startup disable
```

4.4.3.10 `yast keyboard`

Configura o teclado do sistema para os consoles virtuais. Ele não afeta as configurações do teclado em ambientes gráficos de área de trabalho, como GNOME ou KDE. O **`yast keyboard`** aceita os seguintes comandos:

list

Lista todos os layouts de teclado disponíveis.

set

Ativa a nova configuração de layout de teclado:

```
> sudo yast keyboard set layout=czech
```

summary

Exibe a configuração do teclado atual.

4.4.3.11 `yast lan`

Configura as placas de rede. O **`yast lan`** aceita os seguintes comandos:

add

Configura uma nova placa de rede:

```
> sudo yast lan add name=vlan50 ethdevice=eth0 bootproto=dhcp
```

Para obter uma lista completa das opções, execute **`yast lan add help`**.

delete

Apaga uma placa de rede existente:

```
> sudo yast lan delete id=0
```

edit

Muda a configuração de uma placa de rede existente:

```
> sudo yast lan edit id=0 bootproto=dhcp
```

list

Exibe um resumo da configuração da placa de rede:

```
> sudo yast lan list
id name,          bootproto
0 Ethernet Card 0, NONE
```

4.4.3.12 `yast language`

Configura os idiomas do sistema. O `yast language` aceita os seguintes comandos:

list

Lista todos os idiomas disponíveis.

set

Especifica os idiomas principais e secundários do sistema:

```
> sudo yast language set lang=cs_CZ languages=en_US,es_ES no_packages
```

4.4.3.13 `yast mail`

Exibe a configuração do sistema de correio eletrônico:

```
> sudo yast mail summary
```

4.4.3.14 `yast nfs`

Controla o cliente NFS. O `yast nfs` aceita os seguintes comandos:

add

Adiciona uma nova montagem NFS:

```
> sudo yast nfs add spec=remote_host:/path/to/nfs/share file=/local/mount/point
```

Para obter uma lista completa das opções, execute `yast nfs add help`.

delete

Apaga uma montagem NFS existente:

```
> sudo yast nfs delete spec=remote_host:/path/to/nfs/share file=/local/mount/point
```

Para obter uma lista completa das opções, execute `yast nfs delete help`.

edit

Muda uma montagem NFS existente:

```
> sudo yast nfs edit spec=remote_host:/path/to/nfs/share \
```

```
file=/local/mount/point type=nfs4
```

Para obter uma lista completa das opções, execute **yast nfs edit help**.

list

Lista as montagens NFS existentes:

```
> sudo yast nfs list
Server          Remote File System  Mount Point  Options
-----
nfs.example.com /mnt                /nfs/mnt     nfs
nfs.example.com /home/tux/nfs_share /nfs/tux     nfs
```

4.4.3.15 yast nfs-server

Configura o servidor NFS. O **yast nfs-server** aceita os seguintes comandos:

add

Adiciona um diretório para exportação:

```
> sudo yast nfs-server add mountpoint=/nfs/export hosts=*.allowed_hosts.com
```

Para obter uma lista completa das opções, execute **yast nfs-server add help**.

delete

Apaga um diretório da exportação de NFS:

```
> sudo yast nfs-server delete mountpoint=/nfs/export
```

set

Especifica parâmetros adicionais para o servidor NFS:

```
> sudo yast nfs-server set enablev4=yes security=yes
```

Para obter uma lista completa das opções, execute **yast nfs-server set help**.

start

Inicia o serviço do servidor NFS:

```
> sudo yast nfs-server start
```

stop

Interrompe o serviço do servidor NFS:

```
> sudo yast nfs-server stop
```

summary

Exibe um resumo da configuração do servidor NFS:

```
> sudo yast nfs-server summary
NFS server is enabled
NFS Exports
* /mnt
* /home

NFSv4 support is enabled.
The NFSv4 domain for idmapping is localdomain.
NFS Security using GSS is enabled.
```

4.4.3.16 **yast nis**

Configura o cliente NIS. O **yast nis** aceita os seguintes comandos:

configure

Muda as configurações globais de um cliente NIS:

```
> sudo yast nis configure server=nis.example.com broadcast=yes
```

Para obter uma lista completa das opções, execute **yast nis configure help**.

disable

Desabilita o cliente NIS:

```
> sudo yast nis disable
```

enable

Habilita sua máquina como cliente NIS:

```
> sudo yast nis enable server=nis.example.com broadcast=yes automounter=yes
```

Para obter uma lista completa das opções, execute **yast nis enable help**.

find

Mostra os servidores NIS disponíveis para determinado domínio:

```
> sudo yast nis find domain=nisdomain.com
```

summary

Exibe um resumo da configuração de um cliente NIS.

4.4.3.17 **yast nis-server**

Configura um servidor NIS. O **yast nis-server** aceita os seguintes comandos:

master

Configura um servidor NIS master:

```
> sudo yast nis-server master domain=nisdomain.com yppasswd=yes
```

Para obter uma lista completa das opções, execute **yast nis-server master help**.

slave

Configura um servidor de trabalho NIS:

```
> sudo yast nis-server slave domain=nisdomain.com master_ip=10.100.51.65
```

Para obter uma lista completa das opções, execute **yast nis-server slave help**.

stop

Interrompe um servidor NIS:

```
> sudo yast nis-server stop
```

summary

Exibe um resumo da configuração de um servidor NIS:

```
> sudo yast nis-server summary
```

4.4.3.18 **yast proxy**

Define as configurações de proxy. O **yast proxy** aceita os seguintes comandos:

autenticação

Especifica as opções de autenticação de proxy:

```
> sudo yast proxy authentication username=tux password=secret
```

Para obter uma lista completa das opções, execute **yast proxy authentication help**.

enable, disable

Habilita ou desabilita as configurações de proxy.

set

Muda as configurações de proxy atuais:

```
> sudo yast proxy set https=proxy.example.com
```

Para obter uma lista completa das opções, execute **yast proxy set help**.

summary

Exibe as configurações de proxy.

4.4.3.19 **yast rdp**

Controla as configurações de área de trabalho remota. O **yast rdp** aceita os seguintes comandos:

allow

Permite o acesso remoto à área de trabalho do servidor:

```
> sudo yast rdp allow set=yes
```

list

Exibe o resumo da configuração de área de trabalho remota.

4.4.3.20 **yast samba-client**

Define as configurações do cliente Samba. O **yast samba-client** aceita os seguintes comandos:

configure

Muda as configurações globais do Samba:

```
> sudo yast samba-client configure workgroup=FAMILY
```

isdomainmember

Verifica se a máquina é membro de um domínio:

```
> sudo yast samba-client isdomainmember domain=SMB_DOMAIN
```

joindomain

Torna a máquina um membro de um domínio:

```
> sudo yast samba-client joindomain domain=SMB_DOMAIN user=username password=pwd
```


winbind

Habilita ou desabilita os serviços Winbind (o daemon `winbindd`):

```
> sudo yast samba-client winbind enable
> sudo yast samba-client winbind disable
```

4.4.3.21 `yast samba-server`

Define as configurações do servidor Samba. O `yast samba-server` aceita os seguintes comandos:

back end

Especifica o back-end para armazenar as informações de usuário:

```
> sudo yast samba-server backend smbpasswd
```

Para obter uma lista completa das opções, execute `yast samba-server backend help`.

configure

Define as configurações globais do servidor Samba:

```
> sudo yast samba-server configure workgroup=FAMILY description='Home server'
```

Para obter uma lista completa das opções, execute `yast samba-server configure help`.

list

Exibe uma lista dos compartilhamentos disponíveis:

```
> sudo yast samba-server list
Status      Type Name
=====
Disabled    Disk profiles
Enabled     Disk print$
Enabled     Disk homes
Disabled    Disk groups
Enabled     Disk movies
Enabled     Printer printers
```

role

Especifica a função do servidor Samba:

```
> sudo yast samba-server role standalone
```

Para obter uma lista completa das opções, execute `yast samba-server role help`.

service

Habilita ou desabilita os serviços Samba (smb e nmb):

```
> sudo yast samba-server service enable  
> sudo yast samba-server service disable
```

share

Manipula um único compartilhamento do Samba:

```
> sudo yast samba-server share name=movies browseable=yes guest_ok=yes
```

Para obter uma lista completa das opções, execute **yast samba-server share help**.

4.4.3.22 yast security

Controla o nível de segurança do host. O **yast security** aceita os seguintes comandos:

level

Especifica o nível de segurança do host:

```
> sudo yast security level server
```

Para obter uma lista completa das opções, execute **yast security level help**.

set

Define o valor de uma opção específica:

```
> sudo yast security set passwd=sha512 crack=yes
```

Para obter uma lista completa das opções, execute **yast security set help**.

summary

Exibe um resumo da configuração de segurança atual:

```
sudoyast security summary
```

4.4.3.23 yast sound

Define as configurações de placa de som. O **yast sound** aceita os seguintes comandos:

add

Configura uma nova placa de som. Sem nenhum parâmetro, o comando adiciona a primeira placa detectada.

```
> sudo yast sound add card=0 volume=75
```

Para obter uma lista completa das opções, execute **yast sound add help**.

channels

Lista os canais de volume disponíveis de uma placa de som:

```
> sudo yast sound channels card=0  
Master 75  
PCM 100
```

modules

Lista todos os módulos de som do kernel disponíveis:

```
> sudo yast sound modules  
snd-atiixp ATI IXP AC97 controller (snd-atiixp)  
snd-atiixp-modem ATI IXP MC97 controller (snd-atiixp-modem)  
snd-virtuoso Asus Virtuoso driver (snd-virtuoso)  
[...]
```

playtest

Executa um teste de som em uma placa de som:

```
> sudo yast sound playtest card=0
```

remove

Remove uma placa de som configurada:

```
> sudo yast sound remove card=0  
> sudo yast sound remove all
```

set

Especifica novos valores para uma placa de som:

```
> sudo yast sound set card=0 volume=80
```

show

Exibe as informações detalhadas sobre uma placa de som:

```
> sudo yast sound show card=0  
Parameters of card 'ThinkPad X240' (using module snd-hda-intel):  
  
align_buffer_size  
  Force buffer and period sizes to be multiple of 128 bytes.  
bdl_pos_adj  
  BDL position adjustment offset.  
beep_mode
```

```
Select HDA Beep registration mode (0=off, 1=on) (default=1).
Default Value: 0
enable_msi
Enable Message Signaled Interrupt (MSI)
[...]
```

summary

Imprime um resumo da configuração de todas as placas de som no sistema:

```
> sudo yast sound summary
```

volume

Especifica o nível de volume de uma placa de som:

```
sudoyast sound volume card=0 play
```

4.4.3.24 **yast sysconfig**

Controla as variáveis nos arquivos em `/etc/sysconfig`. O **yast sysconfig** aceita os seguintes comandos:

clear

Define o valor vazio como uma variável:

```
> sudo yast sysconfig clear=POSTFIX_LISTEN
```



Dica: Variável em múltiplos arquivos

Se a variável está disponível em diversos arquivos, use a sintaxe `NOME_DA_VARIÁVEL $NOME_DO_ARQUIVO:`

```
> sudo yast sysconfig clear=CONFIG_TYPE$/etc/sysconfig/mail
```

details

Exibe as informações detalhadas sobre uma variável:

```
> sudo yast sysconfig details variable=POSTFIX_LISTEN
Description:
Value:
File: /etc/sysconfig/postfix
Possible Values: Any value
Default Value:
```

```
Configuration Script: postfix
Description:
  Comma separated list of IP's
  NOTE: If not set, LISTEN on all interfaces
```

list

Exibe o resumo das variáveis modificadas. Use all para listar todas as variáveis e seus valores:

```
> sudo yast sysconfig list all
AOU_AUTO_AGREE_WITH_LICENSES="false"
AOU_ENABLE_CRONJOB="true"
AOU_INCLUDE_RECOMMENDS="false"
[...]
```

set

Define um valor para a variável:

```
> sudo yast sysconfig set DISPLAYMANAGER=gdm
```



Dica: Variável em múltiplos arquivos

Se a variável está disponível em diversos arquivos, use a sintaxe NOME_DA_VARIÁVEL \$NOME_DO_ARQUIVO:

```
> sudo yast sysconfig set CONFIG_TYPE$/etc/sysconfig/mail=advanced
```

4.4.3.25 yast tftp-server

Configura um servidor TFTP. O yast tftp-server aceita os seguintes comandos:

directory

Especifica o diretório do servidor TFTP:

```
> sudo yast tftp-server directory path=/srv/tftp
> sudo yast tftp-server directory list
Directory Path: /srv/tftp
```

status

Controla o status do serviço do servidor TFTP:

```
> sudo yast tftp-server status disable
```

```
> sudo yast tftp-server status show
Service Status: false
> sudo yast tftp-server status enable
```

4.4.3.26 **yast timezone**

Configura o fuso horário. O **yast timezone** aceita os seguintes comandos:

list

Lista todos os fusos horários disponíveis agrupados por região:

```
> sudo yast timezone list
Region: Africa
Africa/Abidjan (Abidjan)
Africa/Accra (Accra)
Africa/Addis_Ababa (Addis Ababa)
[...]
```

set

Especifica novos valores para a configuração de fuso horário:

```
> sudo yast timezone set timezone=Europe/Prague hwclock=local
```

summary

Exibe o resumo da configuração de fuso horário:

```
> sudo yast timezone summary
Current Time Zone: Europe/Prague
Hardware Clock Set To: Local time
Current Time and Date: Mon 12. March 2018, 11:36:21 CET
```

4.4.3.27 **yast users**

Gerencia as contas dos usuários. O **yast users** aceita os seguintes comandos:

add

Adiciona um novo usuário:

```
> sudo yast users add username=user1 password=secret home=/home/user1
```

Para obter uma lista completa das opções, execute **yast users add help**.

delete

Apaga uma conta do usuário existente:

```
> sudo yast users delete username=user1 delete_home
```

Para obter uma lista completa das opções, execute **yast users delete help**.

edit

Muda uma conta do usuário existente:

```
> sudo yast users edit username=user1 password=new_secret
```

Para obter uma lista completa das opções, execute **yast users edit help**.

list

Lista os usuários existentes filtrados por tipo de usuário:

```
> sudo yast users list system
```

Para obter uma lista completa das opções, execute **yast users list help**.

show

Exibe os detalhes sobre um usuário:

```
> sudo yast users show username=wwwrun  
Full Name: WWW daemon apache  
List of Groups: www  
Default Group: wwwrun  
Home Directory: /var/lib/wwwrun  
Login Shell: /sbin/nologin  
Login Name: wwwrun  
UID: 456
```

Para obter uma lista completa das opções, execute **yast users show help**.

5 Mudando as configurações de idioma e país com o YaST

Este capítulo explica como definir as configurações de idioma e de país. Você pode mudar o idioma em todo o sistema, apenas para determinados usuários ou desktops ou temporariamente para aplicativos separados. Você também pode configurar idiomas secundários e ajustar as configurações de data e de país.

O trabalho com diferentes países ou em um ambiente multilíngue exige que seu computador seja configurado para oferecer suporte a isso. O SUSE® Linux Enterprise Desktop aceita vários idiomas paralelamente. Idioma é um conjunto de parâmetros que define as configurações de língua e país refletidas na interface do usuário.

O idioma do sistema principal foi selecionado durante a instalação, e as configurações de teclado e fuso horário foram ajustadas. Entretanto, é possível instalar idiomas adicionais no sistema e determinar qual deles será o padrão.

Para estas tarefas, use o módulo de idioma do YaST conforme descrito na [Seção 5.1, “Mudando o idioma do sistema”](#). Instale idiomas secundários para obter uma localização opcional, se precisar iniciar aplicativos ou áreas de trabalho em idiomas diferentes do idioma primário.

Além disso, o módulo de fuso horário do YaST permite ajustar as configurações de país e de fuso horário de acordo. Também permite sincronizar o relógio do sistema com o servidor de horário. Para obter informações detalhadas, consulte a [Seção 5.2, “Mudando as configurações de país e horário”](#).

5.1 Mudando o idioma do sistema

Dependendo de como você usa a área de trabalho e se deseja alternar todo o sistema para outro idioma ou apenas o ambiente de área de trabalho, você terá várias maneiras de fazer isso:

Mudando o idioma do sistema globalmente

Prossiga conforme descrito na [Seção 5.1.1, “Modificando idiomas do sistema com o YaST”](#) e na [Seção 5.1.2, “Trocando o idioma padrão do sistema”](#) para instalar pacotes localizados adicionais com o YaST e definir o idioma padrão. As mudanças entrarão em vigor depois do próximo login. Para garantir que todo o sistema reflita a mudança, reinicialize o sistema ou feche e reinicie todos os serviços, aplicativos e programas em execução.

Mudando o idioma apenas da área de trabalho

Se você instalou os pacotes de idiomas desejados para o seu ambiente de área de trabalho com o YaST, poderá alternar o idioma da área de trabalho usando o respectivo centro de controle, conforme descrito abaixo. Consulte o *Livro “Guia do Usuário do GNOME”, Capítulo 3 “Personalizando as definições de”, Seção 3.2 “Definindo configurações de idioma”* para obter os detalhes. Após a reinicialização do servidor X, toda a sua área de trabalho refletirá a nova opção de idioma. Os aplicativos que não pertencem à estrutura da área de trabalho não serão afetados por esta mudança e ainda poderão aparecer no idioma que foi definido no YaST.

Trocando os idiomas temporariamente em apenas um aplicativo

É possível também executar um único aplicativo em outro idioma (já instalado com o YaST). Para isso, inicie-o pela linha de comando especificando o código do idioma, conforme descrito na *Seção 5.1.3, “Alternando idiomas de aplicativos X padrão e do GNOME”*.

5.1.1 Modificando idiomas do sistema com o YaST

O YaST tem duas categorias de idioma diferentes:

Idioma primário

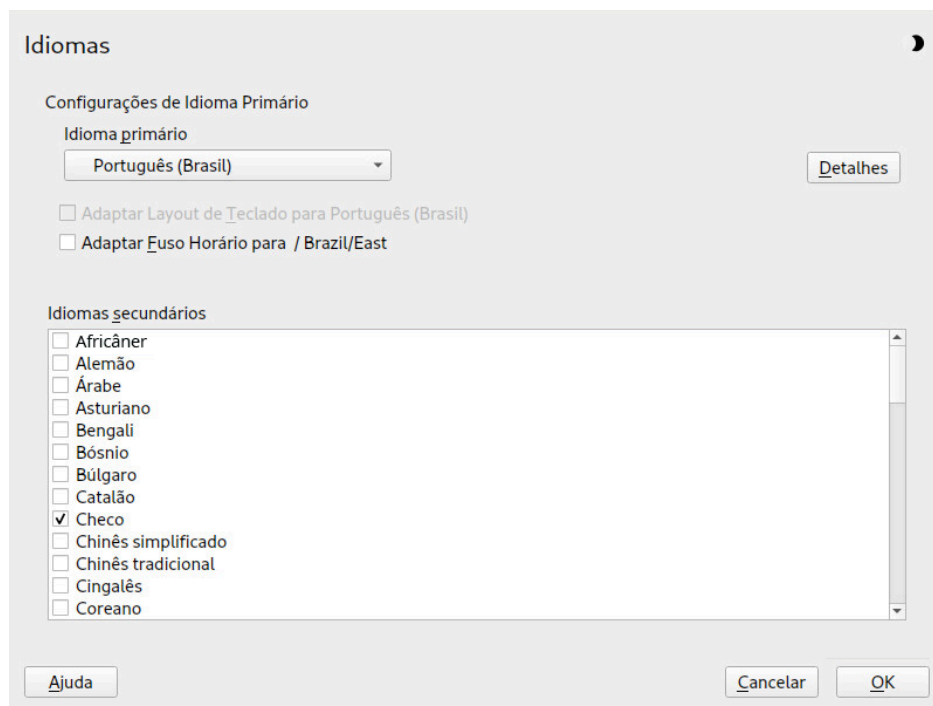
O idioma principal definido no YaST se aplica a todo o sistema, incluindo o YaST e o ambiente de área de trabalho. Esse idioma será usado sempre que estiver disponível, a menos que você especifique um outro idioma manualmente.

Idiomas secundários

Instale idiomas secundários para tornar o sistema multilíngue. Os idiomas instalados como secundários podem ser selecionados manualmente em determinada situação. Por exemplo, use um idioma secundário para iniciar um aplicativo em determinado idioma para processamento de texto nesse idioma.

Antes de instalar idiomas adicionais, determine qual deles será o padrão do sistema (idioma primário).

Para acessar o módulo de idioma do YaST, inicie o YaST e clique em *Sistema > Idioma*. Se preferir, inicie a caixa de diálogo *Idiomas* diretamente, executando `sudo yast2 language &` de uma linha de comando.



PROCEDIMENTO 5.1: INSTALANDO IDIOMAS ADICIONAIS

Ao instalar idiomas adicionais, o YaST também permite definir configurações de idioma diferentes para o usuário `root`, consulte o [Passo 4](#). A opção *Configurações Locais para Usuário root* determina como as variáveis de idioma (`LC_*`) no arquivo `/etc/sysconfig/language` são definidas para o `root`. Você pode defini-las para o mesmo idioma dos usuários comuns. Se preferir, você poderá evitar que ele seja afetado por qualquer mudança de idioma ou apenas definir a variável `RC_LC_CTYPE` para os mesmos valores dos usuários comuns. A variável `RC_LC_CTYPE` define a localização para chamadas de função específicas do idioma.

1. Para adicionar idiomas ao módulo de idioma do YaST, selecione os *Idiomas Secundários* que deseja instalar.
2. Para tornar padrão o idioma, defina-o como *Idioma Primário*.
3. Além disso, adapte o teclado ao novo idioma primário e ajuste o fuso horário, se apropriado.



Dica: Configurações avançadas

Para as configurações avançadas de teclado ou fuso horário, selecione *Hardware > System Keyboard Layout* (Layout do Teclado do Sistema) ou *Sistema > Data e Horário* no YaST para iniciar as respectivas caixas de diálogo. Para obter mais informações, consulte o [Capítulo 32, Configurando o layout do teclado do sistema](#) e a [Seção 5.2, “Mudando as configurações de país e horário”](#).

4. Para mudar as configurações de idioma específicas ao usuário root, clique em *Detalhes*.
 - a. Defina *Configurações Locais para Usuário root* com o valor desejado. Para obter mais informações, clique em *Ajuda*.
 - b. Decida se deseja ou não *Usar Codificação UTF-8* para o root.
5. Se o seu idioma não foi incluído na lista de idiomas primários disponíveis, tente especificá-lo com *Configuração Detalhada de Local*. No entanto, algumas localizações podem estar incompletas.
6. Confirme as mudanças nas caixas de diálogo clicando em *OK*. Se você selecionou idiomas secundários, o YaST instalará os pacotes de software localizados para os idiomas adicionais.

O sistema agora é multilíngue. Entretanto, para iniciar um aplicativo em idioma diferente do primário, você precisa definir o idioma desejado explicitamente conforme explicado na [Seção 5.1.3, “Alternando idiomas de aplicativos X padrão e do GNOME”](#).

5.1.2 Trocando o idioma padrão do sistema

Para mudar globalmente o idioma padrão de um sistema, siga o procedimento abaixo:

1. Inicie o módulo de idioma do YaST.
2. Selecione o novo idioma desejado do sistema como *Idioma Primário*.



Importante: Apagando idiomas anteriores do sistema

Se você mudar para um idioma primário diferente, os pacotes de softwares localizados referentes ao idioma primário anterior serão removidos do sistema. Para alternar o idioma padrão do sistema, mas manter o idioma primário anterior como adicional, adicione-o como *Idioma Secundário* marcando a respectiva caixa de seleção.

3. Ajuste as opções de teclado e fuso horário conforme desejado.
4. Confirme as mudanças clicando em *OK*.
5. Depois que o YaST aplicar as mudanças, reinicie as sessões X atuais (por exemplo, efetuando logout e login novamente) para que o YaST e os aplicativos de área de trabalho reflitam as novas configurações de idioma.

5.1.3 Alternando idiomas de aplicativos X padrão e do GNOME

Após instalar o respectivo idioma com o YaST, você poderá executar um único aplicativo em outro idioma.

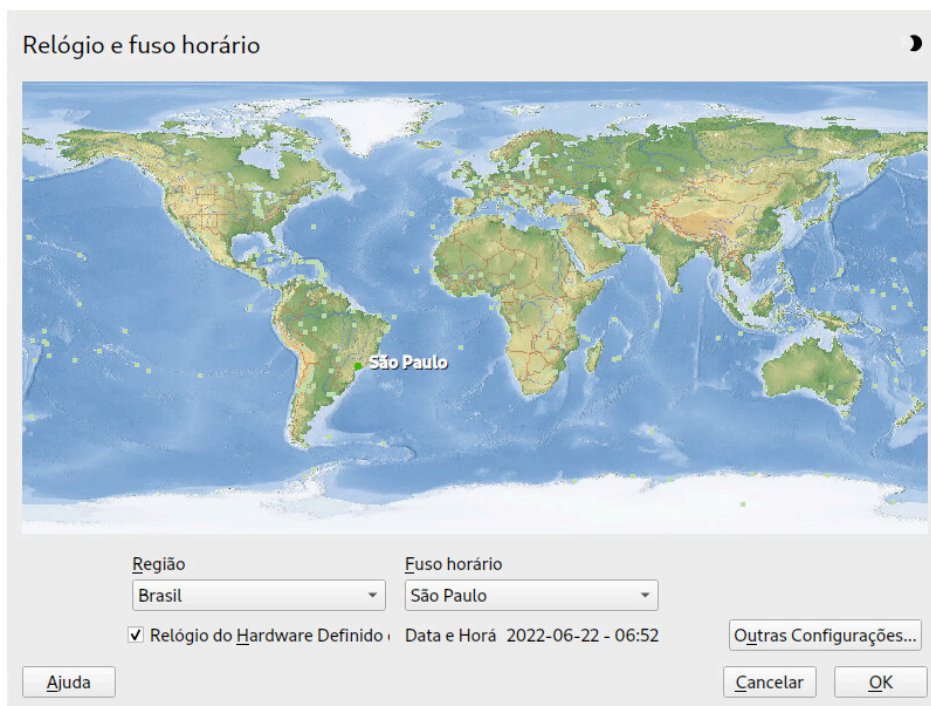
Inicie o aplicativo da linha de comando usando o seguinte comando:

```
LANG=LANGUAGE application
```

Por exemplo, para iniciar o f-spot em alemão, execute **LANG=de_DE f-spot**. Para outros idiomas, use o código de idioma apropriado. Obtenha a lista de todos os códigos de idioma disponíveis usando o comando **locale -av**.

5.2 Mudando as configurações de país e horário

Usando o módulo de data e horário do YaST, ajuste as informações de data, relógio e fuso horário do sistema de acordo com a área em que estiver trabalhando. Para acessar o módulo do YaST, inicie o YaST e clique em *Sistema > Data e Horário*. Se preferir, inicie a caixa de diálogo *Relógio e Fuso Horário* diretamente, executando **sudo yast2 timezone &** de uma linha de comando.



Primeiro, selecione a região geral, como *Europa*. Escolha o país apropriado correspondente ao local onde você está trabalhando, por exemplo, *Alemanha*.

Dependendo dos sistemas operacionais em execução na estação de trabalho, ajuste as configurações do relógio do hardware de acordo:

- Se você executar outro sistema operacional em sua máquina, como o Microsoft Windows*, é provável que seu sistema não use UTC, mas o horário local. Neste caso, desative *Relógio do Hardware Definido Para UTC*.
- Se você executa somente Linux em sua máquina, defina o relógio de hardware como UTC e faça com que o horário padrão alterne automaticamente para o horário de verão.



Importante: Definir o relógio do hardware como UTC

Só é possível alternar do horário padrão para o horário de verão (e vice-versa) automaticamente quando o relógio do hardware (relógio CMOS) está definido como UTC. Isso também se aplica quando você usa a sincronização automática de horário com NTP, pois a sincronização automática só pode ser feita quando a diferença de horário entre o relógio do hardware e do sistema é inferior a 15 minutos.

Como o horário incorreto do sistema pode provocar problemas graves (backups ausentes, mensagens de e-mail descartadas, falhas de montagem em sistemas de arquivos remotos etc.), é altamente recomendado *sempre* definir o relógio do hardware como UTC.

Você pode mudar a data e o horário manualmente ou optar por sincronizar sua máquina com um servidor NTP de forma permanente ou apenas para ajustar o relógio do hardware.

PROCEDIMENTO 5.2: AJUSTANDO DATA E HORÁRIO MANUALMENTE

1. No módulo de fuso horário do YaST, clique em *Outras Configurações* para definir a data e o horário.
2. Selecione *Manualmente* e digite os valores de data e horário.
3. Confirme as mudanças.

PROCEDIMENTO 5.3: DEFININDO A DATA E O HORÁRIO COM O SERVIDOR NTP

1. Clique em *Outras Configurações* para definir a data e o horário.
2. Selecione *Sincronizar com o Servidor NTP*.
3. Digite o endereço de um servidor NTP, caso ainda não tenha sido preenchido.

Mudar Data e Horário

☐ Manualmente

Horário Atual
12:19:34

Data atual
2022-05-22

☒ Mudar Horário Agora

☐ Sincronizar com o servidor NTP

Endereço do servidor NTP
ua.pool.ntp.org

Configurar...

Ajuda Cancelar Aceitar

4. Com o botão *Configurar*, é possível abrir a configuração avançada de NTP. Para obter os detalhes, consulte a [Seção 39.1, "Configurando um cliente NTP com YaST"](#).

5. Confirme as mudanças.

6 Gerenciando usuários com o YaST

Durante a instalação, você pode ter criado um usuário local para o seu sistema. Com o módulo *Gerenciamento de Usuários e Grupos* do YaST, é possível adicionar usuários ou editar usuários existentes. Ele também permite configurar o sistema para autenticar usuários em um servidor de rede.

6.1 Caixa de diálogo Administração de Usuário e Grupo

Para administrar usuários ou grupos, inicie o YaST e clique em *Segurança e Usuários* > *Gerenciamento de Usuários e Grupos*. Se preferir, inicie a caixa de diálogo *Administração de Usuário e Grupo* diretamente, executando `sudo yast2 users &` de uma linha de comando.

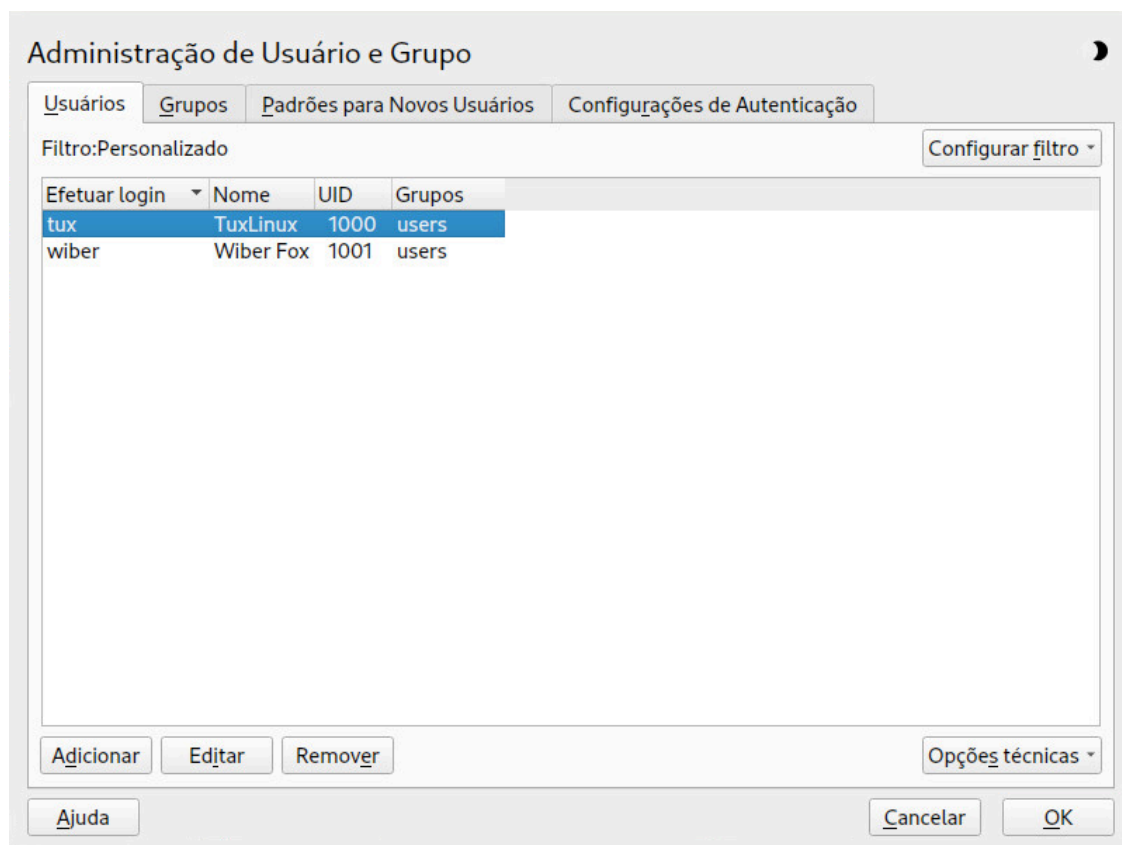


FIGURA 6.1: ADMINISTRAÇÃO DE USUÁRIO E GRUPO DO YAST

Cada usuário recebe um ID de usuário de todo o sistema (UID). Além dos usuários que podem efetuar login na sua máquina, há vários *usuários do sistema* apenas para uso interno. Cada usuário é atribuído a um ou mais grupos. Parecido com os *usuários do sistema*, há também os *grupos de sistema* para uso interno.

Dependendo do conjunto de usuários que você escolher para ver e modificar a caixa de diálogo (usuários locais, usuários de rede, usuários do sistema), a janela principal mostrará diversas guias. Elas permitem que você execute as seguintes tarefas:

Gerenciando contas de usuário

Na guia *Usuários*, crie, modifique, apague ou desabilite temporariamente as contas do usuário conforme descrito na [Seção 6.2, “Gerenciando contas de usuário”](#). Conheça as opções avançadas, como uso obrigatório de políticas de senha, uso de diretórios pessoais criptografados ou gerenciamento de cotas de disco na [Seção 6.3, “Opções adicionais para contas dos usuários”](#).

Mudando as configurações padrão

As contas de usuários locais são criadas de acordo com as configurações definidas na guia *Padrões para Novos Usuários*. Aprenda a mudar a atribuição de grupo padrão ou as permissões de acesso e o caminho padrão de diretórios pessoais na [Seção 6.4, “Mudando as configurações padrão para usuários locais”](#).

Atribuindo usuários a grupos

Aprenda a mudar a atribuição de grupo para usuários individuais na [Seção 6.5, “Atribuindo usuários a grupos”](#).

Gerenciando grupos

Na guia *Grupos*, você pode adicionar, modificar ou apagar grupos existentes. Consulte a [Seção 6.6, “Gerenciando grupos”](#) para obter informações sobre isso.

Mudando o método de autenticação do usuário

Quando a sua máquina está conectada a uma rede que oferece métodos de autenticação de usuário como NIS ou LDAP, você pode escolher dentre diversos métodos de autenticação na guia *Configurações de Autenticação*. Para obter mais informações, consulte a [Seção 6.7, “Mudando o método de autenticação do usuário”](#).

Para o gerenciamento de usuários e grupos, a caixa de diálogo fornece uma funcionalidade semelhante. Para alternar facilmente entre a tela de administração de usuários e grupos, escolha a guia apropriada na parte superior da caixa de diálogo.

As opções de filtro permitem definir o conjunto de usuários ou grupos que você deseja modificar. Na guia *Usuários* ou *Grupo*, clique em *Configurar Filtro* para ver e editar usuários ou grupos. Elas são listadas de acordo com determinadas categorias, como *Usuários Locais* ou *Usuários LDAP*, se aplicável. Com *Configurar Filtro* > *Personalizar Filtro*, você também poderá configurar e usar um filtro personalizado.

Dependendo do filtro escolhido, nem todas as opções e funções a seguir estarão disponíveis na caixa de diálogo.

6.2 Gerenciando contas de usuário

O YaST permite criar, modificar, apagar ou desabilitar temporariamente as contas de usuários. Não modifique as contas do usuário, a menos que você seja um usuário experiente ou administrador.



Nota: Mudando IDs de usuários existentes

A propriedade do arquivo está vinculada ao ID de usuário, e não ao nome de usuário. Após uma mudança de ID de usuário, os arquivos no diretório pessoal do usuário serão automaticamente ajustados para refletir essa mudança. Entretanto, após uma mudança de ID, o usuário não terá mais posse dos arquivos que ele criou em algum local do sistema de arquivos, a menos que a propriedade desses arquivos seja modificada manualmente.

Saiba a seguir como configurar contas de usuários padrão. Para ver mais opções, consulte a [Seção 6.3, “Opções adicionais para contas dos usuários”](#).

PROCEDIMENTO 6.1: ADICIONANDO OU MODIFICANDO CONTAS DE USUÁRIOS

1. Abra a caixa de diálogo *Administração de Usuário e Grupo* do YaST e clique na guia *Usuários*.
2. Com *Configurar Filtro*, defina o conjunto de usuários que deseja gerenciar. A caixa de diálogo mostra uma lista de usuários no sistema e os grupos aos quais eles pertencem.
3. Para modificar as opções de um usuário existente, selecione uma entrada e clique em *Editar*.

Para criar uma nova conta de usuário, clique em *Adicionar*.

4. Digite os dados de usuário apropriados na primeira guia, como *Nome do usuário* (usado para login) e *Senha*. Esses dados são suficientes para criar um novo usuário. Se você clicar em *OK* agora, o sistema atribuirá um ID de usuário automaticamente e definirá todos os outros valores de acordo com o padrão.
5. Ative *Receber Correio do Sistema* para que algum tipo de notificação do sistema seja enviado à caixa de correio do usuário. Isso cria um alias de e-mail para o `root`, e o usuário pode ler e-mails do sistema sem ter que primeiro efetuar login como `root`.
Os e-mails enviados dos serviços do sistema são armazenados em uma caixa de correio local `/var/spool/mail/ USERNAME`, em que `USERNAME` é o nome de login do usuário selecionado. Para ler e-mails, você pode usar o comando `mail`.
6. Para ajustar mais detalhes, como o ID de usuário ou o caminho para o diretório pessoal do usuário, use a guia *Detalhes*.
Se precisar realocar o diretório pessoal de um usuário existente, digite o caminho do novo diretório pessoal e mova o conteúdo do diretório pessoal atual usando *Mover para Nova Localização*. Do contrário, um novo diretório pessoal será criado sem nenhum dado existente.
7. Para forçar os usuários a mudar regularmente a senha ou definir outras opções de senha, alterne para *Configurações de Senha* e ajuste as opções. Para obter mais detalhes, consulte a [Seção 6.3.2, “Assegurando o uso obrigatório de políticas de senha”](#).
8. Clique em *OK* se todas as opções estiverem definidas conforme desejado.
9. Clique em *OK* para fechar a caixa de diálogo de administração e gravar as mudanças. Um usuário recém-adicionado agora poderá efetuar login no sistema usando o nome de login e a senha criada.
Se preferir, grave todas as mudanças sem sair da caixa de diálogo *Administração de Usuário e Grupo* clicando em *Opções de Especialista > Gravar Mudanças Agora*.



Dica: Fazendo a correspondência de IDs de usuário

Convém corresponder o ID de usuário (local) ao ID na rede. Por exemplo, um novo usuário (local) em um laptop deve ser integrado a um ambiente de rede com o mesmo ID de usuário. Esse procedimento garante a mesma propriedade dos arquivos que o usuário cria “offline” daqueles criados diretamente na rede.

1. Abra a caixa de diálogo *Administração de Usuário e Grupo* do YaST e clique na guia *Usuários*.
2. Para desabilitar uma conta de usuário temporariamente sem apagá-la, selecione o usuário na lista e clique em *Editar*. Ative *Desabilitar Login de Usuário*. O usuário não poderá efetuar login em sua máquina até que você habilite a conta novamente.
3. Para apagar uma conta de usuário, selecione o usuário na lista e clique em *Apagar*. Escolha se você também deseja apagar o diretório pessoal do usuário ou manter os dados.

6.3 Opções adicionais para contas dos usuários

Além das configurações para uma conta de usuário padrão, o SUSE® Linux Enterprise Desktop oferece mais opções. Por exemplo, as opções para assegurar o uso obrigatório de políticas de senha, usar diretórios pessoais criptografados ou definir cotas de disco para usuários e grupos.

6.3.1 Login automático e login sem senha

Se você usar o ambiente de área de trabalho do GNOME, poderá configurar o *Auto Login* para determinado usuário e também o *Login sem Senha* para todos os usuários. O login automático faz com que o usuário seja conectado automaticamente ao ambiente de desktop na inicialização. Essa funcionalidade somente poderá ser ativada para um usuário de cada vez. O login sem senha permite que todos os usuários efetuem login no sistema após digitarem seus nomes de usuário no gerenciador de login.



Atenção: Risco de segurança

Habilitar a opção *Auto Login* ou *Login sem Senha* em uma máquina que pode ser acessada por mais de uma pessoa representa um risco de segurança. Qualquer usuário poderá obter acesso ao seu sistema e aos seus dados sem precisar de autenticação. Se o seu sistema contiver dados confidenciais, não use essa funcionalidade.

Para ativar o login automático ou o login sem senha, acesse essas funções em *Administração de Usuário e Grupo* no YaST em *Opções de Especialista > Configurações de Login*.

6.3.2 Assegurando o uso obrigatório de políticas de senha

Em qualquer sistema com vários usuários, convém assegurar o uso obrigatório de, no mínimo, as políticas básicas de segurança de senha. Os usuários devem mudar as senhas regularmente e usar senhas fortes que não possam ser exploradas facilmente. Para usuários locais, proceda da seguinte forma:

PROCEDIMENTO 6.3: DEFININDO CONFIGURAÇÕES DE SENHA

1. Abra a caixa de diálogo *Administração de Usuário e Grupo* do YaST e selecione a guia *Usuários*.
2. Selecione o usuário para o qual mudará as opções de senha e clique em *Editar*.
3. Alterne para a guia *Configurações de Senha*. A última mudança de senha do usuário é exibida na guia.
4. Para que o usuário mude a senha no próximo login, ative *Forçar Mudança de Senha*.
5. Para assegurar o uso obrigatório de um rodízio de senhas, defina um *Número Máximo de Dias para a Mesma Senha* e um *Número Mínimo de Dias para a Mesma Senha*.
6. Para lembrar o usuário de mudar a senha antes de sua expiração, defina o número de *Dias Antes do Aviso do Vencimento de Senha*.
7. Para restringir o período de login do usuário depois que a senha expirar, mude o valor em *Dias Depois do Vencimento da Senha que o Login é Válido*.
8. Você também pode indicar uma data de vencimento específica para a conta completa. Digite a *Data de Vencimento* no formato AAAA-MM-DD. Essa configuração não está relacionada à senha, mas sim à conta propriamente dita.
9. Para obter mais informações sobre as opções e os valores padrão, clique em *Ajuda*.
10. Aplique suas mudanças com *OK*.

6.3.3 Gerenciando cotas

Para evitar o esgotamento dos recursos do sistema sem qualquer notificação, os administradores de sistema podem configurar cotas para usuários ou grupos. É possível definir quotas para um ou mais sistemas de arquivos, e restringir a quantidade de espaço em disco que pode ser usada e o número de inodes (nós do índice) que podem ser criados lá. Os inodes são estruturas de dados em um sistema de arquivos que armazenam informações básicas sobre um arquivo, um

diretório ou outro objeto de sistema de arquivos comum. Eles armazenam todos os atributos de um objeto de sistema de arquivos (como propriedade do usuário e do grupo, permissões de leitura, gravação ou execução), exceto nome de arquivo e conteúdo.

O SUSE Linux Enterprise Desktop permite o uso de cotas flexíveis e fixas. Além disso, é possível definir intervalos extras que permitem que usuários ou grupos violem temporariamente determinadas quantidades de suas cotas.

Cota flexível

Define um nível de aviso em que os usuários são informados de que estão atingindo seu limite. Os administradores alertam os usuários para limparem e reduzirem seus dados na partição. O limite de cota flexível normalmente é menor do que o limite de cota fixa.

Cota fixa

Define o limite em que as solicitações de gravação são negadas. Quando uma cota fixa é atingida, não é possível armazenar mais dados, e os aplicativos podem falhar.

Período extra

Define o período entre o overflow da cota flexível e a emissão do aviso. Normalmente, ele é definido como um valor bastante baixo entre uma ou várias horas.

PROCEDIMENTO 6.4: **HABILITANDO O SUPORTE A QUOTAS PARA UMA PARTIÇÃO**

Para configurar cotas para determinados usuários e grupos, habilite primeiro o suporte a cotas para a respectiva partição no Particionador Técnico do YaST.

1. No YaST, selecione *Sistema > Particionador* e clique em *Sim* para continuar.
2. No *Particionador Técnico*, selecione a partição para a qual habilitará cotas e clique em *Editar*.
3. Clique em *Opções do Fstab* e ative *Habilitar Suporte a Cotas*. Se o pacote quota ainda não foi instalado, a instalação é feita assim que você confirma a respectiva mensagem clicando em *Sim*.
4. Confirme suas mudanças e saia do *Particionador Técnico*.
5. Verifique se o serviço quotaon está em execução digitando o seguinte comando:

```
> sudo systemctl status quotaon.service
```

Ele deve estar marcado como active (ativo). Do contrário, inicie-o com o comando **systemctl start quotaon.service**.

Agora, você poderá definir cotas flexíveis ou fixas para usuários ou grupos específicos e especificar os períodos como intervalos extras.

1. Em *Administração de Usuário e Grupo* do YaST, selecione o usuário ou grupo para o qual deseja definir as cotas e clique em *Editar*.
2. Na guia *Plug-ins*, selecione a entrada *Gerenciar Cotas de Usuário* e clique em *Iniciar* para abrir a caixa de diálogo *Configuração de Cota*.
3. Em *Sistema de Arquivos*, selecione a partição à qual a cota deverá ser aplicada.

Configuração de Cota

Sistema de arquivos
/dev/sda4

Limites de Tamanho

Limite flexível
5000

Limite rígido
75000

Dias: 0 Horas: 0 Minutos: 0 Segundos: 0

Limite de I-nodes

Limite flexível
0

Limite rígido
0

Dias: 0 Horas: 0 Minutos: 0 Segundos: 0

Ajuda Cancelar OK

4. Embaixo de *Limites de Tamanho*, restrinja a quantidade do espaço em disco. Digite o número de blocos de 1 KB que o usuário ou o grupo possa ter nessa partição. Especifique um valor para *Limite Flexível* e outro para *Limite Físico*.
5. Você também pode restringir o número de inodes que o usuário ou o grupo pode ter na partição. Embaixo de *Limites de I-node*, digite um *Limite Flexível* e um *Limite Físico*.
6. Você só poderá definir intervalos extras se o usuário ou o grupo já tiver excedido o limite flexível especificado para tamanho ou inodes. Do contrário, as caixas de texto relacionadas a tempo não estarão ativadas. Especifique o período para o qual o usuário ou o grupo tem permissão para exceder os limites definidos acima.

7. Confirme as configurações com *OK*.
8. Clique em *OK* para fechar a caixa de diálogo de administração e gravar as mudanças.
Se preferir, grave todas as mudanças sem sair da caixa de diálogo *Administração de Usuário e Grupo* clicando em *Opções de Especialista > Gravar Mudanças Agora*.

O SUSE Linux Enterprise Desktop também inclui ferramentas de linha de comando, como repquota ou warnquota. Os administradores de sistema podem usar essas ferramentas para controlar a utilização do disco ou enviar notificações por e-mail aos usuários que excederem a cota. Usando quota_nld, os administradores também podem encaminhar mensagens de kernel sobre as cotas excedidas para D-BUS. Para obter mais informações, consulte as páginas de manual de repquota, warnquota e quota_nld.

6.4 Mudando as configurações padrão para usuários locais

Ao criar novos usuários locais, várias configurações padrão são usadas pelo YaST. Elas incluem, por exemplo, o grupo principal e os grupos secundários aos quais o usuário pertence, ou as permissões de acesso do diretório pessoal do usuário. Você poderá mudar essas configurações padrão de acordo com os seus requisitos:

1. Abra a caixa de diálogo *Administração de Usuário e Grupo* do YaST e selecione a guia *Padrões para Novos Usuários*.
2. Para mudar o grupo principal ao qual os novos usuários deverão pertencer automaticamente, selecione outro grupo em *Grupo Padrão*.
3. Para modificar os grupos secundários para os novos usuários, adicione ou mude os grupos em *Grupos Secundários*. Os nomes de grupo devem ser separados por vírgulas.
4. Se você não deseja usar /home/NOME_DE_USUÁRIO como o caminho padrão dos diretórios pessoais dos novos usuários, modifique o *Prefixo de caminho para diretório pessoal*.
5. Para mudar os modos de permissão padrão dos diretórios pessoais recém-criados, ajuste o valor de umask em *Umask para o Diretório Pessoal*. Para obter mais informações sobre umask, consulte o Livro *"Security and Hardening Guide"*, Capítulo 19 *"Access control lists in Linux"* e a página de manual do umask.
6. Para obter informações sobre as opções individuais, clique em *Ajuda*.

7. Aplique suas mudanças com OK.

6.5 Atribuindo usuários a grupos

Os usuários locais são atribuídos a vários grupos de acordo com as configurações padrão, que podem ser acessadas na caixa de diálogo *Administração de Usuário e Grupo*, na guia *Padrões para Novos Usuários*. Aprenda a seguir como modificar a atribuição de grupo de um usuário individual. Se precisar mudar as atribuições de grupo padrão para os novos usuários, consulte a [Seção 6.4, “Mudando as configurações padrão para usuários locais”](#).

PROCEDIMENTO 6.6: MUDANDO A ATRIBUIÇÃO DE GRUPO DE UM USUÁRIO

1. Abra a caixa de diálogo *Administração de Usuário e Grupo* do YaST e clique na guia *Usuários*. Ela lista os usuários e os grupos aos quais os usuários pertencem.
2. Clique em *Editar* e alterne para a guia *Detalhes*.
3. Para mudar o grupo principal ao qual pertence o usuário, clique em *Grupo Padrão* e selecione o grupo na lista.
4. Para atribuir grupos secundários adicionais de usuários, ative as caixas de seleção correspondentes na lista *Grupos Adicionais*.
5. Clique em OK para aplicar as mudanças.
6. Clique em OK para fechar a caixa de diálogo de administração e gravar as mudanças. Se preferir, grave todas as mudanças sem sair da caixa de diálogo *Administração de Usuário e Grupo* clicando em *Opções de Especialista > Gravar Mudanças Agora*.

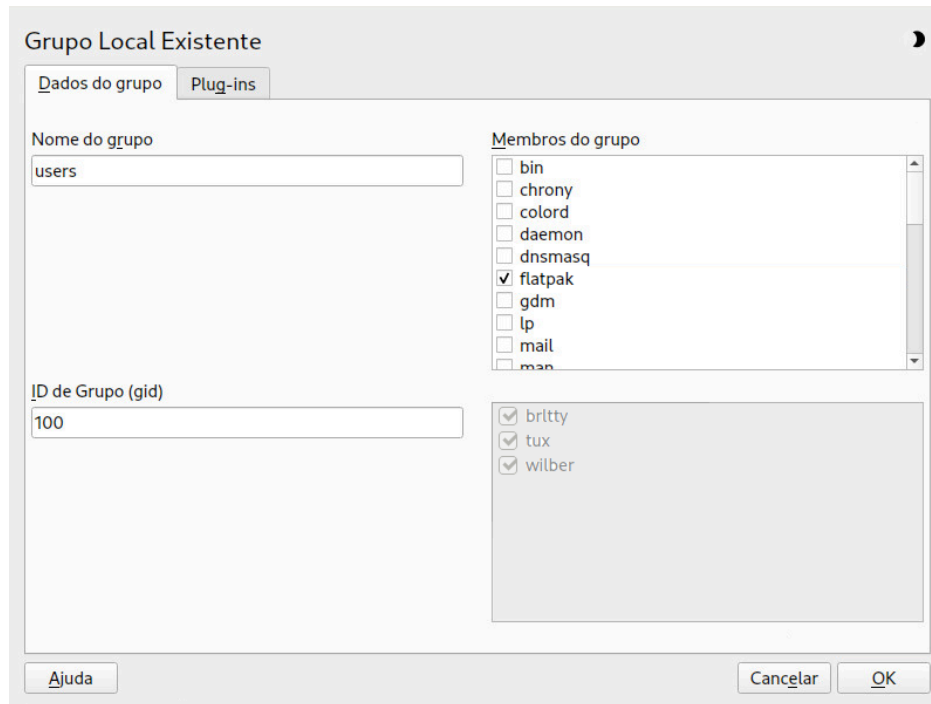
6.6 Gerenciando grupos

Com o YaST, você também pode adicionar, modificar ou apagar grupos facilmente.

PROCEDIMENTO 6.7: CRIANDO E MODIFICANDO GRUPOS

1. Abra a caixa de diálogo *Gerenciamento de Usuários e Grupos* do YaST e clique na guia *Grupos*.
2. Com *Configurar Filtro*, defina o conjunto de grupos a serem gerenciados. A caixa de diálogo lista os grupos no sistema.

3. Para criar um novo grupo, clique em *Adicionar*.
4. Para modificar um grupo existente, selecione o grupo e clique em *Editar*.
5. Na caixa de diálogo seguinte, digite ou mude os dados. A lista à direita mostra uma visão geral de todos os usuários e usuários de sistema disponíveis que podem ser membros do grupo.



6. Para adicionar usuários existentes a um novo grupo, selecione-os na lista de *Membros do grupo* possíveis, marcando a caixa correspondente. Para removê-los do grupo, desmarque a caixa.
7. Clique em *OK* para aplicar as mudanças.
8. Clique em *OK* para fechar a caixa de diálogo de administração e gravar as mudanças. Se preferir, grave todas as mudanças sem sair da caixa de diálogo *Administração de Usuário e Grupo* clicando em *Opções de Especialista > Gravar Mudanças Agora*.

Para apagar um grupo, ele não deve ter nenhum membro. Para apagar um grupo, selecione-o na lista e clique em *Apagar*. Clique em *OK* para fechar a caixa de diálogo de administração e gravar as mudanças. Se preferir, grave todas as mudanças sem sair da caixa de diálogo *Administração de Usuário e Grupo* clicando em *Opções de Especialista > Gravar Mudanças Agora*.

6.7 Mudando o método de autenticação do usuário

Com a máquina conectada à rede, você pode mudar o método de autenticação. As seguintes opções estão disponíveis:

NIS

Os usuários são administrados centralmente em um servidor NIS em todos os sistemas da rede. Para obter os detalhes, consulte o *Livro "Security and Hardening Guide", Capítulo 3 "Using NIS"*.

SSSD

O *System Security Services Daemon* (SSSD) pode armazenar em cache localmente os dados dos usuários e permitir que eles os utilizem mesmo que o serviço de diretório real esteja (temporariamente) inacessível. Para obter os detalhes, consulte o *Livro "Security and Hardening Guide", Capítulo 4 "Setting up authentication clients using YaST", Seção 4.2 "SSSD"*.

Samba

A autenticação SMB é geralmente usada em redes com Linux e Windows. Para obter os detalhes, consulte o *Livro "Security and Hardening Guide", Capítulo 7 "Active Directory support"*.

Para mudar o método de autenticação, faça o seguinte:

1. Abra a caixa de diálogo *Administração de Usuário e Grupo* no YaST.
2. Clique na guia *Configurações de Autenticação* para mostrar uma visão geral dos métodos de autenticação disponíveis e das configurações atuais.
3. Para mudar o método de autenticação, clique em *Configurar* e selecione o método de autenticação que deseja modificar. Isso o levará diretamente para os módulos de configuração de cliente no YaST. Para obter informações sobre a configuração do cliente apropriado, consulte as seguintes seções:

NIS: *Livro "Security and Hardening Guide", Capítulo 3 "Using NIS", Seção 3.2 "Configuring NIS clients"*

LDAP: *Livro "Security and Hardening Guide", Capítulo 4 "Setting up authentication clients using YaST", Seção 4.1 "Configuring an authentication client with YaST"*

SSSD: *Livro "Security and Hardening Guide", Capítulo 4 "Setting up authentication clients using YaST", Seção 4.2 "SSSD"*

4. Após aceitar a configuração, retorne à visão geral de *Administração de Usuário e Grupo*.

5. Clique em **OK** para fechar a caixa de diálogo de administração.

6.8 Usuários do sistema padrão

Por padrão, o SUSE Linux Enterprise Desktop cria nomes de usuário que não podem ser apagados. Esses usuários normalmente são definidos no Linux Standard Base. A lista a seguir apresenta os nomes comuns de usuário e a finalidade deles:

NOMES COMUNS DE USUÁRIOS INSTALADOS POR PADRÃO

bin,

daemon

Usuário legado, incluído para compatibilidade com os aplicativos legados. Os novos aplicativos não devem mais utilizar esse nome de usuário.

gdm

Usado pelo GDM (GNOME Display Manager – Gerenciador de Exibição do Gnome) para fornecer logins gráficos e gerenciar exibições locais e remotas.

lp

Usado pelo daemon Printer para CUPS (Common Unix Printing System).

mail

Reservado pelo usuário para programas de e-mail como sendmail ou postfix.

man

Usado pelo man para acessar páginas de manual.

messagebus

Usado para acessar o D-Bus (barramento de área de trabalho), um barramento de software para comunicação entre processos. O daemon é dbus-daemon.

nobody

Usuário que não tem nenhum arquivo e não está em nenhum grupo privilegiado. Atualmente, seu uso é limitado conforme recomendação do Linux Standard Base para fornecer uma conta do usuário separada para cada daemon.

nscd

Usado pelo Daemon de Cache de Serviço de Nomes. Esse daemon é um serviço de pesquisa que melhora o desempenho com NIS e LDAP. O daemon é nscd.

polkitd

Usado pelo PolicyKit Authorization Framework, que define e manipula solicitações de autorização para processos sem privilégios. O daemon é polkitd.

postfix

Usado pelo programa de correio Postfix.

pulse

Usado pelo servidor de som Pulseaudio.

root

Usado pelo administrador do sistema, concedendo todos os privilégios apropriados.

rpc

Usado pelo comando rpcbind, um mapeador de porta RPC.

rtkit

Usado pelo pacote rtkit que fornece um serviço do sistema D-Bus para o modo de programação em tempo real.

salt

Usuário para execução remota paralela fornecido pelo Salt. O daemon é denominado salt-master.

scard

Usuário para comunicação com smart cards e leitores. O daemon é denominado pcscd.

srvGeoClue

Usado pelo serviço GeoClue D-Bus para fornecer informações de localização.

sshd

Usado pelo daemon Secure Shell (SSH) para garantir a comunicação protegida e criptografada em uma rede não segura.

statd

Usado pelo protocolo Network Status Monitor (NSM), implementado no daemon rpc.statd, para escutar notificações de reinicialização.

systemd-coredump

Usado pelo comando /usr/lib/systemd/systemd-coredump para adquirir, gravar e processar dumps de memória.

systemd-timesync

Usado pelo comando `/usr/lib/systemd/systemd-timesyncd` para sincronizar o relógio do sistema local com um servidor remoto NTP (Network Time Protocol).

7 Atualização online do YaST

O SUSE oferece um fluxo contínuo de atualizações de segurança de software para o seu produto. Por padrão, o applet de atualização é usado para manter o sistema atualizado. Consulte a [Seção 8.5, “Atualizador de pacotes do GNOME”](#) para obter mais informações sobre o applet de atualização. Este capítulo aborda a ferramenta alternativa para atualizar pacotes de software: Atualização Online do YaST.

Os patches atuais para o SUSE® Linux Enterprise Desktop estão disponíveis em um repositório de software de atualização. Se você registrou seu produto durante a instalação, já há um repositório de atualização configurado. Se você não registrou o SUSE Linux Enterprise Desktop, pode fazer isso iniciando o *Registro de Produto* no YaST. Se preferir, adicione manualmente um repositório de atualização de uma fonte confiável. Para adicionar ou remover repositórios, inicie o Gerenciador de Repositórios em *Software > Repositórios de Software* no YaST. Saiba mais sobre o Gerenciador de Repositórios na [Seção 8.4, “Gerenciando repositórios de software e serviços”](#).



Nota: Erro ao acessar o catálogo de atualização

Se você não conseguir acessar o catálogo de atualização, pode ser que a inscrição tenha expirado. Normalmente, o SUSE Linux Enterprise Desktop vem com uma inscrição de um ou três anos, período em que você terá acesso ao catálogo de atualização. O acesso será negado quando a inscrição terminar.

Se um acesso ao catálogo de atualização for negado, aparecerá uma mensagem de aviso solicitando que você visite o SUSE Customer Center e verifique sua assinatura. O SUSE Customer Center está disponível em <https://scc.suse.com/> .



Nota: Configurações de firewall para receber atualizações

Por padrão, o firewall no SUSE Linux Enterprise Desktop bloqueia apenas as conexões de entrada. Se o seu sistema estiver protegido por outro firewall que bloqueia o tráfego de saída, permita conexões com <https://scc.suse.com/> e https://updates.suse.com nas portas 80 e 443 para receber atualizações.

O SUSE oferece atualizações com diferentes níveis de relevância:

Atualizações de segurança

Corrigem riscos graves à segurança e sempre devem ser instaladas.

Atualizações recomendadas

Corrigem problemas que podem comprometer o computador.

Atualizações opcionais

Corrigem problemas não relacionados à segurança ou aplicam melhorias.

7.1 Caixa de diálogo de atualização online

Para abrir a caixa de diálogo *Atualização Online* do YaST, inicie o YaST e selecione *Software > Atualização Online*. Se preferir, inicie-o usando a linha de comando **yast2 online_update**.

A janela *Atualização Online* é composta por quatro seções.

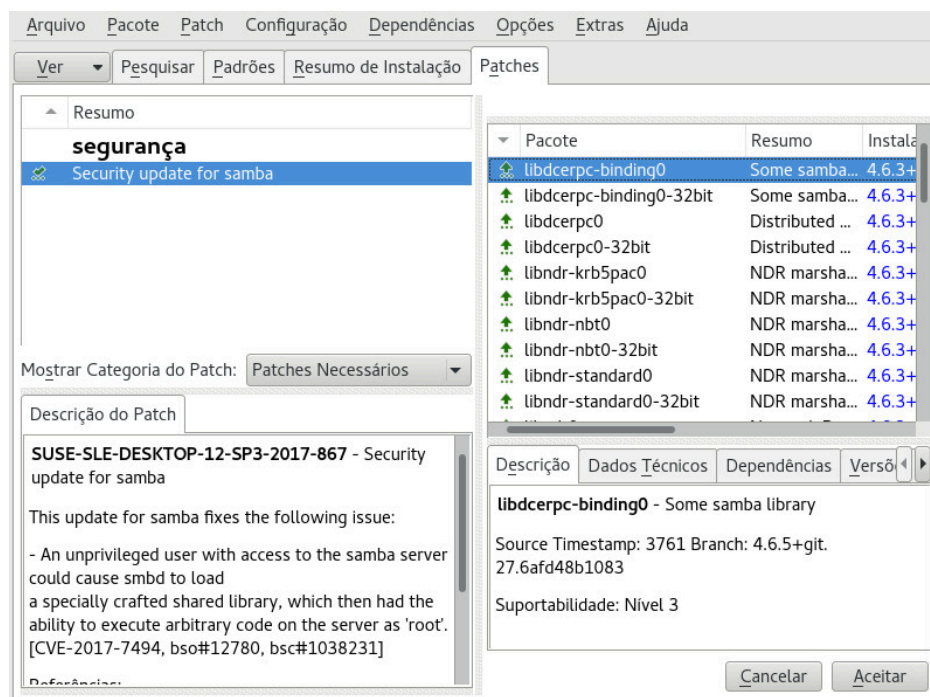


FIGURA 7.1: ATUALIZAÇÃO ONLINE DO YAST

A seção *Resumo* à esquerda lista os patches disponíveis para o SUSE Linux Enterprise Desktop. Os patches são classificados por relevância de segurança: segurança, recomendado e opcional. É possível mudar a tela da seção *Resumo* selecionando uma das seguintes opções em *Mostrar Categoria do Patch*:

Patches necessários (tela padrão)

Patches não instalados que se aplicam aos pacotes instalados no seu sistema.

Patches não necessários

Os patches que se aplicam a pacotes não instalados no seu sistema, ou patches com requisitos que já foram atendidos (porque os pacotes relevantes já foram atualizados de outra fonte).

Todos os patches

Todos os patches disponíveis para o SUSE Linux Enterprise Desktop.

Cada entrada da lista na seção *Resumo* consiste em um símbolo e no nome do patch. Para obter uma visão geral dos símbolos possíveis e seu significado, pressione **Shift + F1**. As ações exigidas pelos patches de *Segurança* e *Recomendados* são predefinidas automaticamente. Essas ações são *Instalar automaticamente*, *Atualizar automaticamente* e *Apagar automaticamente*.

Se você instalar um pacote atualizado de um repositório que não seja o repositório de atualização, os requisitos de um patch para esse pacote poderão ser atendidos com essa instalação. Nesse caso, uma marca de seleção é exibida na frente do resumo do patch. O patch ficará visível na lista até você marcá-lo para instalação. Na verdade, isso não instalará o patch (porque o pacote já está atualizado), mas o marcará como instalado.

Selecione uma entrada na seção *Resumo* para ver uma breve *Descrição do Patch* no canto inferior esquerdo da caixa de diálogo. A seção superior direita lista os pacotes incluídos no patch selecionado (um patch pode incluir vários pacotes). Clique em uma entrada na seção superior direita para ver os detalhes sobre o respectivo pacote que faz parte do patch.


7.2 Instalando patches

A caixa de diálogo Atualização Online do YaST permite instalar todos os patches disponíveis de uma vez ou selecionar manualmente os patches desejados. É possível também reverter os patches que foram aplicados ao sistema.

Por padrão, todos os novos patches (exceto os *opcionais*) disponíveis para o sistema já estão marcados para instalação. Eles serão aplicados automaticamente depois que você clicar em *Aceitar* ou *Aplicar*. Se um ou vários patches exigirem reinicialização do sistema, você será notificado sobre isso antes do início da instalação do patch. Você escolhe entre continuar a instalação dos patches selecionados, ignorar a instalação de todos os patches que precisam de reinicialização e instalar o restante ou voltar para a seleção manual de patch.

PROCEDIMENTO 7.1: APLICANDO PATCHES COM A ATUALIZAÇÃO ONLINE DO YAST

1. Inicie o YaST e selecione *Software > Atualização Online*.

2. Para aplicar automaticamente todos os patches novos (exceto os que são opcionais) atualmente disponíveis para seu sistema, clique em *Aplicar* ou *Aceitar*.
 3. Modifique primeiro a seleção dos patches que deseja aplicar:
 - a. Use os respectivos filtros e telas fornecidos pela interface. Para obter informações detalhadas, consulte a [Seção 7.1, “Caixa de diálogo de atualização online”](#).
 - b. Selecione ou anule a seleção dos patches de acordo com as suas necessidades e com a sua vontade, clicando o botão direito do mouse no patch e escolhendo a respectiva ação no menu de contexto.
-  **Importante: Sempre aplicar as atualizações de segurança**

Não anule a seleção de nenhum patch relacionado à segurança se não tiver um bom motivo para isso. Eles corrigem riscos graves à segurança e impedem que o sistema seja explorado.
- c. A maioria dos patches inclui atualizações para diversos pacotes. Para mudar as ações de pacotes únicos, clique o botão direito do mouse em um pacote na tela de pacotes e escolha uma ação.
 - d. Para confirmar sua seleção e aplicar os patches selecionados, clique em *Aplicar* ou *Aceitar*.
 4. Após o término da instalação, clique em *Concluir* para sair da *Atualização Online* do YaST. Seu sistema agora está atualizado.

7.3 Vendo os patches recolhidos

As atualizações de manutenção são cuidadosamente testadas para minimizar o risco de introdução de bug. Se ficar comprovado que um patch tem um bug, ele será automaticamente recolhido. Uma nova atualização (com um número de versão maior) é emitida para reverter o patch com bug, e qualquer outra instalação dele é bloqueada. Você pode ver os patches recolhidos e o histórico deles na guia *Classificação do pacote*.

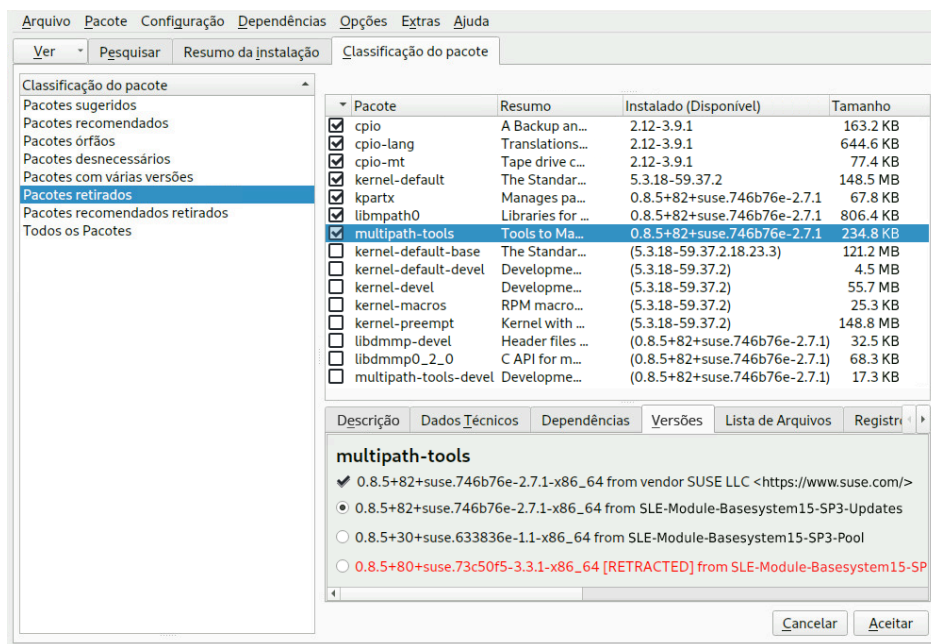


FIGURA 7.2: VENDO OS PATCHES RECOLHIDOS E O HISTÓRICO

7.4 Atualização online automática

Você pode configurar as atualizações automáticas com uma programação diária, semanal ou mensal ao usar o YaST. Instale o pacote `yast2-online-update-configuration`.

Por padrão, o download das atualizações é feito como RPMs delta. Como a reconstrução dos pacotes RPM com base nos RPMs delta é uma tarefa de uso intensivo de memória e de processador, determinadas instalações ou configurações de hardware podem exigir que você desabilite o uso de RPMs delta em benefício do desempenho.

Alguns patches, como atualizações do kernel ou pacotes que exigem contratos de licença, requerem a interação do usuário, o que pode parar o procedimento de atualização automática. É possível configurar uma opção para ignorar os patches que exigem interação do usuário.

Use a guia *Patches* no módulo *Software* do YaST para revisar os patches disponíveis e instalados, incluindo as referências a relatórios de bugs e boletins do CVE.

PROCEDIMENTO 7.2: CONFIGURANDO A ATUALIZAÇÃO ONLINE AUTOMÁTICA

1. Após a instalação, inicie o YaST e selecione *Software > Atualização Online*. Escolha *Configuração > Atualização Online*. Se o `yast2-online-update-configuration` não estiver instalado, você será solicitado a fazer isso.

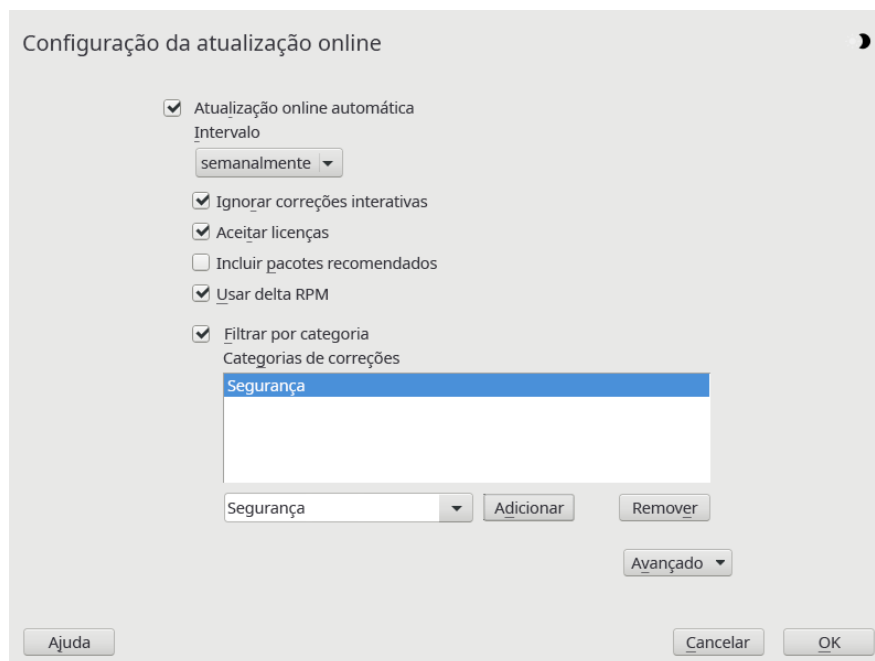


FIGURA 7.3: CONFIGURAÇÃO DA ATUALIZAÇÃO ONLINE DO YAST

Se preferir, inicie o módulo com `yast2 online_update_configuration` pela linha de comando.

- Escolha o intervalo de atualização: *Diariamente*, *Semanalmente* ou *Mensalmente*.
- Às vezes, os patches podem exigir a atenção do administrador, por exemplo, ao reiniciar serviços críticos. Por exemplo, pode se tratar de uma atualização do Docker Open Source Engine que exige a reinicialização de todos os containers. Antes da instalação desses patches, o usuário é informado a respeito das consequências e solicitado a confirmar a instalação deles. Esses patches são chamados de “Patches Interativos”.

Na instalação automática de patches, pressupõe-se que você tenha aceitado a instalação dos patches interativos. Se você preferir revisar esses patches antes da instalação, marque *Ignorar Patches Interativos*. Nesse caso, os patches interativos serão ignorados durante a aplicação automática. Certifique-se de executar uma atualização manual online periodicamente para verificar se os patches interativos estão aguardando para serem instalados.

- Para aceitar automaticamente qualquer contrato de licença, ative *Agree with Licenses* (Concordar com Licenças).
- Para instalar automaticamente todos os pacotes recomendados por pacotes atualizados, ative *Incluir Pacotes Recomendados*.

6. Para desabilitar o uso de RPMs delta (por questões de desempenho), desmarque *Usar RPMs Delta*.
7. Para filtrar os patches por categoria (como segurança ou recomendado), marque *Filtrar por Categoria* e adicione as categorias de patch apropriadas da lista. Apenas os patches das categorias selecionadas serão instalados. Convém habilitar apenas as atualizações automáticas de *Segurança* e revisar todas as outras manualmente. Em geral, a aplicação de patches é confiável, mas talvez você queira testar os patches que não são de segurança e voltá-los se tiver quaisquer problemas.
 - *Packagemanager e YaST* oferece patches para gerenciamento de pacote e recursos e módulos do YaST.
 - Os patches de *Segurança* fornecem atualizações e correções de bug essenciais.
 - Os patches *Recomendados* são correções de bug e aprimoramentos opcionais.
 - *Opcional* refere-se a novos pacotes.
 - *Outros* equivale a diversos.
 - *Documento* não é usado.
8. Clique em *OK* para confirmar sua configuração.

A atualização online automática não reinicia depois o sistema automaticamente. Se houver atualizações de pacotes que exijam reinicialização do sistema, você precisará fazer isso manualmente.

8 Instalando ou removendo software

Use a ferramenta de gerenciamento de software do YaST para pesquisar os componentes de software que deseja adicionar ou remover. O YaST resolve todas as dependências para você. Para instalar pacotes que não acompanham a mídia de instalação, adicione repositórios de software à configuração e deixe que o YaST os gerencie. Mantenha seu sistema atualizado gerenciando as atualizações de software com o applet de atualização.

Mude a coleção de softwares do seu sistema com o Gerenciador de Software do YaST. Esse módulo do YaST está disponível em dois tipos: uma variante gráfica para o X Window e uma variante baseada em texto para usar na linha de comando. O tipo gráfico está descrito aqui. Para saber detalhes do YaST baseado em texto, consulte o [Capítulo 4, YaST em modo de texto](#).



Nota: Confirmação e revisão das mudanças

Durante a instalação, atualização ou remoção de pacotes, qualquer mudança no Gerenciador de Software será aplicada apenas depois de clicar em *Aceitar* ou *Aplicar*. O YaST mantém uma lista com todas as ações, assim você pode revisar e fazer as mudanças antes de aplicá-las ao sistema.

8.1 Definição de termos

Os seguintes termos são importantes para entender a instalação e remoção do software no SUSE Linux Enterprise Desktop.

Repositório

Um diretório local ou remoto incluindo pacotes e informações adicionais sobre eles (metadados do pacote).

(Repositório) *ál*ias/nome do repositório

O nome abreviado do repositório (chamado de *Álias* no Zypper e o *Nome do Repositório* no YaST). Ele pode ser escolhido pelo usuário ao adicionar um repositório e deve ser exclusivo.

Arquivos de descrição de repositório

Cada repositório inclui arquivos que descrevem o conteúdo do repositório (nomes de pacotes, versões etc). O download desses arquivos de descrição de repositório é feito em um cache local usado pelo YaST.

Produto

Representa um produto completo, por exemplo, o SUSE® Linux Enterprise Desktop.

Padrão

Um padrão é um grupo instalável de pacotes dedicado a um fim específico. Por exemplo, o padrão Laptop inclui todos os pacotes necessários a um ambiente de computação móvel. Os padrões definem as dependências dos pacotes (como os pacotes necessários ou recomendados) e vêm com uma pré-seleção de pacotes marcados para instalação. Isso garante que os pacotes mais importantes necessários a determinado propósito fiquem disponíveis no sistema após a instalação do padrão. Se necessário, você poderá selecionar ou anular a seleção manualmente dos pacotes em um padrão.

Pacote

Um pacote é um arquivo compactado em formato rpm que inclui os arquivos de determinado programa.

Patch

Um patch consiste em um ou mais pacotes e pode ser aplicado por meio de RPMs delta. Ele também pode introduzir dependências nos pacotes que ainda não estão instalados.

Resolvível

Um termo genérico para produto, padrão, pacote ou patch. O tipo de resolvível usado com mais frequência é um pacote ou um patch.

RPM Delta

RPM Delta consiste apenas na diferença binária entre duas versões definidas de um pacote e, portanto, tem o menor tamanho de download. Antes de ser instalado, o pacote RPM completo é reconstruído na máquina local.

Dependências de pacotes

Determinados pacotes dependem de outros, como as bibliotecas compartilhadas. Em outros termos, o pacote pode exigir outros pacotes (se os pacotes necessários não estiverem disponíveis, o pacote não será instalado). Além das dependências (requisitos de pacotes)

que devem ser atendidas, alguns pacotes recomendam outros pacotes. Esses pacotes recomendados serão instalados apenas se estiverem realmente disponíveis; do contrário, eles serão ignorados e o pacote que os recomendou será instalado de qualquer maneira.

8.2 Registrando um sistema instalado

Se você ignorou o registro durante a instalação ou deseja registrar seu sistema novamente, pode registrá-lo a qualquer momento. Use o módulo *Registro de Produto* do YaST ou a ferramenta de linha de comando **SUSEConnect**.

8.2.1 Registrando no YaST

Para registrar o sistema, inicie o YaST e alterne para *Software* e *Registro de Produto*.

Por padrão, o sistema é registrado no SUSE Customer Center. Se a sua organização incluir servidores de registro locais, você poderá escolher um na lista de servidores detectados automaticamente ou inserir o URL manualmente.

8.2.2 Registrando no SUSEConnect

Para o registro por linha de comando, use o comando:

```
> sudo SUSEConnect -r REGISTRATION_CODE -e EMAIL_ADDRESS
```

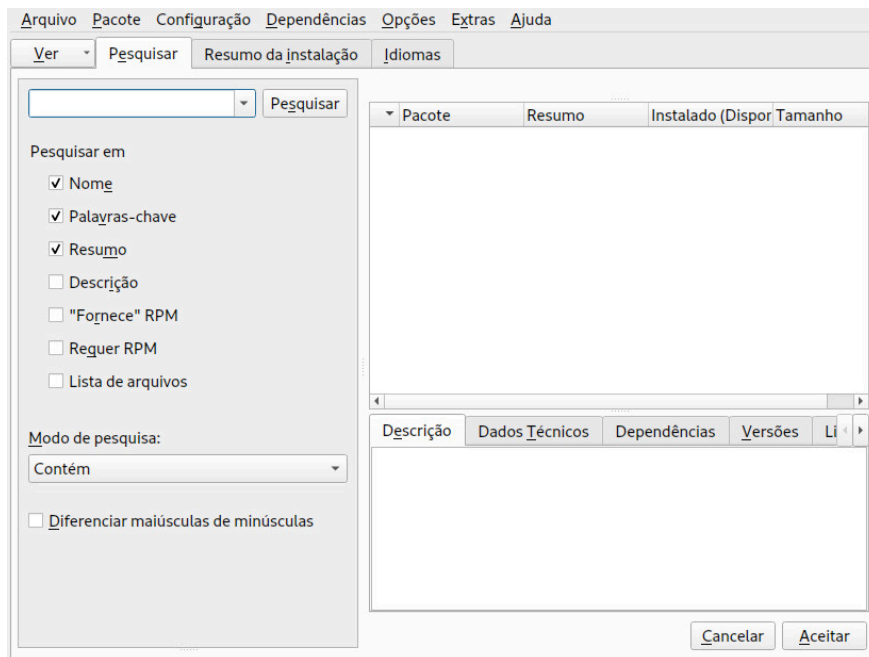
Substitua REGISTRATION_CODE pelo código de registro que você recebeu com a cópia do SUSE Linux Enterprise Desktop. Substitua EMAIL_ADDRESS pelo endereço de e-mail associado à conta do SUSE que você ou sua organização usa para gerenciar assinaturas.

Para o registro por um servidor de registro local, especifique também o URL para o servidor:

```
> sudo SUSEConnect -r REGISTRATION_CODE -e EMAIL_ADDRESS --url "URL"
```

8.3 Usando o gerenciador de software do YaST

Inicie o gerenciador de software do *Centro de Controle do YaST* escolhendo *Software* > *Gerenciamento de Software*.



8.3.1 Pesquisando software

O gerenciador de software do YaST pode instalar pacotes ou padrões de todos os repositórios habilitados. Ele oferece diferentes telas e filtros para facilitar a localização do software que está procurando. A tela *Pesquisar* é a tela padrão da janela. Para mudar a tela, clique em *Ver* e selecione uma das seguintes entradas na caixa suspensa. A tela selecionada é aberta em uma nova guia.

TELAS PARA PESQUISA DE PACOTES OU PADRÕES

Padrões

Lista todos os padrões disponíveis para instalação em seu sistema.

Grupos de Pacotes

Lista todos os pacotes classificados por grupos, como *Gráficos*, *Programação* ou *Segurança*.

Idiomas

Um filtro que lista todos os pacotes necessários para adicionar um novo idioma de sistema.

Repositórios

Um filtro que lista os pacotes por repositório. Para selecionar mais de um repositório, pressione e segure a tecla **Ctrl** e clique nos nomes dos repositórios. O “pseudo-repositório” *@System* lista todos os pacotes instalados.

Serviços

Mostra quais pacotes pertencem a um determinado módulo ou extensão. Selecione uma entrada (por exemplo, Basesystem ou High Availability) para exibir uma lista dos pacotes que pertencem a esse módulo ou extensão.

Pesquisar

Permite pesquisar um pacote de acordo com determinados critérios. Digite um termo de pesquisa e pressione **Enter**. Refine a sua pesquisa especificando o local para *Pesquisar em* e mudando o *Modo de Pesquisa*. Por exemplo, se você não sabe o nome do pacote, mas sabe o nome do aplicativo que está procurando, tente incluir a *Descrição* do pacote no processo de pesquisa.

Resumo da instalação

Caso já tenha selecionado os pacotes para instalação, atualização ou remoção, esta tela mostrará as mudanças que serão aplicadas ao sistema quando você clicar em *Aceitar*. Para filtrar os pacotes com determinado status nesta tela, ative ou desative as respectivas caixas de seleção. Pressione **Shift + F1** para ver os detalhes sobre os flags de status.



Dica: Encontrando pacotes que não pertencem a um repositório ativo

Para listar todos os pacotes que não pertencem a um repositório ativo, escolha *Ver > Repositórios > @System* e depois escolha *Filtro Secundário > Pacotes Não Mantidos*. Isso será útil, por exemplo, se você apagou um repositório e deseja saber se não restou nenhum pacote desse repositório instalado.



Dica: Pesquisando software online

O recurso de pesquisa online permite pesquisar pacotes em todos os módulos e extensões registrados e não registrados.

PROCEDIMENTO 8.1: PESQUISANDO SOFTWARE ONLINE

Para pesquisar pacotes de software online, execute as seguintes etapas:

1. Abra a janela de pesquisa online com *Extras > Pesquisar Online*.
2. Insira o *Nome do Pacote* e pressione **Enter** ou clique em *Pesquisar*. O YaST contata o SUSE Customer Center e mostra os resultados em uma tabela, incluindo o módulo ou a extensão de cada pacote. Selecione um pacote para ver detalhes adicionais.

3. Selecione um ou mais pacotes para instalação clicando na linha da tabela correspondente e em *Alternar Seleção*. Se preferir, clique duas vezes em uma linha. Se o pacote pertencer a um módulo ou extensão não registrado, o YaST solicitará uma confirmação para registrá-lo.
4. Clique em *Próximo*, revise as mudanças e instale os pacotes.

8.3.2 Instalando e removendo pacotes ou padrões

Determinados pacotes dependem de outros, como as bibliotecas compartilhadas. Por outro lado, alguns pacotes não podem coexistir com outros no sistema. Se possível, o YaST resolverá automaticamente as dependências ou conflitos. Se a sua escolha resultar em um conflito de dependência que não puder ser automaticamente resolvido, você precisará resolvê-lo manualmente, conforme descrito na [Seção 8.3.4, “Dependências de pacotes”](#).



Nota: Remoção de pacotes

Ao remover qualquer pacote, por padrão, o YaST só remove os pacotes selecionados. Para que o YaST remova também todos os outros pacotes que forem desnecessários após a remoção do pacote especificado, selecione *Opções > Limpar ao apagar pacotes* no menu principal.

1. Pesquise por pacotes conforme descrito na [Seção 8.3.1, “Pesquisando software”](#).
2. Os pacotes encontrados são listados no painel direito. Para instalar um pacote ou removê-lo, clique o botão direito do mouse nele e escolha *Instalar* ou *Apagar*. Se a opção relevante não estiver disponível, verifique o status do pacote indicado pelo símbolo que fica na frente do nome do pacote. Pressione **Shift + F1** para ver a Ajuda.



Dica: Aplicando uma ação a todos os pacotes da lista

Para aplicar uma ação a todos os pacotes listados no painel direito, vá para o menu principal e escolha uma ação em *Pacote > Tudo Nesta Lista*.

3. Para instalar um padrão, clique o botão direito do mouse no nome do padrão e escolha *Instalar*.

4. Não é possível remover um padrão. Em vez disso, selecione os pacotes do padrão que deseja remover e marque-os para remoção.
 5. Para selecionar mais pacotes, repita as etapas mencionadas anteriormente.
 6. Antes de aplicar as mudanças, você pode revisá-las ou modificá-las clicando em *Ver > Resumo de Instalação*. Por padrão, todos os pacotes com status modificado serão listados.
 7. Para reverter o status de um pacote, clique o botão direito do mouse no pacote e selecione uma das seguintes entradas: *Manter*, se o pacote foi programado para ser apagado ou atualizado, ou *Não Instalar*, se ele foi programado para instalação. Para abandonar todas as mudanças e sair do Gerenciador de Software, clique em *Cancelar e Abandonar*.
 8. Quando tiver concluído, clique em *Aceitar* para aplicar as mudanças.
 9. Se o YaST encontrar dependências em outros pacotes, será apresentada uma lista dos pacotes que foram escolhidos adicionalmente para instalação, atualização ou remoção. Clique em *Continuar* para aceitá-los.
- Após a instalação, atualização ou remoção de todos os pacotes selecionados, o Gerenciador de Software do YaST será fechado automaticamente.



Nota: Instalando pacotes de origem

Não é possível instalar pacotes de origem com o Gerenciador de Software do YaST. Use a ferramenta de linha de comando **zypper** para esse procedimento. Para obter mais informações, consulte a [Seção 9.1.3.5, “Instalando ou fazendo download dos pacotes de origem”](#).

8.3.3 Atualizando pacotes

Em vez de atualizar pacotes individuais, você pode também atualizar todos os pacotes instalados ou todos os pacotes de determinado repositório. Ao atualizar pacotes em massa, geralmente os seguintes aspectos são considerados:

- prioridades dos repositórios que fornecem o pacote,
- arquitetura do pacote (por exemplo, AMD64/Intel 64),

- número da versão do pacote,
- fornecedor do pacote.

O aspecto que tem a maior importância na escolha das atualizações candidatas depende da respectiva opção de atualização escolhida.

1. Para atualizar todos os pacotes instalados para a versão mais recente, escolha *Pacote > Todos os Pacotes > Atualizar se houver versão mais nova disponível* no menu principal. Todos os repositórios são marcados para as possíveis atualizações candidatas usando a seguinte política: o YaST primeiro tenta restringir a pesquisa aos pacotes com a mesma arquitetura e fornecedor do pacote instalado. Se a pesquisa for positiva, a “melhor” atualização candidata será selecionada de acordo com o processo a seguir. No entanto, se não for encontrado nenhum pacote comparativo do mesmo fornecedor, a pesquisa será expandida a todos os pacotes com a mesma arquitetura. Se ainda assim nenhum pacote comparativo for encontrado, todos os pacotes serão considerados e a “melhor” atualização candidata será selecionada de acordo com os seguintes critérios:

1. Prioridade do repositório: Preferência ao pacote do repositório que tem a prioridade mais alta.
2. Se esta seleção resultar em mais de um pacote, escolha o que tem a “melhor” arquitetura (melhor opção: correspondente à arquitetura do pacote instalado).

Se o pacote resultante tiver um número de versão maior do que o pacote instalado, o pacote instalado será atualizado e substituído pela atualização candidata selecionada. Essa opção tenta evitar as mudanças na arquitetura e no fornecedor dos pacotes instalados; porém, sob determinadas circunstâncias, elas serão toleradas.



Nota: Atualizar sempre

Se, em vez disso, você escolher *Pacote > Todos os Pacotes > Atualizar Sempre*, os mesmos critérios serão aplicados, mas o pacote candidato encontrado será sempre instalado. Portanto, essa opção pode levar à instalação de uma versão menos eficiente de alguns pacotes.

2. Para verificar se os pacotes de uma atualização em massa vêm de determinado repositório:
 - a. Escolha o repositório do qual será feita a atualização, conforme descrito na *Seção 8.3.1, “Pesquisando software”*.

- b. Na lateral direita da janela, clique em *Comutar pacotes do sistema para as versões neste repositório*. Isso permitirá explicitamente ao YaST mudar o fornecedor do pacote quando os pacotes forem substituídos.
Quando você clicar em *Aceitar* para prosseguir, todos os pacotes instalados serão substituídos pelos pacotes derivados desse repositório, se disponível. Isso pode levar a mudanças no fornecedor e na arquitetura e, até mesmo, à instalação de uma versão menos eficiente de alguns pacotes.
 - c. Para que isso não aconteça, clique em *Cancelar comutação de pacotes do sistema para versões no repositório*. Observe que você apenas pode cancelar essa opção antes de clicar no botão *Aceitar*.
3. Antes de aplicar as mudanças, você pode revisá-las ou modificá-las clicando em *Ver > Resumo de Instalação*. Por padrão, todos os pacotes que terão seu status modificado são listados.
 4. Se todas as opções forem definidas de acordo com a sua vontade, confirme as mudanças clicando em *Aceitar* para iniciar a atualização em massa.

8.3.4 Dependências de pacotes

A maioria dos pacotes é dependente de outros. Se um pacote, por exemplo, usa uma biblioteca compartilhada, ele é dependente do pacote que fornece essa biblioteca. Por outro lado, alguns pacotes não podem coexistir, gerando um conflito (por exemplo, só é possível instalar um agente de transferência de mensagens: sendmail ou postfix). Ao instalar ou remover software, o Gerenciador de Software verifica se não há dependências ou conflitos não resolvidos para assegurar a integridade do sistema.

Caso exista apenas uma solução para resolver uma dependência ou um conflito, eles serão resolvidos automaticamente. Várias soluções podem causar conflito que precisa ser resolvido manualmente. Se a solução de um conflito envolver mudança de fornecedor ou arquitetura, também será preciso resolver manualmente. Ao clicar em *Aceitar* para aplicar qualquer mudança no Gerenciador de Software, será exibida uma visão geral de todas as ações realizadas pelo resolver automático, que você precisará confirmar.

Por padrão, as dependências são verificadas automaticamente. A verificação é realizada sempre que você muda o status de um pacote (por exemplo, marcando o pacote para instalação ou remoção). Esse recurso em geral é útil, mas pode se tornar exaustivo quando um conflito

de dependência é resolvido manualmente. Para desabilitar esta função, vá para o menu principal e desative *Dependências > Verificar Automaticamente*. Faça a verificação manual de uma dependência clicando em *Dependências > Verificar Agora*. A verificação de consistência é sempre realizada quando você confirma sua seleção pelo botão *Aceitar*.

Para revisar as dependências de um pacote, clique o botão direito do mouse nele e escolha *Mostrar informações do solver*. Aparece um mapa mostrando as dependências. Os pacotes já instalados aparecem em um frame verde.



Nota: Resolvendo conflitos de pacotes manualmente

A menos que você tenha bastante experiência, siga as sugestões do YaST quanto à solução de conflitos de pacote; do contrário, talvez não seja possível resolvê-los. Lembre-se de que toda mudança feita pode gerar outros conflitos, portanto, portanto você pode acabar com um número crescente de conflitos. Se isso acontecer, você deverá *Cancelar* o Gerenciador de Software, *Abandonar* todas as mudanças e iniciar novamente.

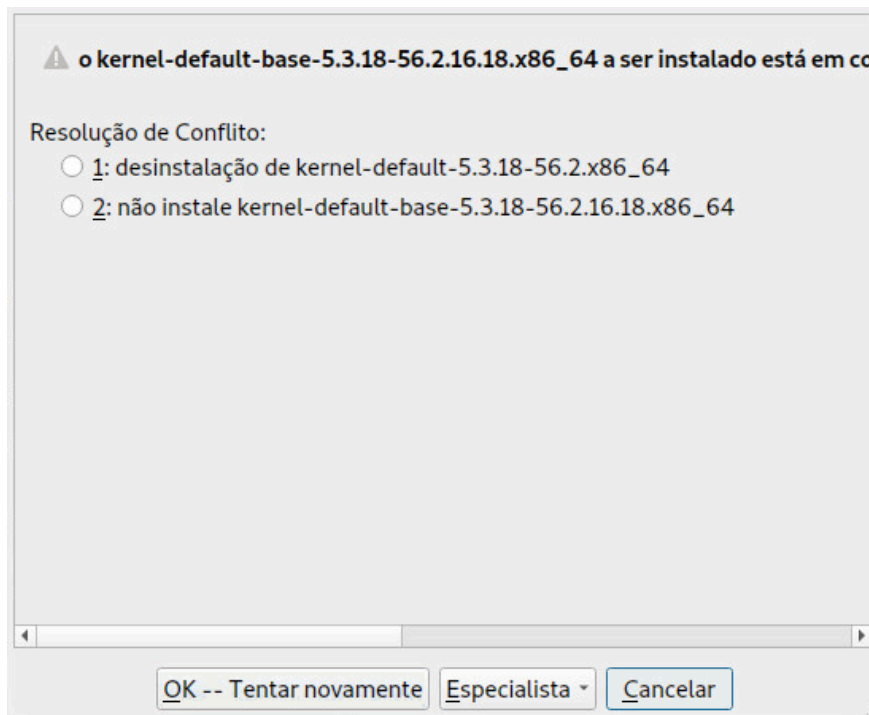


FIGURA 8.1: GERENCIAMENTO DE CONFLITOS DO GERENCIADOR DE SOFTWARE

8.3.5 Lidando com as recomendações de pacotes

Além das dependências fortes necessárias para executar um programa (por exemplo, uma determinada biblioteca), um pacote também pode ter dependências fracas, que agregam funcionalidades extras ou traduções, por exemplo. Essas dependências fracas são chamadas de recomendações de pacote.

Ao instalar um novo pacote, os pacotes recomendados ainda são instalados por padrão. Ao atualizar um pacote existente, as recomendações ausentes não serão instaladas automaticamente. Para mudar isso, defina `PKGMR_RECOMMENDED="yes"` em `/etc/sysconfig/yast2`. Para instalar todas as recomendações ausentes dos pacotes já instalados, inicie o *YaST > Gerenciador de Software* e escolha *Extras > Install All Matching Recommended Packages* (Instalar Todos os Pacotes Recomendados Correspondentes).

Para desabilitar a instalação dos pacotes recomendados ao instalar novos pacotes, desative *Dependências > Instalar Pacotes Recomendados* no Gerenciador de Software do YaST. Ao usar a ferramenta de linha de comando Zypper para instalar pacotes, use a opção `--no-recommends`.

8.4 Gerenciando repositórios de software e serviços

Para instalar software de terceiros, adicione repositórios de software ao sistema. Por padrão, os repositórios de produto, como o DVD do SUSE Linux Enterprise Desktop 15 SP4, e um repositório de atualização correspondente serão automaticamente configurados depois que você registrar seu sistema. Para obter mais informações sobre registro, consulte a *Livro "Deployment Guide", Capítulo 4 "Installation steps", Seção 4.6 "Registration"* ou a *Livro "Upgrade Guide", Capítulo 4 "Upgrading offline", Seção 4.7 "Registering your system"*. Dependendo do produto selecionado no início, um outro repositório com traduções, dicionários etc. também pode ser configurado.

Para gerenciar repositórios, inicie o YaST e selecione *Software > Repositórios de Software*. A caixa de diálogo *Repositórios de Software Configurados* é aberta. Nela, é possível também gerenciar inscrições aos chamados *Serviços*, mudando a opção *Ver* no canto direito da caixa de diálogo para *Todos os Serviços*. Nesse contexto, um Serviço é um RIS (*Serviço de Índice de Repositório*) que pode oferecer um ou mais repositórios de software. Ele pode ser mudado dinamicamente por seu administrador ou fornecedor.

Cada repositório inclui arquivos que descrevem o conteúdo do repositório (nomes de pacotes, versões etc). O download desses arquivos de descrição de repositório é feito em um cache local usado pelo YaST. Para assegurar a integridade, os repositórios de software podem ser assinados com a chave GPG do mantenedor do repositório. Sempre que você adicionar um novo repositório, o YaST oferecerá a opção de importar sua chave.



Atenção: Confiando em fontes de software externas

Antes de adicionar repositórios de software externos à sua lista de repositórios, verifique se é possível confiar nesse repositório. A SUSE não se responsabiliza por nenhum problema resultante da instalação do software de repositórios de software de terceiros.

8.4.1 Adicionando repositórios de software

Você pode adicionar repositórios de DVD/CD, unidade flash USB, diretório local, imagem ISO ou fonte de rede.

Para adicionar repositórios da caixa de diálogo *Repositórios de Software Configurados* no YaST, faça o seguinte:

1. Clique em *Adicionar*.

2. Selecione uma das opções listadas na caixa de diálogo:



FIGURA 8.2: ADICIONANDO UM REPOSITÓRIO DE SOFTWARE

- Para explorar a rede em busca de servidores de instalação que anunciam seus serviços por SLP, selecione *Explorar usando SLP* e clique em *Próximo*.
- Para adicionar um repositório de uma mídia removível, escolha a opção relevante e insira a mídia ou conecte o dispositivo USB na máquina, respectivamente. Clique em *Próximo* para iniciar a instalação.
- Na maioria dos repositórios, será solicitado para você especificar o caminho (ou URL) para a mídia após selecionar a respectiva opção e clicar em *Próximo*. A especificação do *Nome do Repositório* é opcional. Se nada for especificado, o YaST usará o nome do produto ou o URL como nome do repositório.

A opção *Baixar os arquivos de descrição do repositório* está ativada por padrão. Se você desativá-la, o YaST fará download dos arquivos automaticamente mais tarde, se necessário.

3. Dependendo do repositório adicionado, talvez seja solicitado que você importe a chave GPG do repositório ou concorde com a licença.

Após confirmar as mensagens, o YaST fará download e analisará os metadados. Ele adicionará o repositório à lista de *Repositórios Configurados*.

4. Se necessário, ajuste as *Propriedades* do repositório conforme descrito na [Seção 8.4.2, “Gerenciando as propriedades do repositório”](#).
5. Clique em *OK* para confirmar as mudanças e fechar a caixa de diálogo de configuração.
6. Depois que o repositório for adicionado com êxito, o gerenciador de software será iniciado e você poderá instalar pacotes desse repositório. Para obter informações detalhadas, consulte o [Capítulo 8, Instalando ou removendo software](#).

8.4.2 Gerenciando as propriedades do repositório

A visão geral *Repositórios de Software Configurados* de *Repositórios de Software* permite mudar as seguintes propriedades de repositório:

Status

O status do repositório pode ser *Habilitado* ou *Desabilitado*. É possível instalar apenas pacotes de repositórios habilitados. Para desativar um repositório temporariamente, selecione-o e desmarque *Habilitar*. É possível também clicar duas vezes no nome do repositório para alternar seu status. Para remover completamente um repositório, clique em *Apagar*.

Atualizar

Ao atualizar um repositório, o download da descrição do conteúdo dele (nomes de pacotes, versões etc.) é feito em um cache local que é usado pelo YaST. É suficiente fazer isso uma vez para repositórios estáticos, como CDs ou DVDs. Já os repositórios que têm seu conteúdo modificado com frequência devem sempre ser atualizados. A maneira mais fácil de manter o cache de um repositório atualizado é usando a opção *Atualizar Automaticamente*. Para fazer a atualização manual, clique em *Atualizar* e selecione uma das opções.

Manter os Pacotes Baixados

Os pacotes de repositórios remotos são descarregados antes de serem instalados. Por padrão, eles são apagados após instalação bem-sucedida. A ativação da opção *Manter os Pacotes Baixados* impede a exclusão dos pacotes descarregados. O local do download está configurado em `/etc/zypp/zypp.conf`; por padrão, é `/var/cache/zypp/packages`.

Prioridade

A *Prioridade* de um repositório é um valor entre 1 e 200, sendo 1 a prioridade mais alta e 200 a prioridade mais baixa. Qualquer repositório novo adicionado pelo YaST recebe a prioridade 99, por padrão. Se não for importante o valor da prioridade de

determinado repositório, você poderá também definir o valor como `0` para aplicar a prioridade padrão ao repositório (`99`). Se um pacote estiver disponível em mais de um repositório, o repositório com a prioridade mais alta terá preferência. Isso é útil para evitar o download desnecessário de pacotes da Internet, pois concede ao repositório local (por exemplo, um DVD) uma prioridade maior.



Importante: Prioridade em comparação com a versão

O repositório com a prioridade mais alta tem preferência em qualquer situação. Portanto, verifique se o repositório de atualização sempre tem a prioridade mais alta; do contrário, você poderá instalar uma versão desatualizada que não será atualizada até a próxima atualização online.

Nome e URL

Para mudar o nome de um repositório ou seu URL, selecione-o na lista com um clique único e depois clique em *Editar*.

8.4.3 Gerenciando chaves de repositório

Para assegurar a integridade, os repositórios de software podem ser assinados com a chave GPG do mantenedor do repositório. Sempre que você adicionar um novo repositório, o YaST oferecerá para importar sua chave. Verifique isso da mesma forma que faz com qualquer outra chave GPG e confirme se ela não foi modificada. Se detectar uma mudança na chave, algo pode ter acontecido de errado no repositório. Desabilite o repositório como fonte de instalação até que você descubra a causa da modificação na chave.

Para gerenciar todas as chaves importadas, clique em *Chaves GPG* na caixa de diálogo *Repositórios de Software Configurados*. Selecione uma entrada com o mouse para mostrar as propriedades da chave na parte inferior da janela. *Adicione*, *Edite* ou *Apague* as chaves com um clique nos respectivos botões.

8.5 Atualizador de pacotes do GNOME

A SUSE oferece um fluxo contínuo de patches e atualizações de segurança de software para o seu produto. Eles podem ser instalados usando as ferramentas disponíveis com seu desktop ou executando o módulo de *Atualização online do YaST*. Esta seção descreve como atualizar o sistema da área de trabalho do GNOME usando o *Atualizador de Pacotes*.

Diferentemente do módulo Atualização Online do YaST, o *Atualizador de Pacotes* do GNOME não apenas oferece a instalação de patches dos repositórios de atualização, como também novas versões dos pacotes que já estão instalados. (Os patches corrigem problemas de segurança ou falhas. O número da versão e a funcionalidade geralmente não são modificados. As novas versões de um pacote incrementam o número da versão e, geralmente, adicionam funcionalidade ou incluem mudanças importantes.)

Sempre que houver novos patches ou atualizações de pacote disponíveis, o GNOME mostrará uma notificação na área de notificação ou na tela de bloqueio.

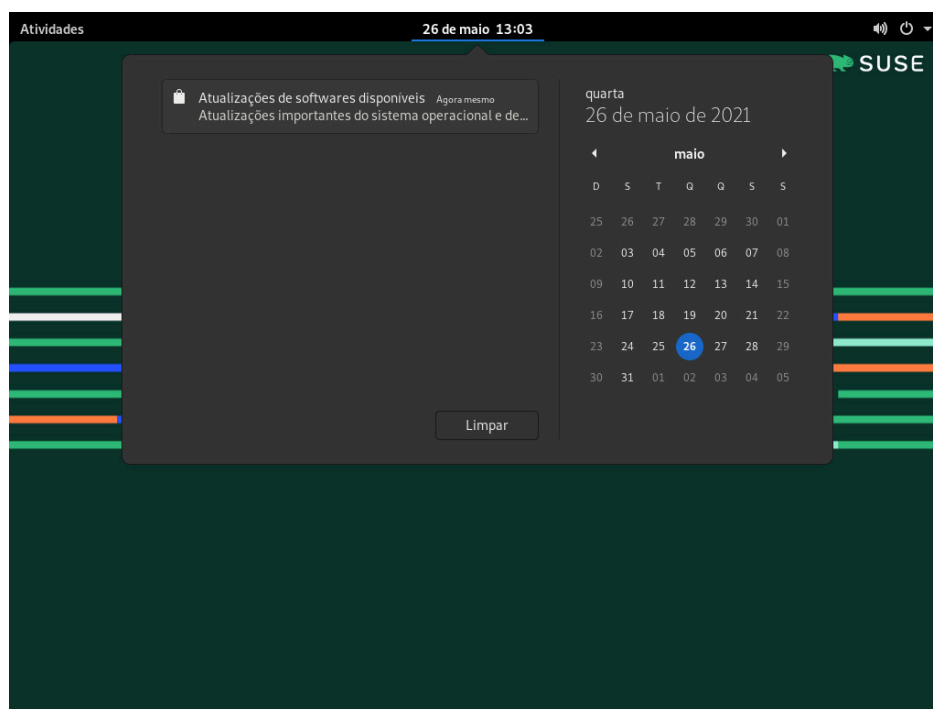
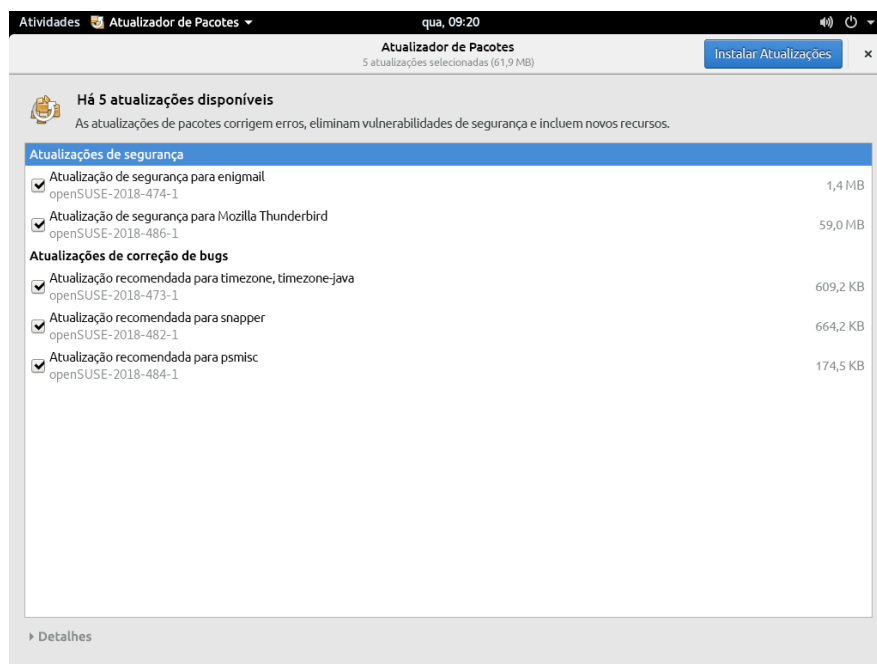


FIGURA 8.3: NOTIFICAÇÃO DE ATUALIZAÇÃO NA ÁREA DE TRABALHO DO GNOME

Para definir as configurações de notificação para o *Atualizador de Pacotes*, inicie as *Configurações* do GNOME e escolha *Notificações* > *Atualizador de Pacotes*.

1. Para instalar patches e atualizações, clique na mensagem de notificação. Esse procedimento abre o *Atualizador de Pacotes* do GNOME. Se preferir, abra o atualizador em *Atividades* digitando Atualizador de P e escolhendo *Atualizador de Pacotes*.



2. As atualizações são classificadas em quatro categorias:

Atualizações de segurança (patches)

Corrigem riscos graves à segurança e sempre devem ser instaladas.

Atualizações recomendadas (patches)

Corrigem problemas que podem comprometer o computador. É altamente recomendável instalá-las.

Atualizações opcionais (patches)

Corrigem problemas não relacionados à segurança ou aplicam melhorias.

Outras atualizações

Novas versões dos pacotes que estão instalados.

Todas as atualizações disponíveis estão pré-selecionadas para instalação. Se você não deseja instalar todas as atualizações, primeiro anule a seleção das atualizações indesejadas. É altamente recomendável sempre instalar todas as atualizações de segurança e recomendadas.

Para obter informações detalhadas sobre uma atualização, clique no título dela e depois em *Detalhes*. As informações serão exibidas em uma caixa abaixo da lista de pacotes.

3. Clique em *Instalar Atualizações* para iniciar a instalação.
4. Algumas atualizações podem exigir a reinicialização da máquina ou o logout. Leia a mensagem exibida após a instalação para obter instruções.

8.6 Atualizando pacotes com o *GNOME Software*

Além do *Atualizador de Pacotes*, o GNOME inclui o *GNOME Software*, que oferece as seguintes funcionalidades:

- Instalar, atualizar e remover software fornecido como um RPM por meio do PackageKit
- Instalar, atualizar e remover software fornecido como um Flatpak
- Instalar, atualizar e remover extensões de shell do GNOME (<https://extensions.gnome.org> ↗)
- Atualizar o firmware para dispositivos de hardware usando o *Linux Vendor Firmware Service* (LVFS: <https://fwupd.org> ↗)

Além disso, o *GNOME Software* oferece instantâneos, classificações e análises do software.

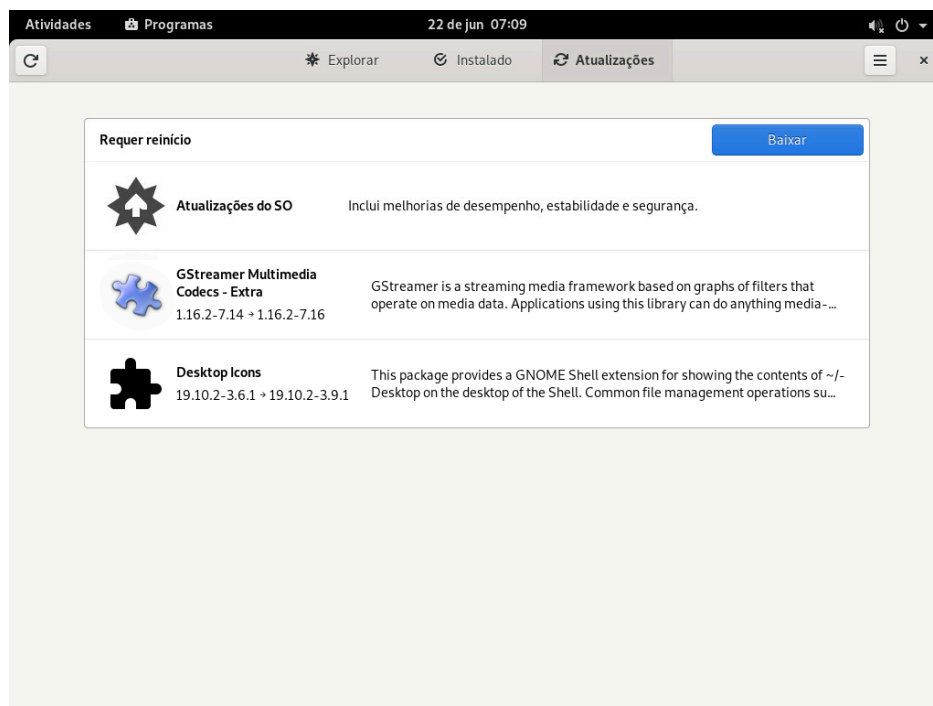


FIGURA 8.4: *GNOME SOFTWARE: TELA ATUALIZAÇÕES*

Veja a seguir as diferenças entre o *GNOME Software* e as outras ferramentas fornecidas no SUSE Linux Enterprise Desktop:

- Diferentemente do YaST ou do Zypper, para a instalação de software incluído em pacote como um RPM, o *GNOME Software* se restringe ao software que fornece metadados do AppStream. Isso inclui a maioria dos aplicativos da área de serviço.
- O *Atualizador de Pacotes* do GNOME atualiza os pacotes no sistema em execução (o que força você a reiniciar os respectivos aplicativos), já o *GNOME Software* faz download das atualizações, mas as aplica apenas na próxima reinicialização do sistema.

9 Gerenciando software com ferramentas de linha de comando

Este capítulo descreve o Zypper e o RPM, duas ferramentas de linha de comando para gerenciar software. Para obter a definição da terminologia usada neste contexto (por exemplo, repositório, patch ou atualização), consulte a [Seção 8.1, “Definição de termos”](#).

9.1 Usando o zypper

Zypper é um gerenciador de pacote de linha de comando para instalação, atualização e remoção de pacotes. Ele também gerencia repositórios. Ele é especialmente útil para realizar tarefas de gerenciamento remoto de software ou gerenciar software de scripts de shell.

9.1.1 Uso geral

A sintaxe geral do zypper é:

```
zypper [--global-options] COMMAND [--command-options] [arguments]
```

Os componentes entre colchetes não são obrigatórios. Consulte **zypper help** para obter uma lista de opções gerais e todos os comandos. Para obter ajuda sobre determinado comando, digite **zypper help** COMANDO.

Comandos do Zypper

A maneira mais simples de executar o zypper é digitar seu nome seguido de um comando. Por exemplo, para aplicar todos os patches necessários ao sistema, use:

```
> sudo zypper patch
```

Opções globais

Você também pode escolher dentre uma ou mais opções globais, digitando-as logo antes do comando:

```
> sudo zypper --non-interactive patch
```

No exemplo acima, a opção `--non-interactive` significa que o comando é executado sem perguntar nada (aplicando as respostas padrão automaticamente).

Opções específicas do comando

Para usar as opções específicas de determinado comando, digite-as logo após o comando:

```
> sudo zypper patch --auto-agree-with-licenses
```

No exemplo acima, a opção `--auto-agree-with-licenses` é usada para aplicar todos os patches necessários a um sistema sem que você precise confirmar todas as licenças. Em vez disso, a licença é aceita automaticamente.

Argumentos

Alguns comandos requerem um ou mais argumentos. Por exemplo, ao usar o comando `install`, você precisa especificar qual pacote (ou pacotes) deseja *instalar*:

```
> sudo zypper install mplayer
```

Algumas opções também requerem um único argumento. O comando a seguir lista todos os padrões conhecidos:

```
> zypper search -t pattern
```

Você pode combinar todos os anteriores. Por exemplo, o comando a seguir instala os pacotes `mc` e `vim` do repositório `factory` durante o modo verboso:

```
> sudo zypper -v install --from factory mc vim
```

A opção `--from` mantém todos os repositórios habilitados (para resolução de dependências) enquanto solicita o pacote do repositório especificado. `--repo` é um alias para `--from`, e você pode usar qualquer um dos dois.

Quase todos os comandos zypper possuem uma opção `dry-run` que simula o comando indicado. Ela pode ser usada para fins de teste.

```
> sudo zypper remove --dry-run MozillaFirefox
```

O Zypper suporta a opção global `--userdata STRING`. É possível especificar uma string com essa opção, que é gravada nos arquivos de registro e plug-ins do Zypper (como o plug-in Btrfs). Ela pode ser usada para marcar e identificar transações nos arquivos de registro.

```
> sudo zypper --userdata STRING patch
```

9.1.2 Usando os subcomandos do Zypper

Os subcomandos do Zypper são executáveis armazenados no diretório especificado pela opção de configuração `zypper_execdir`. Por padrão, ele é `/usr/lib/zypper/commands`. Se um subcomando não for encontrado nesse local, o Zypper pesquisará por ele automaticamente no restante dos locais `$PATH`. Esse procedimento permite criar suas próprias extensões locais e armazená-las no espaço do usuário.

A execução de subcomandos no shell do Zypper e o uso das opções globais do Zypper não são suportados.

Listar os subcomandos disponíveis:

```
> zypper help subcommand
[...]
Available zypper subcommands in '/usr/lib/zypper/commands'

  appstream-cache
  lifecycle
  migration
  search-packages

Zypper subcommands available from elsewhere on your $PATH

  log                      Zypper logfile reader
                           (/usr/sbin/zypper-log)
```

Exibir a tela de Ajuda de um subcomando:

```
> zypper help appstream-cache
```

9.1.3 Instalando e removendo software com o Zypper

Para instalar ou remover pacotes, use os seguintes comandos:

```
> sudo zypper install PACKAGE_NAME
> sudo zypper remove PACKAGE_NAME
```



Atenção: Não remova os pacotes obrigatórios do sistema

Não remova pacotes obrigatórios do sistema, como `glibc`, `zypper` e `kernel`. Se eles forem removidos, o sistema poderá ficar instável ou parar de funcionar completamente.

9.1.3.1 Selecionando os pacotes para instalar ou remover

Há várias maneiras de resolver pacotes com os comandos `zypper install` e `zypper remove`.

Pelo nome exato do pacote

```
> sudo zypper install MozillaFirefox
```

Pelo nome exato do pacote e número da versão

```
> sudo zypper install MozillaFirefox-52.2
```

Pelo alias do repositório e pelo nome do pacote

```
> sudo zypper install mozilla:MozillaFirefox
```

onde `mozilla` é o alias do repositório do qual instalar.

Pelo nome do pacote usando curingas

Você pode selecionar todos os pacotes que tenham nomes iniciando ou terminando com determinada string. Use os curingas com cuidado, principalmente ao remover pacotes. O comando a seguir instala todos os pacotes que começam com “Moz”:

```
> sudo zypper install 'Moz*'
```



Dica: Removendo todos os pacotes -debuginfo

Ao depurar um problema, às vezes você precisa instalar temporariamente muitos pacotes `-debuginfo`, que apresentam mais informações sobre a execução dos processos. Depois que a sessão de depuração termina, e você precisa limpar o ambiente, execute o seguinte:

```
> sudo zypper remove '*-debuginfo'
```

Por recurso

Por exemplo, para instalar um pacote sem saber o nome dele, há recursos que são úteis. O comando a seguir instalará o pacote `MozillaFirefox`:

```
> sudo zypper install firefox
```

Por recurso, arquitetura de hardware ou versão

Juntamente com um recurso, você pode especificar uma arquitetura de hardware e uma versão:

- O nome da arquitetura de hardware desejada é anexado ao recurso após um ponto final. Por exemplo, para especificar as arquiteturas AMD64/Intel 64 (que no Zypper é denominada `x86_64`), use:

```
> sudo zypper install 'firefox.x86_64'
```

- As versões devem ser anexadas ao fim da string e precedidas por um operador: `<` (menor do que), `<=` (menor do que ou igual a), `=` (igual a), `>=` (maior do que ou igual a), `>` (maior do que).

```
> sudo zypper install 'firefox>=74.2'
```

- Você também pode combinar um requisito de versão e arquitetura de hardware:

```
> sudo zypper install 'firefox.x86_64>=74.2'
```

Por caminho para o arquivo RPM

Você também pode especificar um local ou caminho remoto para um pacote:

```
> sudo zypper install /tmp/install/MozillaFirefox.rpm
> sudo zypper install http://download.example.com/MozillaFirefox.rpm
```

9.1.3.2 Combinando a instalação e a remoção de pacotes

Para instalar e remover pacotes simultaneamente, use os modificadores `+/-`. Para instalar o `emacs` e remover o `vim` simultaneamente, use:

```
> sudo zypper install emacs -vim
```

Para remover o `emacs` e instalar o `vim` simultaneamente, use:

```
> sudo zypper remove emacs +vim
```

Para impedir que o nome do pacote iniciado por `-` seja interpretado como uma opção de comando, use-o sempre como segundo argumento. Se isso não for possível, preceda-o com `--`:

```
> sudo zypper install -emacs +vim      # Wrong
```

```
> sudo zypper install vim -emacs      # Correct
> sudo zypper install -- -emacs +vim  # Correct
> sudo zypper remove emacs +vim      # Correct
```

9.1.3.3 Limpando as dependências dos pacotes removidos

Para (com determinado pacote) remover automaticamente qualquer pacote desnecessário após remover o pacote especificado, use a opção `--clean-deps`:

```
> sudo zypper rm --clean-deps PACKAGE_NAME
```

9.1.3.4 Usando o Zypper em scripts

Por padrão, o zypper solicita uma confirmação antes de instalar ou remover um pacote selecionado, ou quando ocorre um problema. Você pode anular esse comportamento usando a opção `--non-interactive`. Essa opção deve ser inserida antes do comando real (**`install`**, **`remove`** e **`patch`**), conforme mostrado a seguir:

```
> sudo zypper --non-interactive install PACKAGE_NAME
```

Essa opção permite o uso do zypper em scripts e tarefas cron.

9.1.3.5 Instalando ou fazendo download dos pacotes de origem

Para instalar o pacote de origem correspondente de um pacote, use:

```
> zypper source-install PACKAGE_NAME
```

Quando executados como `root`, o local padrão para instalar pacotes de origem é `/usr/src/packages/` e `~/rpmbuild`, quando executados como usuário. Esses valores podem ser mudados em sua configuração de **`rpm`** local.

Esse comando também instala as dependências de compilação do pacote especificado. Se não quiser isso, adicione o switch `-D`:

```
> sudo zypper source-install -D PACKAGE_NAME
```

Para instalar apenas as dependências de compilação, use `-d`.

```
> sudo zypper source-install -d PACKAGE_NAME
```

Naturalmente isso só funcionará se o repositório com os pacotes de origem estiver habilitado na sua lista de repositórios (ele é adicionado por padrão, mas não habilitado). Consulte a [Seção 9.1.6, “Gerenciando repositórios com o Zypper”](#) para obter os detalhes sobre o gerenciamento de repositórios.

Uma lista de todos os pacotes de origem disponíveis nos seus repositórios pode ser obtida com:

```
> zypper search -t srcpackage
```

É possível também fazer download dos pacotes de origem para todos os pacotes instalados em um diretório local. Para fazer download dos pacotes de origem, use:

```
> zypper source-download
```

O diretório de download padrão é `/var/cache/zypper/source-download`. Você pode mudá-lo usando a opção `--directory`. Para mostrar apenas os pacotes ausentes ou incorretos sem fazer download nem apagar nada, use a opção `--status`. Para apagar pacotes de origem incorretos, use a opção `--delete`. Para desabilitar a exclusão, use a opção `--no-delete`.

9.1.3.6 Instalando pacotes de repositórios desabilitados

Normalmente, você apenas pode instalar ou atualizar pacotes de repositórios habilitados. A opção `--plus-content TAG` ajuda você a especificar os repositórios que devem ser atualizados, temporariamente habilitados durante a sessão atual do Zypper e desabilitados após sua conclusão.

Por exemplo, para habilitar os repositórios que podem fornecer pacotes `-debuginfo` ou `-debugsource` adicionais, use `--plus-content debug`. É possível especificar essa opção várias vezes.

Para habilitar temporariamente esses repositórios de "depuração" para instalar determinado pacote `-debuginfo`, use a opção da seguinte forma:

```
> sudo zypper --plus-content debug \  
install "debuginfo(build-id)=eb844a5c20c70a59fc693cd1061f851fb7d046f4"
```

A string `build-id` é informada pelo `gdb` a respeito dos pacotes `debuginfo` ausentes.



Nota: Mídia de instalação desabilitada

Os repositórios da mídia de instalação do SUSE Linux Enterprise Desktop ainda estão configurados, mas são desabilitados após a instalação bem-sucedida. Você pode usar a opção `--plus-content` para instalar pacotes da mídia de instalação, em vez dos repositórios online. Antes de chamar o **zypper**, verifique se a mídia está disponível, por exemplo, inserindo o DVD na unidade do computador.

9.1.3.7 Utilitários

Para verificar se todas as dependências ainda são atendidas e para reparar dependências ausentes, use:

```
> zypper verify
```

Além das dependências que precisam ser atendidas, alguns pacotes “recomendam” outros pacotes. Esses pacotes recomendados são instalados apenas quando estão realmente disponíveis e são instaláveis. Caso os pacotes recomendados fiquem disponíveis após a instalação do pacote que os recomendou (adicionando outros pacotes ou hardware), use o seguinte comando:

```
> sudo zypper install-new-recommends
```

Esse comando será muito útil após conectar uma webcam ou um dispositivo Wi-Fi. Ele instala drivers para o dispositivo e software relacionado, se disponíveis. Os drivers e o software relacionado serão instaláveis se determinadas dependências de hardware forem atendidas.

9.1.4 Atualizando software com o zypper

Existem três maneiras diferentes de atualizar o software usando o zypper: instalando patches, instalando uma versão nova de um pacote ou atualizando a distribuição inteira. Para a segunda opção, use o comando **zypper dist-upgrade**. O upgrade do SUSE Linux Enterprise Desktop é abordado no *Livro “Upgrade Guide”, Capítulo 1 “Upgrade paths and methods”*.

9.1.4.1 Instalando todos os patches necessários

A *Aplicação de patches* do SUSE Linux Enterprise é a maneira mais confiável de instalar novas versões de pacotes instalados. Ela garante que todos os pacotes necessários com as versões corretas sejam instalados e que as versões dos pacotes consideradas *conflitantes* sejam omitidas.

Para instalar todos os patches lançados oficialmente que se aplicam ao seu sistema, execute:

```
> sudo zypper patch
```

Todos os patches disponíveis dos repositórios configurados em seu computador são verificados quanto à relevância em sua instalação. Se eles forem relevantes (e não classificados como opcional ou recurso), eles serão instalados imediatamente. Se o **zypper patch** for bem-sucedido, nenhum pacote com versão vulnerável será instalado, a menos que você confirme a exceção. Observe que o repositório de atualização oficial apenas estará disponível após o registro de sua instalação do SUSE Linux Enterprise Desktop.

Se um patch que estiver prestes a ser instalado incluir mudanças que exijam reinicialização do sistema, você será avisado antes.

O comando **zypper patch** simples não se aplica a patches de repositórios de terceiros. Para atualizar também os repositórios de terceiros, use a opção de comando with-update da seguinte maneira:

```
> sudo zypper patch --with-update
```

Para instalar também os patches opcionais, use:

```
> sudo zypper patch --with-optional
```

Para instalar todos os patches referentes a um problema específico do Bugzilla, use:

```
> sudo zypper patch --bugzilla=NUMBER
```

Para instalar todos os patches referentes a uma entrada específica do banco de dados CVE, use:

```
> sudo zypper patch --cve=NUMBER
```

Por exemplo, para instalar um patch de segurança com o número do CVE CVE-2010-2713, execute:

```
> sudo zypper patch --cve=CVE-2010-2713
```

Para instalar apenas os patches que afetam o Zypper e o gerenciamento de pacote propriamente dito, use:

```
> sudo zypper patch --updatestack-only
```

Esteja ciente de que outras opções de comando que também atualizam outros repositórios serão descartadas se você usar a opção de comando updatestack-only.

9.1.4.2 Listando os patches

Para saber se há patches disponíveis, o Zypper permite ver as seguintes informações:

Número de patches necessários

Para listar o número de patches necessários (patches que se aplicam ao seu sistema, mas ainda não foram instalados), use **patch-check**:

```
> zypper patch-check
Loading repository data...
Reading installed packages...
5 patches needed (1 security patch)
```

Esse comando pode ser combinado com a opção **--updatestack-only** para listar apenas os patches que afetam o Zypper e o gerenciamento de pacote propriamente dito.

Lista de patches necessários

Para listar todos os patches necessários (patches que se aplicam ao seu sistema, mas ainda não foram instalados), use **zypper list-patches**.

Lista de todos os patches

Para listar todos os patches disponíveis para o SUSE Linux Enterprise Desktop, independentemente de já estarem instalados ou de se aplicarem à sua instalação, use **zypper patches**.

Também é possível listar e instalar todos os patches relevantes a problemas específicos. Para listar patches específicos, use o comando **zypper list-patches** com as seguintes opções:

Por problemas do Bugzilla

Para listar todos os patches necessários relacionados a problemas do Bugzilla, use a opção **--bugzilla**.

Para listar os patches referentes a um bug específico, você também pode informar o número do bug: **--bugzilla=NÚMERO**. Para pesquisar patches relacionados a vários problemas do Bugzilla, adicione vírgulas entre os números de bug, por exemplo:

```
> zypper list-patches --bugzilla=972197,956917
```

Por número do CVE

Para listar todos os patches necessários relacionados a uma entrada no banco de dados CVE (Common Vulnerabilities and Exposures – Exposições e Vulnerabilidades Comuns), use a opção **--cve**.

Para listar os patches de uma entrada específica do banco de dados CVE, você também pode informar o número do CVE: `--cve=NÚMERO`. Para pesquisar patches relacionados a várias entradas do banco de dados CVE, adicione vírgulas entre os números do CVE, por exemplo:

```
> zypper list-patches --cve=CVE-2016-2315,CVE-2016-2324
```

Listar patches recolhidos

No fluxo de código do SUSE Linux Enterprise 15, alguns patches são automaticamente recolhidos. As atualizações de manutenção são cuidadosamente testadas, pois existe o risco de uma atualização conter um bug novo. Se for comprovado que uma atualização contém um bug, uma nova atualização (com um número de versão maior) será emitida para reverter a atualização com bug, que é impedida de ser instalada novamente. Você pode listar os patches recolhidos com o **zypper**:

```
> zypper lp --all |grep retracted
SLE-Module-Basesystem15-SP3-Updates | SUSE-SLE-Module-Basesystem-15-SP3-2021-1965
| recommended | important | --- | retracted | Recommended update for multipath-
tools
SLE-Module-Basesystem15-SP3-Updates | SUSE-SLE-Module-Basesystem-15-SP3-2021-2689
| security | important | --- | retracted | Security update for cpio
SLE-Module-Basesystem15-SP3-Updates | SUSE-SLE-Module-Basesystem-15-SP3-2021-3655
| security | important | reboot | retracted | Security update for the Linux
Kernel
```

Consulte as informações completas sobre um patch recolhido (ou qualquer outro):

```
> zypper patch-info SUSE-SLE-Product-SLES-15-2021-2689
Loading repository data...
Reading installed packages...

Information for patch SUSE-SLE-Product-SLES-15-2021-2689:
-----
Repository   : SLE-Product-SLES15-LTSS-Updates
Name          : SUSE-SLE-Product-SLES-15-2021-2689
Version       : 1
Arch          : noarch
Vendor        : maint-coord@suse.de
Status        : retracted
Category      : security
Severity       : important
Created On    : Mon 16 Aug 2021 03:44:00 AM PDT
Interactive   : ---
Summary       : Security update for cpio
Description   :
    This update for cpio fixes the following issues:
```

```
It was possible to trigger Remote code execution due to a integer overflow
(CVE-2021-38185, bsc#1189206)
```

```
UPDATE:
```

```
This update was buggy and could lead to hangs, so it has been retracted.
```

```
There will be a follow up update.
```

```
[...]
```

Patch com pacotes conflitantes

```
Information for patch openSUSE-SLE-15.3-2022-333:
```

```
-----
```

```
Repository   : Update repository with updates from SUSE Linux Enterprise 15
```

```
Name         : openSUSE-SLE-15.3-2022-333
```

```
Version      : 1
```

```
Arch         : noarch
```

```
Vendor       : maint-coord@suse.de
```

```
Status       : needed
```

```
Category     : security
```

```
Severity     : important
```

```
Created On   : Fri Feb  4 09:30:32 2022
```

```
Interactive  : reboot
```

```
Summary      : Security update for xen
```

```
Description :
```

```
    This update for xen fixes the following issues:
```

```
    - CVE-2022-23033: Fixed guest_physmap_remove_page not removing the p2m mappings.
      (XSA-393) (bsc#1194576)
```

```
    - CVE-2022-23034: Fixed possible DoS by a PV guest Xen while unmapping a grant.
      (XSA-394) (bsc#1194581)
```

```
    - CVE-2022-23035: Fixed insufficient cleanup of passed-through device IRQs.
      (XSA-395) (bsc#1194588)
```

```
Provides     : patch:openSUSE-SLE-15.3-2022-333 = 1
```

```
Conflicts    : [22]
```

```
    xen.src < 4.14.3_06-150300.3.18.2
```

```
    xen.noarch < 4.14.3_06-150300.3.18.2
```

```
    xen.x86_64 < 4.14.3_06-150300.3.18.2
```

```
    xen-devel.x86_64 < 4.14.3_06-150300.3.18.2
```

```
    xen-devel.noarch < 4.14.3_06-150300.3.18.2
```

```
[...]
```

O patch acima está em conflito com as versões afetadas ou vulneráveis de 22 pacotes. Se qualquer um desses pacotes afetados ou vulneráveis for instalado, ele acionará um conflito, e o patch será classificado como *necessário*. O **zypper patch** tenta instalar todos os patches disponíveis. Se ele encontrar problemas, ele os relatará, informando que nem todas as

atualizações serão instaladas. É possível resolver o conflito atualizando ou removendo os pacotes afetados ou vulneráveis. Como os repositórios de atualização do SUSE também incluem pacotes fixos, a atualização é um método padrão de resolver conflitos. Se não for possível atualizar o pacote, por exemplo, devido a problemas de dependência ou bloqueios de pacote, ele será apagado após a aprovação do usuário.

Para listar todos os patches, independentemente de serem necessários, use também a opção `--all`. Por exemplo, para listar todos os patches com um número do CVE atribuído, use:

```
> zypper list-patches --all --cve
Issue | No.          | Patch                | Category   | Severity   | Status
-----+-----+-----+-----+-----+-----
cve   | CVE-2019-0287 | SUSE-SLE-Module..   | recommended | moderate   | needed
cve   | CVE-2019-3566 | SUSE-SLE-SERVER..   | recommended | moderate   | not needed
[...]
```

9.1.4.3 Instalando novas versões de pacotes

Se um repositório contém apenas pacotes novos, mas não fornece patches, **zypper patch** não surte nenhum efeito. Para atualizar todos os pacotes instalados com as versões mais recentes disponíveis, use o seguinte comando:

```
> sudo zypper update
```



Importante

zypper update ignora pacotes problemáticos. Por exemplo, se um pacote estiver bloqueado, o **zypper update** o omitirá, mesmo que uma versão superior dele esteja disponível. Por outro lado, o **zypper patch** relatará um conflito se o pacote for considerado vulnerável.

Para atualizar pacotes individuais, especifique o pacote com o comando `update` ou `install`:

```
> sudo zypper update PACKAGE_NAME
> sudo zypper install PACKAGE_NAME
```

Uma lista de todos os novos pacotes instaláveis pode ser obtida pelo comando:

```
> zypper list-updates
```

Observe que este comando apenas lista os pacotes correspondentes aos seguintes critérios:

- têm o mesmo fornecedor que o pacote já instalado,
- são fornecidos por repositórios com pelo menos a mesma prioridade que o pacote já instalado,
- são instaláveis (todas as dependências foram atendidas).

Uma lista de *todos* os novos pacotes disponíveis (sejam instaláveis ou não) pode ser obtida com:

```
> sudo zypper list-updates --all
```

Para descobrir o motivo pelo qual um novo pacote não pode ser instalado, use o comando **zypper install** ou **zypper update** conforme descrito acima.

9.1.4.4 Identificando pacotes órfãos

Sempre que você remove um repositório do Zypper ou faz upgrade do sistema, alguns pacotes podem entrar no estado “órfão”. Esses pacotes *órfãos* não pertencem mais a nenhum repositório ativo. O comando a seguir fornece uma lista deles:

```
> sudo zypper packages --orphaned
```

Com essa lista, você pode decidir se um pacote ainda é necessário ou pode ser removido com segurança.

9.1.5 Identificando processos e serviços que usam arquivos apagados

Durante a aplicação de patches, atualização ou remoção de pacotes, pode haver processos em execução no sistema que continuam usando os arquivos que foram apagados pela atualização ou remoção. Use o **zypper ps** para listar os processos que usam arquivos apagados. Se o processo pertence a um serviço conhecido, o nome do serviço é listado para facilitar sua reinicialização. Por padrão, o **zypper ps** mostra uma tabela:

```
> zypper ps
PID | PPID | UID | User | Command | Service | Files
-----+-----+-----+-----+-----+-----+-----
814 | 1 | 481 | avahi | avahi-daemon | avahi-daemon | /lib64/ld-2.19.s->
```

```

|      |      |      |      |      |      | /lib64/libdl-2.1->
|      |      |      |      |      |      | /lib64/libpthrea->
|      |      |      |      |      |      | /lib64/libc-2.19->
[...]
```

PID: ID do processo

PPID: ID do processo pai

UID: ID do usuário que está executando o processo

Login: Nome de login do usuário que está executando o processo

Comando: Comando usado para executar o processo

Serviço: Nome do serviço (apenas se o comando está associado a um serviço do sistema)

Arquivos: A lista de arquivos apagados

O formato de saída do **zypper ps** pode ser controlado da seguinte maneira:

zypper ps -s

Criar uma tabela resumida sem mostrar os arquivos apagados.

```

> zypper ps -s
PID   | PPID | UID  | User   | Command      | Service
-----+-----+-----+-----+-----+-----
814   | 1    | 481  | avahi  | avahi-daemon | avahi-daemon
817   | 1    | 0    | root   | irqbalance   | irqbalance
1567  | 1    | 0    | root   | sshd         | sshd
1761  | 1    | 0    | root   | master       | postfix
1764  | 1761 | 51   | postfix| pickup       | postfix
1765  | 1761 | 51   | postfix| qmgr         | postfix
2031  | 2027 | 1000 | tux    | bash         |
```

zypper ps -ss

Mostrar apenas os processos associados a um serviço do sistema.

```

PID   | PPID | UID  | User   | Command      | Service
-----+-----+-----+-----+-----+-----
814   | 1    | 481  | avahi  | avahi-daemon | avahi-daemon
817   | 1    | 0    | root   | irqbalance   | irqbalance
1567  | 1    | 0    | root   | sshd         | sshd
1761  | 1    | 0    | root   | master       | postfix
1764  | 1761 | 51   | postfix| pickup       | postfix
1765  | 1761 | 51   | postfix| qmgr         | postfix
```

zypper ps -sss

Mostrar apenas os serviços do sistema que usam os arquivos apagados.

```

avahi-daemon
irqbalance
```

```
postfix
sshd
```

zypper ps --print "systemctl status %s"

Mostrar os comandos para recuperar informações de status dos serviços que possam precisar de reinicialização.

```
systemctl status avahi-daemon
systemctl status irqbalance
systemctl status postfix
systemctl status sshd
```

Para obter mais informações sobre o gerenciamento de serviços, consulte o [Capítulo 19, Daemon systemd](#).

9.1.6 Gerenciando repositórios com o Zypper

Todos os comandos de instalação ou patch do zypper dependem de uma lista de repositórios conhecidos. Para listar todos os repositórios conhecidos para o sistema, use o comando:

```
> zypper repos
```

O resultado parecerá com o seguinte:

EXEMPLO 9.1: ZYPPER: LISTA DE REPOSITÓRIOS CONHECIDOS

```
> zypper repos
# | Alias          | Name          | Enabled | Refresh
--+-+-----+-----+-----+-----
1 | SLEHA-15-GE0   | SLEHA-15-GE0 | Yes     | No
2 | SLEHA-15       | SLEHA-15     | Yes     | No
3 | SLES15         | SLES15       | Yes     | No
```

Na especificação de repositórios em vários comandos, é possível usar um alias, URI ou número de repositório da saída do comando **zypper repos**. O alias do repositório é uma versão abreviada do nome do repositório para uso em comandos de gerenciamento de repositórios. Observe que os números dos repositórios podem ser mudados após modificar a lista de repositórios. O alias nunca mudará sozinho.

Por padrão; detalhes, como o URI ou a prioridade do repositório, não são exibidos. Use o seguinte comando para listar todos os detalhes:

```
> zypper repos -d
```


9.1.6.1 Adicionando repositórios

Para adicionar um repositório, execute

```
> sudo zypper addrepo URI ALIAS
```

O URI pode ser um repositório da Internet, um recurso de rede, um diretório ou um CD ou DVD (consulte https://en.opensuse.org/openSUSE:Libzypp_URLs para obter os detalhes). O ÁLIAS é um identificador exclusivo e abreviado do repositório. Você tem livre escolha, com a única condição de que seja exclusivo. O zypper emitirá um aviso se você especificar um alias que já está em uso.

9.1.6.2 Atualizando repositórios

O **zypper** permite buscar mudanças nos pacotes de repositórios configurados. Para buscar as mudanças, execute:

```
> sudo zypper refresh
```



Nota: Comportamento padrão do **zypper**

Por padrão, alguns comandos executam o **refresh** automaticamente, portanto, não é necessário executá-lo explicitamente.

O comando **refresh** permite ver as mudanças também nos repositórios desabilitados usando a opção **--plus-content**:

```
> sudo zypper --plus-content refresh
```

Essa opção busca mudanças nos repositórios, mas mantém os repositórios desabilitados no mesmo estado: desabilitado.

9.1.6.3 Removendo repositórios

Para remover um repositório da lista, use o comando **zypper removerepo** juntamente com o alias ou o número do repositório que você deseja apagar. Por exemplo, para remover o repositório SLEHA-12-GE0 do *Exemplo 9.1, “Zypper: lista de repositórios conhecidos”*, use um dos seguintes comandos:

```
> sudo zypper removerepo 1
```

```
> sudo zypper removerepo "SLEHA-12-GE0"
```

9.1.6.4 Modificando repositórios

Habilite ou desabilite os repositórios com `zypper modifyrepo`. Você também pode alterar as propriedades do repositório (por exemplo, atualizar o comportamento, o nome ou a prioridade) com esse comando. O comando a seguir habilita o repositório chamado `updates`, ativa a atualização automática e define sua prioridade como 20:

```
> sudo zypper modifyrepo -er -p 20 'updates'
```

A modificação de repositórios não se limita a um único repositório, você também pode operar em grupos:

`-a`: todos os repositórios

`-l`: repositórios locais

`-t`: repositórios remotos

`-m TIPO`: repositórios de determinado tipo (em que `TIPO` pode ser um dos seguintes: `http`, `https`, `ftp`, `cd`, `dvd`, `dir`, `file`, `cifs`, `smb`, `nfs`, `hd`, `iso`)

Para renomear o alias de um repositório, use o comando `renamerepo`. O exemplo a seguir muda o alias de `Mozilla Firefox` para `firefox`:

```
> sudo zypper renamerepo 'Mozilla Firefox' firefox
```

9.1.7 Consultando repositórios e pacotes com o Zypper

O `zypper` oferece vários métodos de consulta a repositórios ou pacotes. Para obter as listas de todos os produtos, padrões, pacotes ou patches disponíveis, use os seguintes comandos:

```
> zypper products
> zypper patterns
> zypper packages
> zypper patches
```

Para consultar todos os repositórios para determinados pacotes, use `search`. Para obter informações sobre pacotes específicos, use o comando `info`.

9.1.7.1 Pesquisando um software

O comando **zypper search** funciona em nomes de pacotes ou, opcionalmente, em descrições e resumos de pacotes. Uma string entre `/` é interpretada como expressão regular. Por padrão, a pesquisa não diferencia maiúsculas de minúsculas.

Pesquisa simples de nome de pacote que inclua `fire`

```
> zypper search "fire"
```

Pesquisa simples do pacote exato `MozillaFirefox`

```
> zypper search --match-exact "MozillaFirefox"
```

Pesquisar também em descrições e resumos de pacotes

```
> zypper search -d fire
```

Exibir apenas pacotes ainda não instalados

```
> zypper search -u fire
```

Exibir pacotes que tenham a string `fir`, não seguida por `e`

```
> zypper se "/fir[^e]/"
```

9.1.7.2 Pesquisando pacotes em todos os módulos do SLE

Para pesquisar pacotes tanto dentro quanto fora dos módulos atualmente habilitados do SLE, use o subcomando **search-packages**. Esse comando contata o SUSE Customer Center e pesquisa os pacotes correspondentes em todos os módulos, por exemplo:

```
> zypper search-packages package1 package2
```

zypper search-packages inclui as seguintes opções:

- Procurar uma correspondência exata da sua string de pesquisa: `-x`, `--match-exact`
- Agrupar os resultados por módulo (padrão: agrupar por pacote): `-g`, `--group-by-module`
- Exibir informações mais detalhadas sobre os pacotes: `-d`, `--details`
- Retornar os resultados da pesquisa em XML: `--xmlout`

9.1.7.3 Pesquisando um recurso específico

Para procurar pacotes que oferecem um recurso específico, use o comando `what-provides`. Por exemplo, para saber qual pacote inclui o módulo Perl `SVN::Core`, use o seguinte comando:

```
> zypper what-provides 'perl(SVN::Core)'
```

`What-provides NOME_DO_PACOTE` é semelhante a `rpm -q --whatprovides NOME_DO_PACOTE`, mas o RPM só pode consultar o banco de dados RPM (que é o banco de dados de todos os pacotes instalados). O zypper, por outro lado, o informará sobre fornecedores do recurso a partir de qualquer repositório, não apenas aqueles que estão instalados.

9.1.7.4 Mostrando as informações do pacote

Para consultar pacotes únicos, use `info` com um nome exato de pacote como argumento. Esse recurso exibe informações detalhadas sobre um pacote. Caso o nome do pacote não corresponda a nenhum nome de pacote dos repositórios, o comando exibirá informações detalhadas sobre as correspondências que não são de pacote. Se você solicitar um tipo específico (usando a opção `-t`) e o tipo não existir, o comando exibirá outras correspondências disponíveis, mas sem informações detalhadas.

Se você especificar um pacote de origem, o comando exibirá pacotes binários criados com base no pacote de origem. Se você especificar um pacote binário, o comando exibirá os pacotes de origem usados para criar o pacote de binário.

Para mostrar também o que é exigido/recomendado pelo pacote, use as opções `--requires` e `--recommends`:

```
> zypper info --requires MozillaFirefox
```

9.1.8 Mostrando as informações de ciclo de vida

Normalmente, os produtos SUSE são suportados por 10 anos. Muitas vezes, você pode estender esse ciclo de vida padrão usando as ofertas de suporte estendido da SUSE, que adicionam três anos de suporte. Dependendo do produto, você encontra o ciclo de vida de suporte exato em <https://www.suse.com/lifecycle>.

Para consultar o ciclo de vida do seu produto e o pacote suportado, use o comando `zypper lifecycle` conforme mostrado a seguir:

```
# zypper lifecycle
```

Product end of support	
Codestream: SUSE Linux Enterprise Server 15	2028-07-31
Product: SUSE Linux Enterprise Server 15 SP3	n/a*
Module end of support	
Basesystem Module	n/a*
Desktop Applications Module	n/a*
Server Applications Module	n/a*
Package end of support if different from product:	
autofs	Now, installed 5.1.3-7.3.1, update available
5.1.3-7.6.1	

9.1.9 Configurando o Zypper

O Zypper agora vem com um arquivo de configuração que permite mudar permanentemente o comportamento do Zypper (de todo o sistema ou de um usuário específico). Para mudanças de todo o sistema, edite `/etc/zypp/zypper.conf`. Para mudanças específicas do usuário, edite `~/.zypper.conf`. Se `~/.zypper.conf` ainda não existir, você poderá usar `/etc/zypp/zypper.conf` como gabarito: copie-o para `~/.zypper.conf` e ajuste-o como desejar. Consulte os comentários no arquivo para obter ajuda sobre as opções disponíveis.

9.1.10 Solução de problemas

Se você tiver problemas para acessar os pacotes dos repositórios configurados (por exemplo, o Zypper não encontra determinado pacote mesmo que você saiba que ele existe em um dos repositórios), a atualização dos repositórios poderá ajudar:

```
> sudo zypper refresh
```

Se isso não ajudar, tente

```
> sudo zypper refresh -fdb
```

Isso força uma atualização completa e a reconstrução do banco de dados, incluindo um download forçado dos metadados iniciais.

9.1.11 Recurso de rollback do Zypper no sistema de arquivos Btrfs

Se o sistema de arquivos Btrfs for usado na partição raiz e o **snapper** estiver instalado, o Zypper chamará automaticamente o **snapper** ao confirmar as mudanças no sistema de arquivos para criar os instantâneos apropriados do sistema de arquivos. É possível usar esses instantâneos para reverter as mudanças feitas pelo Zypper. Consulte a [Capítulo 10, Recuperação de sistema e gerenciamento de instantâneos com o Snapper](#) para obter mais informações.

9.1.12 Mais informações

Para obter mais informações sobre gerenciamento de software da linha de comando, digite **zypper help**, **zypper help** *COMANDO* ou consulte a página de manual do **zypper(8)**. Para acessar uma referência completa e detalhada dos comandos, os *folhetos de dicas* com os comandos mais importantes e as informações sobre como usar o Zypper em scripts e aplicativos, visite https://en.opensuse.org/SDB:Zypper_usage. Você encontra uma lista das mudanças de software da versão mais recente do SUSE Linux Enterprise Desktop em https://en.opensuse.org/openSUSE:Zypper_versions.

9.2 RPM: gerenciador de pacotes

O RPM (gerenciador de pacotes RPM) é usado para gerenciar pacotes de software. Seus principais comandos são **rpm** e **rpmbuild**. O banco de dados RPM avançado pode ser consultado pelos usuários, administradores de sistema e construtores de pacotes para obtenção de informações detalhadas sobre o software instalado.

O **rpm** tem cinco modos: instalação, desinstalação (ou atualização) de pacotes de software, reconstrução do banco de dados RPM, consulta de bancos RPM ou de arquivos RPM individuais, verificação de integridade dos pacotes e assinatura de pacotes. O **rpmbuild** pode ser usado para construir pacotes instaláveis de fontes originais.

Os arquivos RPM instaláveis são compactados em um formato binário especial. Esses são arquivos de programa para instalação e determinadas metainformações usadas durante a instalação pelo comando **rpm** para configurar o pacote de softwares. Também são armazenados no banco de dados RPM com o objetivo de documentação. Os arquivos RPM normalmente têm a extensão **.rpm**.



Dica: Pacotes de desenvolvimento de software

Para vários pacotes, os componentes necessários para o desenvolvimento de software (bibliotecas, cabeçalhos, arquivos de inclusões etc.) foram colocados em pacotes separados. Esses pacotes de desenvolvimento só são necessários quando você deseja compilar software por conta própria (por exemplo, os pacotes do GNOME mais recentes). É possível identificá-los pela extensão do nome `-devel`, como os pacotes `alsa-devel` e `gimp-devel`.

9.2.1 Verificando a autenticidade do pacote

Os pacotes RPM têm uma assinatura GPG. Para verificar a assinatura de um pacote RPM, use o comando `rpm --checksig PACOTE-1.2.3.rpm` para determinar se o pacote vem do SUSE ou de outro recurso confiável. Isso é especialmente recomendado para pacotes de atualização da Internet.

Ao corrigir problemas no sistema operacional, talvez seja necessário instalar uma PTF (Problem Temporary Fix – Correção Temporária do Problema) no sistema de produção. Os pacotes oferecidos pelo SUSE são assinados com uma chave PTF especial. No entanto, diferentemente do SUSE Linux Enterprise 11, essa chave não é importada nos sistemas SUSE Linux Enterprise 12 por padrão. Para importar a chave manualmente, use o seguinte comando:

```
> sudo rpm --import \  
/usr/share/doc/packages/suse-build-key/suse_ptf_key.asc
```

Após importar a chave, você poderá instalar os pacotes PTF no sistema.

9.2.2 Gerenciando pacotes: instalar, atualizar e desinstalar

Normalmente, a instalação de um arquivo RPM é bem simples: `rpm -i PACKAGE.rpm`. Com esse comando, o pacote é instalado, mas apenas quando suas dependências são atendidas e quando não há conflitos com outros pacotes. Com uma mensagem de erro, o `rpm` solicita os pacotes que devem ser instalados para atender a requisitos de dependência. No segundo plano, o banco de dados RPM garante que não haja conflitos, pois um arquivo específico pode pertencer somente a um pacote. Ao escolher opções diferentes, você pode forçar o `rpm` a ignorar esses padrões, mas isso é somente para especialistas. Do contrário, você se arrisca a comprometer a integridade do sistema e, possivelmente, ameaça a capacidade de atualização do sistema.

As opções `-U` ou `--upgrade` e `-F` ou `--freshen` podem ser usadas para atualizar um pacote (por exemplo, `rpm -F PACOTE.rpm`). Esse comando remove os arquivos da versão antiga e instala os novos arquivos imediatamente. A diferença entre as duas versões é que o `-U` instala pacotes que ainda não existiam no sistema, enquanto `-F` apenas atualiza os pacotes já instalados. Durante a atualização, o `rpm` atualiza arquivos de configuração cuidadosamente com a seguinte estratégia:

- Se um arquivo de configuração não tiver sido modificado pelo administrador de sistema, o `rpm` instalará a nova versão do arquivo apropriado. O administrador de sistema não precisa adotar nenhuma ação.
- Se um arquivo de configuração foi mudado pelo administrador do sistema antes da atualização, o `rpm` gravará o arquivo modificado com a extensão `.rpmorig` ou `.rpmsave` (arquivo de backup) e instalará a versão do novo pacote. Isso apenas será feito se o arquivo instalado originalmente e a versão mais recente forem diferentes. Nesse caso, compare o arquivo de backup (`.rpmorig` ou `.rpmsave`) com o arquivo recém-instalado e faça novamente as modificações no novo arquivo. Depois disso, apague todos os arquivos `.rpmorig` e `.rpmsave` para evitar problemas com atualizações futuras.
- Arquivos `.rpmnew` são exibidos se o arquivo de configuração já existir e se o rótulo `noreplace` tiver sido especificado no arquivo `.spec`.

Após uma atualização, os arquivos `.rpmsave` e `.rpmnew` devem ser removidos depois de comparados, para que não impeçam atualizações futuras. A extensão `.rpmorig` será atribuída se o arquivo não tiver sido previamente reconhecido pelo banco de dados RPM.

Do contrário, o `.rpmsave` será usado. Em outras palavras, o `.rpmorig` resulta da atualização de um formato estranho ao RPM. O `.rpmsave` resulta da atualização de um RPM mais antigo para um RPM mais novo. O `.rpmnew` não revela nenhuma informação indicando se o administrador do sistema fez modificações no arquivo de configuração. Uma lista destes arquivos está disponível em `/var/adm/rpmconfigcheck`. Alguns arquivos de configuração (como `/etc/httpd/httpd.conf`) não são sobregravados para permitir operação continuada.

O switch `-U` não é apenas um equivalente à desinstalação com a opção `-e` e à instalação com a opção `-i`. Use `-U` sempre que possível.

Para remover um pacote, digite `rpm -e PACOTE`. Este comando só apaga o pacote quando não há dependências não resolvidas. É teoricamente impossível apagar Tcl/Tk, por exemplo, enquanto outro aplicativo exigir sua existência. Mesmo nesse caso, o RPM pede ajuda do banco de dados. Se, por qualquer motivo, a exclusão for impossível (mesmo que não exista *nenhuma* dependência adicional), talvez seja útil reconstruir o banco de dados RPM usando a opção `--rebuilddb`.

9.2.3 Pacotes RPM Delta

Os pacotes RPM Delta possuem uma diferença entre uma versão nova e antiga de um pacote RPM. Aplicar um RPM delta a um RPM antigo resulta em um RPM completamente novo. Não é necessário ter uma cópia do RPM antigo, pois um RPM delta também pode funcionar com um RPM instalado. Os pacotes RPM delta têm tamanho ainda menor que os RPMs com patch, o que é uma vantagem durante a transferência de pacotes de atualização na Internet. A desvantagem é que operações de atualização que envolvem RPMs delta consomem consideravelmente mais ciclos de CPU do que as operações com RPMs com patch ou simples.

Os binários `makedeltarpm` e `applydelta` integram a suíte de RPM delta (pacote `deltarpm`) e ajudam na criação e aplicação de pacotes RPM delta. Com os seguintes comandos, crie um RPM delta chamado `new.delta.rpm`. O comando a seguir pressupõe que `old.rpm` e `new.rpm` estejam presentes:

```
> sudo makedeltarpm old.rpm new.rpm new.delta.rpm
```

Usando `applydeltarpm`, você poderá reconstruir o novo RPM do arquivo de sistema, se o pacote antigo já estiver instalado:

```
> sudo applydeltarpm new.delta.rpm new.rpm
```

Para derivá-lo do RPM antigo sem acessar o sistema de arquivos, use a opção `-r`:

```
> sudo applydeltarpm -r old.rpm new.delta.rpm new.rpm
```

Consulte </usr/share/doc/packages/deltarpm/README> para obter os detalhes técnicos.

9.2.4 RPMconsultas

Com a opção `-q`, o `rpm` inicia consultas, permitindo a inspeção de um arquivo RPM (adicionando a opção `-p`) e a consulta ao banco de dados RPM dos pacotes instalados. Vários switches estão disponíveis para especificar o tipo de informação necessária. Consulte a [Tabela 9.1, “Opções de consulta de RPM essenciais”](#).

TABELA 9.1: OPÇÕES DE CONSULTA DE RPM ESSENCIAIS

<u>-i</u>	Informações de pacote
<u>-l</u>	Lista de arquivos
<u>-f ARQUIVO</u>	Consulte o pacote que contém o arquivo <u>ARQUIVO</u> (o caminho completo deve ser especificado com <u>ARQUIVO</u>)
<u>-s</u>	Lista de arquivos com informações de status (requer <u>-l</u>)
<u>-d</u>	Lista somente arquivos de documentação (requer <u>-l</u>)
<u>-c</u>	Lista somente arquivos de configuração (requer <u>-l</u>)
<u>--dump</u>	Lista de arquivos com detalhes completos (a ser usada com <u>-l</u> , <u>-c</u> ou <u>-d</u>)
<u>--provides</u>	Lista recursos do pacote que outro pacote pode solicitar com <u>--requires</u>
<u>--requires</u> , <u>-R</u>	Recursos exigidos pelo pacote
<u>--scripts</u>	Scripts de instalação (pré-instalação, pós-instalação, desinstalação)

Por exemplo, o comando `rpm -q -i wget` exibe as informações mostradas no *Exemplo 9.2*, “`rpm -q -i wget`”.

EXEMPLO 9.2: `rpm -q -i wget`

```

Name       : wget
Version    : 1.14
Release    : 17.1
Architecture: x86_64
Install Date: Mon 30 Jan 2017 14:01:29 CET
Group      : Productivity/Networking/Web/Utilities
Size       : 2046483
License    : GPL-3.0+
```

```

Signature   : RSA/SHA256, Thu 08 Dec 2016 07:48:44 CET, Key ID 70af9e8139db7c82
Source RPM  : wget-1.14-17.1.src.rpm
Build Date  : Thu 08 Dec 2016 07:48:34 CET
Build Host  : sheep09
Relocations : (not relocatable)
Packager    : https://www.suse.com/
Vendor      : SUSE LLC <https://www.suse.com/>
URL         : http://www.gnu.org/software/wget/
Summary     : A Tool for Mirroring FTP and HTTP Servers
Description :
Wget enables you to retrieve WWW documents or FTP files from a server.
This can be done in script files or via the command line.
Distribution: SUSE Linux Enterprise 15

```

A opção **-f** funcionará somente se você especificar o nome e o caminho completos do arquivo. Insira quantos nomes de arquivo desejar. Por exemplo:

```

> rpm -q -f /bin/rpm /usr/bin/wget
rpm-4.14.1-lp151.13.10.x86_64
wget-1.19.5-lp151.4.1.x86_64

```

Se apenas parte do nome de arquivo for conhecida, use um script de shell conforme mostrado no [Exemplo 9.3, “Script para pesquisar pacotes”](#). Passe o nome de arquivo parcial para o script mostrado como um parâmetro ao executá-lo.

EXEMPLO 9.3: SCRIPT PARA PESQUISAR PACOTES

```

#!/bin/sh
for i in $(rpm -q -a -l | grep $1); do
    echo "\"$i\" is in package:"
    rpm -q -f $i
    echo ""
done

```

O comando **rpm -q --changelog PACOTE** exibe uma lista detalhada das informações de modificação sobre determinado pacote, classificadas por data.

Com o banco de dados RPM instalado, é possível realizar verificações. Inicie as verificações com **-V** ou **--verify**. Com essa opção, o **rpm** mostra todos os arquivos em um pacote que foram modificados desde a instalação. O **rpm** usa oito símbolos de caracteres para apresentar algumas dicas sobre as seguintes mudanças:

TABELA 9.2: OPÇÕES DE VERIFICAÇÃO DO RPM

5	Resumo de verificação MD5
---	---------------------------

<u>S</u>	Tamanho do arquivo
<u>L</u>	Link simbólico
<u>T</u>	Tempo de modificação
<u>D</u>	Números de dispositivo principais e auxiliares
<u>U</u>	Proprietário
<u>C</u>	Grupo
<u>M</u>	Modo (tipo de arquivo e permissões)

No caso de arquivos de configuração, a letra c é impressa. Por exemplo, para modificações no pacote `/etc/wgetrc` (`wget`):

```
> rpm -V wget
S.5....T c /etc/wgetrc
```

Os arquivos do banco de dados RPM são colocados em `/var/lib/rpm`. Se a partição `/usr` tiver o tamanho de 1 GB, esse banco de dados poderá ocupar praticamente 30 MB, especialmente após uma atualização completa. Se o banco de dados for maior do que o esperado, será útil reconstruir o banco de dados com a opção `--rebuilddb`. Antes disso, faça um backup do banco de dados antigo. O script `cron` `cron.daily` faz cópias diárias do banco de dados (compactado com `gzip`) e as armazena em `/var/adm/backup/rpmdb`. O número de cópias é controlado pela variável `MAX_RPMD_BCKUPS` (padrão: 5) em `/etc/sysconfig/backup`. O tamanho de um único backup é de aproximadamente 1 MB para 1 GB em `/usr`.

9.2.5 Instalando e compilando pacotes de fontes

Todos os pacotes de fonte têm a extensão `.src.rpm` (RPM de fonte).



Nota: Pacotes de fontes instalados

Pacotes de fonte podem ser copiados da mídia de instalação para o disco rígido e descompactados com o YaST. Porém, eles não são marcados como instalados (`[i]`) no gerenciador de pacotes. Isso ocorre porque os pacotes de fontes não são inseridos no

banco de dados RPM. Somente o software do sistema operacional *instalado* está listado no banco de dados RPM. Quando você “instalar” um pacote de fontes, somente o código-fonte será adicionado ao sistema.

Os diretórios a seguir devem estar disponíveis para **rpm** e **rpmbuild** em `/usr/src/packages` (a menos que você tenha especificado configurações personalizadas em um arquivo como `/etc/rpmrc`):

SOURCES

para as fontes originais (arquivos `.tar.bz2` ou `.tar.gz` etc.) e para ajustes específicos de distribuição (geralmente arquivos `.diff` ou `.patch`)

SPECS

para os arquivos `.spec`, similares a um metaMakefile, que controla o processo de *construção*

BUILD

diretório em que todas as fontes são descompactadas, corrigidas e compiladas

RPMS

local em que os pacotes binários concluídos são armazenados

SRPMS

local em que estão os RPMs de fonte

Quando você instala um pacote de origem com o YaST, todos os componentes necessários são instalados em `/usr/src/packages`: as origens e os ajustes em SOURCES e o arquivo `.spec` relevante em SPECS.



Atenção: Integridade do sistema

Não faça experiências com os componentes do sistema (`glibc`, `rpm` etc.), pois isso arrisca a estabilidade do sistema.

O exemplo a seguir usa o pacote `wget.src.rpm`. Após instalar o pacote de origem, você deverá ter arquivos semelhantes aos da seguinte lista:

```
/usr/src/packages/SOURCES/wget-1.19.5.tar.bz2
/usr/src/packages/SOURCES/wgetrc.patch
```

```
/usr/src/packages/SPECS/wget.spec
```

rpmbuild -bX /usr/src/packages/SPECS/wget.spec inicia a compilação. X é um curinga para vários estágios do processo de construção (consulte a saída de --help ou a documentação do RPM para obter os detalhes). Veja a seguir uma breve explicação:

-bp

Preparar as fontes em /usr/src/packages/BUILD: descompactar e corrigir.

-bc

Faz o mesmo que -bp, mas com compilação adicional.

-bi

Faz o mesmo que -bp, mas com a instalação adicional do software criado. Cuidado: se o pacote não aceitar o recurso BuildRoot, talvez você sobregrave os arquivos de configuração.

-bb

Faz o mesmo que -bi, mas com a criação adicional do pacote binário. Se a compilação tiver sido bem-sucedida, o binário deverá estar em /usr/src/packages/RPMS.

-ba

Faz o mesmo que -bb, mas com a criação adicional do RPM de fonte. Se a compilação tiver sido bem-sucedida, o binário deverá estar em /usr/src/packages/SRPMS.

--short-circuit

Ignora algumas etapas.

O RPM binário criado agora pode ser instalado com **rpm** -i ou, de preferência, com **rpm** -U. A instalação com **rpm** faz com que ele apareça no banco de dados RPM.

Lembre-se de que a diretiva BuildRoot no arquivo de especificação foi descontinuada. Se você ainda precisa desse recurso, use a opção --buildroot como uma solução alternativa.

9.2.6 Compilando pacotes RPM com build

O perigo de vários pacotes é que arquivos indesejados são adicionados ao sistema em execução durante o processo de construção. Para evitar isso, use build, que cria um ambiente definido para construção do pacote. Para estabelecer esse ambiente chroot, o script **build** deve ser fornecido com uma árvore de pacote completa. Essa árvore pode ser disponibilizada no disco rígido, por meio do NFS ou DVD. Defina a posição com **build** --rpms DIRETÓRIO.

Diferentemente do `rpm`, o comando `build` procura o arquivo `.spec` no diretório de fontes. Para construir o `wget` (como no exemplo acima) com o DVD montado no sistema em `/media/dvd`, use o seguinte comando como `root`:

```
# cd /usr/src/packages/SOURCES/  
# mv ../SPECS/wget.spec .  
# build --rpms /media/dvd/suse/ wget.spec
```

Depois disso, um ambiente mínimo é estabelecido em `/var/tmp/build-root`. O pacote é criado nesse ambiente. Após a conclusão, os pacotes resultantes estarão localizados em `/var/tmp/build-root/usr/src/packages/RPMS`.

O script `build` oferece várias opções adicionais. Por exemplo, fazer com que o script prefira seus próprios RPMs, omitir a inicialização do ambiente de construção ou limitar o comando `rpm` a um dos estágios mencionados acima. Acesse informações adicionais com `build --help` e a leitura da página de manual `build`.

9.2.7 Ferramentas para arquivos e banco de dados RPM

O Midnight Commander (`mc`) pode exibir o conteúdo de arquivos RPM e copiar partes deles. Ele representa arquivos como sistemas de arquivos virtuais, oferecendo todas as opções de menu usuais do Midnight Commander. Exiba o `HEADER` com `F3`. Exiba a estrutura de arquivos com as teclas de cursor e `Enter`. Copie componentes de arquivos com `F5`.

Um gerenciador de pacote completo está disponível como um módulo do YaST. Para obter os detalhes, consulte a [Capítulo 8, Instalando ou removendo software](#).

10 Recuperação de sistema e gerenciamento de instantâneos com o Snapper

O Snapper permite criar e gerenciar instantâneos de sistema de arquivos. Os instantâneos de sistema de arquivos permitem manter uma cópia do estado de um sistema de arquivos em um determinado momento. A configuração padrão do Snapper foi projetada para permitir voltar modificações feitas no sistema. No entanto, você pode usá-la também para criar backups em disco dos dados dos usuários. Como base para essa funcionalidade, o Snapper usa o sistema de arquivos Btrfs ou os volumes LVM com aprovisionamento dinâmico com um sistema de arquivos XFS ou Ext4.

O Snapper tem uma interface de linha de comando e uma interface do YaST. O Snapper permite criar e gerenciar instantâneos nos seguintes tipos de sistema de arquivos:

- Btrfs, um sistema de arquivos de cópia em gravação para Linux que suporta de forma nativa os instantâneos de sistema de arquivos de subvolumes. (Os subvolumes são sistemas de arquivos que podem ser montados separadamente em uma partição física.) Também é possível inicializar por meio de instantâneos do Btrfs. Para obter mais informações, consulte a [Seção 10.3, “Rollback do sistema por inicialização de instantâneos”](#).
- Volumes LVM com aprovisionamento dinâmico formatados com XFS ou Ext4.

Usando o Snapper, é possível executar as seguintes tarefas:

- Desfazer mudanças no sistema feitas pelo **zypper** e pelo YaST. Consulte a [Seção 10.2, “Usando o Snapper para desfazer mudanças”](#) para obter os detalhes.
- Restaurar arquivos de instantâneos anteriores. Consulte a [Seção 10.2.2, “Usando o Snapper para restaurar arquivos”](#) para obter os detalhes.
- Fazer rollback do sistema inicializando de um instantâneo. Consulte a [Seção 10.3, “Rollback do sistema por inicialização de instantâneos”](#) para obter os detalhes.
- Criar e gerenciar instantâneos manualmente, no sistema em execução. Consulte a [Seção 10.6, “Criando e gerenciando instantâneos manualmente”](#) para obter os detalhes.

10.1 Configuração padrão

O Snapper no SUSE Linux Enterprise Desktop foi configurado como uma ferramenta para desfazer e recuperar mudanças no sistema. Por padrão, a partição raiz (`/`) do SUSE Linux Enterprise Desktop está formatada com `Btrfs`. A captura de instantâneos será automaticamente habilitada se a partição raiz (`/`) for grande o suficiente (mais do que aproximadamente 16 GB). Por padrão, os instantâneos estão desabilitados em partições que não são `/`.



Dica: Habilitando o Snapper no sistema instalado

Se você desabilitou o Snapper durante a instalação, pode habilitá-lo a qualquer momento no futuro. Para fazer isso, crie uma configuração padrão do Snapper para o sistema de arquivos raiz executando:

```
> sudo snapper -c root create-config /
```

Em seguida, habilite os tipos diferentes de instantâneo conforme descrito na [Seção 10.1.4.1, “Desabilitando/Habilitando instantâneos”](#).

Em um sistema de arquivos raiz `Btrfs`, observe que os instantâneos exigem um sistema de arquivos com subvolumes configurados conforme proposto pelo instalador e uma partição de pelo menos 16 GB.

Quando um instantâneo é criado, tanto o instantâneo quanto o original apontam para os mesmos blocos no sistema de arquivos. Por isso, o instantâneo inicialmente não ocupa espaço adicional no disco. Se os dados do sistema de arquivos original forem modificados, os blocos dos dados modificados serão copiados, enquanto os blocos dos dados antigos serão mantidos no instantâneo. Portanto, o instantâneo ocupa a mesma quantidade de espaço que os dados modificados. Ao longo do tempo, a quantidade de espaço alocada por um instantâneo cresce constantemente. Como consequência, a exclusão de arquivos do sistema de arquivos `Btrfs` que contém instantâneos pode *não* liberar espaço em disco!



Nota: Local do instantâneo

Os instantâneos residem sempre na mesma partição ou subvolume no qual foram criados. Não é possível armazenar os instantâneos em uma partição ou um subvolume diferente.

Como resultado, as partições com instantâneos precisam ser maiores do que as partições sem instantâneos. A quantidade exata depende bastante do número de instantâneos mantidos e do volume de modificações de dados. Como uma regra geral, atribua às partições o dobro de espaço do que o de costume. Para evitar que os discos fiquem sem espaço, os instantâneos antigos são limpos automaticamente. Consulte o [Seção 10.1.4.4, “Controlando o armazenamento de instantâneos”](#) para obter os detalhes.

10.1.1 Configurações padrão

Discos com mais de 16 GB

- Arquivo de configuração: /etc/snapper/configs/root
- USE_SNAPPER=yes
- TIMELINE_CREATE=no

Discos com menos de 16 GB

- Arquivo de configuração: não criado
- USE_SNAPPER=no
- TIMELINE_CREATE=yes

10.1.2 Tipos de instantâneos

Embora os próprios instantâneos não se diferenciem no sentido técnico, nós os distinguimos entre três tipos, com base nos eventos em que foram acionados:

Instantâneos de linha do tempo

Um único instantâneo é criado a cada hora. Instantâneos antigos são apagados automaticamente. Por padrão, o primeiro instantâneo dos últimos dez dias, meses e anos são mantidos. Usando o método de instalação de OS do YaST (padrão), os instantâneos de linha do tempo são habilitados, exceto para o sistema de arquivos raiz.

Instantâneos de instalação

Sempre que um ou mais pacotes são instalados com o YaST ou o Zypper, um par de instantâneos é criado: um antes do início da instalação (“Pré”) e outro após o término da instalação (“Pós”). Se um componente importante do sistema, como o kernel, for instalado,

o par de instantâneos será marcado como importante (`important=yes`). Instantâneos antigos são apagados automaticamente. Por padrão, os dez últimos instantâneos importantes e os dez últimos instantâneos “regulares” (incluindo os instantâneos de administração) são mantidos. Instantâneos de instalação são habilitados, por padrão.

Instantâneos de administração

Sempre que você administra o sistema com o YaST, um par de instantâneos é criado: um quando algum módulo do YaST é iniciado (“Pré”) e outro quando o módulo é fechado (“Pós”). Instantâneos antigos são apagados automaticamente. Por padrão, os dez últimos instantâneos importantes e os dez últimos instantâneos “regulares” (incluindo os instantâneos de instalação) são mantidos. Instantâneos de administração são habilitados, por padrão.

10.1.3 Diretórios que são excluídos dos instantâneos

Alguns diretórios precisam ser excluídos dos instantâneos por diversos motivos. A seguinte lista mostra todos os diretórios que são excluídos:

/boot/grub2/i386-pc, /boot/grub2/x86_64-efi, /boot/grub2/powerpc-ieee1275, /boot/grub2/s390x-emu

O rollback da configuração do carregador de boot não é suportado. Os diretórios listados acima são específicos da arquitetura. Os dois primeiros diretórios estão presentes nas máquinas AMD64/Intel 64, os dois últimos no IBM POWER e no IBM Z, respectivamente.

/home

Se /home não residir em uma partição separada, ele será excluído para evitar perda de dados nos rollbacks.

/opt

Os produtos de terceiros normalmente são instalados em /opt. Ele é excluído para evitar a desinstalação dos aplicativos nos rollbacks.

/srv

Contém dados de servidores Web e FTP. Ele é excluído para evitar perda de dados nos rollbacks.

/tmp

Todos os diretórios com arquivos temporários e caches são excluídos dos instantâneos.

/usr/local

Esse diretório é usado na instalação manual de softwares. Ele é excluído para evitar a desinstalação das instalações nos rollbacks.

/var

Esse diretório contém muitos arquivos variáveis, incluindo registros, caches temporários, produtos de terceiros em /var/opt e o local padrão para imagens de máquina virtual e bancos de dados. Portanto, o subvolume é criado para excluir todos esses dados variáveis dos instantâneos e tem o recurso Cópia em Gravação desabilitado.

10.1.4 Personalizando a configuração

O SUSE Linux Enterprise Desktop vem com uma configuração padrão lógica, que deve ser suficiente na maioria dos casos de uso. No entanto, todos os aspectos da criação automática e da manutenção de instantâneos podem ser configurados de acordo com as suas necessidades.

10.1.4.1 Desabilitando/Habilitando instantâneos

Cada um dos três tipos de instantâneos (linha do tempo, instalação, administração) pode ser habilitado ou desabilitado de forma independente.

Desabilitando/Habilitando instantâneos de linha do tempo

Habilitar. `snapper -c root set-config "TIMELINE_CREATE=yes"`

Desabilitar. `snapper -c root set-config "TIMELINE_CREATE=no"`

Usando o método de instalação de OS do YaST (padrão), os instantâneos de linha do tempo são habilitados, exceto para o sistema de arquivos raiz.

Desabilitando/Habilitando instantâneos de instalação

Habilitar: Instale o pacote `snapper-zypp-plugin`

Desabilitar: Desinstale o pacote `snapper-zypp-plugin`

Instantâneos de instalação são habilitados, por padrão.

Desabilitando/Habilitando instantâneos de administração

Habilitar: Defina `USE_SNAPPER` como `yes` em `/etc/sysconfig/yast2`.

Desabilitar: Defina `USE_SNAPPER` como `no` em `/etc/sysconfig/yast2`.

Instantâneos de administração são habilitados, por padrão.

10.1.4.2 Controlando instantâneos de instalação

A criação de pares de instantâneos ao instalar pacotes com o YaST ou o Zypper é administrada pelo `snapper-zypp-plugin`. O arquivo de configuração XML `/etc/snapper/zypp-plugin.conf` define quando criar instantâneos. Por padrão, o arquivo é parecido com o seguinte:

```
1 <?xml version="1.0" encoding="utf-8"?>
2 <snapper-zypp-plugin-conf>
3   <solvables>
4     <solvable match="w" ❶ important="true" ❷>kernel-* ❸</solvable>
5     <solvable match="w" important="true">dracut</solvable>
6     <solvable match="w" important="true">glibc</solvable>
7     <solvable match="w" important="true">systemd*</solvable>
8     <solvable match="w" important="true">udev</solvable>
9     <solvable match="w">*</solvable> ❹
10  </solvables>
11 </snapper-zypp-plugin-conf>
```

- ❶ O atributo de correspondência define se o padrão é um curinga no estilo shell do Unix (w) ou uma expressão regular Python (re).
- ❷ Se houver correspondência do padrão especificado e o pacote correspondente estiver marcado como importante (por exemplo, pacotes do kernel), o instantâneo também será marcado como importante.
- ❸ Padrão de correspondência com o nome de um pacote. Com base na configuração do atributo `match`, caracteres especiais são interpretados como curingas do shell ou expressões regulares. Este padrão corresponde todos os nomes de pacotes que começam com `kernel-`.
- ❹ Esta linha corresponde todos os pacotes incondicionalmente.

Com este instantâneo de configuração, os pares são criados sempre que um pacote é instalado (linha 9). Quando são instalados pacotes do kernel, dracut, glibc, systemd ou udev marcados como importantes, o par de instantâneos também é marcado como importante (linhas 4 a 8). Todas as regras são avaliadas.

Para desabilitar uma regra, apague-a ou desative-a usando comentários XML. Para impedir que o sistema crie pares de instantâneos para cada pacote de instalação, por exemplo, comente na linha 9:

```
1 <?xml version="1.0" encoding="utf-8"?>
2 <snapper-zypp-plugin-conf>
3   <solvables>
```

```

4 <solvable match="w" important="true">kernel-*</solvable>
5 <solvable match="w" important="true">dracut</solvable>
6 <solvable match="w" important="true">glibc</solvable>
7 <solvable match="w" important="true">systemd*</solvable>
8 <solvable match="w" important="true">udev</solvable>
9 <!-- <solvable match="w">*</solvable> -->
10 </solvables>
11 </snapper-zypp-plugin-conf>

```

10.1.4.3 Criando e montando novos subvolumes

A criação de um novo subvolume abaixo da hierarquia `/` e sua montagem permanente são suportadas. Esse tipo de subvolume será excluído dos instantâneos. Não o crie dentro de um instantâneo existente, pois você não poderá mais apagar os instantâneos após um rollback.

O SUSE Linux Enterprise Desktop está configurado com o subvolume `/@/`, que serve como uma raiz independente para subvolumes permanentes, como `/opt`, `/srv`, `/home`, etc. Qualquer subvolume novo que você cria e monta permanentemente precisa ser criado nesse sistema de arquivos raiz inicial.

Para isso, execute os comandos a seguir. Neste exemplo, um novo subvolume `/usr/important` é criado do `/dev/sda2`.

```

> sudo mount /dev/sda2 -o subvol=@ /mnt
> sudo btrfs subvolume create /mnt/usr/important
> sudo umount /mnt

```

A entrada correspondente em `/etc/fstab` precisa ter a seguinte aparência:

```
/dev/sda2 /usr/important btrfs subvol=@/usr/important 0 0
```



Dica: Desabilitar Cópia em Gravação (COW, Copy-On-Write)

Um subvolume pode conter arquivos que mudam constantemente, como imagens de disco virtualizado, arquivos de banco de dados ou arquivos de registro. Se este for o caso, considere desabilitar o recurso de cópia em gravação para este volume a fim de evitar a duplicação de blocos de disco. Use a opção de montagem `nodatacow` em `/etc/fstab` para fazer isso:

```
/dev/sda2 /usr/important btrfs nodatacow,subvol=@/usr/important 0 0
```

Como alternativa, para desabilitar a cópia em gravação para arquivos ou diretórios separados, use o comando `chattr +C CAMINHO`.

10.1.4.4 Controlando o armazenamento de instantâneos

Instantâneos ocupam espaço no disco. Para evitar que os discos fiquem sem espaço e, por essa razão, provoquem interrupções no sistema, os instantâneos antigos são apagados automaticamente. Por padrão, no máximo dez instantâneos de instalação e administração importantes e dez regulares são mantidos. Se esses instantâneos ocuparem mais do que 50% do tamanho do sistema de arquivos raiz, os instantâneos adicionais serão apagados. Sempre é mantido um mínimo de quatro instantâneos importantes e dois regulares.

Consulte a [Seção 10.5.1, “Gerenciando configurações existentes”](#) para ver instruções sobre como mudar os valores.

10.1.4.5 Usando o Snapper em volumes LVM com provisionamento dinâmico

Além dos instantâneos nos sistemas de arquivos `Btrfs`, o Snapper também suporta criação de instantâneos em volumes LVM com provisionamento dinâmico (instantâneos em volumes LVM regulares *não* são suportados) formatados com XFS, Ext4 ou Ext3. Para obter mais informações e instruções de configuração de volumes LVM, consulte a *Livro “Deployment Guide”, Capítulo 6 “Expert Partitioner”, Seção 6.2 “LVM configuration”*.

Para usar o Snapper em um volume LVM com provisionamento dinâmico, você precisa criar para ele uma configuração do Snapper. No LVM, é necessário especificar o sistema de arquivos com `--fstype=lvm(SISTEMADEARQUIVOS)`. `ext3`, `ext4` ou `xfs` são valores válidos para `SISTEMADEARQUIVOS`. Exemplo:

```
> sudo snapper -c lvm create-config --fstype="lvm(xfs)" /thin_lvm
```

É possível ajustar essa configuração de acordo com as suas necessidades conforme descrito na [Seção 10.5.1, “Gerenciando configurações existentes”](#).

10.2 Usando o Snapper para desfazer mudanças

O Snapper no SUSE Linux Enterprise Desktop é pré-configurado para atuar como uma ferramenta capaz de desfazer as mudanças feitas pelo **zypper** e pelo YaST. Para esta finalidade, o Snapper é configurado para criar um par de instantâneos antes e depois de cada execução do **zypper** e do YaST. O Snapper permite também restaurar arquivos do sistema que foram acidentalmente apagados ou modificados. Os instantâneos de linha do tempo da partição raiz precisam ser habilitados para essa finalidade. Consulte a [Seção 10.1.4.1, “Desabilitando/Habilitando instantâneos”](#) para obter detalhes.

Por padrão, os instantâneos automáticos, conforme descrito anteriormente, são configurados para a partição raiz e seus subvolumes. Para disponibilizar os instantâneos para outras partições, como `/home`, é possível criar configurações personalizadas.



Importante: Comparação entre desfazer mudanças e rollback

Ao trabalhar com instantâneos para restaurar dados, é importante saber que há dois cenários fundamentalmente distintos nos quais o Snapper pode atuar:

Desfazendo mudanças

Ao desfazer mudanças conforme descrito a seguir, dois instantâneos são comparados, e as mudanças entre eles são desfeitas. O uso deste método também permite selecionar explicitamente os arquivos que devem ser restaurados.

Rollback

Ao fazer rollbacks conforme descrito na [Seção 10.3, “Rollback do sistema por inicialização de instantâneos”](#), o sistema é redefinido para o estado do momento em que o instantâneo foi criado.

Ao desfazer mudanças, é possível também comparar um instantâneo com o sistema atual. Ao restaurar *todos* os arquivos com base nesta comparação, o resultado será igual a fazer rollback. No entanto, o uso do método descrito na [Seção 10.3, “Rollback do sistema por inicialização de instantâneos”](#) para rollbacks deve ser preferencial, pois é mais rápido e permite revisar o sistema antes de fazer rollback.



Atenção: Consistência de dados

Não existe nenhum mecanismo que assegure a consistência dos dados ao criar um instantâneo. Sempre que um arquivo (por exemplo, um banco de dados) for gravado enquanto o instantâneo estiver sendo criado, o resultado será um arquivo corrompido ou parcialmente gravado. A restauração desse arquivo causa problemas. Além disso, alguns arquivos do sistema, como `/etc/mtab`, nunca devem ser restaurados. Portanto, é altamente recomendável *sempre* revisar com cuidado a lista de arquivos modificados e suas diffs. Restaure apenas arquivos realmente relevantes à ação que deseja reverter.

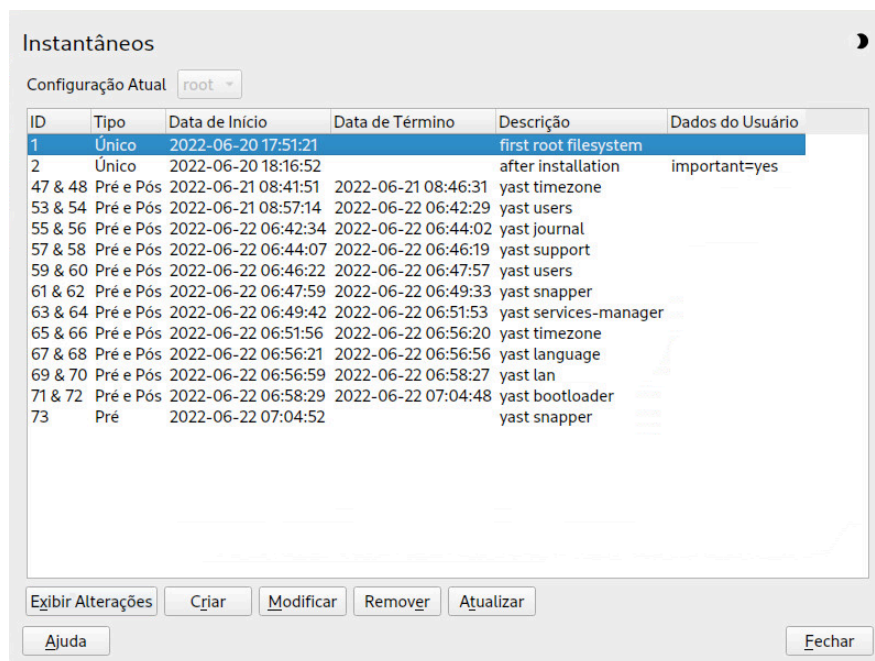
10.2.1 Desfazendo mudanças do YaST e do Zypper

Se você configurar a partição raiz com o `Btrfs` durante a instalação, o Snapper (pré-configurado para fazer rollback das mudanças do YaST ou do Zypper) será instalado automaticamente. Sempre que você iniciar um módulo do YaST ou uma transação do Zypper, serão criados dois instantâneos: um “pré-instantâneo”, que captura o estado do sistema de arquivos antes do início do módulo, e um “pós-instantâneo” após o término do módulo.

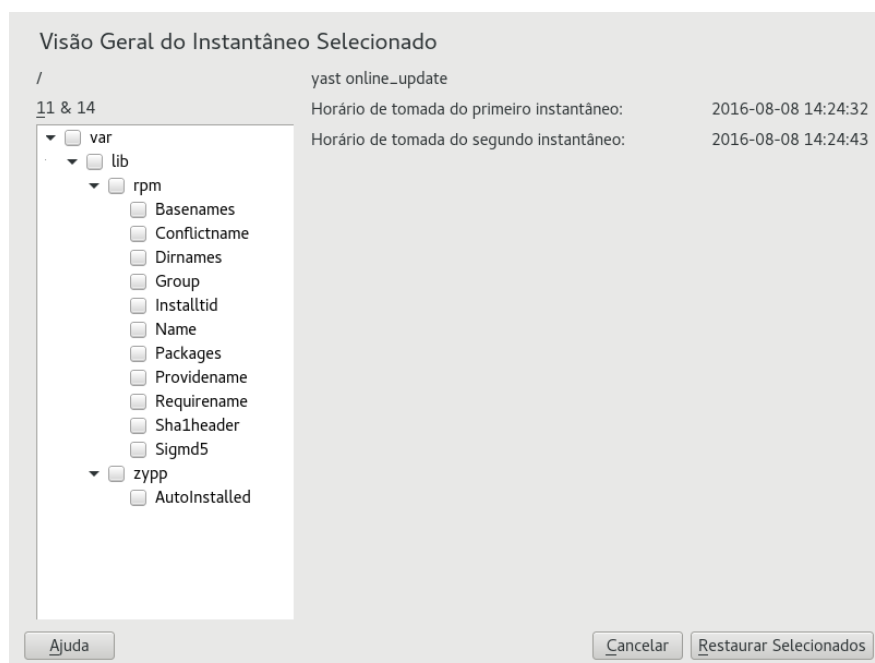
Usando o módulo Snapper do YaST ou a ferramenta de linha de comando `snapper`, é possível desfazer as mudanças feitas pelo YaST/Zypper restaurando os arquivos do “pré-instantâneo”. Pela comparação dos dois instantâneos, as ferramentas permitem ver quais arquivos foram modificados. É possível também exibir as diferenças entre as duas versões de um arquivo (diff).

PROCEDIMENTO 10.1: DESFAZENDO MUDANÇAS USANDO O MÓDULO `SNAPPER` DO YAST

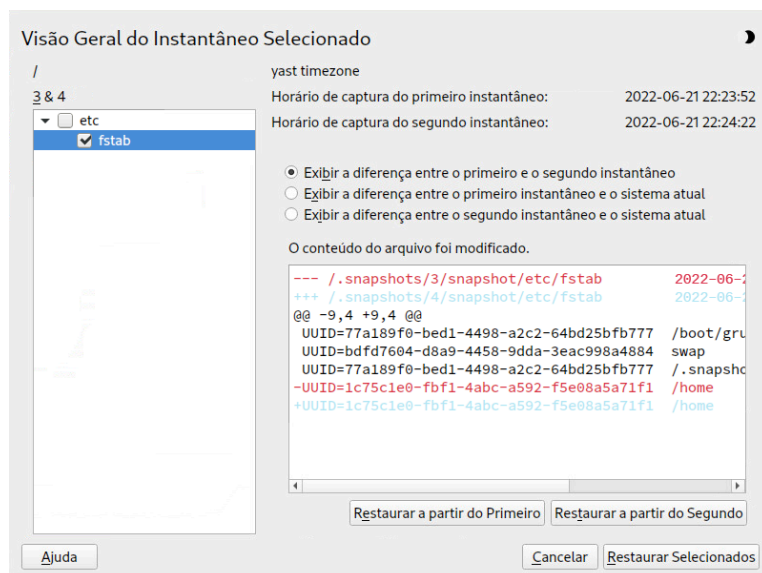
1. Inicie o módulo *Snapper* pela seção *Diversos* no YaST ou digitando `yast2 snapper`.
2. Confirme se a *Configuração Atual* está definida como *root*. Esse é sempre o caso, a não ser que você tenha adicionado manualmente configurações personalizadas do Snapper.
3. Escolha o par de pré e pós-instantâneos na lista. Ambos os pares de instantâneos do YaST e do Zypper são do tipo *Pré e Pós*. Os instantâneos do YaST são denominados `zypp(y2base)` na *coluna Descrição*; os instantâneos do Zypper são denominados `zypp(zypper)`.



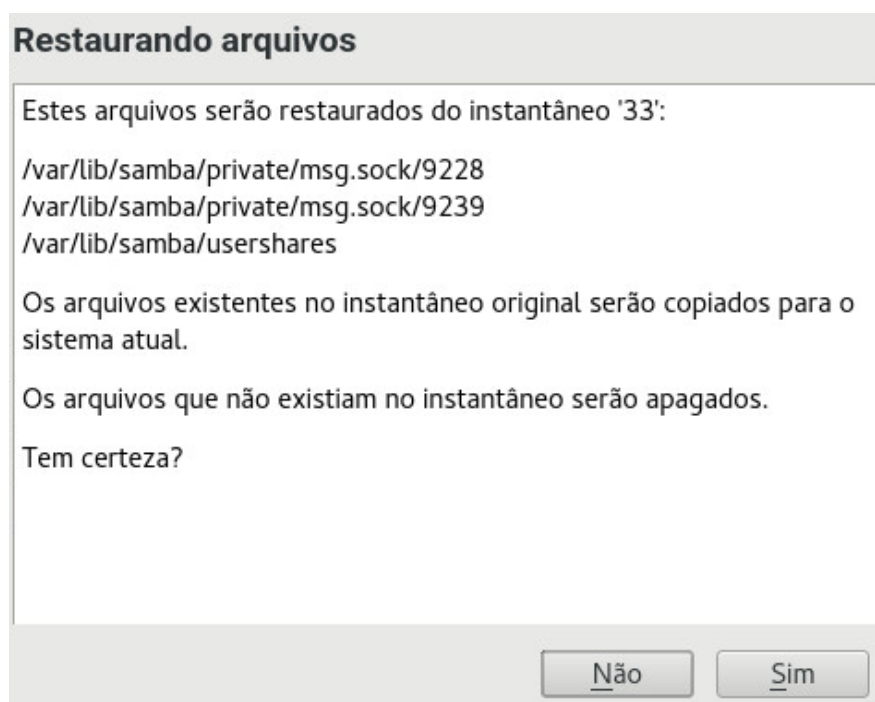
4. Clique em *Mostrar Mudanças* para abrir a lista de arquivos que são diferentes entre os dois instantâneos.



5. Revise a lista de arquivos. Para exibir a diferença (“diff”) entre a versão pré e pós de um arquivo, selecione-o na lista.



6. Para restaurar um ou mais arquivos, selecione os arquivos ou diretórios relevantes marcando a respectiva caixa de seleção. Clique em *Restaurar Selecionados* e clique em *Sim* para confirmar a ação.



Para restaurar um único arquivo, ative sua tela de comparação clicando em seu nome. Clique em *Restaurar a partir do Primeiro* e clique em *Sim* para confirmar sua seleção.

1. Obtenha uma lista dos instantâneos do YaST e do Zypper executando o comando **snapper list -t pre-post**. Os instantâneos do YaST são denominados yast *NOME_DO_MÓDULO* na *coluna Descrição*. Os instantâneos do Zypper são denominados zypp(zypper).

```
> sudo snapper list -t pre-post
```

Pre #	Post #	Pre Date	Post Date	Description
311	312	Tue 06 May 2018 14:05:46 CEST	Tue 06 May 2018 14:05:52 CEST	zypp(y2base)
340	341	Wed 07 May 2018 16:15:10 CEST	Wed 07 May 2018 16:15:16 CEST	zypp(zypper)
342	343	Wed 07 May 2018 16:20:38 CEST	Wed 07 May 2018 16:20:42 CEST	zypp(y2base)
344	345	Wed 07 May 2018 16:21:23 CEST	Wed 07 May 2018 16:21:24 CEST	zypp(zypper)
346	347	Wed 07 May 2018 16:41:06 CEST	Wed 07 May 2018 16:41:10 CEST	zypp(y2base)
348	349	Wed 07 May 2018 16:44:50 CEST	Wed 07 May 2018 16:44:53 CEST	zypp(y2base)
350	351	Wed 07 May 2018 16:46:27 CEST	Wed 07 May 2018 16:46:38 CEST	zypp(y2base)

2. Obtenha uma lista dos arquivos modificados de um par de instantâneos com **snapper status PRÉ..PÓS**. Os arquivos com mudanças de conteúdo são marcados com *c*, os arquivos que foram adicionados são marcados com *+* e os arquivos apagados são marcados com *-*.

```
> sudo snapper status 350..351
```

```
+..... /usr/share/doc/packages/mikachan-fonts
+..... /usr/share/doc/packages/mikachan-fonts/COPYING
+..... /usr/share/doc/packages/mikachan-fonts/dl.html
c..... /usr/share/fonts/truetype/fonts.dir
c..... /usr/share/fonts/truetype/fonts.scale
+..... /usr/share/fonts/truetype/#####-p.ttf
+..... /usr/share/fonts/truetype/#####-pb.ttf
+..... /usr/share/fonts/truetype/#####-ps.ttf
+..... /usr/share/fonts/truetype/#####.ttf
c..... /var/cache/fontconfig/7ef2298fde41cc6eeb7af42e48b7d293-x86_64.cache-4
c..... /var/lib/rpm/Basenames
c..... /var/lib/rpm/Dirnames
c..... /var/lib/rpm/Group
c..... /var/lib/rpm/Installtid
c..... /var/lib/rpm/Name
c..... /var/lib/rpm/Packages
c..... /var/lib/rpm/Providename
c..... /var/lib/rpm/Requirename
c..... /var/lib/rpm/Shalheader
c..... /var/lib/rpm/Sigmd5
```

3. Para exibir a diff de determinado arquivo, execute **snapper diff PRÉ..PÓS *NOMEDOARQUIVO***. Se você não especificar *NOMEDOARQUIVO*, será exibida a diff de todos os arquivos.

```
> sudo snapper diff 350..351 /usr/share/fonts/truetype/fonts.scale
--- /.snapshots/350/snapshot/usr/share/fonts/truetype/fonts.scale      2014-04-23
    15:58:57.000000000 +0200
+++ /.snapshots/351/snapshot/usr/share/fonts/truetype/fonts.scale      2014-05-07
    16:46:31.000000000 +0200
@@ -1,4 +1,4 @@
-1174
+1486
  ds=y:ai=0.2:luximr.ttf -b&h-luxi mono-bold-i-normal--0-0-0-c-0-iso10646-1
  ds=y:ai=0.2:luximr.ttf -b&h-luxi mono-bold-i-normal--0-0-0-c-0-iso8859-1
[...]
```

4. Para restaurar um ou mais arquivos, execute **snapper -v undochange** PRÉ..PÓS NOME DOS ARQUIVOS. Se você não especificar os NOME DOS ARQUIVOS, todos os arquivos serão restaurados.

```
> sudo snapper -v undochange 350..351
  create:0 modify:13 delete:7
  undoing change...
  deleting /usr/share/doc/packages/mikachan-fonts
  deleting /usr/share/doc/packages/mikachan-fonts/COPYING
  deleting /usr/share/doc/packages/mikachan-fonts/dl.html
  deleting /usr/share/fonts/truetype/#####-p.ttf
  deleting /usr/share/fonts/truetype/#####-pb.ttf
  deleting /usr/share/fonts/truetype/#####-ps.ttf
  deleting /usr/share/fonts/truetype/#####.ttf
  modifying /usr/share/fonts/truetype/fonts.dir
  modifying /usr/share/fonts/truetype/fonts.scale
  modifying /var/cache/fontconfig/7ef2298fde41cc6eeb7af42e48b7d293-x86_64.cache-4
  modifying /var/lib/rpm/Basenames
  modifying /var/lib/rpm/Dirnames
  modifying /var/lib/rpm/Group
  modifying /var/lib/rpm/Installtid
  modifying /var/lib/rpm/Name
  modifying /var/lib/rpm/Packages
  modifying /var/lib/rpm/Providename
  modifying /var/lib/rpm/Requirename
  modifying /var/lib/rpm/Shalheader
  modifying /var/lib/rpm/Sigmd5
  undoing change done
```



Atenção: Revertendo adições de usuário

Não é recomendado reverter adições de usuário desfazendo mudanças com o Snapper. Como alguns diretórios são excluídos dos instantâneos, os arquivos pertencentes a estes usuários permanecerão no sistema de arquivos. Se for criado um usuário com o mesmo ID de usuário daquele que foi apagado, ele herdar os arquivos. Portanto, é altamente recomendável usar a ferramenta *Gerenciamento de Usuários e Grupos* do YaST para remover usuários.

10.2.2 Usando o Snapper para restaurar arquivos

Além dos instantâneos de instalação e administração, o Snapper cria instantâneos de linha do tempo. É possível usar os instantâneos de backup para restaurar arquivos que foram apagados acidentalmente ou para restaurar a versão anterior de um arquivo. Usando o recurso diff do Snapper, é possível também descobrir quais modificações foram feitas em um período específico. A capacidade de restaurar arquivos é interessante principalmente no que diz respeito a dados, que podem residir em subvolumes ou partições dos quais os instantâneos não são criados por padrão. Para restaurar arquivos de diretórios pessoais, por exemplo, crie uma configuração separada do Snapper para `/home` para criar instantâneos de linha do tempo automáticos. Consulte a [Seção 10.5, “Criando e modificando as configurações do Snapper”](#) para obter instruções.



Atenção: Comparação entre restaurar arquivos e rollback

Os instantâneos criados do sistema de arquivos raiz (definido pela configuração raiz do Snapper) podem ser usados para fazer rollback do sistema. A forma recomendada de fazer o rollback é inicializar do instantâneo e depois fazer o rollback. Consulte a [Seção 10.3, “Rollback do sistema por inicialização de instantâneos”](#) para obter os detalhes.

É possível também fazer rollback restaurando todos os arquivos de um instantâneo do sistema de arquivos raiz, conforme descrito a seguir. No entanto, isso não é recomendado. É possível restaurar arquivos únicos, por exemplo, um arquivo de configuração do diretório `/etc`, mas não a lista completa de arquivos do instantâneo.

Esta restrição afeta apenas os instantâneos criados do sistema de arquivos raiz!

PROCEDIMENTO 10.3: RESTAURANDO ARQUIVOS USANDO O MÓDULO SNAPPER DO YAST

1. Inicie o módulo *Snapper* pela seção *Diversos* no YaST ou digitando `yast2 snapper`.

2. Selecione a *Configuração Atual* da qual escolher o instantâneo.
3. Selecione o instantâneo de linha do tempo do qual restaurar o arquivo e escolha *Mostrar Mudanças*. Os instantâneos de linha do tempo são do tipo *Único*, com um valor descritivo de *linha do tempo*.
4. Selecione um arquivo na caixa de texto clicando no nome dele. A diferença entre a versão do instantâneo e o sistema atual é exibida. Marque a caixa de seleção para escolher o arquivo para restauração. Faça isso para todos os arquivos que deseja restaurar.
5. Clique em *Restaurar Selecionados* e clique em *Sim* para confirmar a ação.

PROCEDIMENTO 10.4: RESTAURANDO ARQUIVOS USANDO O COMANDO **snapper**

1. Obtenha a lista de instantâneos de linha do tempo para determinada configuração executando o seguinte comando:

```
> sudo snapper -c CONFIG list -t single | grep timeline
```

CONFIG precisa ser substituído pela configuração existente do Snapper. Use **snapper list-configs** para exibir uma lista.

2. Obtenha a lista de arquivos modificados de determinado instantâneo executando o seguinte comando:

```
> sudo snapper -c CONFIG status SNAPSHOT_ID..0
```

Substitua ID_DO_INSTANTÂNEO pelo ID do instantâneo do qual deseja restaurar o(s) arquivo(s).

3. Se preferir, liste as diferenças entre a versão do arquivo atual e a versão do instantâneo executando

```
> sudo snapper -c CONFIG diff SNAPSHOT_ID..0 FILE NAME
```

Se você não especificar <NOME DE ARQUIVO>, será mostrada a diferença de todos os arquivos.

4. Para restaurar um ou mais arquivos, execute

```
> sudo snapper -c CONFIG -v undochange SNAPSHOT_ID..0 FILENAME1 FILENAME2
```

Se você não especificar nomes de arquivos, todos os arquivos mudados serão restaurados.

10.3 Rollback do sistema por inicialização de instantâneos

A versão GRUB 2 incluída no SUSE Linux Enterprise Desktop pode inicializar de instantâneos Btrfs. Juntamente com o recurso de rollback do Snapper, ela permite recuperar um sistema mal configurado. Apenas os instantâneos criados com a configuração padrão do Snapper (`root`) são inicializáveis.



Importante: Configuração suportada

A partir do SUSE Linux Enterprise Desktop 15 SP4, os rollbacks de sistema apenas serão suportados se a configuração de subvolume padrão da partição raiz não tiver sido mudada.

Ao inicializar um instantâneo, as partes do sistema de arquivos incluídas no instantâneo são montadas como apenas leitura; todos os outros sistemas de arquivos e partes excluídos dos instantâneos são montados como leitura-gravação e podem ser modificados.



Importante: Comparação entre desfazer mudanças e rollback

Ao trabalhar com instantâneos para restaurar dados, é importante saber que há dois cenários fundamentalmente distintos nos quais o Snapper pode atuar:

Desfazendo mudanças

Ao desfazer mudanças conforme descrito na [Seção 10.2, “Usando o Snapper para desfazer mudanças”](#), dois instantâneos são comparados e as mudanças entre eles são revertidas. O uso deste método também permite excluir explicitamente os arquivos selecionados para não serem restaurados.

Rollback

Ao fazer rollbacks conforme descrito a seguir, o sistema é redefinido para o estado do momento em que o instantâneo foi criado.

Para fazer rollback de um instantâneo inicializável, os seguintes requisitos devem ser atendidos. Em uma instalação padrão, o sistema é configurado apropriadamente.

REQUISITOS PARA ROLLBACK DE UM INSTANTÂNEO INICIALIZÁVEL

- O sistema de arquivos raiz precisa ser o Btrfs. A inicialização de instantâneos de volume LVM não é suportada.
- O sistema de arquivos raiz precisa estar em um único dispositivo, uma única partição e um único subvolume. Os diretórios excluídos dos instantâneos, como `/srv` (consulte [Seção 10.1.3, “Diretórios que são excluídos dos instantâneos”](#) para ver a lista completa) podem residir em partições separadas.
- O sistema precisa ser inicializável pelo carregador de boot instalado.

Para fazer rollback de um instantâneo inicializável, faça o seguinte:

1. Inicialize o sistema. No menu de boot, escolha *Bootable snapshots* (Instantâneos inicializáveis) e selecione o instantâneo que deseja inicializar. A lista de instantâneos é classificada por data: o instantâneo mais recente é listado primeiro.
2. Efetue login no sistema. Verifique com atenção se tudo funciona conforme esperado. Observe que você não pode gravar em nenhum diretório que faça parte do instantâneo. Os dados gravados em outros diretórios *não* serão perdidos, independentemente do que você faça a seguir.
3. Dependendo se você deseja ou não fazer rollback, escolha a próxima etapa:
 - a. Se o sistema está em um estado no qual você não deseja fazer rollback, reinicialize-o para inicializá-lo no estado atual do sistema. Em seguida, você pode escolher um instantâneo diferente ou iniciar o sistema de recuperação.
 - b. Para fazer o rollback, execute

```
> sudo snapper rollback
```

e reinicialize posteriormente. Na tela de boot, escolha a entrada de boot padrão para reinicializar no sistema restaurado. É criado um instantâneo do status do sistema de arquivos antes do rollback. O subvolume padrão da raiz será substituído por um novo instantâneo de leitura-gravação. Para obter os detalhes, consulte a [Seção 10.3.1, “Instantâneos após rollback”](#).

Isso é útil para adicionar uma descrição sobre o instantâneo com a opção `-d`. Por exemplo:

```
New file system root since rollback on DATE TIME
```



Dica: Voltando para um estado da instalação específico

Se os instantâneos não forem desabilitados durante a instalação, um instantâneo inicializável inicial será criado ao término da instalação do sistema inicial. É possível voltar para esse estado a qualquer momento inicializando o instantâneo. É possível identificar o instantâneo pela descrição após instalação.

Um instantâneo inicializável também é criado ao iniciar o upgrade do sistema para um service pack ou uma nova versão principal (desde que os instantâneos não estejam desabilitados).

10.3.1 Instantâneos após rollback

Antes da execução de um rollback, é criado um instantâneo do sistema de arquivos em execução. A descrição faz referência ao ID do instantâneo que foi restaurado no rollback.

Os instantâneos criados por rollbacks recebem o valor `number` para o atributo `Cleanup`. Portanto, os instantâneos de rollback são automaticamente apagados quando o número definido de instantâneos é atingido. Consulte o [Seção 10.7, “Limpeza automática de instantâneos”](#) para obter os detalhes. Se o instantâneo contém dados importantes, extraia os dados dele antes que ele seja removido.

10.3.1.1 Exemplo de instantâneo de rollback

Por exemplo, após uma nova instalação, os seguintes instantâneos estarão disponíveis no sistema:

```
# snapper --iso list
```

Type	#	Cleanup	Description	Userdata
single	0		current	
single	1		first root filesystem	
single	2	number	after installation	important=yes

Após a execução do comando `sudo snapper rollback`, o instantâneo 3 será criado com o estado do sistema antes da execução do rollback. O instantâneo 4 é o novo subvolume Btrfs padrão e, portanto, o sistema após uma reinicialização.

```
# snapper --iso list
```

Type	#	Cleanup	Description	Userdata
------	---	---------	-------------	----------

```

-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
single | 0 | | | current | |
single | 1 | | | number | first root filesystem |
single | 2 | | | number | after installation | important=yes
single | 3 | | | number | rollback backup of #1 | important=yes
single | 4 | | | | |

```

10.3.2 Acessando e identificando entradas de boot de instantâneos

Para inicializar de um instantâneo, reinicialize a máquina e escolha *Start Bootloader from a read-only snapshot* (Iniciar Carregador de Boot de instantâneo apenas leitura). Aparece uma tela com todos os instantâneos inicializáveis. O instantâneo mais recente é listado primeiro, o mais antigo por último. Use as teclas **↓** e **↑** para navegar e pressione **Enter** para ativar o instantâneo selecionado. A ativação de um instantâneo pelo menu de boot não reinicializa a máquina imediatamente; mas, em vez disso, abre o carregador de boot do instantâneo selecionado.



FIGURA 10.1: CARREGADOR DE BOOT: INSTANTÂNEOS

Cada entrada de instantâneo no carregador de boot segue um esquema de nomeação que torna possível identificá-lo facilmente:

```
[*] ① OS ② ( KERNEL ③ , DATE ④ TIME ⑤ , DESCRIPTION ⑥ )
```

- ❶ Se o instantâneo foi marcado como importante, a entrada é marcada com um *.
- ❷ Rótulo do sistema operacional.
- ❹ Data no formato AAAA-MM-DD.
- ❺ Horário no formato HH:MM.
- ❻ Esse campo mostra a descrição do instantâneo. No caso de um instantâneo criado manualmente, trata-se da string criada com a opção --description ou de uma string personalizada (consulte a *Dica: Definindo uma descrição personalizada para as entradas de instantâneos do carregador de boot*). No caso de um instantâneo criado automaticamente, trata-se da ferramenta que foi chamada, por exemplo zypp(zypper) ou yast_sw_single. Descrições extensas podem ser truncadas, dependendo do tamanho da tela de boot.



Dica: Definindo uma descrição personalizada para as entradas de instantâneos do carregador de boot

É possível substituir a string padrão no campo da descrição de um instantâneo por uma string personalizada. Isso é útil, por exemplo, quando uma descrição criada automaticamente não é suficiente, ou quando uma descrição inserida pelo usuário é muito longa. Para definir uma string personalizada STRING para o instantâneo NÚMERO, use o seguinte comando:

```
> sudo snapper modify --userdata "bootloader=STRING" NUMBER
```

A descrição deve ter no máximo 25 caracteres, tudo o que ultrapassar esse tamanho não poderá ser lido na tela de boot.

10.3.3 Limitações

O rollback do sistema *completo*, restauração do sistema completo para o estado idêntico ao que ele estava quando o instantâneo foi capturado, não é possível.

10.3.3.1 Diretórios excluídos dos instantâneos

Os instantâneos do sistema de arquivos raiz não contêm todos os diretórios. Consulte *Seção 10.1.3, "Diretórios que são excluídos dos instantâneos"* para ver os detalhes e motivos. Como consequência geral, os dados desses diretórios não são restaurados, resultando nas seguintes limitações.

Complementos e software de terceiros podem se tornar inutilizáveis após um rollback

Os aplicativos e complementos que instalam dados em subvolumes excluídos do instantâneo, como `/opt`, poderão não funcionar após o rollback, se outras partes dos dados dos aplicativos também forem instaladas em subvolumes incluídos no instantâneo. Reinstale o aplicativo ou complemento para resolver o problema.

Problemas de acesso a arquivos

Se um aplicativo mudar as permissões e/ou a propriedade do arquivo no meio tempo entre o instantâneo e o sistema atual, o aplicativo talvez não consiga acessar o arquivo. Redefina as permissões e/ou a propriedade dos arquivos afetados após o rollback.

Formatos de dados incompatíveis

Se um serviço ou aplicativo estabelecer um novo formato de dados no meio tempo entre o instantâneo e o sistema atual, o aplicativo talvez não consiga ler os arquivos de dados afetados após o rollback.

Subvolumes com mistura de códigos e dados

Subvolumes como `/srv` podem incluir uma mistura de códigos e dados. O rollback pode resultar em código não funcional. A instalação de uma versão PHP menos eficiente, por exemplo, pode resultar em scripts PHP com defeito no servidor Web.

Dados do usuário

Se o rollback remover usuários do sistema, os dados de propriedade desses usuários nos diretórios excluídos do instantâneo serão removidos. Se for criado um usuário com o mesmo ID de usuário, ele herdará os arquivos. Use uma ferramenta como `find` para localizar e remover arquivos órfãos.

10.3.3.2 Nenhum rollback dos dados do carregador de boot

Não é possível fazer rollback do carregador de boot, pois todas as “fases” do carregador de boot devem se ajustar. Isso não é garantido no caso de rollbacks de `/boot`.

10.4 Habilitando o Snapper em diretórios pessoais dos usuários

É possível habilitar instantâneos para os diretórios `/home` dos usuários, o que suporta vários casos de uso:

- Usuários individuais podem gerenciar seus próprios instantâneos e rollbacks.
- Usuários do sistema, por exemplo, administradores de banco de dados, sistema e rede, que desejam monitorar cópias de arquivos de configuração, documentação, etc.
- Compartilhamentos do Samba com diretórios pessoais e back end btrfs.

O diretório de cada usuário é um subvolume Btrfs de `/home`. É possível configurar isso manualmente (consulte a [Seção 10.4.3, “Habilitando manualmente os instantâneos em diretórios pessoais”](#)). Entretanto, o modo mais prático é usar o `pam_snapper`. O pacote `pam_snapper` instala o módulo `pam_snapper.so` e os scripts ajudantes, o que automatiza a criação de usuário e a configuração do Snapper.

O `pam_snapper` permite a integração com o comando `useradd`, os PAMs (Pluggable Authentication Modules – Módulos de Autenticação Conectáveis) e o Snapper. Por padrão, ele cria instantâneos no login e logout do usuário e também cria instantâneos com base no tempo, pois alguns usuários permanecem conectados por longos períodos. Você pode mudar os padrões usando os comandos e arquivos de configuração normais do Snapper.

10.4.1 Instalando o pam_snapper e criando usuários

A maneira mais fácil é começar com um novo diretório `/home` formatado com Btrfs e nenhum usuário existente. Instale o `pam_snapper`:

```
# zypper in pam_snapper
```

Adicione esta linha a `/etc/pam.d/common-session`:

```
session optional pam_snapper.so
```

Use o script `/usr/lib/pam_snapper/pam_snapper_useradd.sh` para criar um novo usuário e um diretório pessoal. Por padrão, o script executa um dry run. Edite o script para mudar `DRYRUN=1` para `DRYRUN=0`. Agora você pode criar um novo usuário:

```
# /usr/lib/pam_snapper/pam_snapper_useradd.sh \
```

```
username group passwd=password
Create subvolume '/home/username'
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
```

Os arquivos de `/etc/skel` serão copiados para o diretório pessoal do usuário na primeira vez que ele efetuar login. Liste suas configurações do Snapper para verificar se a configuração do usuário foi criada:

```
# snapper list --all
Config: home_username, subvolume: /home/username
Type   | # | Pre # | Date | User | Cleanup | Description | Userdata
-----+---+-----+-----+-----+-----+-----+-----
single | 0 |      |      | root |          | current     |
```

Ao longo do tempo, essa saída será preenchida com uma lista de instantâneos, que o usuário poderá gerenciar com os comandos padrão do Snapper.

10.4.2 Removendo usuários

Remova usuários com o script `/usr/lib/pam_snapper/pam_snapper_userdel.sh`. Por padrão, ele executa um dry run, portanto edite-o para mudar `DRYRUN=1` para `DRYRUN=0`. Isso remove o usuário, o subvolume pessoal do usuário, a configuração do Snapper e apaga todos os instantâneos.

```
# /usr/lib/pam_snapper/pam_snapper_userdel.sh username
```

10.4.3 Habilitando manualmente os instantâneos em diretórios pessoais

Estas são as etapas para a configuração manual dos diretórios pessoais dos usuários com o Snapper. O `/home` deve ser formatado com Btrfs, e os usuários ainda não devem ser criados.

```
# btrfs subvol create /home/username
# snapper -c home_username create-config /home/username
# sed -i -e "s/ALLOW_USERS=\"\"/ALLOW_USERS=\"username\"/g" \
/etc/snapper/configs/home_username
# yast users add username=username home=/home/username password=password
# chown username.group /home/username
# chmod 755 /home/username/.snapshots
```

10.5 Criando e modificando as configurações do Snapper

O modo como o Snapper se comporta é definido em um arquivo de configuração específico a cada partição ou subvolume Btrfs. Esses arquivos de configuração residem em /etc/snapper/configs/.

Caso o sistema de arquivos raiz seja grande o suficiente (aproximadamente 12 GB), os instantâneos serão habilitados automaticamente no sistema de arquivos raiz / na instalação. A configuração padrão correspondente é denominada raiz. Ela cria e gerencia os instantâneos do YaST e do Zypper. Consulte a [Seção 10.5.1.1, “Dados de configuração”](#) para obter uma lista dos valores padrão.



Nota: Tamanho mínimo do sistema de arquivos raiz para habilitar instantâneos

Conforme explicado na [Seção 10.1, “Configuração padrão”](#), a habilitação de instantâneos requer espaço livre adicional no sistema de arquivos raiz. A quantidade depende do número de pacotes instalados e de mudanças feitas no volume que está incluído nos instantâneos. A frequência e o número de instantâneos que são armazenados também são considerados.

Há um tamanho mínimo de sistema de arquivos raiz que é necessário para habilitar instantâneos automaticamente durante a instalação. Atualmente, esse tamanho está por volta de 12 GB. Esse valor pode mudar no futuro, dependendo da arquitetura e do tamanho do sistema básico. Ele depende dos valores para as seguintes tags no arquivo /control.xml da mídia de instalação:

```
<root_base_size>  
<btrfs_increase_percentage>
```

Ele é calculado com a seguinte fórmula: $\text{TAMANHO_BASE_RAIZ} * (1 + \text{PORCENTAGEM_AUMENTO_BTRFS} / 100)$

Lembre-se de que esse valor é um tamanho mínimo. Considere usar mais espaço para o sistema de arquivos raiz. Como regra geral, dobre o tamanho que você usa quando não tem instantâneos habilitados.

É possível criar suas próprias configurações para outras partições formatadas com `Btrfs` ou subvolumes existentes em uma partição `Btrfs`. No exemplo a seguir, nós definimos uma configuração do Snapper para backup dos dados do servidor Web que residem em uma partição separada formatada por `Btrfs` montada em `/srv/www`.

Após a criação de uma configuração, é possível usar o próprio `snapper` ou o módulo `Snapper` do YaST para restaurar arquivos desses instantâneos. No YaST, você precisa selecionar a *Configuração Atual* e especificar a configuração do `snapper` com o switch global `-c` (por exemplo, `snapper -c myconfig list`).

Para criar uma nova configuração do Snapper, execute `snapper create-config`:

```
> sudo snapper -c www-data❶ create-config /srv/www❷
```

❶ Nome do arquivo de configuração.

❷ Ponto de montagem da partição ou subvolume `Btrfs` no qual criar instantâneos.

Este comando cria um novo arquivo de configuração `/etc/snapper/configs/www-data` com valores padrão lógicos (obtidos de `/etc/snapper/config-templates/default`). Consulte a [Seção 10.5.1, “Gerenciando configurações existentes”](#) para obter instruções de como ajustar os padrões.



Dica: Padrões de configuração

Os valores padrão para uma nova configuração são obtidos de `/etc/snapper/config-templates/default`. Para usar seu próprio conjunto de padrões, crie uma cópia desse arquivo no mesmo diretório e ajuste-o de acordo com as suas necessidades. Para usá-lo, especifique a opção `-t` com o comando `create-config`:

```
> sudo snapper -c www-data create-config -t MY_DEFAULTS /srv/www
```

10.5.1 Gerenciando configurações existentes

O comando `snapper` oferece vários subcomandos para gerenciar as configurações existentes. É possível listar, mostrar, apagar e modificá-las:

Listando configurações

Use o subcomando `snapper list-configs` para obter todas as configurações existentes:

```
> sudo snapper list-configs
```

Config	Subvolume
root	/
usr	/usr
local	/local

Mostrando uma configuração

Use o subcomando **snapper -c CONFIG get-config** para exibir a configuração especificada. Substitua CONFIG por um dos nomes de configuração mostrados pelo **snapper list-configs**. Para obter mais informações sobre as opções de configuração, consulte [Seção 10.5.1.1, “Dados de configuração”](#).

Para exibir a configuração padrão, execute:

```
> sudo snapper -c root get-config
```

Modificando uma configuração

Use o subcomando **snapper -c CONFIG set-config OPÇÃO=VALOR** para modificar uma opção na configuração especificada. Substitua CONFIG por um dos nomes de configuração mostrados pelo **snapper list-configs**. Os valores possíveis para OPÇÃO e VALOR estão listados na [Seção 10.5.1.1, “Dados de configuração”](#).

Apagando uma configuração

Use o subcomando **snapper -c CONFIG delete-config** para apagar uma configuração. Substitua CONFIG por um dos nomes de configuração mostrados pelo **snapper list-configs**.

10.5.1.1 Dados de configuração

Cada configuração possui uma lista das opções que podem ser modificadas por linha de comando. A seguinte lista mostra os detalhes de cada opção. Para mudar um valor, execute **snapper -c CONFIG set-config "CHAVE=VALOR"**.

ALLOW_GROUPS, ALLOW_USERS

Conceder permissões para usar instantâneos a usuários regulares. Consulte a [Seção 10.5.1.2, “Usando o Snapper como usuário comum”](#) para obter mais informações.

O valor padrão é `""`.

BACKGROUND_COMPARISON

Define se os instantâneos pré e pós devem ser comparados em segundo plano após a criação.

O valor padrão é "yes" (sim).

EMPTY_*

Define o algoritmo de limpeza de pares de instantâneos com instantâneos pré e pós idênticos. Consulte a [Seção 10.7.3, “Limpendo pares de instantâneos que não são diferentes”](#) para obter os detalhes.

FSTYPE

Tipo de sistema de arquivos da partição. Não alterar.

O valor padrão é "btrfs".

NÚMERO_*

Define o algoritmo de limpeza de instantâneos de instalação e admin. Consulte a [Seção 10.7.1, “Limpendo instantâneos numerados”](#) para obter os detalhes.

QGROUP / SPACE_LIMIT

Adiciona suporte a cotas aos algoritmos de limpeza. Consulte a [Seção 10.7.5, “Adicionando suporte a cotas de disco”](#) para obter os detalhes.

SUBVOLUME

Ponto de montagem da partição ou do subvolume para o instantâneo. Não alterar.

O valor padrão é "/".

SYNC_ACL

Se o Snapper for utilizado por usuários regulares (consulte a [Seção 10.5.1.2, “Usando o Snapper como usuário comum”](#)), eles deverão ter acesso e ler os arquivos dos diretórios `.snapshot`. Se `SYNC_ACL` estiver definido como yes, o Snapper os tornará acessíveis automaticamente usando ACLs para usuários e grupos das entradas `ALLOW_USERS` ou `ALLOW_GROUPS`.

O valor padrão é "no".

TIMELINE_CREATE

Se definido como yes, serão criados instantâneos por hora. Valores válidos: yes, no.

O valor padrão é "no".

TIMELINE_CLEANUP / TIMELINE_LIMIT_*

Define o algoritmo de limpeza de instantâneos de linha do tempo. Consulte a [Seção 10.7.2, “Limpendo instantâneos de linha do tempo”](#) para obter os detalhes.

10.5.1.2 Usando o Snapper como usuário comum

Por padrão, o Snapper só pode ser usado pelo root. No entanto, há casos em que determinados grupos ou usuários precisam criar instantâneos ou desfazer mudanças revertendo um instantâneo:

- administradores de site na Web que desejam criar instantâneos de /srv/www
- Usuários que desejam capturar um instantâneo de seu diretório pessoal

Para essas finalidades, você pode criar configurações do Snapper que concedam permissões a usuários e/ou grupos. Os usuários especificados devem conseguir ler e acessar o diretório .snapshots correspondente. A maneira mais fácil de fazer isso é definir a opção SYNC_ACL como yes.

PROCEDIMENTO 10.5: HABILITANDO USUÁRIOS COMUNS A USAR O SNAPPER

Observe que todas as etapas deste procedimento devem ser executadas pelo root.

1. Se ainda não existir uma configuração do Snapper, crie uma para a partição ou o subvolume em que o usuário poderá usar o Snapper. Consulte a *Seção 10.5, "Criando e modificando as configurações do Snapper"* para obter instruções. Exemplo:

```
> sudo snapper --config web_data create /srv/www
```

2. O arquivo de configuração é criado em /etc/snapper/configs/CONFIG, em que CONFIG é o valor que você especificou com -c/--config na etapa anterior (por exemplo, /etc/snapper/configs/web_data). Ajuste-o de acordo com as suas necessidades. Para obter mais informações, consulte a *Seção 10.5.1, "Gerenciando configurações existentes"*.
3. Defina os valores de ALLOW_USERS e ALLOW_GROUPS para conceder permissões a usuários e grupos, respectivamente. Separe várias entradas com **Space**. Para conceder permissões ao usuário www_admin, por exemplo, execute:

```
> sudo snapper -c web_data set-config "ALLOW_USERS=www_admin" SYNC_ACL="yes"
```

4. Agora o(s) usuário(s) e grupo(s) pode(m) utilizar a configuração especificada do Snapper. É possível testá-la com o comando list, por exemplo:

```
www_admin:~ > snapper -c web_data list
```

10.6 Criando e gerenciando instantâneos manualmente

Não é possível apenas criar e gerenciar os instantâneos automaticamente pela configuração do Snapper, você também pode criar pares de instantâneos (“antes e após”) ou instantâneos únicos manualmente usando a ferramenta de linha de comando ou o módulo do YaST.

Todas as operações do Snapper são executadas de acordo com uma configuração existente (consulte a [Seção 10.5, “Criando e modificando as configurações do Snapper”](#) para obter os detalhes). Você só pode criar instantâneos de partições ou volumes em que exista uma configuração. Por padrão, a configuração do sistema (`root`) é usada. Para criar ou gerenciar instantâneos com sua própria configuração, selecione-a de maneira clara. Use a caixa suspensa *Configuração Atual* no YaST ou especifique `-c` na linha de comando (`snapper -c MINHACONFIG COMANDO`).

10.6.1 Metadados de instantâneos

Cada instantâneo consiste no próprio instantâneo e em alguns metadados. Ao criar um instantâneo, você também precisa especificar os metadados. A modificação de um instantâneo também altera seus metadados; não é possível modificar seu conteúdo. Use `snapper list` para mostrar os instantâneos existentes e seus metadados:

`snapper --config home list`

Lista os instantâneos da configuração `home`. Para listar os instantâneos da configuração padrão (raiz), use `snapper -c root list` ou `snapper list`.

`snapper list -a`

Lista os instantâneos de todas as configurações existentes.

`snapper list -t pre-post`

Lista todos os pares de instantâneos pré e pós da configuração padrão (`raiz`).

`snapper list -t single`

Lista todos os instantâneos do tipo `único` da configuração padrão (`raiz`).

Os seguintes metadados estão disponíveis para cada instantâneo:

- **Tipo:** Tipo do instantâneo, consulte a [Seção 10.6.1.1, “Tipos de instantâneos”](#) para obter os detalhes. Esses dados não podem ser mudados.
- **Número:** Número exclusivo do instantâneo. Esses dados não podem ser mudados.

- **Número do Pré:** Especifica o número do pré-instantâneo correspondente. Apenas para instantâneos do tipo pós. Esses dados não podem ser mudados.
- **Descrição:** A descrição do instantâneo.
- **Dados de usuário:** Uma descrição estendida que especifica os dados personalizados no formato de uma lista de chave=valor separada por vírgula: `reason=testing, project=foo`. Este campo também é usado para marcar um instantâneo como importante (`important=yes`) e listar o usuário que criou o instantâneo (`user=tux`).
- **Algoritmo de Limpeza:** Algoritmo de limpeza do instantâneo. Consulte a [Seção 10.7, “Limpeza automática de instantâneos”](#) para obter os detalhes.

10.6.1.1 Tipos de instantâneos

O Snapper reconhece três tipos diferentes de instantâneos: pre (pré), post (pós) e single (único). Eles são iguais fisicamente, mas o Snapper trabalha com eles de forma diferente.

pre

Instantâneo de um sistema de arquivos *antes* da modificação. Cada instantâneo pre corresponde a um instantâneo post. Por exemplo, ele é usado para instantâneos automáticos do YaST/Zypper.

post

Instantâneo de um sistema de arquivos *após* a modificação. Cada instantâneo post corresponde a um instantâneo pre. Por exemplo, ele é usado para instantâneos automáticos do YaST/Zypper.

single

Instantâneo independente. Por exemplo, ele é usado para os instantâneos automáticos por hora. Esse é o tipo padrão quando se cria instantâneos.

10.6.1.2 Algoritmos de limpeza

O Snapper oferece três algoritmos para limpeza de instantâneos antigos. Os algoritmos são executados em uma tarefa cron diária. É possível definir o número de tipos diferentes de instantâneos para serem mantidos na configuração do Snapper (consulte a [Seção 10.5.1, “Gerenciando configurações existentes”](#) para obter detalhes).

number

Apaga instantâneos antigos quando determinado número de instantâneos é atingido.

timeline

Apaga os instantâneos antigos que passaram de uma determinada duração, mas mantém vários instantâneos por hora, dia, mês e ano.

empty-pre-post

Apaga os pares de pré/pós-instantâneos com diffs vazias.

10.6.2 Criando instantâneos

Para criar um instantâneo, execute o **snapper create** ou clique em *Criar* no módulo *Snapper* do YaST. Os exemplos a seguir explicam como criar instantâneos da linha de comando. A interface do YaST para o Snapper não está especificamente descrita aqui, mas oferece uma funcionalidade equivalente.



Dica: Descrição do instantâneo

Especifique sempre uma descrição significativa para, no futuro, conseguir identificar sua finalidade. Você também pode especificar mais informações pela opção `--userdata`.

`snapper create --from 17 --description "with package2"`

Cria um instantâneo independente (tipo único) com base em um instantâneo existente, que é especificado pelo número do instantâneo de **`snapper list`**. (Isso se aplica a partir da versão 0.8.4 do Snapper.)

`snapper create --description "Instantâneo da 2ª semana de 2014"`

Cria um instantâneo independente (tipo único) na configuração padrão (`root`) com uma descrição. Como nenhum algoritmo de limpeza foi especificado, o instantâneo nunca será apagado automaticamente.

`snapper --config home create --description "Limpeza no ~tux"`

Cria um instantâneo independente (tipo único) em uma configuração personalizada chamada `home` com uma descrição. Como nenhum algoritmo de limpeza foi especificado, o instantâneo nunca será apagado automaticamente.

`snapper --config home create --description "Backup de dados diário" --cleanup-algorithm timeline >`

Cria um instantâneo independente (tipo único) em uma configuração personalizada chamada `home` com uma descrição. O instantâneo é apagado automaticamente quando atende aos critérios especificados para o algoritmo de limpeza de linha do tempo na configuração.

`snapper create --type pre --print-number --description "Antes da limpeza de config. do Apache" --userdata "important=yes"`

Cria um instantâneo do tipo `pre` e imprime o número do instantâneo. Primeiro comando necessário para criar um par de instantâneos usado para gravar o estado “antes” e “após.” O instantâneo é marcado como importante.

`snapper create --type post --pre-number 30 --description "Após a limpeza de config. do Apache" --userdata "important=yes"`

Cria um instantâneo do tipo `post` ligado a seu par `pre` de número `30`. Segundo comando necessário para criar um par de instantâneos usado para gravar o estado “antes” e “após.” O instantâneo é marcado como importante.

`snapper create --command COMANDO --description "Antes e depois do COMANDO"`

Cria automaticamente um par de instantâneos antes e após a execução do `COMANDO`. Essa opção só está disponível ao usar o `snapper` na linha de comando.

10.6.3 Modificando os metadados do instantâneo

O Snapper permite modificar a descrição, o algoritmo de limpeza e os dados do usuário de um instantâneo. Todos os outros metadados não podem ser mudados. Os exemplos a seguir explicam como modificar instantâneos da linha de comando. Eles são fáceis de adotar ao usar a interface do YaST.

Para modificar um instantâneo na linha de comando, você precisa saber o número dele. Use **`snapper list`** para exibir todos os instantâneos e seus números.

O módulo *Snapper* do YaST já lista todos os instantâneos. Escolha um na lista e clique em *Modificar*.

`snapper modify --cleanup-algorithm "timeline" 10`

Modifica os metadados do instantâneo `10` na configuração padrão (`root`). O algoritmo de limpeza é definido como `timeline`.


```
snapper --config home modify --description "backup diário" -cleanup-algorithm  
"timeline" 120
```

Modifica os metadados do instantâneo 120 na configuração personalizada chamada home. Uma nova descrição é definida e o algoritmo de limpeza fica indefinido.

10.6.4 Apagando instantâneos

Para apagar um instantâneo com o módulo *Snapper* do YaST, escolha-o na lista e clique em *Apagar*.

Para apagar um instantâneo com a ferramenta de linha de comando, você precisa saber o número dele. Para saber, execute **snapper list**. Para apagar um instantâneo, execute **snapper delete NÚMERO**.

Não é permitido apagar o instantâneo do subvolume padrão atual.

Ao apagar instantâneos com o Snapper, o espaço liberado é requerido pelo processo do Btrfs que está sendo executado em segundo plano. Portanto, há um atraso na visibilidade e disponibilidade do espaço livre. Se você precisar que o espaço liberado após apagar um instantâneo fique disponível imediatamente, use a opção **--sync** com o comando de exclusão.



Dica: Apagando pares de instantâneos

Ao apagar um instantâneo pre, sempre apague seu post correspondente (e vice-versa).

snapper delete 65

Apaga o instantâneo 65 na configuração padrão (root).

snapper -c home delete 89 90

Apaga os instantâneos 89 e 90 na configuração personalizada chamada home.

snapper delete --sync 23

Apaga o instantâneo 23 da configuração padrão (root) e torna o espaço liberado disponível imediatamente.



Dica: Apagar instantâneos não referenciados

Às vezes, o instantâneo do Btrfs está presente, mas o arquivo XML que contém os metadados do Snapper está ausente. Nesse caso, o instantâneo não fica visível para o Snapper e precisa ser apagado manualmente:

```
btrfs subvolume delete /.snapshots/SNAPSHOTNUMBER/snapshot
rm -rf /.snapshots/SNAPSHOTNUMBER
```



Dica: Instantâneos antigos ocupam mais espaço em disco

Se você apagar instantâneos para liberar espaço no disco rígido, apague primeiro os instantâneos antigos. Quanto mais antigo for o instantâneo, mais espaço em disco ele ocupa.

Os instantâneos também são automaticamente apagados por uma tarefa cron diária. Consulte o [Seção 10.6.1.2, “Algoritmos de limpeza”](#) para obter os detalhes.

10.7 Limpeza automática de instantâneos

Os instantâneos ocupam espaço em disco e, ao longo do tempo, a quantidade de espaço em disco ocupado pelos instantâneos pode ficar grande. Para evitar que os discos fiquem sem espaço, o Snapper oferece algoritmos para apagar automaticamente os instantâneos antigos. Esses algoritmos diferenciam entre instantâneos de linha do tempo e numerados (pares de instantâneos de administração e instalação). Você pode especificar quantos instantâneos de cada tipo devem ser mantidos.

Além disso, você pode especificar uma cota de espaço em disco definindo a quantidade máxima de espaço em disco que os instantâneos podem ocupar. Também é possível apagar automaticamente pares de instantâneos pré e pós que não são diferentes.

Um algoritmo de limpeza está sempre associado a uma única configuração do Snapper, portanto, talvez seja necessário definir algoritmos para cada configuração. Para impedir que determinados instantâneos sejam automaticamente apagados, consulte [P.:](#)

A configuração padrão (raiz) é definida para limpar instantâneos numerados e esvaziar pares de instantâneos pré e pós. O suporte a cotas está habilitado, os instantâneos não podem ocupar mais do que 50% do espaço em disco disponível da partição raiz. Por padrão, os instantâneos de linha do tempo estão desabilitados, portanto, o algoritmo de limpeza de linha do tempo também está desabilitado.

10.7.1 Limpando instantâneos numerados

A limpeza de instantâneos numerados, pares de instantâneos de administração e de instalação, é controlada pelos seguintes parâmetros de uma configuração do Snapper.

NUMBER_CLEANUP

Habilita ou desabilita a limpeza de pares de instantâneos de instalação e admin. Se habilitado, os pares de instantâneos são apagados quando o número total de instantâneos exceder o número especificado com NUMBER_LIMIT e/ou NUMBER_LIMIT_IMPORTANT e uma duração especificada com NUMBER_MIN_AGE. Valores válidos: yes (habilitar), no (desabilitar).

O valor padrão é "yes" (sim).

Exemplo de comando para mudar ou definir:

```
> sudo snapper -c CONFIG set-config "NUMBER_CLEANUP=no"
```

NUMBER_LIMIT / NUMBER_LIMIT_IMPORTANT

Define quantos pares de instantâneos de instalação e administração regulares e/ou importantes devem ser mantidos. Ignorado se NUMBER_CLEANUP for definido como "no". O valor padrão é "2-10" para NUMBER_LIMIT e "4-10" para NUMBER_LIMIT_IMPORTANT. Os algoritmos de limpeza apagam os instantâneos acima do valor máximo especificado, sem levar em consideração o espaço do instantâneo e do sistema de arquivos. Os algoritmos também apagam os instantâneos acima do valor mínimo até que os limites do instantâneo e do sistema de arquivos sejam atingidos.

Exemplo de comando para mudar ou definir:

```
> sudo snapper -c CONFIG set-config "NUMBER_LIMIT=10"
```



Importante: Comparação entre valores de faixa e constantes

Se o suporte a cotas estiver habilitado (consulte a [Seção 10.7.5, “Adicionando suporte a cotas de disco”](#)), o limite deverá ser especificado como uma faixa de mínimo-máximo, por exemplo, 2-10. Se o suporte a cotas estiver desabilitado, um valor constante, como 10, deverá ser informado; do contrário, haverá falha na limpeza com um erro.

NUMBER_MIN_AGE

Define a duração mínima em segundos do instantâneo antes de ser automaticamente apagado. Os instantâneos mais novos do que o valor especificado aqui não serão apagados, independentemente de quantos existirem.

O valor padrão é "1800".

Exemplo de comando para mudar ou definir:

```
> sudo snapper -c CONFIG set-config "NUMBER_MIN_AGE=864000"
```



Nota: Limite e duração

NUMBER_LIMIT, NUMBER_LIMIT_IMPORTANT e NUMBER_MIN_AGE são sempre avaliados. Os instantâneos são apagados apenas quando ocorrem *todas* as condições.

Se você deseja sempre manter o número de instantâneos definido com NUMBER_LIMIT*, independentemente da duração deles, defina NUMBER_MIN_AGE como 0.

O exemplo a seguir mostra uma configuração para manter os 10 últimos instantâneos importantes e regulares, independentemente da data em que foram criados:

```
NUMBER_CLEANUP=yes
NUMBER_LIMIT_IMPORTANT=10
NUMBER_LIMIT=10
NUMBER_MIN_AGE=0
```

Por outro lado, se você não deseja manter os instantâneos que passarem de uma determinada duração, defina NUMBER_LIMIT* como 0 e informe a duração usando NUMBER_MIN_AGE.

O exemplo a seguir mostra uma configuração para manter apenas instantâneos com menos de dez dias:

```
NUMBER_CLEANUP=yes
NUMBER_LIMIT_IMPORTANT=0
```

```
NUMBER_LIMIT=0
NUMBER_MIN_AGE=864000
```

10.7.2 Limpando instantâneos de linha do tempo

A limpeza de instantâneos de linha do tempo é controlada pelos seguintes parâmetros de uma configuração do Snapper.

TIMELINE_CLEANUP

Habilita ou desabilita a limpeza de instantâneos de linha do tempo. Se habilitado, os instantâneos são apagados quando o número total excede o número especificado com TIMELINE_LIMIT_* e a duração especificada com TIMELINE_MIN_AGE. Valores válidos: yes, no.

O valor padrão é "yes" (sim).

Exemplo de comando para mudar ou definir:

```
> sudo snapper -c CONFIG set-config "TIMELINE_CLEANUP=yes"
```

TIMELINE_LIMIT_DAILY, TIMELINE_LIMIT_HOURLY, TIMELINE_LIMIT_MONTHLY, TIMELINE_LIMIT_WEEKLY, TIMELINE_LIMIT_YEARLY

Número de instantâneos para manter por hora, dia, mês, semana e ano.

O valor padrão de cada entrada é "10", exceto para TIMELINE_LIMIT_WEEKLY, que, por padrão, é definido como "0".

TIMELINE_MIN_AGE

Define a duração mínima em segundos do instantâneo antes de ser automaticamente apagado.

O valor padrão é "1800".

EXEMPLO 10.1: EXEMPLO DE CONFIGURAÇÃO DE LINHA DO TEMPO

```
TIMELINE_CLEANUP="yes"
TIMELINE_CREATE="yes"
TIMELINE_LIMIT_DAILY="7"
TIMELINE_LIMIT_HOURLY="24"
TIMELINE_LIMIT_MONTHLY="12"
TIMELINE_LIMIT_WEEKLY="4"
TIMELINE_LIMIT_YEARLY="2"
TIMELINE_MIN_AGE="1800"
```

Este exemplo de configuração habilita os instantâneos por hora, que são limpos automaticamente. `TIMELINE_MIN_AGE` e `TIMELINE_LIMIT_*` são sempre avaliados juntos. Neste exemplo, a duração mínima de um instantâneo, antes de ser apagado, está definida como 30 minutos (1800 segundos). Como nós criamos instantâneos por hora, isso garante que apenas os instantâneos mais recentes sejam mantidos. Se `TIMELINE_LIMIT_DAILY` não estiver definido como zero, significa que o primeiro instantâneo do dia também será mantido.

INSTANTÂNEOS QUE DEVEM SER MANTIDOS

- De hora em hora: Os últimos 24 instantâneos que foram capturados.
- Diariamente: O primeiro instantâneo diário que foi capturado é mantido para os últimos sete dias.
- Mensalmente: O primeiro instantâneo capturado no último dia do mês é mantido para os últimos 20 meses.
- Semanalmente: O primeiro instantâneo capturado no último dia da semana é mantido para as últimas quatro semanas.
- Anualmente: O primeiro instantâneo capturado no último dia do ano é mantido para os últimos dois anos.

10.7.3 Limpando pares de instantâneos que não são diferentes

Conforme explicado em [Seção 10.1.2, “Tipos de instantâneos”](#), sempre que você executar um módulo do YaST ou o Zypper, um pré-instantâneo é criado na inicialização, e um pós-instantâneo é criado durante o encerramento. Se você não fez nenhuma mudança, não haverá diferença entre os instantâneos pré e pós. Esses tipos de pares de instantâneos “vazios” podem ser automaticamente apagados ao definir os seguintes parâmetros em uma configuração do Snapper:

`EMPTY_PRE_POST_CLEANUP`

Se definido como yes (sim), os pares de instantâneos pré e pós que forem iguais serão apagados.

O valor padrão é "yes" (sim).

`EMPTY_PRE_POST_MIN_AGE`

Define a duração mínima, em segundos, do par de instantâneos pré e pós iguais antes de ser automaticamente apagado.

O valor padrão é "1800".

10.7.4 Limpando instantâneos criados manualmente

O Snapper não oferece algoritmos de limpeza personalizados para instantâneos criados manualmente. No entanto, você pode atribuir o algoritmo de limpeza de número ou linha do tempo a um instantâneo criado manualmente. Se você fizer isso, o instantâneo ingressará na “fila de limpeza” do algoritmo especificado. Você pode especificar um algoritmo de limpeza ao criar um instantâneo ou modificar um instantâneo existente:

snapper create --description "Teste" --cleanup-algorithm number

Cria um instantâneo independente (tipo único) para a configuração padrão (raiz) e atribui o algoritmo de limpeza de número.

snapper modify --cleanup-algorithm "timeline" 25

Modifica o instantâneo com o número 25 e atribui o algoritmo de limpeza de linha do tempo.

10.7.5 Adicionando suporte a cotas de disco

Além dos algoritmos de limpeza de número e/ou linha do tempo descritos anteriormente, o Snapper suporta cotas. Você pode definir a porcentagem de espaço disponível que os instantâneos podem ocupar. Esse valor percentual é sempre aplicado ao subvolume Btrfs definido na respectiva configuração do Snapper.

As cotas do Btrfs são aplicadas aos subvolumes, e não aos usuários. Você pode aplicar as cotas de espaço em disco a usuários e grupos (por exemplo, com o comando **quota**), além de usar as cotas do Btrfs.

Se o Snapper foi habilitado durante a instalação, o suporte a cotas é automaticamente habilitado. Se você habilitar manualmente o Snapper em algum momento futuro, poderá habilitar o suporte a cotas executando **snapper setup-quota**. Isso exige uma configuração válida (consulte a [Seção 10.5, “Criando e modificando as configurações do Snapper”](#) para obter mais informações).

O suporte a cotas é controlado pelos seguintes parâmetros de uma configuração do Snapper.

QGROUP

O grupo de cotas Btrfs usado pelo Snapper. Se não foi definido, execute `snapper setup-quota`. Se já foi definido, apenas mude se você estiver familiarizado com `man 8 btrfs-qgroup`. Esse valor é definido com `snapper setup-quota` e não deve ser mudado.

SPACE_LIMIT

Limite de espaço que os instantâneos podem ocupar em frações de 1 (100%). Os valores válidos são de 0 a 1 (0,1 = 10%, 0,2 = 20%, etc.).

As seguintes diretrizes e limitações são aplicadas:

- As cotas apenas são ativadas *adicionalmente* a um algoritmo de limpeza de número e/ou linha do tempo existente. Se nenhum algoritmo de limpeza estiver ativo, as restrições de cotas não serão aplicadas.
- Com o suporte a cotas habilitado, o Snapper executa duas limpezas, se necessário. A primeira execução aplica-se às regras especificadas para os instantâneos de número e linha do tempo. Apenas se a cota for excedida após essa execução, as regras específicas da cota serão aplicadas em uma segunda execução.
- Mesmo se o suporte a cotas estiver habilitado, o Snapper sempre manterá o número de instantâneos especificado com os valores `NUMBER_LIMIT*` e `TIMELINE_LIMIT*`, até quando a cota for excedida. Portanto, é recomendável especificar valores de faixa (*MÍN-MÁX*) para `NUMBER_LIMIT*` e `TIMELINE_LIMIT*` para garantir que a cota seja aplicada. Por exemplo, se for definido `NUMBER_LIMIT=5-20`, o Snapper executará uma primeira limpeza e reduzirá o número de instantâneos numerados regulares para 20. Se esses 20 instantâneos excederem a cota, o Snapper apagará os mais antigos em uma segunda execução até que a cota seja atendida. Um mínimo de cinco instantâneos é sempre mantido, independentemente da quantidade de espaço que ocupam.

10.8 Mostrando o espaço em disco exclusivo usado pelos instantâneos

Os instantâneos compartilham dados para uso eficiente do espaço de armazenamento, portanto, o uso de comandos comuns como **du** e **df** não medirá o espaço em disco usado com precisão. Para liberar espaço em disco no Btrfs com as cotas habilitadas, você precisa saber quanto espaço em disco exclusivo é usado por cada instantâneo, em vez do espaço compartilhado. A partir do Snapper 0.6, o espaço em disco usado é relatado para cada instantâneo na coluna Used Space:

```
# snapper--iso list
# | Type | Pre # | Date | User | Used Space | Cleanup | Description
| Userdata
-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
0 | single | | | root | | | current
|
1* | single | | 2019-07-22 13:08:38 | root | 16.00 KiB | | first root
filesystem |
2 | single | | 2019-07-22 14:21:05 | root | 14.23 MiB | number | after
installation | important=yes
3 | pre | | 2019-07-22 14:26:03 | root | 144.00 KiB | number | zypp(zypper)
| important=no
4 | post | 3 | 2019-07-22 14:26:04 | root | 112.00 KiB | number |
| important=no
5 | pre | | 2019-07-23 08:19:36 | root | 128.00 KiB | number | zypp(zypper)
| important=no
6 | post | 5 | 2019-07-23 08:19:43 | root | 80.00 KiB | number |
| important=no
7 | pre | | 2019-07-23 08:20:50 | root | 256.00 KiB | number | yast sw_single
|
8 | pre | | 2019-07-23 08:23:22 | root | 112.00 KiB | number |
zypp(ruby.ruby2.5) | important=no
9 | post | 8 | 2019-07-23 08:23:35 | root | 64.00 KiB | number |
| important=no
10 | post | 7 | 2019-07-23 08:24:05 | root | 16.00 KiB | number |
|
```

O comando **btrfs** apresenta outra exibição do espaço usado pelos instantâneos:

```
# btrfs qgroup show -p /
qgroupid      rfer      excl parent
-----
0/5          16.00KiB   16.00KiB ---
[...]
```

0/272	3.09GiB	14.23MiB	1/0
0/273	3.11GiB	144.00KiB	1/0
0/274	3.11GiB	112.00KiB	1/0
0/275	3.11GiB	128.00KiB	1/0
0/276	3.11GiB	80.00KiB	1/0
0/277	3.11GiB	256.00KiB	1/0
0/278	3.11GiB	112.00KiB	1/0
0/279	3.12GiB	64.00KiB	1/0
0/280	3.12GiB	16.00KiB	1/0
1/0	3.33GiB	222.95MiB	---

A coluna `qgroupid` exibe o número de identificação de cada subvolume, atribuindo uma combinação de nível/ID do qgroup.

A coluna `rfer` exibe o volume total de dados mencionados no subvolume.

A coluna `excl` exibe os dados exclusivos em cada subvolume.

A coluna `parent` mostra o qgroup pai dos subvolumes.

O item final `1/0` mostra os totais para o qgroup pai. No exemplo acima, 222,95 MiB serão liberados se todos os subvolumes forem removidos. Execute o comando a seguir para ver os instantâneos que estão associados a cada subvolume:

```
# btrfs subvolume list -st /
ID gen top level path
-- --
267 298 266 @/.snapshots/1/snapshot
272 159 266 @/.snapshots/2/snapshot
273 170 266 @/.snapshots/3/snapshot
274 171 266 @/.snapshots/4/snapshot
275 287 266 @/.snapshots/5/snapshot
276 288 266 @/.snapshots/6/snapshot
277 292 266 @/.snapshots/7/snapshot
278 296 266 @/.snapshots/8/snapshot
279 297 266 @/.snapshots/9/snapshot
280 298 266 @/.snapshots/10/snapshot
```

Um upgrade de um pacote de serviço para outro resulta em instantâneos que ocupam muito espaço em disco nos subvolumes do sistema. É recomendada a exclusão manual dos instantâneos quando eles não são mais necessários. Consulte a [Seção 10.6.4, “Apagando instantâneos”](#) para obter os detalhes.

10.9 Perguntas frequentes

P: Por que o Snapper nunca mostra as mudanças em `/var/log`, `/tmp` e outros diretórios?

R: Para alguns diretórios, nós decidimos excluí-los dos instantâneos. Consulte a [Seção 10.1.3, “Diretórios que são excluídos dos instantâneos”](#) para ver a lista e os motivos. Para excluir um caminho dos instantâneos, nós criamos um subvolume para esse caminho.

P: Posso inicializar um instantâneo do carregador de boot?

R: Sim, veja os detalhes na [Seção 10.3, “Rollback do sistema por inicialização de instantâneos”](#).

P: Um instantâneo pode ser protegido contra exclusão?

R: Atualmente, o Snapper não oferece meios para evitar que um instantâneo seja apagado manualmente. No entanto, você pode impedir que os instantâneos sejam automaticamente apagados por algoritmos de limpeza. Os instantâneos criados manualmente (consulte a [Seção 10.6.2, “Criando instantâneos”](#)) não têm algoritmo de limpeza atribuído, a menos que você especifique um com `--cleanup-algorithm`. Os instantâneos criados automaticamente sempre têm o algoritmo de `número` ou de `linha do tempo` atribuído. Para remover esse tipo de atribuição de um ou mais instantâneos, faça o seguinte:

1. Liste todos os instantâneos disponíveis:

```
> sudo snapper list -a
```

2. Memorize o número de instantâneos cuja exclusão deve ser evitada.

3. Execute o seguinte comando e substitua os marcadores de número pelos números que você memorizou:

```
> sudo snapper modify --cleanup-algorithm "" #1 #2 #n
```

4. Verifique o resultado executando `snapper list -a` novamente. Agora, a entrada na coluna `Limpeza` deve estar vazio para os instantâneos que você modificou.

P: Onde encontro mais informações sobre o Snapper?

R: Consulte a home page do Snapper em <http://snapper.io/>.

11 Kernel Live Patching com KLP

Este documento descreve os princípios básicos da tecnologia Kernel Live Patching (KLP) e apresenta as diretrizes de uso para o serviço SLE Live Patching.

O KLP possibilita a aplicação das atualizações de segurança mais recentes aos kernels do Linux sem reinicialização. Esse procedimento maximiza o tempo de atividade e a disponibilidade do sistema, que são essenciais para sistemas de extrema importância.

As informações contidas neste documento são relacionadas às arquiteturas AMD64/Intel 64, POWER e IBM Z.

11.1 Vantagens do Kernel Live Patching

O KLP oferece vários benefícios.

- Manter um grande número de servidores automaticamente atualizados é essencial para que as organizações obtenham ou mantenham determinadas certificações de conformidade. O KLP pode ajudar a atingir a conformidade e reduzir a necessidade de janelas de manutenção dispendiosas.
- As empresas que trabalham com contratos de nível de serviço devem garantir um nível específico de acessibilidade e tempo de atividade do sistema. O Live Patching possibilita a aplicação de patches aos sistemas sem causar tempo de espera.
- Como o KLP faz parte do mecanismo de atualização do sistema padrão, não há necessidade de treinamento especializado nem de introdução de rotinas de manutenção complicadas.

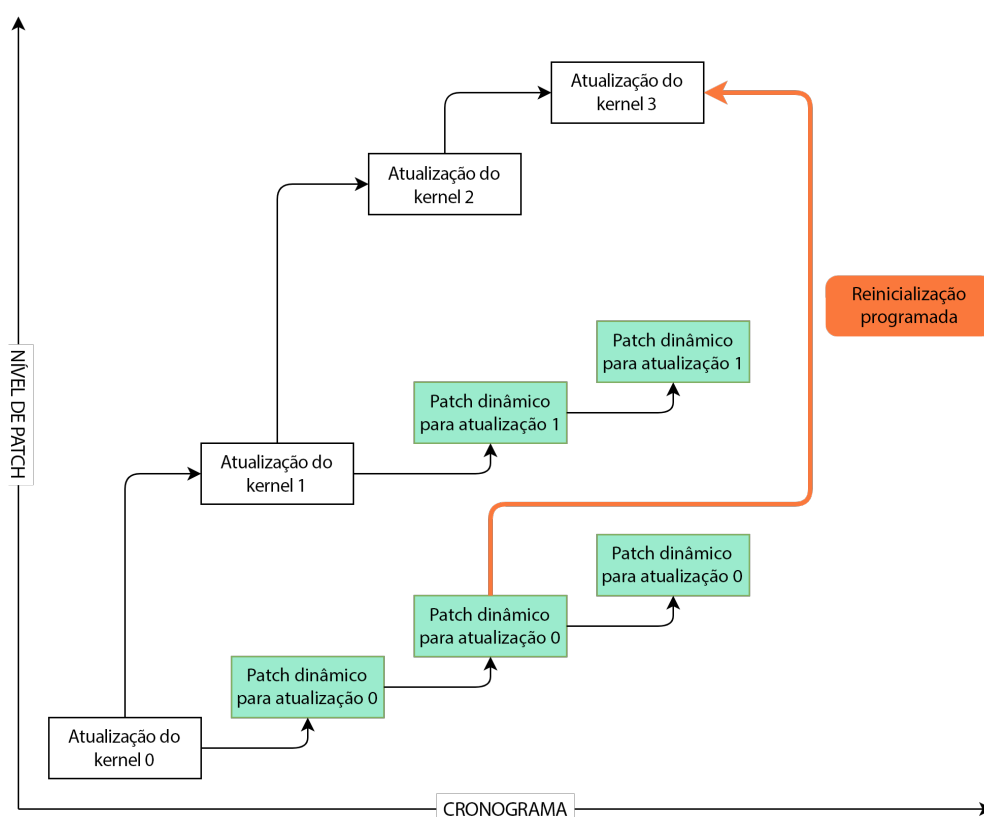
11.2 Visão geral do Kernel Live Patching

Os patches ativos do kernel são oferecidos como pacotes com código modificado, separados do pacote do kernel principal. Os patches ativos são cumulativos, portanto, o patch mais recente contém todas as correções dos anteriores no pacote do kernel. Cada pacote ativo do kernel está vinculado à revisão exata do kernel para a qual ele foi gerado. O número da versão do pacote ativo do kernel aumenta a cada adição de correções.

! Importante: Patches ativos comparados com as atualizações do kernel

Os patches ativos contêm apenas as correções críticas e não substituem as atualizações regulares do kernel que exigem reinicialização. Considere os patches ativos como medidas temporárias que protegem o kernel até que uma atualização apropriada e uma reinicialização do kernel sejam executadas.


O diagrama abaixo ilustra o relacionamento geral entre os patches ativos e as atualizações do kernel. É possível ver a lista de CVEs e os relatórios de defeitos resolvidos pelo patch ativo atual usando o comando `klp -v patches`.



É possível ter várias versões do pacote do kernel instaladas junto com os patches ativos. Esses pacotes não entram em conflito. Você pode instalar os pacotes do kernel atualizados junto com os patches ativos do kernel em execução. Nesse caso, talvez seja solicitado para você reiniciar o sistema. Os usuários com assinaturas do SLE Live Patching estão qualificados para suporte técnico, desde que haja atualizações de patch ativas para o kernel em execução (consulte a [Seção 11.5.1, “Verificando a data de vencimento do patch ativo”](#)).

Com o KLP ativado, todas as atualizações de kernel vêm com um pacote de patch ativo. Esse patch ativo não contém nenhuma correção e funciona como uma propagação para patches ativos futuros do kernel correspondente. Esses patches de propagação vazios são chamados de patches iniciais.


11.2.1 Escopo do Kernel Live Patching

O escopo do SLE Live Patching inclui correções de vulnerabilidades de nível 7 ou superior do SUSE Common Vulnerability Scoring System (CVSS: o SUSE CVSS é baseado no sistema CVSS v3.0) e correções de bugs relacionadas à estabilidade do sistema ou corrupção de dados. No entanto, talvez não seja tecnicamente viável criar patches ativos para todas as correções que se enquadram nas categorias especificadas. Portanto, a SUSE reserva o direito de ignorar as correções em situações em que a criação de um patch ativo do kernel não seja possível por motivos técnicos. Atualmente, mais de 95% das correções qualificadas são lançadas como patches ativos. Para obter mais informações sobre o CVSS (a base para a classificação SUSE CVSS), consulte [Common Vulnerability Scoring System SIG \(https://www.first.org/cvss/\)](https://www.first.org/cvss/) .

11.2.2 Limitações do Kernel Live Patching

O KLP envolve a substituição de funções e o tratamento adequado da substituição de conjuntos de funções interdependentes. Isso é feito redirecionando as chamadas do código antigo para o código atualizado em um local de memória diferente. As mudanças nas estruturas de dados tornam a situação mais complicada, pois os dados permanecem no local e não podem ser estendidos ou reinterpretados. Existem técnicas que permitem a alteração indireta das estruturas de dados, mas algumas correções não podem ser convertidas em patches ativos. Nessa situação, a reinicialização do sistema é a única maneira de aplicar as correções.

11.3 Ativando o Kernel Live Patching por meio do YaST

Para ativar o KLP no sistema, você precisa ter assinaturas ativas do SLES e do SLE Live Patching. Visite o [SUSE Customer Center \(https://scc.suse.com/\)](https://scc.suse.com/)  para verificar o status das suas assinaturas e obter um código de registro para a assinatura do SLE Live Patching.

Para ativar o Kernel Live Patching no sistema, siga estas etapas:

1. Execute o comando **yast2 registration** e clique em *Selecionar Extensões*.
2. Selecione *SUSE Linux Enterprise Live Patching 15* na lista de extensões disponíveis e clique em *Próximo*.
3. Confirme os termos da licença e clique em *Próximo*.
4. Digite o código de registro do SLE Live Patching e clique em *Próximo*.
5. Confira o *Resumo da Instalação* e os *Padrões* selecionados. Os padrões *Live Patching* e *SLE Live Patching Lifecycle Data* devem estar automaticamente selecionados para instalação junto com outros pacotes para atender às dependências.
6. Clique em *Aceitar* para concluir a instalação. Isso instalará os componentes base do Kernel Live Patching no sistema, o patch ativo inicial e as dependências necessárias.

11.4 Ativando o Kernel Live Patching pela linha de comando

Para ativar o Kernel Live Patching, você precisa ter assinaturas ativas do SLES e do SLES Live Patching. Visite o [SUSE Customer Center \(https://scc.suse.com/\)](https://scc.suse.com/) para verificar o status das suas assinaturas e obter um código de registro para a assinatura do SLES Live Patching.

1. Execute **sudo SUSEConnect --list-extensions**. Observe o comando de ativação exato do SLES Live Patching. Exemplo de saída de comando (abreviado):

```
$ SUSEConnect --list-extensions
...
SUSE Linux Enterprise Live Patching 15 SP4 x86_64
Activate with: SUSEConnect -p sle-module-live-patching/15.4/x86_64 \
-r ADDITIONAL REGCODE
```

2. Ative o SLES Live Patching usando o comando obtido seguido de **-r LIVE_PATCHING_REGISTRATION_CODE**, por exemplo:

```
SUSEConnect -p sle-module-live-patching/15.4/x86_64 \
-r LIVE_PATCHING_REGISTRATION_CODE
```


3. Instalar os pacotes e as dependências necessários usando o comando **zypper install -t pattern lp_sles**

Neste ponto, o patch ativo já foi aplicado ao sistema.

Veja como o processo é realizado: Quando o sistema de instalação de pacotes detecta que há um kernel instalado ao qual pode ser aplicado um patch ativo e que existe um patch ativo para ele no canal de software, o sistema seleciona o patch ativo para instalação. Em seguida, o kernel recebe as correções de patch ativo *como parte da instalação do pacote*. O kernel recebe o patch ativo mesmo antes da conclusão da instalação do produto.

11.5 Executando o Kernel Live Patching

Os patches ativos do kernel são instalados como parte das atualizações regulares do sistema. No entanto, há várias informações que você deve saber.

- O kernel recebe patches ativos se um pacote `kernel-livepatch-*` foi instalado para o kernel em execução. Você pode usar o comando `zypper se --details kernel-livepatch-*` para verificar se os pacotes de patch ativo do kernel estão instalados no seu sistema.
- Quando o pacote `kernel-default` está instalado, o gerenciador de atualizações solicita para você reinicializar o sistema. Para evitar que essa mensagem apareça, você pode remover essas atualizações do kernel da operação de aplicação de patches. Para fazer isso, você pode adicionar bloqueios de pacote com o Zypper. O SUSE Manager também possibilita filtrar o conteúdo do canal (consulte [Live Patching with SUSE Manager \(https://documentation.suse.com/external-tree/en-us/suma/4.1/suse-manager/administration/live-patching.html\)](https://documentation.suse.com/external-tree/en-us/suma/4.1/suse-manager/administration/live-patching.html) .
- Você pode verificar o status da aplicação de patches usando o comando `klp status`. Para examinar os patches instalados, execute o comando `klp -v patches`.
- Mesmo que haja vários pacotes de kernel instalados no sistema, lembre-se de que apenas um deles estará em execução em um determinado momento. Da mesma forma, pode haver vários pacotes de patches ativos instalados, mas apenas um patch ativo será carregado no kernel.
- O patch ativo está incluído no `initrd`. Isso significa que, no caso de uma reinicialização inesperada, o sistema já vem com as correções de patch ativo aplicadas, portanto, não há necessidade de executar a aplicação de patches novamente.

11.5.1 Verificando a data de vencimento do patch ativo

Verifique se o `lifecycle-data-sle-module-live-patching` está instalado e execute o comando `zypper lifecycle`. Você deve ver as datas de vencimento dos patches ativos na seção `Package end of support if different from product` (Fim do suporte do pacote se diferente do produto) da saída.

Cada patch ativo recebe atualizações por um ano a partir do lançamento do pacote de kernel subjacente. A página [Maintained kernels, patch updates and lifecycle](https://www.suse.com/products/live-patching/current-patches/) (<https://www.suse.com/products/live-patching/current-patches/>) (Kernels mantidos, atualizações de patch e ciclo de vida) permite verificar as datas de vencimento com base na versão do kernel em execução sem instalar a extensão do produto.

11.6 Solucionando problemas do Kernel Live Patching

11.6.1 Downgrade manual do patch

Se o patch ativo mais recente for problemático, você poderá fazer downgrade do patch ativo instalado no momento para a versão anterior. Recomendamos fazer o downgrade do patch antes que o sistema comece a apresentar problemas. Lembre-se de que um sistema com avisos de kernel ou rastreamentos de erro de kernel no registro do sistema pode não ser adequado para o procedimento de downgrade de patch. Se você não tiver certeza se o sistema atende aos requisitos para um downgrade de patch, contate o Suporte Técnico da SUSE para obter ajuda.

PROCEDIMENTO 11.1: DOWNGRADE MANUAL DO PATCH

1. Identifique o patch ativo em execução usando o comando `klp -v patches`. Você pode ver o patch que está em execução na linha que começa com `RPM:`. Por exemplo:

```
RPM: kernel-livepatch-5_3_18-24_29-default-2-2.1.x86_64
```

O `5_3_18-24_29-default` no exemplo acima indica a versão exata do kernel em execução.

2. Use o comando `zypper search -s kernel-livepatch-VERSÃO_DO_KERNEL_EM_EXECUÇÃO-default` para pesquisar versões anteriores do patch. O comando retorna uma lista de versões de pacote disponíveis. Para cada novo lançamento de pacote de patch ativo, lembre-se de que o número da versão aumenta em um. Escolha a versão com um número abaixo da versão atual.
3. Instale a versão desejada com o comando `zypper in --oldpackage kernel-livepatch-VERSÃO_DO_KERNEL_EM_EXECUÇÃO-default=VERSÃO_DESEJADA`.

12 Aplicação de patches ativos no espaço do usuário

Este documento descreve os princípios básicos e o uso da aplicação de patches ativos no espaço do usuário.

12.1 Sobre a aplicação de patches ativos no espaço do usuário

A aplicação de patches ativos no espaço do usuário (ULP, Userspace Live Patching) refere-se ao processo de aplicar patches às bibliotecas usadas por um processo em execução sem o interromper. As operações de aplicação de patches ativos são executadas usando a ferramenta ulp, que faz parte do libpulp.

O libpulp é uma estrutura que permite a aplicação de patches ativos no espaço do usuário. Ele consiste na biblioteca libpulp.so e em ferramentas que tornam possível aplicar patches ativos às bibliotecas (o binário ulp).

12.1.1 Pré-requisitos

Para que a ULP funcione, é necessário cumprir dois requisitos.

- Para que possa receber patches ativos, uma biblioteca deve ser compilada com o flag -fpatchable-function-entry do GCC. Não é necessária nenhuma mudança no código-fonte da biblioteca.
- Os processos devem pré-carregar a biblioteca libpulp.so.

12.1.2 Usando o libpulp

Para usar o libpulp com um aplicativo, você deve executar as seguintes etapas:

1. Permita que uma biblioteca receba patches ativos.
2. Ao iniciar o aplicativo, pré-carregue o libpulp usando o comando LD_PRELOAD=/usr/lib64/libpulp.so ./APLICATIVO.

12.1.2.1 Preparando uma biblioteca para receber patch ativos

Para que seja possível aplicar patches ativos a uma biblioteca, ela deve conter um prólogo `NOP` em todas as chamadas de função. O GCC versão 8 e posterior, bem como a versão do GCC que acompanha o SUSE Linux Enterprise Server, oferece a função `-fpatchable-function-entry` especificamente para essa finalidade. Portanto, na arquitetura AMD64/Intel 64, compilar uma biblioteca escrita em C com o flag `-fpatchable-function-entry=16,14` é suficiente para permitir que ela receba patches ativos.

As bibliotecas `glibc`, `libssl.so.1.1` e `libcrypto.so.1.1` já podem receber patches ativos no SUSE Linux Enterprise 15 SP4.

12.1.2.2 Verificando se uma biblioteca pode receber patches ativos

Para verificar se uma biblioteca pode receber patches ativos, use o seguinte comando:

```
ulp livepatchable LIBRARY
```

12.1.2.3 Aplicando patches ativos

Os patches ativos são aplicados usando o comando `ulp trigger`, por exemplo:

```
ulp trigger -p PID LIVEPATCH.ulp
```

Neste exemplo, o `PID` é do processo em execução que usa a biblioteca que receberá o patch, e `LIVEPATCH.ulp` é o arquivo de patch ativo específico.

A mensagem `live patching succeeded` indica que a operação de aplicação de patches ativos foi bem-sucedida.

12.1.2.4 Revertendo patches ativos

É possível usar o `ulp trigger` para reverter patches ativos. Há duas maneiras de reverter patches ativos. Você pode aplicar o patch `.rev` apropriado:

```
ulp trigger -p PID LIVEPATCH.rev
```

Se preferir, remova todos os patches associados a uma biblioteca específica. Por exemplo:


```
ulp trigger -p PID --revert-all=LIBRARY
```

No exemplo acima, *LIBRARY* refere-se à biblioteca específica, por exemplo: libcrypto.so.1.1.1.

A última abordagem pode ser útil quando o código-fonte do patch ativo original não está disponível ou para remover um determinado patch antigo e aplicar um novo, sem que o aplicativo de destino execute um código que talvez não seja seguro. Por exemplo:

```
ulp trigger -p PID --revert-all=libcrypto.so.1.1.1 new_livepatch2.ulp
```

12.2 Mais informações

Há mais informações sobre o libpulp disponíveis no [repositório Git \(https://github.com/SUSE/libpulp\)](https://github.com/SUSE/libpulp)  do projeto.

13 Atualizações transacionais

As atualizações transacionais estão disponíveis no SUSE Linux Enterprise Desktop como prévia de tecnologia para atualizar o SLES quando o sistema de arquivos raiz é apenas leitura. As atualizações transacionais são atômicas (todas as atualizações serão aplicadas apenas se todas forem bem-sucedidas) e suportam rollbacks. Isso não afeta o sistema em execução, já que as mudanças não são ativadas até o sistema ser reiniciado. Como as reinicializações são interruptivas, o administrador deve decidir se a reinicialização é mais onerosa do que a desestabilização dos serviços em execução. Se as reinicializações forem muito onerosas, não use as atualizações transacionais.

As atualizações transacionais são executadas diariamente pelo script **transactional-update**. O script verifica as atualizações que estão disponíveis. Se houver quaisquer atualizações, ele criará um novo instantâneo do sistema de arquivos raiz em segundo plano e, em seguida, buscará as atualizações dos canais de versão. Depois que o novo instantâneo for totalmente atualizado, ele será marcado como ativo e será o novo sistema de arquivos raiz padrão após a próxima reinicialização do sistema. Quando o **transactional-update** está definido para ser executado automaticamente (que é o comportamento padrão), ele também reinicializa o sistema. O tempo de execução da atualização e a janela de manutenção da reinicialização são configuráveis.

Apenas os pacotes que fazem parte do instantâneo do sistema de arquivos raiz podem ser atualizados. Se os pacotes contiverem arquivos que não fazem parte do instantâneo, a atualização poderá falhar ou danificar o sistema.

Os RPMs que requerem a aceitação de uma licença não podem ser atualizados.

13.1 Limitações da prévia de tecnologia

Como uma prévia de tecnologia, há algumas limitações de funcionalidade. Os seguintes pacotes não funcionarão com o **transactional-update**:

- A página `index.html` padrão de `nginx` talvez não esteja disponível
- `tomcat-webapps` e `tomcat-admin-webapps`
- `phpMyAdmin`
- `sca-appliance-*`
- `mpi-selector`
- `emacs` funciona exceto para jogos do Emacs
- `bind` e `bind-chrootenv`
- `docbook*`
- `sblim-sfcb*`
- `texlive*`
- `iso_ent`
- `openjade`
- `opensp`
- `pcp`
- `plymouth`
- `postgresql-server-10`
- `pulseaudio-gdm-hooks`
- `smartmontools`

O componente atualizador do instalador do sistema não funciona com um sistema de arquivos apenas leitura porque ele não tem suporte para atualizações transacionais.

Outras considerações:

- Em geral, convém minimizar o tempo entre a atualização do sistema e a reinicialização da máquina.
- É possível aplicar apenas uma atualização de cada vez. Certifique-se de reinicializar após uma atualização e antes que a próxima atualização seja aplicada.
- **update-alternatives** apenas deve ser executado após uma atualização transacional depois que a máquina for reinicializada.
- Somente crie novos usuários ou grupos de sistema após uma atualização transacional depois da reinicialização. É aceitável criar usuários e grupos normais (UID > 1000, GID > 1000).
- O YaST ainda não reconhece as atualizações transacionais. Se um módulo do YaST precisar instalar mais pacotes, esse procedimento não funcionará. Operações de sistema normais que apenas modificam os arquivos de configuração em /etc funcionarão.
- Para php7-fastcgi, você deve criar um link simbólico manualmente, /srv/www/cgi-bin/php, que aponta para /usr/bin/php-cgi.
- ntp faz parte do Módulo Legacy para migração de versões mais antigas do SLES. Ele não é suportado em uma nova instalação do SUSE Linux Enterprise Desktop e foi substituído pelo chrony. Se você continuar usando o ntp, uma nova instalação será necessária para funcionar corretamente com as atualizações transacionais.
- sblim-sfcb: Todo o ecossistema do sblim é incompatível com a atualização transacional.
- O **btrfs-defrag** do pacote btrfsmaintenance não funciona com um sistema de arquivos raiz apenas leitura.
- Para **btrfs-balance**, a variável BTRFS_BALANCE_MOUNTPOINTS em /etc/sysconfig/btrfsmaintenance deve ser mudada de / para /.snapshots.
- Para **btrfs-scrub**, a variável BTRFS_SCRUB_MOUNTPOINTS em /etc/sysconfig/btrfsmaintenance deve ser mudada de / para /.snapshots.

13.2 Habilitar transactional-update

Você deve habilitar o Módulo Servidor Transacional durante a instalação do sistema e, em seguida, selecionar a Função do Sistema Servidor Transacional. NÃO há suporte para a instalação de qualquer pacote a partir do Módulo Servidor Transacional em um sistema em execução, e isso pode danificar o sistema.

Observe que não é suportado mudar o layout do subvolume da partição raiz nem colocar subdiretórios ou subvolumes da partição raiz em suas próprias partições (exceto /home, /var, /srv e /opt), e isso muito provavelmente danificará o sistema.

13.3 Gerenciando as atualizações automáticas

As atualizações automáticas são controladas por um **systemd.timer** que é executado uma vez por dia. Ele é aplicado a todas as atualizações e informa o **rebootmgrd** de que a máquina deve ser reinicializada. Você pode ajustar o horário de execução da atualização. Consulte **systemd.timer(5)**. Para ajustar a janela de manutenção, que é quando o **rebootmgrd** reinicializa o sistema, consulte **rebootmgrd(8)**.

Você pode desabilitar as atualizações transacionais automáticas com este comando:

```
# systemctl --now disable transactional-update.timer
```

13.4 Comando transactional-update

O comando **transactional-update** habilita a instalação atômica ou a remoção de atualizações. As atualizações serão aplicadas apenas se todas elas puderem ser instaladas com êxito. O **transactional-update** cria um instantâneo do seu sistema antes de aplicar a atualização, e você pode restaurar esse instantâneo. Todas as mudanças se tornarão ativas apenas após a reinicialização.

--continue

A opção **--continue** é usada para fazer várias mudanças em um instantâneo existente sem reinicialização.

O comportamento padrão do **transactional-update** é criar um novo instantâneo do sistema de arquivos raiz atual. Se você se esquecer de alguma coisa, como de instalar um novo pacote, terá de reinicializar para aplicar as mudanças anteriores,

executar o **transactional-update** novamente para instalar o pacote que ficou faltando e reinicializar outra vez. Não é possível executar o comando **transactional-update** várias vezes sem reinicialização para adicionar outras mudanças ao instantâneo, pois isso cria instantâneos independentes separados que não incluem as mudanças dos instantâneos anteriores.

Use a opção **--continue** para fazer quantas mudanças desejar sem reinicialização. Um instantâneo separado é gerada toda vez, e cada instantâneo contém todas as mudanças efetuadas nos instantâneos anteriores, além das novas mudanças. Repita esse processo quantas vezes desejar e, quando o instantâneo final incluir tudo o que você quer, reinicialize o sistema para que o instantâneo final se torne o novo sistema de arquivos raiz. Outro recurso útil da opção **--continue** é que você pode selecionar um instantâneo existente como base para seu novo instantâneo. O seguinte exemplo demonstra a execução do **transactional-update** para instalar um novo pacote em um instantâneo com base no instantâneo 13 e, em seguida, uma nova execução para instalar outro pacote:

```
# transactional-update pkg install package_1
```

```
# transactional-update --continue 13 pkg install package_2
```

A opção **--continue [num]** chama **snapper create --from**. Consulte a [Seção 10.6.2, “Criando instantâneos”](#).

cleanup

Se o sistema de arquivos raiz atual for idêntico ao sistema de arquivos raiz ativo (após uma reinicialização, antes que **transactional-update** crie um novo instantâneo com as atualizações), todos os instantâneos antigos sem um algoritmo de limpeza terão esse algoritmo definido. Isso garante que o Snapper apague os instantâneos antigos. (Consulte a seção sobre algoritmos de limpeza em `snapper(8)`.) Isso também remove todos os diretórios sobrepostos `/etc` não referenciados (e, portanto, não utilizados) em `/var/lib/overlay`:

```
# transactional-update cleanup
```

pkg in/install

Instala pacotes individuais dos canais disponíveis usando o comando **zypper install**. Também é possível usar esse comando para instalar arquivos RPM de Correção Temporária do Programa (PTF, Program Temporary Fix).

```
# transactional-update pkg install package_name
```

ou

```
# transactional-update pkg install rpm1 rpm2
```

pkg rm/remove

Remove pacotes individuais do instantâneo ativo usando o comando **zypper remove**. Também é possível usar esse comando para remover arquivos RPM de PTF.

```
# transactional-update pkg remove package_name
```

pkg up/update

Atualiza pacotes individuais do instantâneo ativo usando o comando **zypper update**. Apenas os pacotes que fazem parte do instantâneo do sistema de arquivos base podem ser atualizados.

```
# transactional-update pkg remove package_name
```

up/update

Se houver novas atualizações disponíveis, um novo instantâneo será criado, e o **zypper up/update** atualizará o instantâneo.

```
# transactional-update up
```

dup

Se houver novas atualizações disponíveis, um novo instantâneo será criado, e o **zypper dup --no-allow-vendor-change** atualizará o instantâneo. Na sequência, o instantâneo será ativado e se tornará o novo sistema de arquivos raiz após a reinicialização.

```
# transactional-update dup
```

patch

Se houver novas atualizações disponíveis, um novo instantâneo será criado, e o **zypper patch** atualizará o instantâneo.

```
# transactional-update patch
```

rollback

Ele define o subvolume padrão. Em sistemas com um sistema de arquivos apenas leitura, **snapper rollback** é chamado. Em um sistema de arquivos apenas leitura e sem argumentos, o sistema atual é definido como um novo sistema de arquivos raiz padrão. Se você especificar um número, esse instantâneo será usado como o sistema de arquivos raiz padrão. Em um sistema de arquivos apenas leitura, ele não cria nenhum instantâneo adicional.

```
# transactional-update rollback snapshot_number
```

grub.cfg

Ele cria uma nova configuração do GRUB2. Às vezes, é necessário ajustar a configuração de boot, por exemplo, adicionando outros parâmetros do kernel. Edite /etc/default/grub, execute **transactional-update grub.cfg** e, em seguida, reinicialize para ativar a mudança. Você deve reinicializar imediatamente, ou a nova configuração do GRUB2 será sobregravada pelo padrão na próxima execução do transactional-update.

```
# transactional-update grub.cfg
```

reboot

Esse parâmetro aciona uma reinicialização depois que a ação é concluída.

```
# transactional-update dup reboot
```

--help

Ele imprime uma tela de Ajuda com as opções e os subcomandos.

```
# transactional-update --help
```

13.5 Solução de problemas

Em caso de falha no upgrade, execute **supportconfig** para coletar os dados de registro. Envie os arquivos resultantes, incluindo o /var/log/transactional-update.log, ao Suporte da SUSE.

14 Sessões gráficas remotas com VNC

O VNC (Virtual Network Computing) permite acessar um computador remoto por meio de uma área de trabalho gráfica e executar aplicativos gráficos remotos. O VNC é independente de plataforma e acessa a máquina remota de qualquer sistema operacional. Este capítulo descreve como se conectar a um servidor VNC com os clientes de área de trabalho `vncviewer` e `Remmina` e como operar um servidor VNC.

O SUSE Linux Enterprise Desktop suporta dois tipos diferentes de sessões VNC: sessões únicas, que permanecem “ativas” enquanto a conexão VNC do cliente está ativada, e sessões persistentes, que permanecem “ativas” até serem explicitamente terminadas.

Um servidor VNC é capaz de oferecer ambos os tipos de sessões simultaneamente em portas diferentes, mas uma sessão aberta não pode ser convertida de um tipo em outro.

14.1 Cliente `vncviewer`

Para se conectar a um serviço VNC fornecido por um servidor, é necessário um cliente. O padrão no SUSE Linux Enterprise Desktop é o `vncviewer`, incluído no pacote `tigervnc`.

14.1.1 Conexão por meio da CLI do `vncviewer`

Para iniciar o viewer do VNC e começar uma sessão com o servidor, use o comando:

```
> vncviewer jupiter.example.com:1
```

Em vez do número de exibição do VNC, você também pode especificar o número da porta com dois-pontos duplos:

```
> vncviewer jupiter.example.com::5901
```



Nota: Número de exibição e de porta

O número real de exibição ou de porta especificado no cliente VNC deve ser igual ao número selecionado pelo comando `vncserver` na máquina de destino. Consulte a [Seção 14.4, “Configurando sessões persistentes do servidor VNC”](#) para obter mais informações.

14.1.2 Conexão por meio da GUI do vncviewer

Ao executar o `vncviewer` sem especificar `--listen` nem um host ao qual se conectar, será exibida uma janela solicitando detalhes da conexão. Informe o host no campo *Servidor VNC*, conforme mostrado na [Seção 14.1.1, “Conexão por meio da CLI do vncviewer”](#), e clique em *Conectar*.

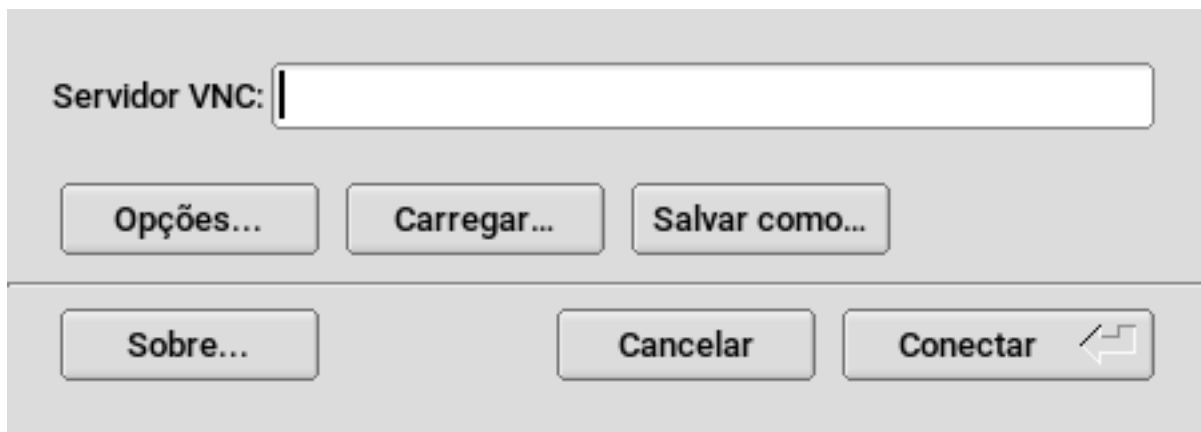


FIGURA 14.1: VNCVIEWER

14.1.3 Notificação de conexões não criptografadas

O protocolo VNC suporta diferentes tipos de conexões criptografadas, o que não deve ser confundido com autenticação de senha. Se uma conexão não usar TLS, o texto “(Conexão não criptografada)!” poderá aparecer no título da janela do viewer do VNC.

14.2 Remmina: o cliente de área de trabalho remota

Remmina é um cliente de área de trabalho remota moderno e cheio de recursos. Ele suporta vários métodos de acesso, por exemplo VNC, SSH, RDP e Spice.

14.2.1 Instalação

Para usar o Remmina, verifique se o pacote `remmina` está instalado no sistema e, se não estiver, instale-o. Lembre-se também de instalar o plug-in VNC para Remmina:

```
# zypper in remmina remmina-plugin-vnc
```

14.2.2 Janela principal

Execute o Remmina digitando o comando `remmina`.

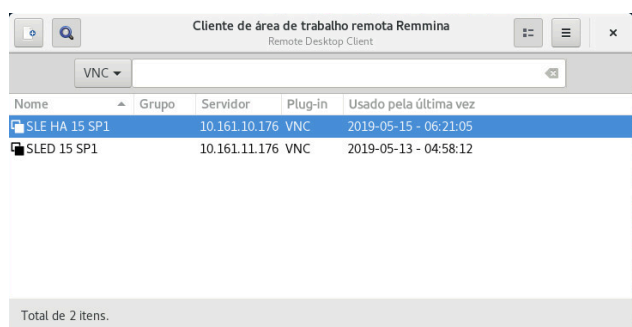



FIGURA 14.2: JANELA PRINCIPAL DO REMMINA

A janela principal do aplicativo mostra a lista de sessões remotas armazenadas. Nela, você pode adicionar e gravar uma nova sessão remota, iniciar rapidamente uma nova sessão sem gravá-la, iniciar uma sessão que já foi gravada ou definir as preferências globais do Remmina.

14.2.3 Adicionando sessões remotas

Para adicionar e gravar uma nova sessão remota, clique em  na parte superior esquerda da janela principal. A janela *Preferência da Área de Trabalho Remota* é aberta.

Perfil

Nome: SLE HA 15 SP1

Grupo: [vazio]

Protocolo: VNC - VNC viewer

Pré-Comando: command %h %u %t %U %p %g --option

Pós-Comando: /path/to/command -opt1 arg %h %u %t -opt2 %U %p %g

Básico | Avançado | Túnel SSH

Servidor: 10.161.10.176

Repetidor: [vazio]

Nome de usuário: [vazio]

Senha do Usuário: [vazio]

Profundidade de cores: High color (16 bpp)

Qualidade: Boa

Mapa do teclado: [vazio]

Cancelar Gravar como Padrão Gravar Conectar Gravar e Conectar

FIGURA 14.3: PREFERÊNCIA DA ÁREA DE TRABALHO REMOTA

Preencha os campos que especificam o perfil da sessão remota recém-adicionada. Os mais importantes são:

Nome

Nome do perfil. Ele será listado na janela principal.

Protocolo

O protocolo a ser usado na conexão com a sessão remota. Por exemplo, VNC.

Servidor

O endereço IP ou DNS e o número de exibição do servidor remoto.

Nome de usuário, senha

As credenciais que serão usadas para autenticação remota. Deixe vazio para nenhuma autenticação.

Profundidade de cores, qualidade

Selecione as melhores opções de acordo com a velocidade e a qualidade da conexão.

Selecione a guia *Avançado* para inserir configurações mais específicas.



Dica: Desabilitar criptografia

Se a comunicação entre o cliente e o servidor remoto não for criptografada, ative *Desabilitar Criptografia*; do contrário, haverá falha na conexão.

Selecione a guia *SSH* para opções avançadas de autenticação e túnel SSH.

Confirme com *Salvar*. Seu novo perfil será listado na janela principal.

14.2.4 Iniciando sessões remotas

Você pode iniciar uma sessão que já foi gravada ou iniciar rapidamente uma sessão remota sem gravar os detalhes da conexão.

14.2.4.1 Iniciando sessões remotas rapidamente

Para iniciar uma sessão remota rapidamente, sem adicionar e gravar os detalhes da conexão, use a caixa suspensa e a caixa de texto na parte superior da janela principal.



FIGURA 14.4: INICIANDO RAPIDAMENTE

Selecione o protocolo de comunicação na caixa suspensa (por exemplo, “VNC”) e digite o endereço DNS ou IP do servidor VNC seguido de uma vírgula e de um número de exibição. Em seguida, pressione **Enter** para confirmar.

14.2.4.2 Abrindo sessões remotas gravadas

Para abrir uma sessão remota específica, clique duas vezes nela na lista de sessões.

14.2.4.3 Janela de sessões remotas

As sessões remotas são abertas nas guias de uma janela separada. Cada guia hospeda uma sessão. A barra de ferramentas à esquerda da janela permite gerenciar as janelas/sessões, como alternar para o modo de tela cheia, redimensionar a janela para corresponder ao tamanho de tela da sessão, enviar toques específicos para a sessão, fazer capturas de tela da sessão ou definir a qualidade da imagem.

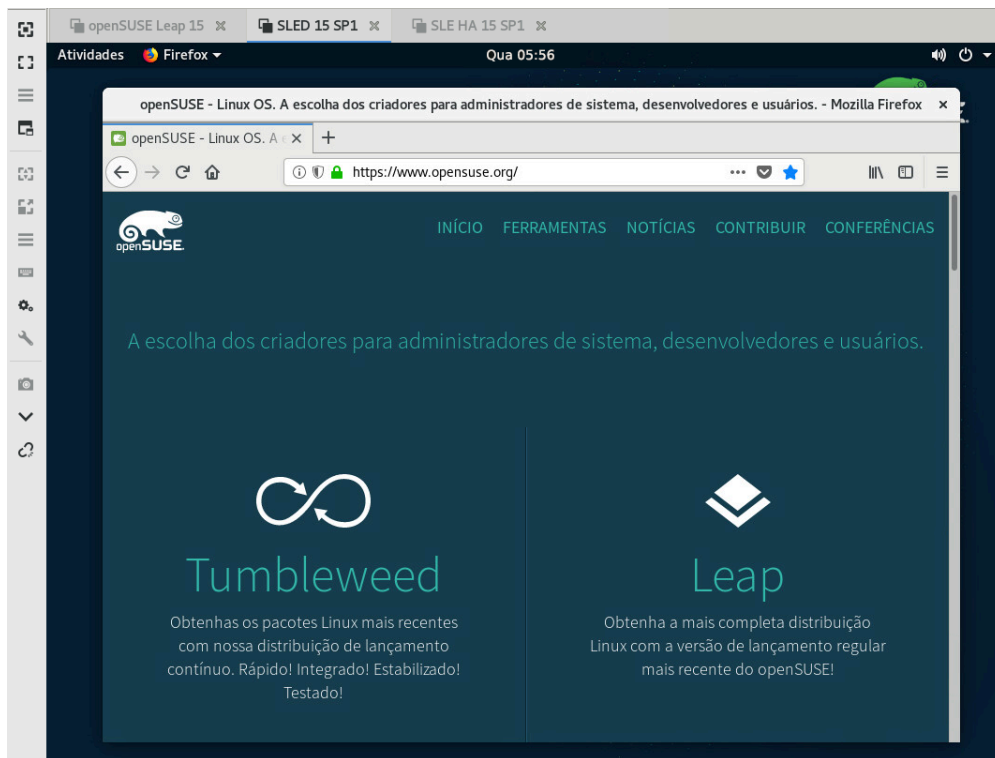


FIGURA 14.5: VENDO SESSÃO REMOTA NO REMMINA

14.2.5 Editando, copiando e apagando sessões gravadas

Para *editar* uma sessão remota gravada, clique o botão direito do mouse no nome dela na janela principal do Remmina e selecione *Editar*. Consulte a [Seção 14.2.3, “Adicionando sessões remotas”](#) para ver a descrição dos campos relevantes.

Para *copiar* uma sessão remota gravada, clique o botão direito do mouse no nome dela na janela principal do Remmina e selecione *Copiar*. Na janela *Preferência da Área de Trabalho Remota*, mude o nome do perfil, ajuste as opções relevantes (opcional) e clique em *Gravar* para confirmar.

Para *apagar* uma sessão remota gravada, clique o botão direito do mouse no nome dela na janela principal do Remmina e selecione *Apagar*. Na caixa de diálogo, clique em *Sim* para confirmar.

14.2.6 Executando sessões remotas da linha de comando

Se você precisar abrir uma sessão remota da linha de comando ou de um arquivo de lote sem primeiro abrir a janela principal do aplicativo, use a seguinte sintaxe:

```
> remmina -c profile_name.remmina
```

Os arquivos de perfil do Remmina são armazenados no diretório `.local/share/remmina/` em seu diretório pessoal. Para determinar qual arquivo de perfil pertence à sessão que você deseja abrir, execute o Remmina, clique no nome da sessão na janela principal e leia o caminho para o arquivo de perfil na linha de status da janela na parte inferior.

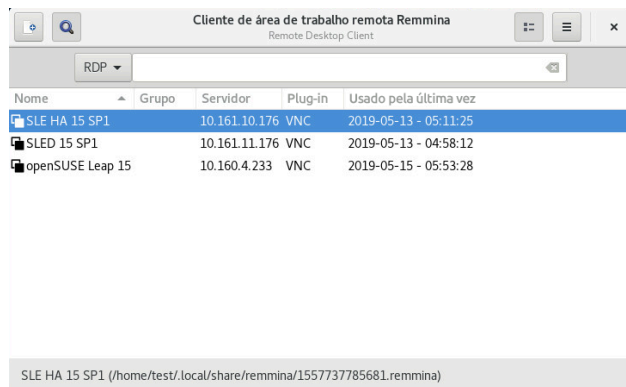


FIGURA 14.6: LENDO O CAMINHO PARA O ARQUIVO DE PERFIL

Enquanto o Remmina não estiver em execução, você poderá renomear o arquivo de perfil para um nome de arquivo mais apropriado, como `sle15.remmina`. Você pode até copiar o arquivo de perfil para o seu diretório personalizado e executá-lo usando o comando `remmina -c` nesse diretório.

14.3 Configurando sessões únicas no servidor VNC

Uma sessão única é iniciada por um cliente remoto. Ela inicia uma tela gráfica de login no servidor. Desse modo, você pode escolher o usuário que inicia a sessão e, se suportado pelo gerenciador de login, o ambiente de área de trabalho. Quando você terminar a conexão do cliente com essa sessão VNC, todos os aplicativos iniciados nessa sessão também serão terminados. Sessões VNC únicas não podem ser compartilhadas, mas é possível ter várias sessões em um único host ao mesmo tempo.

PROCEDIMENTO 14.1: HABILITANDO SESSÕES VNC ÚNICAS

1. Inicie o YaST > *Serviços de Rede* > *Administração Remota (VNC)*.
2. Marque *Permitir Administração Remota sem Gerenciamento de Sessões*.
3. Ative *Permitir acesso usando um browser da Web* se você pretende acessar a sessão VNC em uma janela do browser da Web.

4. Se necessário, marque também *Abrir Porta no Firewall* (por exemplo, quando a interface de rede estiver configurada para ficar na Zona Externa). Se você tem mais de uma interface de rede, restrinja a abertura de portas no firewall a uma interface específica em *Detalhes do Firewall*.
5. Confirme as configurações com *Próximo*.
6. Caso nem todos os pacotes necessários já estejam disponíveis, aprove a instalação dos pacotes ausentes.



Dica: Reiniciar o gerenciador de exibição

O YaST faz mudanças nas configurações do gerenciador de exibição. Você precisará efetuar logout da sessão gráfica atual e reiniciar o gerenciador de exibição para que as mudanças entrem em vigor.



FIGURA 14.7: ADMINISTRAÇÃO REMOTA

14.3.1 Configurações disponíveis

A configuração padrão no SUSE Linux Enterprise Desktop confere às sessões uma resolução de 1024 x 768 pixels com profundidade de cores de 16 bits. As sessões estão disponíveis nas portas 5901 para viewers VNC “regulares” (equivalente à exibição VNC 1) e na porta 5801 para browsers da Web.

É possível disponibilizar outras configurações em portas diferentes. Peça os detalhes ao administrador do sistema, se você precisar modificar a configuração.

Os números de exibição VNC e os números de exibição X são independentes nas sessões únicas. Um número de exibição VNC é atribuído manualmente a todas as configurações suportadas pelo servidor (:1 no exemplo acima). Sempre que uma sessão VNC é iniciada com uma das configurações, ela recebe automaticamente um número de exibição X livre.

Por padrão, tanto o cliente quanto o servidor VNC tentam se comunicar de forma segura por meio de um certificado SSL autoassinado, que será gerado após a instalação. É possível usar o padrão ou substituí-lo pelo seu próprio certificado. Ao usar o certificado autoassinado, você precisa confirmar sua assinatura antes da primeira conexão, tanto no viewer do VNC quanto no browser da web.

14.3.2 Iniciando uma sessão VNC única

Para conectar-se a uma sessão VNC única, é necessário instalar o viewer do VNC. Consulte também a [Seção 14.1, “Cliente vncviewer”](#). Se preferir, use um browser da Web compatível com JavaScript para ver a sessão VNC digitando o seguinte URL: <http://jupiter.example.com:5801>

14.3.3 Configurando sessões VNC únicas

Você poderá ignorar esta seção se não precisar nem desejar modificar a configuração padrão.

As sessões VNC únicas são iniciadas pelo `systemd` soquete `xvnc.socket`. Por padrão, ele oferece seis blocos de configuração: três para viewers do VNC (`vnc1` a `vnc3`) e três que atendem a um cliente JavaScript (`vnchttpd1` a `vnchttpd3`). Por padrão, apenas `vnc1` e `vnchttpd1` estão ativos.

Para ativar o soquete do servidor VNC no momento da inicialização, execute o seguinte comando:

```
> sudo systemctl enable xvnc.socket
```

Para iniciar o soquete imediatamente, execute:

```
> sudo systemctl start xvnc.socket
```

O servidor **Xvnc** pode ser configurado por meio da opção `server_args`. Para obter uma lista de opções, consulte **Xvnc --help**.

Ao adicionar configurações padrão, certifique-se de que elas não usem portas já em uso por outras configurações, outros serviços ou sessões VNC persistentes existentes no mesmo host.

Ative as mudanças na configuração digitando o seguinte comando:

```
> sudo systemctl reload xvnc.socket
```



Importante: Firewall e portas VNC

Ao ativar a Administração Remota conforme descrito no *Procedimento 14.1, "Habilitando sessões VNC únicas"*, as portas `5801` e `5901` são abertas no firewall. Se a interface de rede que atende às sessões VNC for protegida por firewall, será necessário abrir manualmente as respectivas portas ao ativar portas adicionais para as sessões VNC. Consulte a *Livro "Security and Hardening Guide", Capítulo 23 "Masquerading and firewalls"* para obter instruções.

14.4 Configurando sessões persistentes do servidor VNC

É possível acessar uma sessão persistente de vários clientes ao mesmo tempo. Isso é ideal para fins de demonstração em que um cliente tem acesso total, e todos os outros têm acesso apenas exibição. Outro caso de uso são sessões de treinamento em que o instrutor pode precisar acessar a área de trabalho do aluno.



Dica: Conectando-se a uma sessão VNC persistente

Para conectar-se a uma sessão VNC persistente, é preciso instalar o viewer do VNC. Consulte a [Seção 14.1, “Cliente **vncviewer**”](#) para obter mais detalhes. Se preferir, use um browser da Web compatível com JavaScript para ver a sessão VNC digitando o seguinte URL: <http://jupiter.example.com:5801>

Há dois tipos de sessões VNC persistentes:

- *Sessão VNC iniciada usando **vncserver***
- *Sessão VNC iniciada usando **vncmanager***

14.4.1 Sessão VNC iniciada usando **vncserver**

Esse tipo de sessão VNC persistente é iniciado no servidor. A sessão e todos os aplicativos iniciados nessa sessão são executados independentemente das conexões do cliente até a sessão ser terminada. O acesso às sessões persistentes é protegido por dois tipos de senhas possíveis:

- uma senha regular que permite acesso total ou
- uma senha opcional apenas exibição que permite acesso não interativo (apenas exibição).

Uma sessão pode ter várias conexões de cliente de ambos os tipos de uma só vez.

PROCEDIMENTO 14.2: INICIANDO UMA SESSÃO VNC PERSISTENTE PELO **vncserver**

1. Abra um shell e verifique se você está conectado como o usuário proprietário da sessão VNC.
2. Se a interface de rede que atende às sessões VNC for protegida por firewall, será necessário abrir manualmente a porta usada pela sessão no firewall. Se você iniciar várias sessões, poderá também abrir uma faixa de portas. Consulte o *Livro “Security and Hardening Guide”, Capítulo 23 “Masquerading and firewalls”* para obter os detalhes sobre como configurar o firewall.

O **vncserver** usa as portas 5901 para exibição :1, 5902 para exibição :2, e assim por diante. Para sessões persistentes, a exibição VNC e a exibição X geralmente têm o mesmo número.

3. Para iniciar uma sessão com resolução de 1024 x 768 pixels e profundidade de cores de 16 bits, digite o seguinte comando:

```
vncserver -alwaysshared -geometry 1024x768 -depth 16
```

O comando **vncserver** escolhe um número de exibição não usado quando nenhum número é especificado e imprime essa escolha. Consulte **man 1 vncserver** para ver mais opções.

Quando o **vncserver** é executado pela primeira vez, ele pede uma senha para acesso total à sessão. Se necessário, forneça também uma senha de acesso apenas exibição à sessão.

A(s) senha(s) inserida(s) aqui também será(ão) usada(s) em sessões futuras iniciadas pelo mesmo usuário. Elas podem ser modificadas com o comando **vncpasswd**.



Importante: Considerações de segurança

Verifique se está usando senhas avançadas de tamanho significativo (oito ou mais caracteres). Não compartilhe essas senhas.

Para terminar a sessão, encerre o ambiente de área de trabalho executado na sessão VNC pelo viewer do VNC, da mesma forma que você encerra uma sessão X local regular.

Se preferir terminar a sessão manualmente, abra um shell no servidor VNC e certifique-se de estar conectado como o usuário que possui a sessão VNC que deseja terminar. Execute o seguinte comando para terminar a sessão em execução na exibição **:1**: **vncserver -kill :1**

14.4.1.1 Configurando sessões VNC persistentes

É possível configurar as sessões VNC persistentes editando **\$HOME/.vnc/xstartup**. Por padrão, o script shell inicia o mesmo gerenciador de janelas/GUI do qual ele foi iniciado. No SUSE Linux Enterprise Desktop, pode ser o GNOME ou o IceWM. Para iniciar a sessão com um gerenciador de janelas de sua escolha, defina a variável **WINDOWMANAGER**:

```
WINDOWMANAGER=gnome vncserver -geometry 1024x768  
WINDOWMANAGER=icewm vncserver -geometry 1024x768
```




Nota: Uma configuração para cada usuário

Sessões VNC persistentes são configuradas em uma única configuração por usuário. Várias sessões iniciadas pelo mesmo usuário utilizarão todos os mesmos arquivos de inicialização e senha.

14.4.2 Sessão VNC iniciada usando vncmanager

PROCEDIMENTO 14.3: HABILITANDO SESSÕES VNC PERSISTENTES

1. Inicie o *YaST* > *Serviços de Rede* > *Administração Remota (VNC)*.
2. Ative *Permitir Administração Remota com Gerenciamento de Sessões*.
3. Ative *Permitir acesso usando um browser da Web* se você pretende acessar a sessão VNC em uma janela do browser da Web.
4. Se necessário, marque também *Abrir Porta no Firewall* (por exemplo, quando a interface de rede estiver configurada para ficar na Zona Externa). Se você tem mais de uma interface de rede, restrinja a abertura de portas no firewall a uma interface específica em *Detalhes do Firewall*.
5. Confirme as configurações com *Próximo*.
6. Caso nem todos os pacotes necessários já estejam disponíveis, aprove a instalação dos pacotes ausentes.



Dica: Reiniciar o gerenciador de exibição

O YaST faz mudanças nas configurações do gerenciador de exibição. Você precisará efetuar logout da sessão gráfica atual e reiniciar o gerenciador de exibição para que as mudanças entrem em vigor.

14.4.2.1 Configurando sessões VNC persistentes

Após habilitar o gerenciamento de sessões VNC conforme descrito no [Procedimento 14.3, "Habilitando sessões VNC persistentes"](#), você poderá conectar-se normalmente ao seu viewer do VNC favorito, como vncviewer ou Remmina. Você verá a tela de login. Depois que você efetuar

login, o ícone “VNC” será exibido na bandeja do sistema do ambiente de área de trabalho. Clique no ícone para abrir a janela *Sessão VNC*. Se ele não aparecer ou se o seu ambiente de área de trabalho não oferecer suporte a ícones na bandeja do sistema, execute `vncmanager-controller` manualmente.

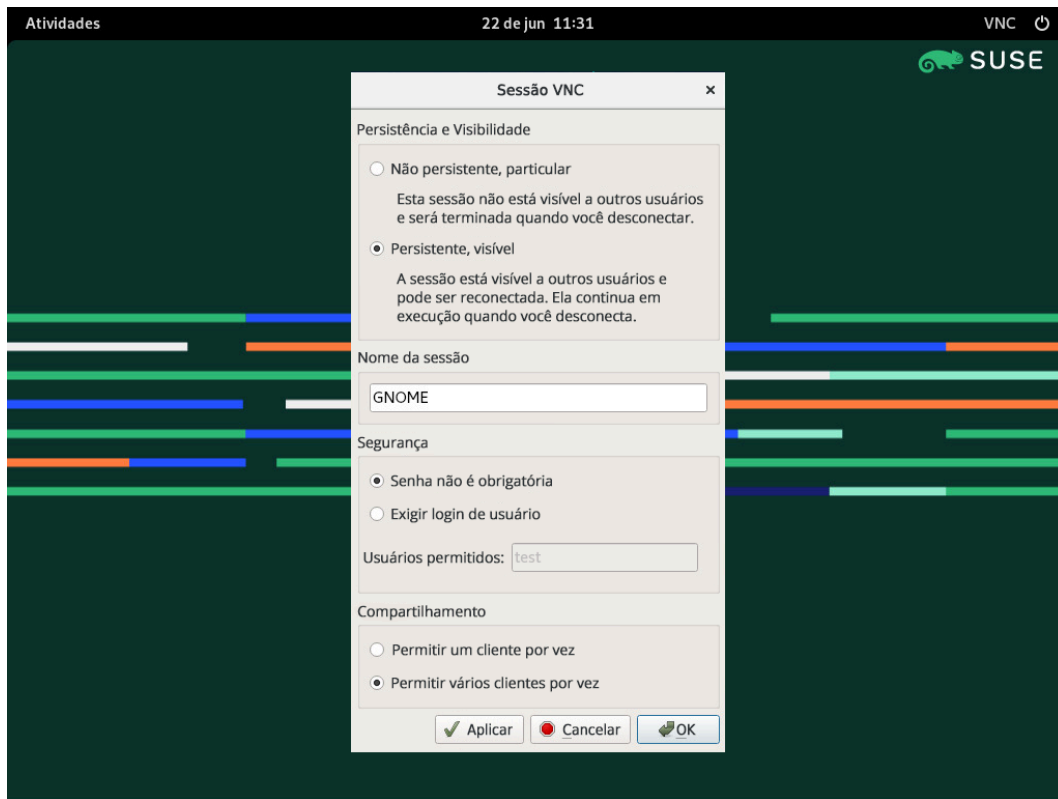


FIGURA 14.8: CONFIGURAÇÕES DE SESSÃO VNC

Há várias configurações que afetam o comportamento da sessão VNC:

Não persistente, particular

Isso é equivalente a uma sessão única. Ela não fica visível a outros usuários e será terminada depois que você se desconectar. Consulte o [Seção 14.3, “Configurando sessões únicas no servidor VNC”](#) para obter mais informações.

Persistente, visível

A sessão fica visível a outros usuários e continuará em execução mesmo depois que você se desconectar.

Nome da sessão

Aqui você pode especificar o nome da sessão persistente para que ela seja facilmente identificada ao reconectar-se.

Senha não é obrigatória

A sessão será livremente acessível sem necessidade de efetuar login com credenciais de usuário.

Exigir login de usuário

Você precisa efetuar login com um nome de usuário e uma senha válidos para acessar a sessão. Lista os nomes válidos de usuário na caixa de texto *Usuários permitidos*.

Permitir um cliente por vez

Impede que vários usuários ingressem na sessão ao mesmo tempo.

Permitir vários clientes por vez

Permite que vários usuários ingressem na sessão persistente ao mesmo tempo. Um recurso útil para apresentações ou sessões de treinamento remotas.

Confirme com *OK*.

14.4.2.2 Ingressando em sessões VNC persistentes

Após configurar uma sessão VNC persistente, conforme descrito na [Seção 14.4.2.1, “Configurando sessões VNC persistentes”](#), você poderá ingressar nela com o viewer do VNC. Depois que o cliente VNC conectar-se ao servidor, será solicitado que você escolha se deseja criar uma nova sessão ou ingressar em uma existente:

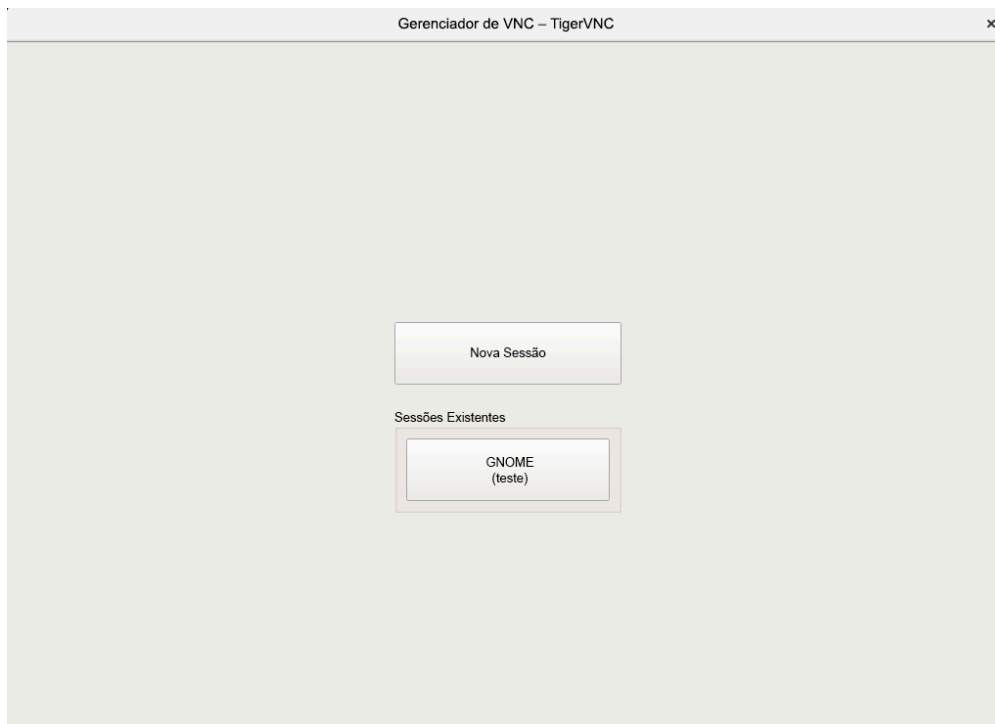


FIGURA 14.9: INGRESSANDO EM UMA SESSÃO VNC PERSISTENTE

Após clicar no nome da sessão existente, talvez você tenha que inserir as credenciais de login, dependendo das configurações de sessão persistente.

14.5 Configurando a criptografia no servidor VNC

Se o servidor VNC estiver configurado apropriadamente, todas as comunicações entre o cliente e o servidor VNC serão criptografadas. A autenticação ocorre no início da sessão. A transferência real dos dados começa somente depois.

Seja para uma sessão VNC única ou persistente, as opções de segurança são configuradas por meio do parâmetro `-securitytypes` do comando `/usr/bin/Xvnc` localizado na linha `server_args`. O parâmetro `-securitytypes` seleciona tanto o método de autenticação quanto a criptografia. Ele tem as seguintes opções:

AUTENTICAÇÕES

None, TLSNone, x509None

Nenhuma autenticação.

VncAuth, TLSVnc, x509Vnc

Autenticação com senha personalizada.

Plain, TLSPlain, x509Plain

Autenticação que usa PAM para verificar a senha do usuário.

CRIPTOGRAFIAS

None, vncAuth, plain

Sem criptografia.

TLSNone, TLSVnc, TLSPlain

Criptografia TLS anônima. Tudo é criptografado, mas não há nenhuma verificação do host remoto. Portanto, você está protegido contra invasores passivos, mas não contra invasores man-in-the-middle.

X509None, x509Vnc, x509Plain

Criptografia TLS com certificado. Se você usar um certificado autoassinado, será solicitado a verificá-lo na primeira conexão. Nas conexões subsequentes, você será avisado apenas se o certificado for mudado. Portanto, você está protegido contra tudo, exceto man-in-the-middle na primeira conexão (similar ao uso comum de SSH). Se você usar um certificado assinado por uma autoridade de certificação que corresponde ao nome da máquina, terá segurança total (similar ao uso comum de HTTPS).



Dica: Caminho para certificado e chave

Com a criptografia baseada em X509, você precisa especificar o caminho para o certificado e a chave X509 com as opções `-X509Cert` e `-X509Key`.

Se você selecionar vários tipos de segurança separados por vírgula, o primeiro que for suportado e permitido pelo cliente e pelo servidor será utilizado. Dessa forma, você pode configurar criptografia oportunista no servidor. Isso é útil se você precisa suportar clientes VNC que não aceitam criptografia.

No cliente, você também pode especificar os tipos de segurança permitidos para impedir ataque de instalação de uma versão menos eficiente, se estiver conectando-se a um servidor que você sabe que tem a criptografia habilitada (embora nosso vncviewer o avisará com a mensagem "Conexão não criptografada!" nesse caso).

15 Cópia de arquivo com RSync

Hoje em dia, um usuário comum possui vários computadores: em casa e no local de trabalho, um laptop, um smartphone ou um tablet. Isso torna muito mais importante a tarefa de manter os arquivos e documentos sincronizados entre vários dispositivos.



Atenção: Risco de perda de dados

Antes de começar a usar uma ferramenta de sincronização, você deve se familiarizar com os recursos e as funcionalidades. Faça backup de seus arquivos importantes.

15.1 Visão geral conceitual

Para sincronizar uma grande quantidade de dados em uma conexão de rede lenta, o Rsync oferece um método confiável para transmitir apenas as mudanças nos arquivos. Isso não se aplica apenas a arquivos de texto, mas também a arquivos binários. Para detectar as diferenças entre os arquivos, o Rsync os subdivide em blocos e calcula seus checksums.

A detecção de mudanças requer alguma capacidade de computação. Portanto, verifique se as máquinas em ambas as extremidades têm recursos suficientes, incluindo memória RAM.

O Rsync pode ser útil principalmente quando grandes quantidades de dados que contêm apenas pequenas mudanças precisam ser transmitidas regularmente. Geralmente, esse é o caso quando se trabalha com backups. O Rsync também pode ser útil para espelhamento de servidores para testes que armazenam árvores completas de diretórios de servidores Web em um servidor Web na DMZ.

Apesar do nome, o Rsync não é uma ferramenta de sincronização. Rsync é uma ferramenta que copia dados apenas em uma direção de cada vez. Ele não faz e não pode fazer o contrário. Se você precisa de uma ferramenta bidirecional capaz de sincronizar a origem e o destino, use o Csync.

15.2 Sintaxe básica

O Rsync é uma ferramenta de linha de comando que tem a seguinte sintaxe básica:

```
rsync [OPTION] SOURCE [SOURCE]... DEST
```

Você pode usar o Rsync em qualquer máquina local ou remota, desde que tenha acesso e permissões de gravação. É possível ter várias entradas SOURCE. Os marcadores SOURCE e DEST podem ser caminhos, URLs ou ambos.

Veja a seguir as opções mais comuns do Rsync:

-v

Gera um texto mais verboso

-a

Modo de arquivamento: copia arquivos recursivamente e preserva marcações de horário, propriedade de usuário/grupo, permissões de arquivos e links simbólicos

-z

Comprime os dados transmitidos



Nota: Total de barras à direita

Ao trabalhar com o Rsync, você deve prestar atenção especial às barras à direita. Uma barra à direita após o diretório indica o *conteúdo* do diretório. Nenhuma barra à direita indica o *próprio diretório*.

15.3 Copiando arquivos e diretórios localmente

A seguinte descrição pressupõe que o usuário atual tem permissões de gravação para o diretório /var/backup. Para copiar um único arquivo de um diretório em sua máquina para outro caminho, use o seguinte comando:

```
> rsync -avz backup.tar.xz /var/backup/
```

O arquivo backup.tar.xz é copiado para /var/backup/; o caminho absoluto será /var/backup/backup.tar.xz.

Lembre-se de adicionar a *barra à direita* após o diretório /var/backup/! Se você não inserir a barra, o arquivo backup.tar.xz será copiado para /var/backup (arquivo), e *não* dentro do diretório /var/backup/!

Copiar um diretório é semelhante a copiar um arquivo único. O exemplo a seguir copia o diretório tux/ e seu conteúdo para o diretório /var/backup/:

```
> rsync -avz tux /var/backup/
```


Localize a cópia no caminho absoluto /var/backup/tux/.

15.4 Copiando arquivos e diretórios remotamente

A ferramenta Rsync é necessária em ambas as máquinas. Para copiar arquivos de ou para diretórios remotos, é necessário um endereço IP ou um nome de domínio. Um nome de usuário será opcional caso os nomes de usuários atuais na máquina local e remota sejam os mesmos.

Para copiar o arquivo file.tar.xz de seu host local para o host remoto 192.168.1.1 com os mesmos usuários (sendo local e remoto), use o seguinte comando:

```
> rsync -avz file.tar.xz tux@192.168.1.1:
```

Dependendo do que você preferir, estes comandos também serão possíveis e equivalentes:

```
> rsync -avz file.tar.xz 192.168.1.1:~  
> rsync -avz file.tar.xz 192.168.1.1:/home/tux
```

Em todos os casos com configuração padrão, você será solicitado a inserir a frase secreta do usuário remoto. Esse comando copiará o file.tar.xz para o diretório pessoal do usuário tux (normalmente, /home/tux).

Copiar um diretório remotamente é semelhante a copiar um diretório localmente. O exemplo a seguir copia o diretório tux/ e seu conteúdo para o diretório remoto /var/backup/ no host 192.168.1.1:

```
> rsync -avz tux 192.168.1.1:/var/backup/
```

Supondo que você tenha permissões de gravação no host 192.168.1.1, encontrará a cópia no caminho absoluto /var/backup/tux.

15.5 Configurando e usando um servidor Rsync

O Rsync pode ser executado como um daemon (rsyncd) que escuta na porta padrão 873 para conexões recebidas. Esse daemon pode receber “destinos de cópia”.

A descrição a seguir explica como criar um servidor Rsync em jupiter com um destino de *backup*. Esse destino pode ser usado para armazenar os backups. Para criar um servidor Rsync, faça o seguinte:

PROCEDIMENTO 15.1: CONFIGURANDO UM SERVIDOR RSYNC

1. No jupiter, crie um diretório para armazenar todos os seus arquivos de backup. Neste exemplo, usamos /var/backup:

```
# mkdir /var/backup
```

2. Especifique a propriedade. Neste caso, o diretório pertence ao usuário tux no grupo users:

```
# chown tux.users /var/backup
```

3. Configure o daemon rsyncd.

Separaremos o arquivo de configuração em um arquivo principal e alguns “módulos”, que contêm o destino de backup. Isso facilita adicionar outros destinos futuramente. É possível armazenar valores globais nos arquivos /etc/rsyncd.d/*.inc, enquanto os módulos são armazenados nos arquivos /etc/rsyncd.d/*.conf:

- a. Crie um diretório /etc/rsyncd.d/:

```
# mkdir /etc/rsyncd.d/
```

- b. No arquivo de configuração principal /etc/rsyncd.conf, adicione as seguintes linhas:

```
# rsyncd.conf main configuration file
log file = /var/log/rsync.log
pid file = /var/lock/rsync.lock

&merge /etc/rsyncd.d ❶
&include /etc/rsyncd.d ❷
```

- ❶ Faz a fusão dos valores globais dos arquivos /etc/rsyncd.d/*.inc no arquivo de configuração principal.
- ❷ Carrega quaisquer módulos (ou destinos) dos arquivos /etc/rsyncd.d/*.conf. Esses arquivos não devem conter nenhuma referência a valores globais.

- c. Crie o módulo (destino de backup) no arquivo `/etc/rsyncd.d/backup.conf` com as seguintes linhas:

```
# backup.conf: backup module
[backup] ❶
  uid = tux ❷
  gid = users ❷
  path = /var/backup ❸
  auth users = tux ❹
  secrets file = /etc/rsyncd.secrets ❺
  comment = Our backup target
```

- ❶ O destino de *backup*. Você pode usar qualquer nome que desejar. No entanto, convém nomear um destino de acordo com sua finalidade e usar o mesmo nome em seu arquivo `*.conf`.
 - ❷ Especifica o nome de usuário ou nome do grupo que é usado quando a transferência de arquivos é feita.
 - ❸ Define o caminho para armazenar os backups (da *Passo 1*).
 - ❹ Especifica uma lista separada por vírgulas de usuários permitidos. Em sua forma mais simples, ela contém os nomes de usuário que têm permissão para conectar-se a este módulo. Em nosso caso, apenas o usuário `tux` é permitido.
 - ❺ Especifica o caminho de um arquivo que contém as linhas com os nomes de usuário e as senhas simples.
- d. Crie o arquivo `/etc/rsyncd.secrets` com o seguinte conteúdo e substitua *FRASE SECRETA*:

```
# user:passwd
tux:PASSPHRASE
```

- e. Verifique se o arquivo pode ser lido apenas por `root`:

```
# chmod 0600 /etc/rsyncd.secrets
```

4. Inicie e habilite o daemon `rsyncd` com:

```
# systemctl enable rsyncd
# systemctl start rsyncd
```

5. Teste o acesso ao servidor Rsync:

```
> rsync jupiter::
```

Você deve ver uma resposta parecida com esta:

```
backup          Our backup target
```

Do contrário, verifique o arquivo de configuração, as configurações de rede e de firewall.

As etapas acima criam um servidor Rsync que agora pode ser usado para armazenar backups. O exemplo também cria um arquivo de registro listando todas as conexões. Esse arquivo é armazenado em `/var/log/rsyncd.log`. Isso é útil para depurar suas transferências.

Para listar o conteúdo do destino de backup, use o seguinte comando:

```
> rsync -avz jupiter::backup
```

Esse comando lista todos os arquivos presentes no diretório `/var/backup` no servidor. Essa solicitação também é registrada no arquivo de registro `/var/log/rsyncd.log`. Para iniciar uma transferência real, especifique um diretório de origem. Use `.` para o diretório atual. Por exemplo, o comando a seguir copia o diretório atual para o servidor de backup Rsync:

```
> rsync -avz . jupiter::backup
```

Por padrão, o Rsync não apaga arquivos e diretórios quando ele é executado. Para habilitar a exclusão, a opção adicional `--delete` deve ser especificada. Para garantir que nenhum arquivo novo seja apagado, use a opção `--update` como alternativa. Qualquer conflito ocorrido deve ser resolvido manualmente.

15.6 Mais informações

Csync

Ferramenta de sincronização bidirecional de arquivos. Consulte <https://csync.org/>.

RSnapshot

Cria backups incrementais. Consulte <https://rsnapshot.org/>.

Unison

Uma ferramenta de sincronização de arquivos semelhante ao CSync, mas com uma interface gráfica. Consulte <https://www.seas.upenn.edu/~bcpierce/unison/>.

Rear

Uma estrutura de recuperação de desastres, consulte o *Administration Guide* (Guia de Administração) da SUSE Linux Enterprise High Availability Extension, capítulo *Disaster Recovery with Rear (Relax-and-Recover)* (<https://documentation.suse.com/sle-ha-15/html/SLE-HA-all/cha-ha-rear.html>)  (Recuperação de desastres com Rear (Relax-and-Recover)).

II Inicializando um sistema Linux

- 16 Introdução ao processo de boot 225
- 17 UEFI (Unified Extensible Firmware Interface) 234
- 18 Carregador de boot GRUB 2 243
- 19 Daemon systemd 263

16 Introdução ao processo de boot

A inicialização de um sistema Linux envolve componentes e tarefas diferentes. Após um processo de inicialização de firmware e de hardware, que depende da arquitetura da máquina, o kernel será iniciado pelo carregador de boot GRUB 2. A partir deste ponto, o processo de boot é completamente controlado pelo sistema operacional e administrado pelo `systemd`. O `systemd` oferece um conjunto de “destinos” que inicializam configurações para uso diário, manutenção ou emergências.

16.1 Terminologia

Este capítulo usa termos que podem ter interpretação ambígua. Para entender como eles são usados neste documento, leia as definições a seguir:

init

Dois processos diferentes são normalmente chamados “init”:

- O processo `initramfs`, que monta o sistema de arquivos raiz
- O processo do sistema operacional, que inicia todos os outros processos executados do sistema de arquivos raiz real

Nos dois casos, o programa `systemd` é responsável por essa tarefa. Ele é executado do `initramfs` para montar o sistema de arquivos raiz. Depois de bem-sucedido, ele será executado novamente no sistema de arquivos raiz como o processo inicial. Para evitar confusão entre esses dois processos do `systemd`, chamamos o primeiro processo de *init no initramfs* e o segundo de *systemd*.

initrd/initramfs

Um `initrd` (disco RAM inicial) é um arquivo de imagem que inclui a imagem do sistema de arquivos raiz, que é carregada pelo kernel e montada do `/dev/ram` como o sistema de arquivos raiz temporário. A montagem desse sistema de arquivos exige um driver.

A partir do kernel 2.6.13, o `initrd` foi substituído pelo `initramfs` (sistema de arquivos RAM inicial), que não exige a montagem de um driver do sistema de arquivos. O SUSE Linux Enterprise Desktop usa exclusivamente um `initramfs`. No entanto, como o `initramfs` é armazenado como `/boot/initrd`, ele costuma ser chamado de “`initrd`”. Neste capítulo, usamos exclusivamente o nome `initramfs`.

16.2 Processo de boot do Linux

O processo de boot do Linux consiste em vários estágios, cada um deles representado por um componente diferente:

1. *Seção 16.2.1, “Fase de inicialização e do carregador de boot”*
2. *Seção 16.2.2, “Fase do kernel”*
3. *Seção 16.2.3, “Fase do `init` no `initramfs`”*
4. *Seção 16.2.4, “Fase do `systemd`”*

16.2.1 Fase de inicialização e do carregador de boot

Durante a fase de inicialização, o hardware da máquina é configurado e os dispositivos são preparados. Esse processo varia bastante entre as arquiteturas de hardware.

O SUSE Linux Enterprise Desktop usa o carregador de boot GRUB 2 em todas as arquiteturas. Dependendo da arquitetura e do firmware, o processo para iniciar o carregador de boot GRUB 2 pode ter várias etapas. A finalidade do carregador de boot é carregar o kernel e o sistema de arquivos inicial baseado em RAM (`initramfs`). Para obter mais informações sobre o GRUB 2, consulte o *Capítulo 18, Carregador de boot GRUB 2*.

16.2.1.1 Fase de inicialização e do carregador de boot no AArch64 e no AMD64/Intel 64

Após ligar o computador, o BIOS ou a UEFI inicializa a tela e o teclado e testa a memória principal. Até esse estágio, a máquina não acessa nenhuma mídia de armazenamento em massa. Em seguida, as informações sobre a data e o horário atuais e sobre os periféricos mais importantes são carregadas dos valores do CMOS. Quando a mídia de boot e sua geometria são reconhecidas, o controle do sistema passa do BIOS/UEFI para o carregador de boot.

Em uma máquina equipada com BIOS tradicional, apenas o código do primeiro setor de dados físico de 512 bytes, MBR (Master Boot Record), do disco de boot pode ser carregado. Apenas o GRUB 2 mínimo é adequado ao MBR. Sua única finalidade é carregar uma imagem do núcleo do GRUB 2 com os drivers do sistema de arquivos do espaço entre o MBR e a primeira partição (tabela de partição MBR) ou da partição de boot BIOS (tabela de partição GPT). Essa imagem inclui os drivers do sistema de arquivos, portanto, ela pode acessar o `/boot` localizado no sistema de arquivos raiz. O `/boot` contém módulos adicionais para o núcleo do GRUB 2, além do kernel e da imagem `initramfs`. Quando ele tem acesso a essa partição, o GRUB 2 carrega o kernel e a imagem `initramfs` na memória e transfere o controle ao kernel.

Ao inicializar um sistema BIOS de um sistema de arquivos criptografado que inclui uma partição `/boot` criptografada, você precisa inserir a senha de decodificação duas vezes. O GRUB 2 precisa dela primeiro para decodificar o `/boot` e depois o `systemd` para montar os volumes criptografados.

Nas máquinas com UEFI, o processo de boot é muito mais simples do que nas máquinas com BIOS tradicional. O firmware pode ler a partição de discos do sistema formatado em FAT com uma tabela de partição GPT. Esta partição de sistema EFI (no sistema em execução montado como `/boot/efi`) contém espaço suficiente para hospedar um GRUB 2 de pleno direito, que é carregado diretamente e executado pelo firmware.

Se o BIOS/UEFI suportar inicialização por rede, também será possível configurar um servidor de boot que ofereça o carregador de boot. Em seguida, o sistema será inicializado por PXE. O BIOS/UEFI funciona como o carregador de boot. Ele obtém a imagem do servidor de boot e inicia o sistema. Isso é totalmente independente dos discos rígidos locais.

16.2.1.2 Fase de inicialização e do carregador de boot no IBM Z

No IBM z, o processo de boot deve ser inicializado por um carregador de boot denominado **zipl** (carga inicial de programa z). Embora o **zipl** suporte a leitura de vários sistemas de arquivos, ele não suporta o sistema de arquivos padrão SLE (Btrfs) ou a inicialização de instantâneos. Portanto, o SUSE Linux Enterprise Desktop usa um processo de boot de duas fases que garante suporte total ao Btrfs no momento da inicialização:

1. O **zipl** é inicializado da partição `/boot/zipl`, que pode ser formatada com o sistema de arquivos Ext2, Ext3, Ext4 ou XFS. Essa partição inclui um kernel mínimo e um `initramfs`, que são carregados na memória. O `initramfs` contém um driver Btrfs (entre outros) e o carregador de boot GRUB 2. O kernel é iniciado com um parâmetro `initgrub`, que o instrui a iniciar o GRUB 2.
2. O kernel monta o sistema de arquivos raiz para que `/boot` se torne acessível. Agora, o GRUB 2 é iniciado do `initramfs`. Ele lê a configuração em `/boot/grub2/grub.cfg` e carrega o kernel final e o `initramfs` do `/boot`. Agora, o novo kernel é carregado pelo Kexec.

16.2.2 Fase do kernel

Depois que o carregador de boot passar no controle do sistema, o processo de boot será o mesmo em todas as arquiteturas. O carregador de boot carrega tanto o kernel quanto um sistema de arquivos inicial baseado em RAM (`initramfs`) na memória, e o kernel assume o controle.

Depois que o kernel configurar o gerenciamento de memória e detectar o tipo de CPU e seus recursos, ele inicializará o hardware e montará o sistema de arquivos raiz temporário que foi carregado com o `initramfs` da memória.

16.2.2.1 O arquivo `initramfs`

O `initramfs` (sistema de arquivos RAM inicial) é um pequeno arquivo `cpio` que pode ser carregado pelo kernel em um disco RAM. Ele está localizado em `/boot/initrd`. É possível criá-lo com uma ferramenta chamada **dracut**. Consulte **man 8 dracut** para obter detalhes.

O `initramfs` fornece um ambiente Linux mínimo que permite a execução de programas antes da montagem do sistema de arquivos raiz real. Este ambiente mínimo do Linux é carregado na memória pelas rotinas do BIOS ou da UEFI e não tem outros requisitos de

hardware específicos além de memória suficiente. O arquivo `initramfs` sempre deve incluir um executável denominado `init`, que executa o daemon `systemd` no sistema de arquivos raiz para realização do processo de boot.

Antes da montagem do sistema de arquivos raiz e da inicialização do sistema operacional, o kernel precisa dos drivers correspondentes para acessar o dispositivo em que o sistema de arquivos raiz está localizado. Esses drivers podem incluir drivers especiais para determinados tipos de unidades de discos rígidos ou até drivers de rede para acesso a um sistema de arquivos de rede. Os módulos necessários ao sistema de arquivos raiz são carregados pelo `init` no `initramfs`. Depois de carregados os módulos, o `udev` fornecerá os dispositivos necessários ao `initramfs`. Posteriormente no processo de inicialização, depois de mudar o sistema de arquivos raiz, será necessário gerar novamente os dispositivos. Esse procedimento é feito pela unidade `systemd-udev-trigger.service` do `systemd`.

16.2.2.1.1 Gerando o `initramfs` novamente

Como o `initramfs` contém drivers, é necessário atualizá-lo sempre que uma nova versão de um dos drivers é disponibilizada. Isso é feito automaticamente ao instalar o pacote que contém a atualização de driver. O YaST ou o zypper informará você sobre isso mostrando a saída do comando que gera o `initramfs`. Em algumas ocasiões, entretanto, você precisa gerar um `initramfs` outra vez, manualmente:

- *Adicionando drivers por causa de mudanças no hardware*
- *Movendo diretórios de sistema para um RAID ou LVM*
- *Adicionando discos a um grupo de LVM ou RAID Btrfs com o sistema de arquivos raiz*
- *Mudando as variáveis do kernel*

Adicionando drivers por causa de mudanças no hardware

Se você precisar mudar o hardware (por exemplo, discos rígidos), e esse hardware exigir drivers diferentes no kernel durante a inicialização, será necessário atualizar o arquivo `initramfs`

Abra ou crie o arquivo `/etc/dracut.conf.d/10-DRIVER.conf` e adicione a seguinte linha (observe o espaço em branco à esquerda):

```
force_drivers+=" DRIVER1 "
```

Substitua DRIVER1 pelo nome do driver do módulo. Se for necessário adicionar mais do que um driver, liste-os separados com espaço:

```
force_drivers+=" DRIVER1 DRIVER2 "
```

Avance para o [Procedimento 16.1, "Gerar um initramfs"](#).

Movendo diretórios de sistema para um RAID ou LVM

Sempre que você mover arquivos de troca (swap) ou diretórios de sistema, como /usr, em um sistema em execução para um RAID ou volume lógico, será necessário criar um initramfs que ofereça suporte a drivers RAID ou LVM de software.

Para isso, crie as respectivas entradas em /etc/fstab e monte as novas entradas. Por exemplo, com **mount -a** e/ou **swapon -a**.

Avance para o [Procedimento 16.1, "Gerar um initramfs"](#).

Adicionando discos a um grupo de LVM ou RAID Btrfs com o sistema de arquivos raiz

Sempre que você adicionar (ou remover) um disco de um grupo de volumes lógicos ou de um RAID Btrfs com o sistema de arquivos raiz, será necessário criar um initramfs que ofereça suporte ao volume ampliado. Siga as instruções no [Procedimento 16.1, "Gerar um initramfs"](#).

Avance para o [Procedimento 16.1, "Gerar um initramfs"](#).

Mudando as variáveis do kernel

Se você mudar os valores das variáveis do kernel pela interface do **sysctl**, editando os arquivos relacionados (/etc/sysctl.conf ou /etc/sysctl.d/*.conf), a mudança será perdida na próxima reinicialização do sistema. Mesmo que você carregue os valores com **sysctl --system** em tempo de execução, as mudanças não são gravadas no arquivo initramfs. Você precisa atualizá-lo de acordo com a instrução no [Procedimento 16.1, "Gerar um initramfs"](#).

PROCEDIMENTO 16.1: GERAR UM INITRAMFS

Veja que todos os comandos no procedimento a seguir precisam ser executados como usuário root.

1. Insira o diretório /boot:

```
# cd /boot
```

2. Gere um novo arquivo `initramfs` com `dracut` substituindo `MY_INITRAMFS` pelo nome do arquivo de sua escolha:

```
# dracut MY_INITRAMFS
```

Se preferir, execute `dracut -f NOME DO ARQUIVO` para substituir um arquivo init existente.

3. (Ignore esta etapa se você executou `dracut -f` na etapa anterior.) Crie um link simbólico do arquivo `initramfs` criado na etapa anterior para o `initrd`:

```
# ln -sf MY_INITRAMFS initrd
```

4. Na arquitetura do IBM Z, execute também o `grub2-install`.

16.2.3 Fase do init no initramfs

O sistema de arquivos raiz temporário montado pelo kernel do `initramfs` contém o executável `systemd` (que é denominado `init` no `initramfs`). Consulte também a [Seção 16.1, “Terminologia”](#). Este programa executa todas as ações necessárias para montar o sistema de arquivos raiz apropriado. Ele oferece a funcionalidade do kernel para os drivers necessários de sistema de arquivos e de dispositivo para controladoras de armazenamento em massa com o `udev`.

O principal objetivo do `init` no `initramfs` é preparar a montagem e o acesso ao sistema de arquivos raiz real. Dependendo da configuração do sistema, o `init` no `initramfs` será responsável pelas tarefas a seguir.

Carregando módulos do kernel

Dependendo da configuração do hardware, drivers especiais poderão ser necessários para acessar os componentes de hardware do computador (sendo que o componente mais importante é o disco rígido). Para acessar o sistema de arquivos raiz final, o kernel precisa carregar os drivers adequados do sistema de arquivos.

Fornecendo arquivos especiais de bloco

O kernel gera eventos de dispositivo de acordo com os módulos carregados. O `udev` gerencia esses eventos e gera os arquivos de bloco especiais necessários em um sistema de arquivos RAM em `/dev`. Sem esses arquivos especiais, o sistema de arquivos e outros dispositivos não estariam acessíveis.

Gerenciando configurações RAID e LVM

Se você configurar o sistema para armazenar o sistema de arquivos raiz no RAID ou no LVM, o `init` no `initramfs` configurará o LVM ou o RAID para permitir acesso ao sistema de arquivos raiz posteriormente.

Gerenciando a configuração de rede

Se você tiver configurado o sistema para usar um sistema de arquivos raiz montado em rede (via NFS), o `init` deverá verificar se os drivers de rede corretos foram carregados e estão configurados para permitir acesso ao sistema de arquivos raiz.

Se o sistema de arquivos residir em um dispositivo de blocos de rede, como iSCSI ou SAN, a conexão com o servidor de armazenamento também será configurada pelo `init` no `initramfs`. O SUSE Linux Enterprise Desktop permitirá a inicialização de um destino iSCSI secundário se o destino primário não estiver disponível.



Nota: Resolvendo falhas de montagem

Se o sistema de arquivos raiz não puder ser montado no ambiente de boot, ele deverá ser verificado e consertado antes de prosseguir com a inicialização. O verificador de sistema de arquivos será iniciado automaticamente nos sistemas de arquivos Ext3 e Ext4. O processo de conserto não é automatizado nos sistemas de arquivos XFS e Btrfs, e o usuário vê as informações que descrevem as opções disponíveis para consertar o sistema de arquivos. Quando o sistema de arquivos é consertado com êxito, sair do ambiente de boot faz com que o sistema repita a montagem do sistema de arquivos raiz. Em caso de êxito, o boot continuará normalmente.

16.2.3.1 Fase do `init` no `initramfs` no processo de instalação

Quando o `init` no `initramfs` é chamado durante o boot inicial como parte do processo de instalação, suas tarefas são diferentes das que foram mencionadas acima. Observe que o sistema de instalação não inicia também o `systemd` do `initramfs`. Esse tipo de tarefa é executado pelo `linuxrc`.

Localizando o meio de instalação

Ao iniciar o processo de instalação, a máquina carrega um kernel de instalação e um `init` especial que inclui o instalador do YaST. O instalador do YaST é executado em um sistema de arquivos RAM e precisa ter informações sobre a localização do meio de instalação para acessá-lo e instalar o sistema operacional.

Iniciando o reconhecimento de hardware e carregando os módulos do kernel apropriados

Conforme mencionado na [Seção 16.2.2.1, “O arquivo initramfs”](#), o processo de boot começa com um conjunto mínimo de drivers que pode ser usado com a maioria das configurações de hardware. Em máquinas com AArch64, POWER e AMD64/Intel 64, o **linuxrc** inicializa um processo de varredura de hardware inicial que determina o conjunto de drivers adequado à sua configuração de hardware. No IBM Z, uma lista de drivers e seus parâmetros precisam ser fornecidos, por exemplo, por meio do `linuxrc` ou de um `parmfile`. Esses drivers são usados para gerar um `initramfs` personalizado necessário para inicializar o sistema. Se os módulos não forem necessários para inicialização, mas forem para coldplug, eles poderão ser carregados com `systemd`. Para obter mais informações, consulte a [Seção 19.6.4, “Carregando módulos do kernel”](#).

Carregando o sistema de instalação

Quando o hardware é adequadamente reconhecido, os drivers apropriados são carregados. O programa `udev` cria os arquivos de dispositivo especiais, e o **linuxrc** inicia o sistema de instalação com o instalador do YaST.

Inicialização do YaST

Por fim, o **linuxrc** inicia o YaST, que inicia a instalação do pacote e a configuração do sistema.

16.2.4 Fase do systemd

Após encontrar o sistema de arquivos raiz “real”, será verificado se há erros nele e se ele foi montado. Se esse procedimento for bem-sucedido, o `initramfs` será limpo e o daemon `systemd` no sistema de arquivos raiz será executado. O `systemd` é um gerenciador de serviços e sistemas do Linux. Trata-se do processo pai que é iniciado como PID 1 e age como um sistema `init` que ativa e mantém os serviços no espaço do usuário. Consulte a [Capítulo 19, Daemon systemd](#) para obter os detalhes.


17 UEFI (Unified Extensible Firmware Interface)

UEFI (Unified Extensible Firmware Interface) é a interface entre o firmware que vem com o hardware do sistema, todos os componentes do hardware do sistema e o sistema operacional.

A UEFI está se tornando cada vez mais disponível em sistemas PC e substituindo o PC-BIOS tradicional. Por exemplo, a UEFI suporta apropriadamente sistemas de 64 bits e oferece inicialização segura (“Boot Seguro”, firmware versão 2.3.1c ou superior necessário), que é um dos recursos mais importantes. Por fim, com a UEFI, um firmware padrão estará disponível em todas as plataformas x86.

A UEFI oferece também as seguintes vantagens:

- Inicialização de discos grandes (mais de 2 TiB) com GPT (Tabela de Partição GUID).
- Drivers e arquitetura independente da CPU.
- Ambiente pré-OS flexível com recursos de rede.
- CSM (Módulo de Suporte de Compatibilidade) para suportar inicialização de sistemas operacionais legados por emulação do tipo PC-BIOS.

Para obter mais informações, consulte a http://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface . As seguintes seções não representam uma visão geral da UEFI, são apenas dicas sobre como alguns recursos são implementados no SUSE Linux Enterprise Desktop.

17.1 Boot seguro

Para a UEFI, proteger o processo de boot significa estabelecer uma cadeia de confiança. A “plataforma” é a raiz da cadeia de confiança. No contexto do SUSE Linux Enterprise Desktop, a placa-mãe e o firmware on-board podem ser considerados a “plataforma”. Em outras palavras, imagine o fornecedor do hardware e a cadeia de confiança que parte desse fornecedor para os fabricantes dos componentes, os fornecedores de OS, etc

A confiança é expressada através da criptografia de chave pública. O fornecedor do hardware coloca a chamada PK (Chave de Plataforma) no firmware, representando a base da confiança. A relação de confiança com os fornecedores do sistema operacional e os outros é documentada pela assinatura das chaves usando a Chave de Plataforma.

Por fim, a segurança é estabelecida exigindo que nenhum código seja executado pelo firmware, exceto se tiver sido assinado por uma das chaves “confiáveis”, seja um carregador de boot de OS, algum driver localizado na memória flash de uma placa PCI Express ou no disco, seja uma atualização do próprio firmware.

Para usar Boot Seguro, o carregador de OS deve ser assinado com uma chave de confiança do firmware, e você precisa que o carregador de OS verifique se o kernel que ele carrega é confiável. É possível adicionar Chaves de Troca de Chave (KEK) ao banco de dados de chaves UEFI. Dessa forma, é possível usar outros certificados, desde que sejam assinados com a parte privada da PK.

17.1.1 Implementação no SUSE Linux Enterprise Desktop

A Chave de Troca de Chave (KEK) da Microsoft é instalada por padrão.



Nota: Tabela de partição GUID (GPT) obrigatória

Por padrão, o recurso Boot Seguro está habilitado nas instalações UEFI/x86_64. Você encontra a opção *Habilitar Suporte a Boot Seguro* na guia *Opções de Código de Boot* da caixa de diálogo *Configurações do Carregador de Boot*. Ela suporta a inicialização quando o boot seguro está ativado no firmware, tornando possível inicializar mesmo quando está desativada.

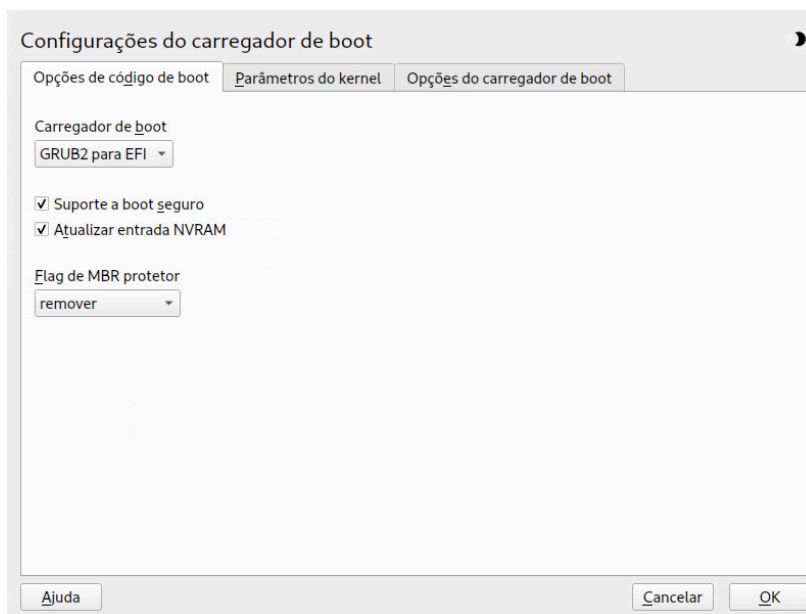


FIGURA 17.1: SUPORTE A BOOT SEGURO

O recurso Boot Seguro requer que a GPT (Tabela de Partição GUID) substitua o particionamento antigo por um MBR (Master Boot Record). Se o YaST detectar o modo EFI durante a instalação, ele tentará criar uma partição GPT. A UEFI espera encontrar os programas EFI na ESP (Partição de Sistema EFI) formatada por FAT.

O suporte a Boot Seguro UEFI requer um carregador de boot com assinatura digital que o firmware reconheça como uma chave confiável. Teoricamente, essa chave é de confiança do firmware, sem exigir intervenção manual.

Há duas formas de conseguir isso. Uma é trabalhar com os fornecedores do hardware para que eles endossem uma chave do SUSE, que o SUSE usará para assinar o carregador de boot. A outra é utilizar o programa de Certificação de Logotipo do Windows da Microsoft para certificar o carregador de boot e para a Microsoft reconhecer a chave de assinatura do SUSE (isto é, assiná-lo com sua KEK). Até agora, o SUSE assinava o carregador pelo Serviço de Assinatura UEFI (que é a Microsoft, neste caso).

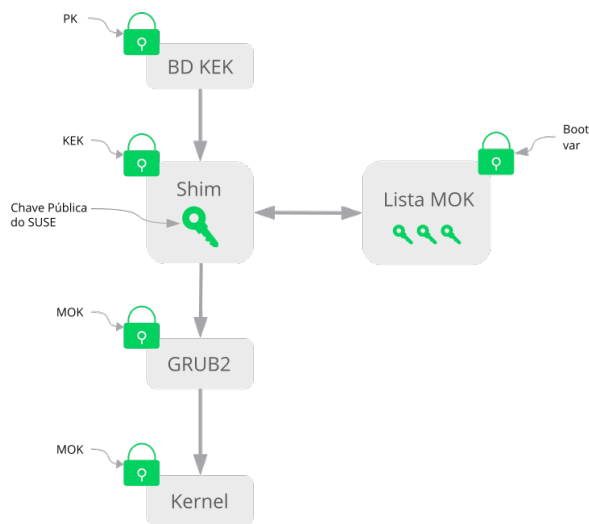


FIGURA 17.2: UEFI: PROCESSO DE BOOT SEGURO

Na camada de implementação, o SUSE usa o carregador `shim`, que é instalado por padrão. Trata-se de uma solução inteligente que evita problemas legais e simplifica consideravelmente as etapas de certificação e assinatura. A tarefa do carregador `shim` é carregar um carregador de boot, como GRUB 2, e verificá-lo; por sua vez, o carregador de boot carrega os kernels assinados apenas por uma chave do SUSE. O SUSE oferece esta funcionalidade desde o SLE11 SP3 em instalações novas que tenham o Boot Seguro UEFI habilitado.

Há dois tipos de usuários confiáveis:

- Primeiro, os que detêm as chaves. A Chave de Plataforma (PK) permite quase tudo. A Chave de Troca de Chave (KEK) permite tudo o que pode uma PK, exceto modificar a PK.
- Segundo, qualquer pessoa com acesso físico à máquina. Um usuário com acesso físico pode reinicializar a máquina e configurar a UEFI.

A UEFI oferece dois tipos de variáveis para atender às necessidades desses usuários:

- O primeiro tipo são as chamadas “Variáveis Autenticadas”, que podem ser atualizadas tanto do processo de boot (conhecido como Ambiente de Serviços de Boot) quanto do OS em execução. Isso pode ser feito apenas quando o novo valor da variável é assinado com a mesma chave que assinou o valor antigo da variável. E elas só podem ser anexadas ou modificadas para um valor com número de série maior.
- A segunda são as chamadas “Variáveis Apenas de Serviços de Boot”. Essas variáveis estão acessíveis a qualquer código executado durante o processo de boot. Após o término do processo de boot e antes de iniciar o OS, o carregador de boot deve chamar ExitBootServices. Depois disso, essas variáveis não estarão mais acessíveis, e o OS não poderá usá-las.

As várias listas de chaves UEFI são do primeiro tipo, já que permitem atualização online, adição e lista negra de chaves, drivers e impressões digitais do firmware. É o segundo tipo de variável (“Variável Apenas de Serviços de Boot”) que ajuda a implementar o Boot Seguro de maneira segura, pronta para código-fonte aberto e, portanto, compatível com GPLv3.

O SUSE começa com shim: um carregador de boot EFI pequeno e simples assinado pela SUSE e pela Microsoft.

Dessa forma, o shim pode ser carregado e executado.

O shim continua para verificar se o carregador de boot que deseja carregar é confiável. Em uma situação padrão, o shim usa um certificado do SUSE independente incorporado. Além disso, o shim permite “inscrever” outras chaves, anulando a chave padrão do SUSE. A seguir, nós as chamamos de “Chaves do Proprietário da Máquina” ou MOKs, para abreviar.

Em seguida, o carregador de boot verifica e inicializa o kernel, e o kernel faz o mesmo com os módulos.

17.1.2 MOK (Chave do Proprietário da Máquina)

Para substituir kernels, drivers ou outros componentes específicos que fazem parte do processo de boot, você precisa usar as Chaves do Proprietário da Máquina (MOKs, Machine Owner Keys). A ferramenta `mokutil` pode ajudá-lo a gerenciar as MOKs.

Você pode criar uma solicitação de registro de MOK com `mokutil`. A solicitação é armazenada em uma variável em tempo de execução (RT, Runtime) UEFI chamada `MokNew`. No próximo boot, o carregador de boot `shim` detecta a `MokNew` e carrega o `MokManager`, que inclui várias opções. Você pode usar as opções *Registrar chave do disco* e *Registrar hash do disco* para adicionar a chave à `MokList`. Use a opção *Registrar MOK* para copiar a chave da variável `MokNew`.

O registro de uma chave do disco geralmente é feito quando o `shim` falha ao carregar o `grub2` e efetua fallback para carregar o `MokManager`. Como a `MokNew` ainda não existe, você tem a opção de localizar a chave na partição UEFI.

17.1.3 Inicializando um kernel personalizado

As informações a seguir são baseadas no https://en.opensuse.org/openSUSE:UEFI#Booting_a_custom_kernel.

O Boot Seguro não impede você de usar um kernel autocompilado. Você deve assiná-lo com seu próprio certificado e tornar esse certificado reconhecível para o firmware ou a MOK.

1. Crie uma chave X.509 personalizada e um certificado usados para assinatura:

```
openssl req -new -x509 -newkey rsa:2048 -keyout key.asc \
-out cert.pem -nodes -days 666 -subj "/CN=$USER/"
```

Para obter mais informações sobre como criar certificados, consulte https://en.opensuse.org/openSUSE:UEFI_Image_File_Sign_Tools#Create_Your_Own_Certificate.

2. Empacote a chave e o certificado como uma estrutura PKCS#12:

```
> openssl pkcs12 -export -inkey key.asc -in cert.pem \
-name kernel_cert -out cert.p12
```

3. Gere um banco de dados NSS para usar com o comando `pesign`:

```
> certutil -d . -N
```

4. Importe a chave e o certificado incluídos no PKCS#12 para o banco de dados NSS:

```
> pk12util -d . -i cert.pl2
```

5. “Proteja” o kernel com a nova assinatura usando o comando **pesign**:

```
> pesign -n . -c kernel_cert -i arch/x86/boot/bzImage \
-o vmlinuz.signed -s
```

6. Liste as assinaturas na imagem do kernel:

```
> pesign -n . -S -i vmlinuz.signed
```

Neste momento, é possível instalar o kernel em `/boot`, como de costume. Como o kernel agora tem uma assinatura personalizada, o certificado usado para a assinatura deve ser importado para o firmware ou a MOK UEFI.

7. Converta o certificado no formato DER para importá-lo para o firmware ou a MOK:

```
> openssl x509 -in cert.pem -outform der -out cert.der
```

8. Copie o certificado para o ESP para facilitar o acesso:

```
> sudo cp cert.der /boot/efi/
```

9. Use **mokutil** para iniciar a lista de MOKs automaticamente.

- a. Importe o certificado para o MOK:

```
> mokutil --root-pw --import cert.der
```

A opção `--root-pw` habilita a utilização do usuário `root` diretamente.

- b. Consulte a lista dos certificados preparados para inscrição:

```
> mokutil --list-new
```

- c. Reinicialize o sistema. O `shim` deve iniciar o MokManager. É necessário digitar a senha de `root` para confirmar a importação do certificado para a lista da MOK.

- d. Verifique se a chave recém-importada foi inscrita:

```
> mokutil --list-enrolled
```

- - a. Se preferir, este é o procedimento para iniciar a MOK manualmente:
Reinicialize
 - b. No menu do GRUB 2, pressione a tecla "c".
 - c. Tipo:


```
chainloader $efibootdir/MokManager.efi
boot
```
 - d. Selecione *Enroll key from disk* (Inscrever chave do disco).
 - e. Navegue até o arquivo `cert.der` e pressione **Enter**.
 - f. Siga as instruções para inscrever a chave. Normalmente, você pressiona '0' e 'y' para confirmar.
Se preferir, o menu do firmware pode oferecer maneiras de adicionar uma nova chave ao Banco de Dados de Assinatura.

17.1.4 Usando drivers que não são de caixa de entrada

Não há suporte para adição de drivers que não são de caixa de entrada (isto é, drivers que não vêm com o SUSE Linux Enterprise Desktop) durante a instalação com o Boot Seguro habilitado. Por padrão, a chave de assinatura usada para SolidDriver/PLDP não é confiável.

É possível instalar drivers de terceiros durante a instalação, com o Boot Seguro habilitado de duas formas diferentes. Nos dois casos:

- Adicionar as chaves necessárias ao banco de dados do firmware usando as ferramentas de gerenciamento do firmware/sistema antes da instalação. Essa opção depende do hardware específico que você usa. Fale com o fornecedor do hardware para obter mais informações.
- Usar uma ISO do driver inicializável em <https://drivers.suse.com/> ou pedir ao fornecedor do hardware para inscrever as chaves necessárias na lista MOK na primeira inicialização.

Para usar a ISO do driver inicializável para inscrever as chaves do driver na lista MOK, siga estas etapas:

1. Grave a imagem ISO acima em um meio de CD/DVD vazio.
2. Inicie a instalação usando o novo meio de CD/DVD, com a mídia de instalação padrão em mãos ou um URL para um servidor de instalação de rede.

Ao fazer uma instalação de rede, digite o URL da fonte de instalação de rede na linha de comando de boot usando a opção `install=`.

Ao instalar de uma mídia ótica, o instalador inicializará primeiro do kit do driver e, em seguida, solicitará para inserir o primeiro disco de instalação do produto

3. Um `initrd` com os drivers atualizados será usado para instalação.

Para obter mais informações, consulte a https://drivers.suse.com/doc/Usage/Secure_Boot_Certificate.html.

17.1.5 Recursos e limitações

Ao inicializar no modo Boot Seguro, os seguintes recursos se aplicam:






- Instalação no local do carregador de boot padrão UEFI, um mecanismo para manter ou restaurar a entrada de boot EFI.
- Reinicialização por UEFI.
- O hipervisor do Xen inicializará com UEFI quando não houver nenhum BIOS legado para o qual fazer fallback.
- Suporte a boot PXE IPv6 da UEFI.
- Suporte ao modo de vídeo da UEFI. O kernel pode recuperar o modo de vídeo da UEFI para configurar o modo KMS com os mesmos parâmetros.
- A inicialização UEFI de dispositivos USB é suportada.

Ao inicializar no modo Boot Seguro, as seguintes limitações se aplicam:

- Para que o Boot Seguro não seja facilmente desviado, alguns recursos do kernel são desabilitados durante a execução no modo Boot Seguro.
- O carregador de boot, o kernel e os módulos do kernel devem ser assinados.
- Kexec e Kdump estão desabilitados.
- A hibernação (suspensão no disco) é desabilitada.
- O acesso a `/dev/kmem` e `/dev/mem` não é possível, nem mesmo como usuário root.
- O acesso à porta de E/S não é possível, nem mesmo como usuário root. Todos os drivers gráficos X11 devem usar um driver do kernel.

- O acesso a PCI BAR por sysfs não é possível.
- O `custom_method` em ACPI não está disponível.
- Debugfs para o módulo `asus-wmi` não está disponível.
- O parâmetro `acpi_rsdp` não tem nenhum efeito sobre o kernel.

17.2 Mais informações

- <https://www.uefi.org> : Home page da UEFI onde você encontra as especificações atuais da UEFI.
- Publicações no blog por Olaf Kirch e Vojtěch Pavlík (o capítulo acima é quase todo baseado nessas publicações):
 - <https://www.suse.com/c/uefi-secure-boot-plan/> 
 - <https://www.suse.com/c/uefi-secure-boot-overview/> 
 - <https://www.suse.com/c/uefi-secure-boot-details/> 
- <https://en.opensuse.org/openSUSE:UEFI> : UEFI com openSUSE.

18 Carregador de boot GRUB 2

Este capítulo descreve como configurar o GRUB 2, o carregador de boot usado no SUSE® Linux Enterprise Desktop. Ele é o sucessor do carregador de boot GRUB tradicional, agora chamado de “GRUB Legacy”. O GRUB 2 tem sido o carregador de boot padrão no SUSE® Linux Enterprise Desktop desde a versão 12. Um módulo do YaST está disponível para definir as configurações mais importantes. O procedimento de boot como um todo é detalhado no [Capítulo 16, Introdução ao processo de boot](#). Para obter detalhes sobre o suporte a Boot Seguro para máquinas UEFI, consulte o [Capítulo 17, UEFI \(Unified Extensible Firmware Interface\)](#).

18.1 Principais diferenças entre o GRUB legado e o GRUB 2

- A configuração é armazenada em arquivos diferentes.
- Mais sistemas de arquivos são suportados (por exemplo, Btrfs).
- Pode ler arquivos armazenados em dispositivos LVM ou RAID diretamente.
- A interface do usuário pode ser traduzida e alterada com temas.
- Inclui um mecanismo para carregar módulos que suportam recursos adicionais, como sistemas de arquivos, etc
- Pesquisa e gera automaticamente entradas de boot para outros kernels e sistemas operacionais, como o Windows.
- Inclui um console mínimo do tipo Bash.

18.2 Estrutura do arquivo de configuração

A configuração do GRUB 2 baseia-se nos seguintes arquivos:

/boot/grub2/grub.cfg

Este arquivo inclui a configuração dos itens de menu do GRUB 2. Ele substitui o menu.lst usado no GRUB Legacy. O grub.cfg não deve ser editado. Ele é gerado automaticamente pelo comando **grub2-mkconfig -o /boot/grub2/grub.cfg**.

/boot/grub2/custom.cfg

Este arquivo opcional é diretamente originado pelo grub.cfg no momento da inicialização e pode ser usado para adicionar itens personalizados ao menu de boot. A partir do SUSE Linux Enterprise Desktop 12 SP2, essas entradas também serão analisadas ao usar o **grub-once**.

/etc/default/grub

Este arquivo controla as configurações do usuário do GRUB 2 e, normalmente, inclui outras configurações de ambiente, como fundos e temas.

Scripts em /etc/grub.d/

Os scripts nesse diretório são lidos durante a execução do comando **grub2-mkconfig -o /boot/grub2/grub.cfg**. Suas instruções estão integradas ao arquivo de configuração principal /boot/grub/grub.cfg.

/etc/sysconfig/bootloader

Esse arquivo de configuração armazena algumas configurações básicas, como o tipo de carregador de boot e se é para habilitar o suporte a Boot Seguro UEFI.

/boot/grub2/x86_64-efi, /boot/grub2/power-ieee1275

Estes arquivos de configuração incluem opções específicas da arquitetura.

O GRUB 2 pode ser controlado de várias maneiras. As entradas de boot de uma configuração existente podem ser selecionadas no menu gráfico (splash screen). A configuração é carregada do arquivo /boot/grub2/grub.cfg, que é compilado de outros arquivos de configuração (veja abaixo). Todos os arquivos de configuração do GRUB 2 são considerados arquivos do sistema, e você precisa de privilégios de root para editá-los.



Nota: Ativando mudanças de configuração

Após editar os arquivos de configuração do GRUB 2 manualmente, você precisará executar **`grub2-mkconfig -o /boot/grub2/grub.cfg`** para ativar as mudanças. No entanto, isso não é necessário ao mudar a configuração com o YaST, já que ele executa esse comando automaticamente.

18.2.1 Arquivo `/boot/grub2/grub.cfg`

A splash screen gráfica com o menu de boot baseia-se no arquivo de configuração do GRUB 2 `/boot/grub2/grub.cfg`, que contém as informações sobre todas as partições ou sistemas operacionais que podem ser inicializados pelo menu.

Todas as vezes que o sistema é inicializado, o GRUB 2 carrega o arquivo de menu diretamente do sistema de arquivos. Por essa razão, o GRUB 2 não precisa ser reinstalado após as modificações no arquivo de configuração. O `grub.cfg` é recriado automaticamente com as instalações ou remoções do kernel.

O `grub.cfg` é compilado do arquivo `/etc/default/grub` e dos scripts localizados no diretório `/etc/grub.d/` ao executar o comando **`grub2-mkconfig -o /boot/grub2/grub.cfg`**. Portanto, você nunca deve editar o arquivo manualmente. Em vez disso, edite os arquivos de origem relacionados ou use o módulo *Carregador de Boot* do YaST para modificar a configuração, conforme descrito na [Seção 18.3, “Configurando o carregador de boot com o YaST”](#).

18.2.2 Arquivo `/etc/default/grub`

Há mais opções gerais do GRUB 2 nesse local, como o horário em que o menu é exibido ou o OS padrão para inicializar. Para listar todas as opções disponíveis, consulte a saída do seguinte comando:

```
> grep "export GRUB_DEFAULT" -A50 /usr/sbin/grub2-mkconfig | grep GRUB_
```

Além das variáveis já definidas, o usuário pode incluir suas próprias variáveis e usá-las posteriormente nos scripts que estão no diretório `/etc/grub.d`.

Após editar o `/etc/default/grub`, atualize o arquivo de configuração principal com o **`grub2-mkconfig -o /boot/grub2/grub.cfg`**.



Nota: Escopo

Todas as opções definidas neste arquivo são opções gerais que afetam todas as entradas de boot. É possível definir opções específicas para os kernels ou o hipervisor do Xen usando as opções de configuração `GRUB_*_XEN_*`. Veja os detalhes a seguir.

GRUB_DEFAULT

Define a entrada do menu de boot que será inicializada por padrão. Seu valor pode ser numérico, o nome completo de uma entrada do menu ou “saved” (gravado).

`GRUB_DEFAULT=2` inicializa a terceira entrada (contada a partir de zero) do menu de boot.

`GRUB_DEFAULT="2>0"` inicializa a primeira entrada do submenu da terceira entrada do menu de nível superior.

`GRUB_DEFAULT="Exemplo de entrada do menu de boot"` inicializa a entrada do menu com o título “Exemplo de entrada do menu de boot”.

`GRUB_DEFAULT=saved` inicializa a entrada especificada pelos comandos **`grub2-once`** ou **`grub2-set-default`**. Enquanto **`grub2-reboot`** define a entrada de boot padrão apenas para a próxima reinicialização, o **`grub2-set-default`** define a entrada de boot padrão até ser modificada. **`grub2-editenv list`** lista a entrada de boot seguinte.

GRUB_HIDDEN_TIMEOUT

Aguarda o usuário pressionar uma tecla durante o número especificado de segundos. Durante o período, nenhum menu é exibido, exceto se o usuário pressionar uma tecla. Se nenhuma tecla for pressionada durante o período especificado, o controle será passado para `GRUB_TIMEOUT`. `GRUB_HIDDEN_TIMEOUT=0` verifica primeiro se a tecla **Shift** foi pressionada e mostra o menu de boot em caso afirmativo, do contrário, inicializa a entrada do menu padrão imediatamente. Esse é o procedimento padrão quando apenas um OS inicializável é identificado pelo GRUB 2.

GRUB_HIDDEN_TIMEOUT_QUIET

Se `false` (falso) for especificado, um temporizador de contagem regressiva será exibido em uma tela em branco quando o recurso `GRUB_HIDDEN_TIMEOUT` estiver ativo.

GRUB_TIMEOUT

O período em segundos durante o qual o menu de boot é exibido antes de inicializar a entrada de boot padrão automaticamente. Se você pressionar uma tecla, o tempo de espera será cancelado, e o GRUB 2 aguardará você fazer uma seleção manualmente. `GRUB_TIMEOUT=-1` exibe o menu até você selecionar a entrada de boot manualmente.

GRUB_CMDLINE_LINUX

As entradas nesta linha são adicionadas ao fim das entradas de boot para o modo normal e de recuperação. Use-a para adicionar parâmetros do kernel à entrada de boot.

GRUB_CMDLINE_LINUX_DEFAULT

Igual a GRUB_CMDLINE_LINUX, mas as entradas são anexadas apenas no modo normal.

GRUB_CMDLINE_LINUX_RECOVERY

Igual a GRUB_CMDLINE_LINUX, mas as entradas são anexadas apenas no modo de recuperação.

GRUB_CMDLINE_LINUX_XEN_REPLACE

Esta entrada substitui completamente os parâmetros de GRUB_CMDLINE_LINUX por todas as entradas de boot do Xen.

GRUB_CMDLINE_LINUX_XEN_REPLACE_DEFAULT

Igual a GRUB_CMDLINE_LINUX_XEN_REPLACE, mas substitui apenas os parâmetros de GRUB_CMDLINE_LINUX_DEFAULT.

GRUB_CMDLINE_XEN

Esta entrada especifica os parâmetros de kernel apenas para o kernel convidado do Xen. O princípio da operação é o mesmo de GRUB_CMDLINE_LINUX.

GRUB_CMDLINE_XEN_DEFAULT

Igual a GRUB_CMDLINE_XEN. O princípio da operação é o mesmo de GRUB_CMDLINE_LINUX_DEFAULT.

GRUB_TERMINAL

Habilita e especifica um dispositivo de terminal de entrada/saída. Pode ser console (consoles BIOS e EFI do PC), serial (terminal serial), ofconsole (console do Open Firmware) ou o gfxterm padrão (saída do modo gráfico). É possível também habilitar mais de um dispositivo colocando as opções necessárias entre aspas, por exemplo, GRUB_TERMINAL="console serial".

GRUB_GFXMODE

A resolução usada para o terminal gráfico gfxterm. Observe que você só pode usar os modos suportados por sua placa gráfica (VBE). O padrão é "auto", que tenta selecionar uma resolução preferencial. É possível exibir as resoluções de tela disponíveis para o GRUB 2 digitando videoinfo na linha de comando do GRUB 2. Para acessar a linha de comando, digite **C** quando aparecer a tela do menu de boot do GRUB 2.

É possível também especificar a profundidade de cores anexando-a à configuração da resolução, por exemplo, `GRUB_GFXMODE=1280x1024x24`.

GRUB_BACKGROUND

Defina uma imagem de fundo para o terminal gráfico `gfxterm`. A imagem deve ser um arquivo legível pelo GRUB 2 no momento da inicialização, que deve terminar com o sufixo `.png`, `.tga`, `.jpg` ou `.jpeg`. Se necessário, a imagem será dimensionada para caber na tela.

GRUB_DISABLE_OS_PROBER

Se esta opção for definida como `true` (verdadeiro), a pesquisa automática de outros sistemas operacionais será desabilitada. Apenas as imagens do kernel em `/boot/` e as opções de seus próprios scripts em `/etc/grub.d/` serão detectadas.

SUSE_BTRFS_SNAPSHOT_BOOTING

Se essa opção for definida como `true` (verdadeiro), o GRUB 2 poderá ser inicializado diretamente nos instantâneos do Snapper. Para obter mais informações, consulte a [Seção 10.3, “Rollback do sistema por inicialização de instantâneos”](#).

Para ver a lista completa de opções, consulte o [manual do GNU GRUB \(http://www.gnu.org/software/grub/manual/grub.html#Simple-configuration\)](http://www.gnu.org/software/grub/manual/grub.html#Simple-configuration).

18.2.3 Scripts em `/etc/grub.d`

Os scripts nesse diretório são lidos durante a execução do comando `grub2-mkconfig -o /boot/grub2/grub.cfg`. As instruções deles estão incorporadas ao `/boot/grub2/grub.cfg`. A ordem dos itens de menu no `grub.cfg` é determinada pela ordem em que os arquivos são executados nesse diretório. Os arquivos com um número à esquerda são executados primeiro, começando pelo número mais baixo. `00_header` é executado antes de `10_linux`, que é executado antes de `40_custom`. Se houver arquivos com nomes alfabéticos, eles serão executados depois dos arquivos com números nos nomes. Apenas os arquivos executáveis geram uma saída para `grub.cfg` durante a execução de `grub2-mkconfig`. Por padrão, todos os arquivos no diretório `/etc/grub.d` são executáveis.



Dica: Conteúdo personalizado persistente no `grub.cfg`

Como `/boot/grub2/grub.cfg` é recompilado sempre que `grub2-mkconfig` é executado, qualquer conteúdo personalizado é perdido. Para inserir as linhas diretamente no `/boot/grub2/grub.cfg` sem perdê-las após a execução de `grub2-mkconfig`, insira-as entre

```
### BEGIN /etc/grub.d/90_persistent ###
```

e

```
### END /etc/grub.d/90_persistent ###
```

O script `90_persistent` garante que o conteúdo seja preservado.

Veja a seguir uma lista dos scripts mais importantes:

00_header

Define variáveis de sistema, como locais de arquivos do sistema, configurações de tela, temas e entradas que já foram gravadas. Ele também importa as preferências armazenadas no `/etc/default/grub`. Normalmente, não é necessário modificar este arquivo.

10_linux

Identifica os kernels do Linux no dispositivo raiz e cria entradas de menu relevantes. Inclui a opção de modo de recuperação associada, se habilitada. Somente o kernel mais recente é exibido na página de menu principal, com kernels adicionais incluídos em um submenu.

30_os-prober

Esse script usa o `os-prober` para procurar o Linux e outros sistemas operacionais e apresenta os resultados no menu do GRUB 2. Há seções para identificar outros sistemas operacionais específicos, como Windows ou macOS.

40_custom

Este arquivo oferece uma forma simples de incluir entradas de boot personalizadas no `grub.cfg`. Não mude a parte `exec tail -n +3 $0` que fica no começo.

A sequência de processamento é definida pelos números precedentes, sendo o menor número executado primeiro. Se os scripts forem precedidos pelo mesmo número, a ordem alfabética do nome completo determinará a disposição.



Dica: `/boot/grub2/custom.cfg`

Se você criar o `/boot/grub2/custom.cfg` e preenchê-lo com conteúdo, ele será automaticamente incluído no `/boot/grub2/grub.cfg` logo após `40_custom` no momento da inicialização.

18.2.4 Mapeamento entre unidades BIOS e dispositivos Linux

No GRUB Legacy, o arquivo de configuração `device.map` era usado para derivar nomes de dispositivos Linux dos números das unidades BIOS. O mapeamento entre as unidades BIOS e os dispositivos Linux nem sempre pode ser previsto corretamente. Por exemplo, o GRUB Legacy obterá a ordem incorreta se a sequência de boot das unidades IDE e SCSI for trocada na configuração do BIOS.

O GRUB 2 evita este problema usando strings de ID de dispositivo (UUIDs) ou rótulos de sistema de arquivos ao gerar o `grub.cfg`. Os utilitários do GRUB 2 criam um mapa de dispositivos temporário simultaneamente, que, na maioria das vezes, é suficiente, sobretudo em caso de sistemas de disco único.

Porém, se você tiver que anular o mecanismo de mapeamento de dispositivos automático do GRUB 2, crie seu arquivo de mapeamento personalizado `/boot/grub2/device.map`. O seguinte exemplo muda o mapeamento para transformar o `DISK 3` no disco de boot. Observe que os números de partição do GRUB 2 começam com `1`, e não com `0` como no GRUB Legacy.

```
(hd1) /dev/disk-by-id/DISK3 ID
(hd2) /dev/disk-by-id/DISK1 ID
(hd3) /dev/disk-by-id/DISK2 ID
```

18.2.5 Editando as entradas de menu durante o procedimento de boot

É útil editar diretamente as entradas de menu quando o sistema não é mais inicializado por causa de falha na configuração. Ele também pode ser usado para testar novas configurações sem alterar a configuração do sistema.

1. No menu gráfico de boot, selecione a entrada que deseja editar com as teclas de seta.
2. Pressione **E** para abrir o editor baseado em texto.

3. Use as teclas de seta para ir até a linha que deseja editar.



```
GNU GRUB version 2.04

set root='hd0,gpt2'
if [ x$feature_platform_search_hint = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint='hd0,gpt2' 3c2\
51c37-7ebb-4aaa-a658-eca1e810198d
else
  search --no-floppy --fs-uuid --set=root 3c251c37-7ebb-4aaa-a65\
8-eca1e810198d
fi
echo      'Loading Linux 5.3.18-8-default ...'
linux     /boot/vmlinuz-5.3.18-8-default root=UUID=3c251c37-7\
ebb-4aaa-a658-eca1e810198d $!extra_cmdline splash=silent resume=/dev/v\
da4 mitigations=auto quiet crashkernel=195M,high crashkernel=72M,low
echo      'Loading initial ramdisk ...'
initrd    /boot/initrd-5.3.18-8-default

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB
menu.
```

FIGURA 18.1: EDITOR DE BOOT DO GRUB 2

Agora você tem duas opções:

- a. Adicione parâmetros separados por espaço ao fim da linha que começa com `linux` ou `linuxefi` para editar os parâmetros de kernel. Há uma lista completa de parâmetros disponível em <https://en.opensuse.org/Linuxrc>.
 - b. Se preferir, edite as opções gerais para mudar a versão do kernel, por exemplo. A tecla `→|` sugere todas as complementações possíveis.
4. Pressione **F10** para inicializar o sistema com as mudanças feitas ou pressione **Esc** para descartar suas edições e retornar ao menu do GRUB 2.

As mudanças feitas desta maneira só se aplicam ao processo de boot atual, elas não são gravadas permanentemente.



Importante: Layout do teclado durante o procedimento de boot

O layout do teclado norte-americano é o único disponível na hora de inicializar. Consulte a *Livro "Deployment Guide", Capítulo 8 "Troubleshooting", Seção 8.3 "Bootting from installation media fails", US keyboard layout*.



Nota: Carregador de boot na mídia de instalação

O Carregador de Boot da mídia de instalação em sistemas com BIOS tradicional ainda é o GRUB Legacy. Para adicionar parâmetros de boot, selecione uma entrada e comece a digitar. As adições feitas à entrada de boot de instalação são gravadas no sistema instalado permanentemente.

18.2.6 Definindo uma senha de boot

Mesmo antes da inicialização do sistema operacional, o GRUB 2 permite acessar os sistemas de arquivos. Os usuários que não têm permissões de root poderão acessar os arquivos no sistema Linux aos quais não têm acesso depois que o sistema for inicializado. Para bloquear esse tipo de acesso ou impedir que os usuários inicializem determinadas entradas de menu, defina uma senha de boot.



Importante: A inicialização exige uma senha

Se definida, a senha de boot será necessária em cada inicialização, o que significa que o sistema não será inicializado automaticamente.

Para definir uma senha de boot, faça o seguinte. Se preferir, use o YaST (*Proteger Carregador de Boot com Senha*).

1. Criptografe a senha usando **grub2-mkpasswd-pbkdf2**:

```
> sudo grub2-mkpasswd-pbkdf2
Password: ****
Reenter password: ****
PBKDF2 hash of your password is grub.pbkdf2.sha512.10000.9CA4611006FE96BC77A...
```

2. Cole a string resultante no arquivo **/etc/grub.d/40_custom** juntamente com o comando **set superusers**.

```
set superusers="root"
password_pbkdf2 root grub.pbkdf2.sha512.10000.9CA4611006FE96BC77A...
```

3. Para importar as mudanças para o arquivo de configuração principal, execute:

```
> sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

Após a reinicialização, você terá que informar o nome de usuário e a senha ao tentar inicializar uma entrada de menu. Insira `root` e a senha digitada durante o comando `grub2-mkpasswd-pbkdf2`. Se as credenciais estiverem corretas, o sistema inicializará a entrada de boot selecionada.

Para obter mais informações, consulte a <https://www.gnu.org/software/grub/manual/grub.html#Security>.

18.2.7 Acesso autorizado às entradas do menu de boot

Você pode configurar o GRUB 2 para permitir acesso às entradas do menu de boot, dependendo do nível de autorização. Você pode configurar várias contas de usuário protegidas por senhas e atribuir a elas acesso a entradas de menu diferentes. Para configurar a autorização no GRUB 2, siga estas etapas:

1. Crie e criptografe uma senha para cada conta de usuário que deseja usar no GRUB 2. Use o comando `grub2-mkpasswd-pbkdf2` conforme descrito na [Seção 18.2.6, “Definindo uma senha de boot”](#).
2. Apague o arquivo `/etc/grub.d/10_linux`. Isso impede a saída das entradas do menu padrão do GRUB 2.
3. Edite o arquivo `/boot/grub2/custom.cfg` e adicione entradas de menu personalizadas manualmente. O seguinte gabarito é um exemplo, ajuste-o de acordo com o seu caso de uso:

```
set superusers=admin
password admin ADMIN_PASSWORD
password maintainer MAINTAINER_PASSWORD

menuentry 'Operational mode' {
    insmod ext2
    set root=hd0,1
    echo 'Loading Linux ...'
    linux /boot/vmlinuz root=/dev/vda1 $GRUB_CMDLINE_LINUX_DEFAULT $GRUB_CMDLINE_LINUX
    mode=operation
    echo 'Loading Initrd ...'
    initrd /boot/initrd
}

menuentry 'Maintenance mode' --users maintainer {
    insmod ext2
```

```
set root=hd0,1
echo 'Loading Linux ...'
linux /boot/vmlinuz root=/dev/vda1 $GRUB_CMDLINE_LINUX_DEFAULT $GRUB_CMDLINE_LINUX
mode=maintenance
echo 'Loading Initrd ...'
initrd /boot/initrd
}
```

4. Importe as mudanças para o arquivo de configuração principal:

```
> sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

No exemplo acima:

- O menu do GRUB 2 tem duas entradas: *Modo de operação* e *Modo de manutenção*.
- Se nenhum usuário for especificado, ambas as entradas do menu de boot estarão acessíveis, mas ninguém poderá acessar a linha de comando do GRUB 2 nem editar as entradas do menu existentes.
- O usuário admin pode acessar a linha de comando do GRUB 2 e editar as entradas do menu existentes.
- O usuário maintenance pode selecionar o item do menu de recuperação.

18.3 Configurando o carregador de boot com o YaST

O modo mais fácil de configurar opções gerais do carregador de boot no sistema SUSE Linux Enterprise Desktop é usar o módulo do YaST. No *Centro de Controle do YaST*, selecione *Sistema > Carregador de Boot*. O módulo mostra a configuração do carregador de boot atual do sistema e permite fazer mudanças.

Use a guia *Opções de Código de Boot* para ver e mudar configurações relativas a tipo, local e definições avançadas do carregador. Você pode especificar se é para usar o GRUB 2 no modo padrão ou EFI.



Importante: Sistemas EFI exigem GRUB2-EFI

Se você tem um sistema EFI, é possível instalar apenas o GRUB2-EFI, senão o sistema não poderá mais ser inicializado.



Importante: Reinstalando o carregador de boot

Para reinstalar o carregador de boot, mude uma configuração no YaST e, em seguida, reverta-a. Por exemplo, para reinstalar o GRUB2-EFI, selecione *GRUB2* primeiro e, em seguida, alterne imediatamente para *GRUB2-EFI*.

Do contrário, o carregador de boot poderá ser apenas parcialmente reinstalado.



Nota: Carregador de boot personalizado

Para usar um carregador de boot diferente dos que estão na lista, selecione *Não Instalar Nenhum Carregador de Boot*. Leia a documentação do seu carregador de boot cuidadosamente antes de escolher esta opção.

18.3.1 Local do carregador de boot e opções de código de boot

O local padrão do carregador de boot depende da configuração da partição e é o MBR (Master Boot Record – Registro Mestre de Boot) ou o setor de boot da partição /. Para modificar o local do carregador de boot, siga estas etapas:

PROCEDIMENTO 18.1: MUDANDO O LOCAL DO CARREGADOR DE BOOT

1. Selecione a guia *Opções de Código de Boot* e escolha uma das seguintes opções para *Localização do Carregador de Boot*:

Boot do Master Boot Record

Esse procedimento instala o carregador de boot no MBR do disco que contém o diretório /boot. Normalmente, esse será o disco montado em /, mas se /boot estiver montado em uma partição separada em um disco diferente, o MBR desse disco será usado.

Boot da partição raiz

Instala o carregador de boot no setor de boot da partição /.

Partição Raiz Personalizada

Use esta opção para especificar a localização do carregador de boot manualmente.

2. Clique em *OK* para aplicar as mudanças.

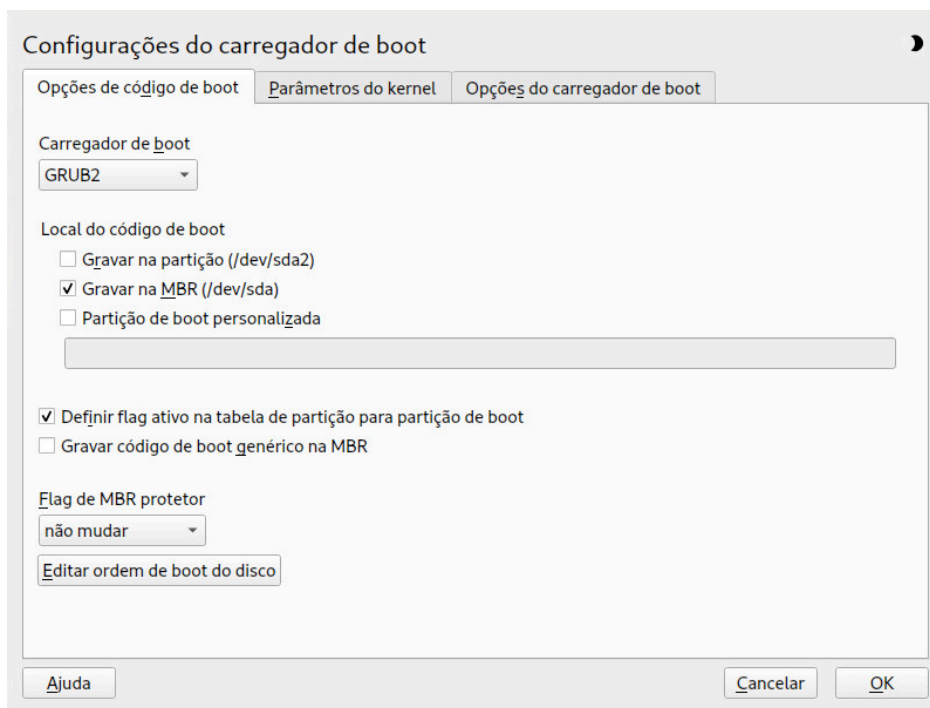


FIGURA 18.2: OPÇÕES DE CÓDIGO DE BOOT

A guia *Opções de Código de Boot* inclui as seguintes opções adicionais:

Definir Flag ativo na Tabela de Partição para Partição de Boot

Ativa a partição que contém o diretório `/boot`. Para os sistemas POWER, ela ativa a partição PReP. Use essa opção nos sistemas com BIOS antigo e/ou sistemas operacionais legados, porque eles podem não ser inicializados de uma partição não ativa. É seguro deixar essa opção ativa.

Gravar Código de Boot genérico no MBR

Se o MBR incluir um código personalizado “não GRUB”, essa opção o substituirá por um código genérico e independente do sistema operacional. Se você desativar essa opção, o sistema poderá se tornar não inicializável.

Habilitar Suporte a Boot Confiável

Inicia o TrustedGRUB2, que suporta a funcionalidade de computação confiável (Trusted Platform Module, TPM). Para obter mais informações, consulte <https://github.com/Sirrix-AG/TrustedGRUB2>.

A seção *Flag de MBR protetor* inclui as seguintes opções:

set

Essa opção é apropriada para inicialização do BIOS legado tradicional.

remove

Essa opção é apropriada para inicialização da UEFI.

do not change

Geralmente, essa é a melhor opção se você já tem um sistema em funcionamento.

Na maioria dos casos, o YaST usa como padrão a opção apropriada.

18.3.2 Ajustando a ordem dos discos

Se o computador tiver mais do que um disco rígido, você poderá especificar a sequência de boot dos discos. O primeiro disco na lista é onde o GRUB 2 será instalado no caso da inicialização do MBR. Ele é o disco no qual o SUSE Linux Enterprise Desktop é instalado por padrão. O restante da lista é uma dica para o mapeador de dispositivos do GRUB 2 (consulte a [Seção 18.2.4, “Mapeamento entre unidades BIOS e dispositivos Linux”](#)).



Atenção: Sistema não inicializável

Normalmente, o valor padrão é válido para quase todas as implantações. Se você mudar a ordem de boot dos discos incorretamente, o sistema poderá se tornar não inicializável na próxima reinicialização. Por exemplo, se o primeiro disco na lista não fizer parte da ordem de boot do BIOS e os outros discos na lista tiverem MBRs vazios.

PROCEDIMENTO 18.2: DEFININDO A ORDEM DOS DISCOS

1. Abra a guia *Opções de Código de Boot*.
2. Clique em *Editar Ordem de Boot do Disco*.
3. Se mais de um disco for listado, selecione um disco e clique em *Para cima* ou *Para baixo* para reordenar os discos exibidos.
4. Clique em *OK* duas vezes para gravar as mudanças.

18.3.3 Configurando as opções avançadas

É possível configurar as opções de boot avançadas na guia *Opções do Carregador de Boot*.

18.3.3.1 Guia Opções do Carregador de Boot

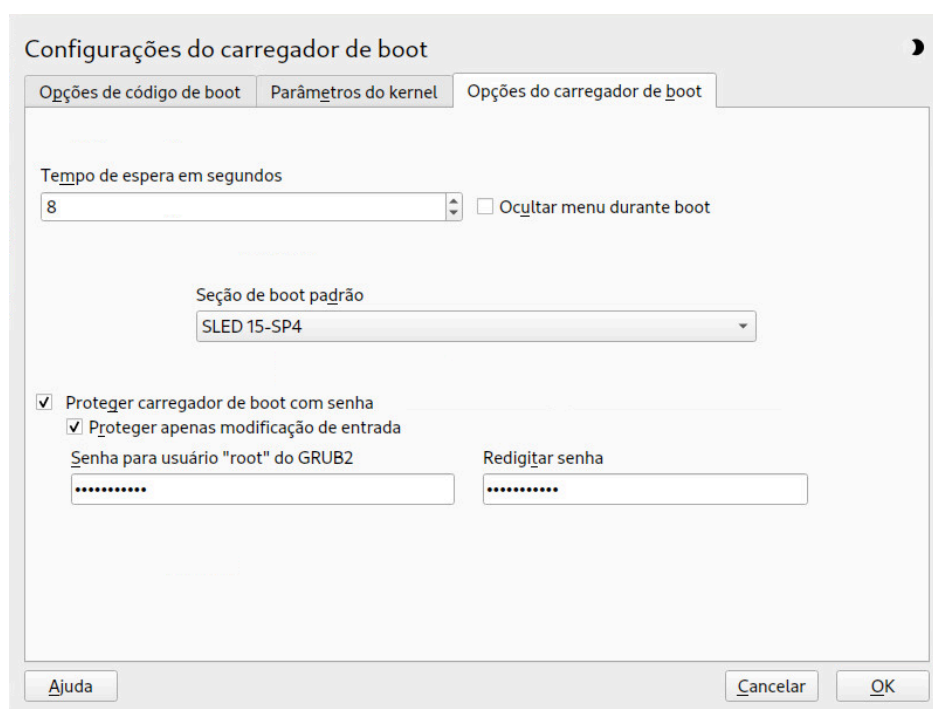


FIGURA 18.3: OPÇÕES DO CARREGADOR DE BOOT

Tempo de espera do carregador de boot

Mude o valor de *Tempo de Espera em Segundos* digitando um novo valor e clicando na tecla de seta apropriada com o mouse.

Investigar OS Estrangeiro

Quando selecionada, o carregador de boot procura por outros sistemas, como Windows ou outras instalações do Linux.

Ocultar Menu na Inicialização

Oculto o menu de boot e a entrada padrão.

Ajustando a entrada de boot padrão

Selecione a entrada desejada na lista “Seção de Boot Padrão.” Observe que o sinal de “>” no nome da entrada de boot delimita a seção de boot e sua subseção.

Proteger Carregador de Boot com Senha

Protege o carregador de boot e o sistema com uma senha adicional. Para obter detalhes sobre a configuração manual, consulte a [Seção 18.2.6, “Definindo uma senha de boot”](#). Se essa opção for ativada, a senha de boot será necessária em cada inicialização, o que

significa que o sistema não será inicializado automaticamente. No entanto, se você prefere o comportamento do GRUB 1, habilite também *Proteger apenas modificação de entrada*. Com essa configuração, qualquer pessoa tem permissão para selecionar uma entrada de boot e inicializar o sistema, enquanto a senha para o usuário root do GRUB 2 apenas é necessária para modificar as entradas de boot.

18.3.3.2 Guia *Parâmetros de Kernel*

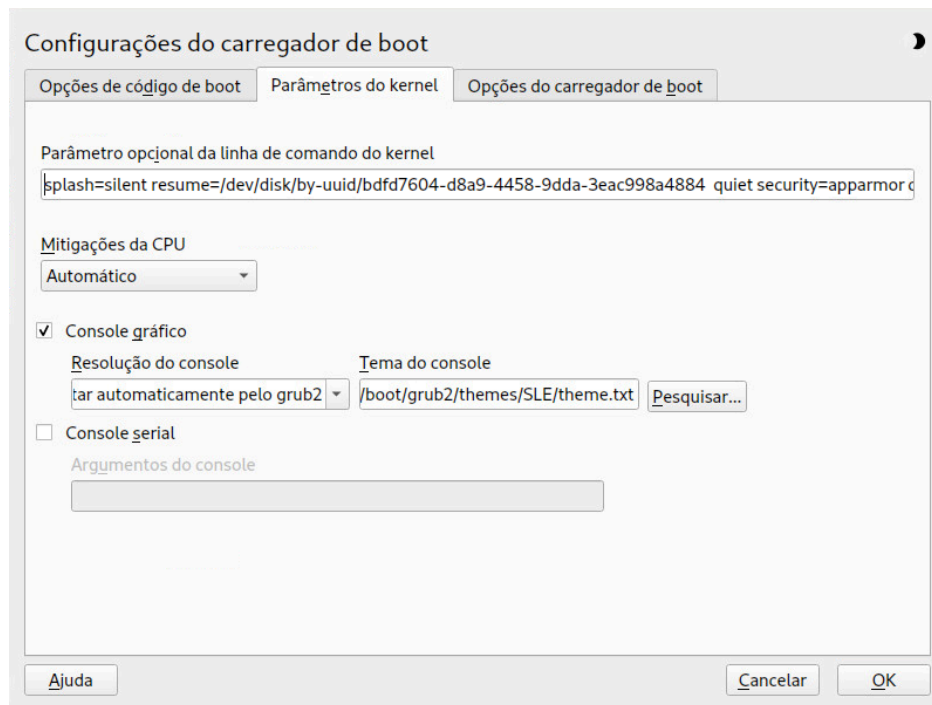


FIGURA 18.4: PARÂMETROS KERNEL

Parâmetro opcional da linha de comando do kernel

Especifique parâmetros opcionais do kernel aqui para habilitar/desabilitar recursos do sistema, adicionar drivers etc

Mitigações da CPU

A SUSE lançou um ou mais parâmetros de linha de comando de boot do kernel para todas as mitigações de software que foram implantadas com a finalidade de evitar ataques de temporização na CPU. Alguns deles podem resultar em perda de desempenho. Escolha uma das seguintes opções para encontrar um equilíbrio entre segurança e desempenho, dependendo da sua configuração:

Automático. Habilita todas as mitigações necessárias para o modelo de CPU, mas não protege contra ataques de thread entre CPUs. Essa configuração pode afetar o desempenho a um certo nível, dependendo da carga de trabalho.

Auto + Sem SMT. Fornece o conjunto completo de mitigações de segurança disponíveis. Habilita todas as mitigações necessárias para o modelo de CPU. Além disso, ela desabilita o Multithreading Simultâneo (SMT, Simultaneous Multithreading) para evitar ataques de temporização em vários threads de CPU. Essa configuração pode prejudicar o desempenho, dependendo da carga de trabalho.


Desativado. Desabilita todas as mitigações. Os ataques de temporização contra a CPU são possíveis, dependendo do modelo dela. Essa configuração não afeta o desempenho.

Manual. Não define nenhum nível de mitigação. Especifique suas mitigações da CPU manualmente usando as opções de linha de comando do kernel.

Usar console gráfico

Quando marcada, o menu de boot aparece na splash screen gráfica, e não em modo de texto. Por padrão, a resolução da tela de boot é definida automaticamente, mas você pode defini-la manualmente em *Resolução do console*. O arquivo de definição de tema gráfico pode ser especificado com o seletor de arquivos *Tema do console*. Mude essa opção apenas se você deseja aplicar seu próprio tema personalizado.

Usar o console serial

Se a sua máquina é controlada por um console serial, ative essa opção e especifique a porta COM que será usada e em qual velocidade. Consulte [**info grub**](#) ou o site <http://www.gnu.org/software/grub/manual/grub.html#Serial-terminal> 

18.4 Comandos úteis do GRUB 2

grub2-mkconfig

Gera um novo `/boot/grub2/grub.cfg` com base no `/etc/default/grub` e nos scripts de `/etc/grub.d/`.

EXEMPLO 18.1: USO DO GRUB2-MKCONFIG

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```



Dica: Verificação de sintaxe

A execução de **grub2-mkconfig** sem nenhum parâmetro imprime a configuração em STDOUT, de onde é possível revisá-la. Use **grub2-script-check** após a gravação de `/boot/grub2/grub.cfg` para verificar sua sintaxe.



Importante: O **grub2-mkconfig** não conserta tabelas de boot seguro UEFI

Se você usa Boot Seguro UEFI e o sistema não consegue mais acessar o GRUB 2 corretamente, talvez seja necessário reinstalar o Shim e gerar novamente a tabela de boot UEFI. Para fazer isso, use:

```
# shim-install --config-file=/boot/grub2/grub.cfg
```

grub2-mkrescue

Cria uma imagem de recuperação inicializável da configuração do GRUB 2 instalado.

EXEMPLO 18.2: USO DO GRUB2-MKRESCUE

```
grub2-mkrescue -o save_path/name.iso iso
```

grub2-script-check

Verifica se há erros de sintaxe no arquivo especificado.

EXEMPLO 18.3: USO DO GRUB2-SCRIPT-CHECK

```
grub2-script-check /boot/grub2/grub.cfg
```

grub2-once

Defina a entrada de boot padrão apenas para a próxima inicialização. Para ver a lista de entradas de boot disponíveis, use a opção `--list`.

EXEMPLO 18.4: USO DO GRUB2-ONCE

```
grub2-once number_of_the_boot_entry
```



Dica: Ajuda do grub2-once


Chame o programa sem nenhuma opção para obter a lista completa de todas as opções possíveis.

18.5 Mais informações

Em <https://www.gnu.org/software/grub/>, há informações abrangentes sobre o GRUB 2. Consulte também a página de informações **grub**. Você também pode pesquisar a palavra-chave “GRUB 2” na Pesquisa de Informações Técnicas em <https://www.suse.com/support> para obter informações sobre problemas específicos.

19 Daemon systemd

O systemd é responsável pela inicialização do sistema e tem o ID de processo 1. O systemd é iniciado diretamente pelo kernel e resiste ao sinal 9, que normalmente termina os processos. Todos os outros programas são iniciados diretamente pelo systemd ou por um de seus processos filho. O systemd é um substituto do daemon init do System V e é totalmente compatível com o init do System V (por meio do suporte a scripts init).

A principal vantagem do systemd é que ele acelera consideravelmente o tempo de boot ao paralelizar as inicializações de serviços. Além disso, o systemd apenas inicia um serviço quando é realmente necessário. Os daemons não são iniciados incondicionalmente no momento da inicialização, mas quando são solicitados pela primeira vez. O systemd também suporta Grupos de Controle de Kernel (cgroups), criando instantâneos e restaurando o estado do sistema. Para obter mais detalhes, consulte <http://www.freedesktop.org/wiki/Software/systemd/> .

19.1 Conceito do systemd

A seção a seguir explica o conceito por trás do systemd.

O systemd é um gerenciador de sistema e sessão para Linux, compatível com os scripts init do System V e do LSB. Os principais recursos do systemd são:


- recursos de paralelização
- ativação de soquete e D-Bus para iniciar serviços
- iniciar daemons sob demanda
- monitoramento de processos usando cgroups do Linux
- criação de instantâneos e restauração do estado do sistema
- manutenção dos pontos de montagem e automount
- implementação de uma lógica elaborada de controle de serviço baseada em dependência transacional

19.1.1 Arquivo unit

O arquivo de configuração unit contém informações sobre serviço, soquete, dispositivo, ponto de montagem, ponto de automount, arquivo de troca (swap) ou partição, destino de inicialização, caminho do sistema de arquivos monitorado, temporizador controlado e supervisionado pelo systemd, instantâneo de estado do sistema temporário, fração de gerenciamento de recursos ou grupo de processos criados externamente.

O “arquivo unit” é um termo genérico usado pelo systemd para o seguinte:

- **Serviço.** Informações sobre um processo (por exemplo, a execução de um daemon); o arquivo termina com `.service`
- **Destinos.** Usado para agrupar unidades e como pontos de sincronização durante a inicialização; o arquivo termina com `.target`
- **Soquetes.** Informações sobre um soquete de rede, IPC ou FIFO do sistema de arquivos, para ativação baseada em soquete (como inetd); o arquivo termina com `.socket`
- **Caminho.** Usado para acionar outras unidades (por exemplo, executar um serviço quando houver mudanças nos arquivos); o arquivo termina com `.path`
- **Timer.** Informações sobre um temporizador controlado, para ativação baseada em temporizador; o arquivo termina com `.timer`
- **Ponto de montagem.** Normalmente, gerado de forma automática pelo gerador `fstab`; o arquivo termina com `.mount`
- **Ponto de automount.** Informações sobre um ponto de automount do sistema de arquivos; o arquivo termina com `.automount`
- **Swap.** Informações sobre um dispositivo ou arquivo de troca para paginação de memória; o arquivo termina com `.swap`
- **Dispositivo.** Informações sobre uma unidade de dispositivo conforme exposta na árvore de dispositivos do `sysfs/udev(7)`; o arquivo termina com `.device`
- **Escopo/Fração.** Um conceito de gerenciamento hierárquico de recursos de um grupo de processos; o arquivo termina com `.scope/.slice`

Para obter mais informações sobre arquivos de unidade do systemd, acesse <http://www.freedesktop.org/software/systemd/man/systemd.unit.html> 

19.2 Uso básico

O sistema init do System V usa vários comandos para gerenciar serviços: scripts `init`, `insserv`, `telinit` e outros. O `systemd` facilita gerenciar serviços, já que existe apenas um comando para ser memorizado para a maioria das tarefas de gerenciamento de serviços: `systemctl`. Ele usa a notação “command plus subcommand”, como `git` ou `zypper`:

```
systemctl GENERAL OPTIONS SUBCOMMAND SUBCOMMAND OPTIONS
```

Consulte `man 1 systemctl` para obter o manual completo.



Dica: Saída de terminal e complementação do bash

Se a saída chegar a um terminal (e não a um pipe ou arquivo, por exemplo), por padrão, os comandos `systemd` enviarão uma saída extensa para um pager. Use a opção `--no-pager` para desativar o modo de paginação.

O `systemd` também suporta a complementação do bash, que permite digitar as primeiras letras de um subcomando e pressionar `→|`. Esse recurso está disponível apenas no shell `bash` e requer a instalação do pacote `bash-completion`.

19.2.1 Gerenciando serviços em um sistema em execução

Os subcomandos de gerenciamento de serviços são os mesmos usados para gerenciar um serviço com o init do System V (`start`, `stop`, etc.). A sintaxe geral dos comandos de gerenciamento de serviços é a seguinte:

`systemd`

```
systemctl reload|restart|start|status|stop|... MY_SERVICE(S)
```

Init do System V

```
rcMY_SERVICE(S) reload|restart|start|status|stop|...
```

O `systemd` permite gerenciar vários serviços de uma só vez. Em vez de executar os scripts `init` um após o outro como acontece com o init do System V, execute um comando da seguinte forma:

```
> sudo systemctl start MY_1ST_SERVICE MY_2ND_SERVICE
```

Para listar todos os serviços disponíveis no sistema:

```
> sudo systemctl list-unit-files --type=service
```

A tabela a seguir lista os comandos de gerenciamento de serviços mais importantes para o systemd e o init do System V:

TABELA 19.1: **COMANDOS DE GERENCIAMENTO DE SERVIÇOS**

Tarefa	Comando <u>systemd</u>	Comando <u>init</u> do System V
Iniciando.	start	start
Parar.	stop	stop
Reiniciar. Encerra os serviços e os inicia na sequência. Se algum serviço ainda não estiver em execução, ele será iniciado.	restart	restart
Reiniciar condicionalmente. Reinicia os serviços se já estiverem em execução. Não faz nada para os serviços que não estão em execução.	try-restart	try-restart
Recarregar. Instrui os serviços a recarregarem seus arquivos de configuração sem interromper a operação. Caso de uso: Instruir o Apache a recarregar um arquivo de configuração <u>httpd.conf</u> modificado. Observe que nem todos os serviços suportam recarregamento.	reload	reload
Recarregar ou reiniciar. Recarrega os serviços quando o recarregamento é suportado; do contrário, reinicia-os. Se algum serviço ainda não estiver em execução, ele será iniciado.	reload-or-restart	n/a
Recarregar ou reiniciar condicionalmente. Recarrega os serviços se o recarregamento for suportado; do contrário reinicia-os, se estiverem em execução. Não faz nada para os serviços que não estão em execução.	reload-or-try-restart	n/a

Tarefa	Comando <u>systemd</u>	Comando init do System V
Obter informações detalhadas sobre status. Lista as informações sobre o status dos serviços. O comando <u>systemd</u> mostra detalhes, como descrição, executável, status, cgroup e as últimas mensagens emitidas por um serviço (consulte a Seção 19.6.9, “Depurando serviços”). O nível dos detalhes exibidos com o init do System V varia de acordo com cada serviço.	status	status
Obter informações resumidas sobre status. Mostra se os serviços estão ou não ativos.	is-active	status

19.2.2 Habilitando/Desabilitando serviços permanentemente

Os comandos de gerenciamento de serviços mencionados na seção anterior permitem manipular serviços na seção atual. O systemd também permite habilitar ou desabilitar serviços permanentemente para serem iniciados automaticamente quando solicitados ou para ficarem sempre indisponíveis. É possível fazer isso com o YaST ou por linha de comando.

19.2.2.1 Habilitando/Desabilitando serviços na linha de comando

A tabela a seguir lista os comandos de habilitação e desabilitação pelo systemd e pelo init do System V:



Importante: Inicialização de serviço

Ao habilitar um serviço na linha de comando, ele não é iniciado automaticamente. Ele é programado para iniciar na próxima inicialização do sistema ou mudança de nível de execução/destino. Para iniciar um serviço logo após habilitá-lo, execute explicitamente **systemctl start MEU_SERVIÇO** ou **rc MEU_SERVIÇO start**.

TABELA 19.2: COMANDOS PARA HABILITAR E DESABILITAR SERVIÇOS

Tarefa	Comando <u>systemd</u>	Comando init do System V
Habilitar.	<u>systemctl enable</u> <u>MEU(S)_SERVIÇO(S)</u>	<u>insserv</u> <u>MEU(S)_SERVIÇO(S)</u> , <u>chkconfig -a</u> <u>MEU(S)_SERVIÇO(S)</u>
Desabilitar.	<u>systemctl disable</u> <u>MEU(S)_SERVIÇO(S).service</u>	<u>insserv -r</u> <u>MEU(S)_SERVIÇO(S)</u> , <u>chkconfig -d</u> <u>MEU(S)_SERVIÇO(S)</u>
Verificar. Mostra se um serviço está ou não habilitado.	<u>systemctl is-enabled</u> <u>MEU_SERVIÇO</u>	<u>chkconfig</u> <u>MEU_SERVIÇO</u>
Reabilitar. Semelhante a reiniciar um serviço, este comando primeiro desabilita e depois habilita um serviço. Útil para restaurar um serviço aos seus padrões.	<u>systemctl reenable</u> <u>MEU_SERVIÇO</u>	n/d
Mascarar. Após “desabilitar” um serviço, ele ainda poderá ser iniciado manualmente. Para desabilitar um serviço completamente, é necessário mascará-lo. Use com cuidado.	<u>systemctl mask</u> <u>MEU_SERVIÇO</u>	n/d
Desmascarar. Só será possível usar novamente um	<u>systemctl unmask</u> <u>MEU_SERVIÇO</u>	n/d

Tarefa	Comando <u>systemd</u>	Comando init do System V
serviço mascarado depois que ele for desmascarado.		

19.3 Inicialização do sistema e gerenciamento de destino

Todo o processo de inicialização e encerramento do sistema é mantido pelo systemd. Desse ponto de vista, o kernel pode ser considerado um processo em segundo plano para manter todos os outros processos e ajustar o horário da CPU e o acesso ao hardware de acordo com as solicitações de outros programas.

19.3.1 Comparação entre destinos e níveis de execução

Com o init do System V, o sistema era inicializado no chamado “Nível de execução”. O nível de execução define como o sistema é iniciado e quais serviços estão disponíveis no sistema em execução. Os níveis de execução são numerados: os mais conhecidos são 0 (encerramento do sistema), 3 (multiusuário com rede) e 5 (multiusuário com rede e gerenciador de exibição).

O systemd apresenta um novo conceito usando as chamadas “unidades de destino”. No entanto, ele continua totalmente compatível com o conceito de nível de execução. As unidades de destino são nomeadas, e não numeradas, e possuem finalidades específicas. Por exemplo, os destinos local-fs.target e swap.target montam sistemas de arquivos locais e espaços de troca.

O destino graphical.target oferece recursos de sistema multiusuário com rede e gerenciador de exibição e equivale ao nível de execução 5. Destinos complexos, como graphical.target, agem como destinos “meta”, combinando um subconjunto de outros destinos. Como o systemd facilita criar destinos personalizados combinando destinos existentes, ele oferece excelente flexibilidade.

A lista a seguir mostra as unidades de destino mais importantes do systemd. Para ver a lista completa, consulte man 7 systemd.special.

default.target

O destino que é inicializado por padrão. Não um destino “real”, mas um link simbólico para outro destino, como `graphic.target`. Pode ser modificado permanentemente pelo YaST (consulte a [Seção 19.4, “Gerenciando serviços com o YaST”](#)). Para mudá-lo em uma sessão, use o parâmetro do kernel `systemd.unit=MEU_DESTINO.destino` no prompt de boot.

emergency.target

Inicia o shell de emergência no console. Use-o apenas no prompt de boot como `systemd.unit=emergency.target`.

graphical.target

Inicia um sistema com suporte a rede multiusuário e um gerenciador de exibição.

halt.target

Encerra o sistema.

mail-transfer-agent.target

Inicia todos os serviços necessários para enviar e receber e-mails.

multi-user.target

Inicia um sistema multiusuário com rede.

reboot.target

Reinicializa o sistema.

rescue.target

Inicia um sistema de usuário único sem rede.

Para continuar compatível com o sistema de nível de execução `init` do System V, o `systemd` oferece destinos especiais chamados `runlevelX.target` que mapeiam os níveis de execução correspondentes numerados `X`.

Para saber o destino atual, use o comando: `systemctl get-default`

TABELA 19.3: NÍVEIS DE EXECUÇÃO DO SYSTEM V E UNIDADES DE DESTINO DO `systemd`

Nível de execução do System V	<code>systemd</code> destino	Finalidade
0	<code>runlevel0.target</code> , <code>halt.target</code> , <code>poweroff.target</code>	Encerramento do sistema

Nível de execução do System V	<u>systemd</u> destino	Finalidade
1, S	<u>runlevel1.target</u> , <u>rescue.target</u> ,	Modo de usuário único
2	<u>runlevel2.target</u> , <u>multi-user.target</u> ,	Multiusuário local sem rede remota
3	<u>runlevel3.target</u> , <u>multi-user.target</u> ,	Multiusuário completo com rede
4	<u>runlevel4.target</u>	Não usado/Definido pelo usuário
5	<u>runlevel5.target</u> , <u>graphical.target</u> ,	Multiusuário completo com rede e gerenciador de exibição
6	<u>runlevel6.target</u> , <u>reboot.target</u> ,	Reinicialização do sistema

! Importante: O systemd ignora o `/etc/inittab`

Os níveis de execução em um sistema `init` do System V são configurados em `/etc/inittab`. O systemd *não* usa essa configuração. Consulte a [Seção 19.5.4, “Criando destinos personalizados”](#) para obter instruções sobre como criar seu próprio destino inicializável.

19.3.1.1 Comandos para mudar os destinos

Use os seguintes comandos para operar com unidades de destino:

Tarefa	Comando <u>systemd</u>	Comando <code>init</code> do System V
Mudar o destino/nível de execução atual	<code>systemctl isolate</code> <u>MEU_DESTINO</u> .target	<code>telinit</code> <u>X</u>

Tarefa	Comando <u>systemd</u>	Comando init do System V
Mudar para o destino/nível de execução padrão	<u>systemctl default</u>	n/d
Obter o destino/nível de execução atual	<u>systemctl list-units --type=target</u> Com o <u>systemd</u> , normalmente há mais de um destino ativo. O comando lista todos os destinos que estão ativos.	<u>who -r</u> ou <u>runlevel</u>
Mudar o nível de execução padrão de forma persistente	Use o Gerenciador de Serviços ou execute o seguinte comando: <u>Em -sf /usr/lib/systemd/system/MEU_DESTINO.target /etc/systemd/system/default.target</u>	Use o Gerenciador de Serviços ou mude a linha <u>id: X:initdefault:</u> em <u>/etc/inittab</u>
Mudar o nível de execução padrão para o processo de boot atual	Digite a seguinte opção no prompt de boot <u>systemd.unit= MEU_DESTINO.target</u>	Digite o número do nível de execução desejado no prompt de boot.
Mostrar as dependências de um destino/nível de execução	<u>systemctl show -p "Requires" MEU_DESTINO.target</u> <u>systemctl show -p "Wants" MEU_DESTINO.target</u> “Requires” lista as dependências obrigatórias (hard) (aquelas que devem ser resolvidas), enquanto “Wants” lista as dependências desejadas (soft) (aquelas que são resolvidas quando possível).	n/d

19.3.2 Depurando a inicialização do sistema

O `systemd` oferece os meios para a análise dos processos de inicialização do sistema. É possível revisar a lista de todos os serviços e os respectivos status (em vez de analisar o `/var/log/`). O `systemd` permite também explorar o procedimento de inicialização para descobrir quanto tempo leva para inicializar cada serviço.

19.3.2.1 Revisar inicialização dos serviços

Para revisar a lista completa dos serviços que foram iniciados desde a inicialização do sistema, digite o comando `systemctl`. Ele lista todos os serviços ativos, conforme mostrado a seguir (resumidamente). Para obter mais informações sobre determinado serviço, use `systemctl status MEU_SERVIÇO`.

EXEMPLO 19.1: LISTAR SERVIÇOS ATIVOS

```
# systemctl
UNIT                                LOAD    ACTIVE SUB    JOB DESCRIPTION
[...]
iscsi.service                       loaded active exited Login and scanning of iSC+
kmod-static-nodes.service           loaded active exited Create list of required s+
libvirtd.service                   loaded active running Virtualization daemon
nscd.service                       loaded active running Name Service Cache Daemon
chronyd.service                    loaded active running NTP Server Daemon
polkit.service                     loaded active running Authorization Manager
postfix.service                    loaded active running Postfix Mail Transport Ag+
rc-local.service                   loaded active exited /etc/init.d/boot.local Co+
rsyslog.service                    loaded active running System Logging Service
[...]
LOAD    = Reflects whether the unit definition was properly loaded.
ACTIVE  = The high-level unit activation state, i.e. generalization of SUB.
SUB      = The low-level unit activation state, values depend on unit type.

161 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'.
```

Para restringir o resultado a serviços com falha na inicialização, use a opção `--failed`:

EXEMPLO 19.2: LISTAR SERVIÇOS COM FALHA

```
# systemctl --failed
```

UNIT	LOAD	ACTIVE	SUB	JOB	DESCRIPTION
apache2.service	loaded	failed	failed		apache
NetworkManager.service	loaded	failed	failed		Network Manager
plymouth-start.service	loaded	failed	failed		Show Plymouth Boot Screen
[...]					

19.3.2.2 Depurar o tempo de inicialização

Para depurar o tempo de inicialização do sistema, o `systemd` oferece o comando **`systemd-analyze`**. Ele mostra o tempo total de inicialização, uma lista dos serviços solicitados por tempo de inicialização e também gera um gráfico SVG mostrando o tempo que os serviços levaram para serem iniciados em relação a outros serviços.

Listando o tempo de inicialização do sistema

```
# systemd-analyze
Startup finished in 2666ms (kernel) + 21961ms (userspace) = 24628ms
```

Listando o tempo de inicialização dos serviços

```
# systemd-analyze blame
15.000s backup-rpmdb.service
14.879s mandb.service
7.646s backup-sysconfig.service
4.940s postfix.service
4.921s logrotate.service
4.640s libvirtd.service
4.519s display-manager.service
3.921s btrfsmaintenance-refresh.service
3.466s lvm2-monitor.service
2.774s plymouth-quit-wait.service
2.591s firewalld.service
2.137s initrd-switch-root.service
1.954s ModemManager.service
1.528s rsyslog.service
1.378s apparmor.service
[...]
```

Gráficos do tempo de inicialização dos serviços

```
# systemd-analyze plot > jupiter.example.com-startup.svg
```


19.3.3 Compatibilidade com o System V

O `systemd` é compatível com o System V, o que ainda permite usar os scripts init existentes do System V. Entretanto, há pelo menos um problema conhecido em que o script init do System V não funciona com o `systemd` out-of-the-box: iniciar um serviço como outro usuário por meio de `su` ou `sudo` nos scripts init resulta em falha do script, gerando um erro de “Acesso negado”. Ao mudar o usuário com `su` ou `sudo`, é iniciada uma sessão PAM. Essa sessão será terminada após a conclusão do script init. Como consequência, o serviço que foi iniciado pelo script init também será terminado. Para solucionar esse erro, faça o seguinte:

1. Crie um agrupador de arquivo de serviço com o mesmo nome do script init e mais a extensão de nome de arquivo `.service`:

```
[Unit]
Description=DESCRIPTION
After=network.target

[Service]
User=USER
Type=forking❶
PIDFile=PATH TO PID FILE❶
ExecStart=PATH TO INIT SCRIPT start
ExecStop=PATH TO INIT SCRIPT stop
ExecStopPost=/usr/bin/rm -f PATH TO PID FILE❶

[Install]
WantedBy=multi-user.target❷
```

Substitua todos os valores gravados em `LETRAS MAIÚSCULAS` pelos valores apropriados.

- ❶ Opcional: use apenas se o script init iniciar um daemon.
- ❷ O `multi-user.target` também inicia o script init ao inicializar no `graphical.target`. Se ele tiver que ser iniciado apenas ao inicializar no gerenciador de exibição, use o `graphical.target` aqui.

2. Inicie o daemon com `systemctl start APLICATIVO`.

19.4 Gerenciando serviços com o YaST

O gerenciamento básico de serviços também pode ser feito com o módulo Gerenciador de Serviços do YaST. Ele permite iniciar, parar, habilitar e desabilitar serviços. Ele permite também mostrar o status e mudar o destino padrão de um serviço. Inicie o módulo do YaST em *YaST > Sistema > Services Manager* (Gerenciador de Serviços).

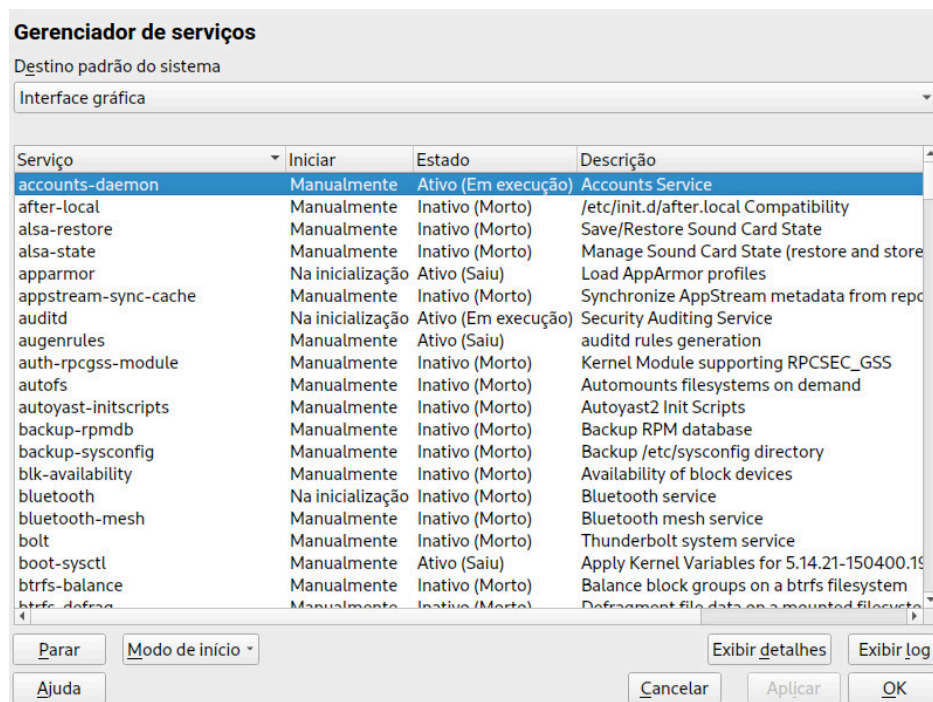


FIGURA 19.1: GERENCIADOR DE SERVIÇOS

Mudando o destino padrão do sistema

Para mudar o destino de inicialização do sistema, escolha o destino na caixa suspensa *Default System Target* (Destino Padrão do Sistema). Os destinos mais usados são *Graphical Interface* (Interface Gráfica) (iniciando uma tela gráfica de login) e *Multiusuário* (iniciando o sistema no modo de linha de comando).

Iniciando ou parando um serviço

Selecione um serviço da tabela. A coluna *Estado* mostra se ele está em execução (*Ativo*) ou não (*Inativo*). Para alternar o status, escolha *Iniciar* ou *Parar*.

Quando um serviço é iniciado ou parado, seu status muda na sessão que está em execução. Para mudar seu status em todas as reinicializações, é necessário habilitá-lo ou desabilitá-lo.

Definindo o comportamento de inicialização dos serviços

Os serviços podem ser iniciados automaticamente no momento da inicialização ou manualmente. Selecione um serviço da tabela. A coluna *Início* mostra se ele foi iniciado *Manualmente* ou *Na inicialização*. Para alternar o status, escolha *Modo de início*.

Para mudar o status de um serviço na sessão atual, você precisa iniciá-lo ou interrompê-lo conforme descrito acima.

Ver uma mensagem de status

Para ver a mensagem de status de um serviço, selecione-o na lista e escolha *Mostrar Detalhes*. A saída exibida será idêntica a que foi gerada pelo comando `systemctl -l status MEU_SERVIÇO`.

19.5 Personalizando systemd

As seções a seguir mostram alguns exemplos de personalização do `systemd`.



Atenção: Impedindo que sua personalização seja sobregravada

Ao personalizar o `systemd`, use sempre o diretório `/etc/systemd/`, *nunca* use o `/usr/lib/systemd/`. Do contrário, as mudanças serão sobregravadas na próxima atualização do `systemd`.

19.5.1 Personalizando os arquivos unit

A maneira recomendada de personalizar arquivos unit é usar o comando `systemctl edit SERVICE`. Esse comando inicia o editor de texto padrão e cria um diretório com o arquivo `override.conf` em `/etc/systemd/system/NAME.service.d/`. O comando também garante que o processo `systemd` em execução seja notificado sobre as mudanças.

Se preferir, você poderá abrir uma cópia do arquivo original para edição em vez de um arquivo em branco executando `systemctl edit --full SERVICE`. Ao editar o arquivo, não remova nenhuma das seções existentes.

Como exercício, mude por quanto tempo o sistema aguarda pela inicialização do MariaDB. Como root, execute `systemctl edit --full mariadb.service`. O arquivo aberto terá aparência similar à seguinte:

```
[Unit]
```

```

Description=MySQL server
Wants=basic.target
Conflicts=mariadb.target
After=basic.target network.target

[Install]
WantedBy=multi-user.target
Alias=mysql.service

[Service]
Restart=on-abort
Type=notify
ExecStartPre=/usr/lib/mysql/mysql-systemd-helper install
ExecStartPre=/usr/lib/mysql/mysql-systemd-helper upgrade
ExecStart=/usr/lib/mysql/mysql-systemd-helper start

# Configures the time to wait for start-up/stop
TimeoutSec=300

# Prevent writes to /usr, /boot, and /etc
ProtectSystem=full

# Prevent accessing /home, /root and /run/user
ProtectHome=true

UMask=007

```

Ajuste o valor de `TimeoutSec` e grave as mudanças. Para habilitar as mudanças, execute **`systemctl daemon-reload`** como root.

Para obter mais informações, consulte as páginas de manual que podem ser chamadas com o comando **`man 1 systemctl`**.

19.5.2 Criando arquivos drop-in

Para pequenas mudanças de um arquivo de configuração, use os chamados arquivos drop-in. Esses arquivos permitem estender a configuração dos arquivos de unidade sem ter que editá-los ou anulá-los realmente.

Por exemplo, para mudar um valor único no serviço `FOOBAR` localizado em `/usr/lib/systemd/system/FOOBAR.SERVICE`, faça o seguinte:

1. Crie um diretório chamado `/etc/systemd/system/FOOBAR.service.d/`. Observe o sufixo `.d`. O diretório deve receber outro nome de acordo com o serviço que você deseja corrigir com o arquivo dropin.

2. Nesse diretório, crie um arquivo `sua_modificação.conf`.
Verifique se ele contém somente a linha com o valor que deseja modificar.
3. Grave as mudanças feitas no arquivo



Nota: Evitando conflitos de nome

Para evitar conflitos de nome entre os arquivos drop-in e os arquivos fornecidos pelo SUSE, é recomendável prefixar todos os nomes de arquivos drop-in com um número de dois dígitos e um traço: por exemplo, `80-override.conf`.

As seguintes faixas são reservadas:

- `0-19` é reservada para upstream do `systemd`
- `20-25` é reservada para o `systemd` fornecido pelo SUSE
- `26-29` é reservada para pacotes do SUSE (diferentes do `systemd`)
- `50` é reservada para arquivos drop-in criados com `systemctl set-property`.

Use um número de dois dígitos acima dessa faixa para garantir que nenhum dos arquivos drop-in fornecidos pelo SUSE anule os seus próprios arquivos drop-in.

Você pode usar `systemctl cat $UNIT` para listar e verificar quais arquivos são levados em consideração na configuração dos units.

19.5.3 Convertendo serviços xinetd em systemd

Desde o lançamento do SUSE Linux Enterprise Desktop 15, a infraestrutura do `xinetd` foi removida. Esta seção descreve como converter arquivos existentes de serviço do `xinetd` em soquetes do `systemd`.

Para cada arquivo de serviço do `xinetd`, você precisa de pelo menos dois arquivos unit do `systemd`: o arquivo de soquete (`*.socket`) e um arquivo de serviço associado (`*.service`). O arquivo de soquete informa ao `systemd` qual soquete criar, e o arquivo de serviço informa ao `systemd` qual executável iniciar.

Considere o seguinte arquivo de serviço do `xinetd` de exemplo:

```
# cat /etc/xinetd.d/example
service example
```

```
{
    socket_type = stream
    protocol = tcp
    port = 10085
    wait = no
    user = user
    group = users
    groups = yes
    server = /usr/libexec/example/example
    server_args = -auth=bsdtcp example
    disable = no
}
```

Para convertê-lo em `systemd`, você precisa dos dois arquivos correspondentes a seguir:

```
# cat /usr/lib/systemd/system/example.socket
[Socket]
ListenStream=0.0.0.0:10085
Accept=false

[Install]
WantedBy=sockets.target
```

```
# cat /usr/lib/systemd/system/example.service
[Unit]
Description=example

[Service]
ExecStart=/usr/libexec/example/example -auth=bsdtcp example
User=user
Group=users
StandardInput=socket
```

Para obter uma lista completa das opções de arquivo de “soquete” e de “serviço” do `systemd`, consulte as páginas de manual `systemd.socket` e `systemd.service` (**`man 5 systemd.socket`**, **`man 5 systemd.service`**).

19.5.4 Criando destinos personalizados

Nos sistemas init SUSE do System V, o nível de execução 4 não costuma ser usado para permitir que administradores criem sua própria configuração de nível de execução. O `systemd` permite criar qualquer número de destinos personalizados. A sugestão é começar adaptando um destino existente, como `graphical.target`.

1. Copie o arquivo de configuração `/usr/lib/systemd/system/graphical.target` para `/etc/systemd/system/MEU_DESTINO.target` e ajuste-o de acordo com as suas necessidades.
2. O arquivo de configuração copiado na etapa anterior já inclui as dependências obrigatórias (“hard”) do destino. Para incluir também as dependências desejadas (“soft”), crie um diretório `/etc/systemd/system/MEU_DESTINO.target.wants`.
3. Para cada serviço desejado, crie um link simbólico de `/usr/lib/systemd/system` para `/etc/systemd/system/MEU_DESTINO.target.wants`.
4. Após concluir a configuração do destino, recarregue a configuração do `systemd` para disponibilizar o novo destino:

```
> sudo systemctl daemon-reload
```

19.6 Uso avançado

As seções a seguir abordam tópicos avançados para administradores do sistema. Para conferir uma documentação ainda mais avançada do `systemd`, consulte a série de Lennart Pöttering sobre o `systemd` para administradores em <http://0pointer.de/blog/projects> [↗](#).

19.6.1 Limpando diretórios temporários

O `systemd` suporta a limpeza de diretórios temporários regularmente. A configuração da versão do sistema anterior é automaticamente migrada e ativada. O `tmpfiles.d`, que é responsável por gerenciar arquivos temporários, lê sua configuração dos arquivos `/etc/tmpfiles.d/*.conf`, `/run/tmpfiles.d/*.conf` e `/usr/lib/tmpfiles.d/*.conf`. A configuração armazenada no `/etc/tmpfiles.d/*.conf` anula as configurações relacionadas dos outros dois diretórios (`/usr/lib/tmpfiles.d/*.conf` é o local onde os pacotes armazenam seus arquivos de configuração).

O formato da configuração é de uma linha por caminho incluindo ação e caminho; e, opcionalmente, modo, propriedade e os campos de idade e argumento, dependendo da ação. O exemplo a seguir desvincula os arquivos de bloqueio do X11:

Type	Path	Mode	UID	GID	Age	Argument
r	/tmp/.X[0-9]*-lock					

Para obter o status do temporizador `tmpfile`:

```
> sudo systemctl status systemd-tmpfiles-clean.timer
systemd-tmpfiles-clean.timer - Daily Cleanup of Temporary Directories
Loaded: loaded (/usr/lib/systemd/system/systemd-tmpfiles-clean.timer; static)
Active: active (waiting) since Tue 2018-04-09 15:30:36 CEST; 1 weeks 6 days ago
Docs: man:tmpfiles.d(5)
      man:systemd-tmpfiles(8)

Apr 09 15:30:36 jupiter systemd[1]: Starting Daily Cleanup of Temporary Directories.
Apr 09 15:30:36 jupiter systemd[1]: Started Daily Cleanup of Temporary Directories.
```

Para obter mais informações sobre como lidar com os arquivos temporários, consulte [man 5 tmpfiles.d](#).

19.6.2 Registro do sistema

A [Seção 19.6.9, “Depurando serviços”](#) explica como ver mensagens de registro de determinado serviço. No entanto, a exibição de mensagens de registro não se restringe a registros de serviços. É possível também acessar e consultar as mensagens de registro completas gravadas pelo `systemd`, o chamado “Diário”. Use o comando `journalctl` para exibir as mensagens de registro completas começando pelas entradas mais antigas. Consulte [man 1 journalctl](#) para ver as opções. Por exemplo, aplicação de filtros ou mudança do formato de saída.

19.6.3 Instantâneos

É possível gravar o estado atual do `systemd` em um instantâneo nomeado e mais tarde reverterlo com o subcomando `isolate`. Isso é útil para testar serviços ou destinos personalizados, pois permite retornar para um estado definido a qualquer momento. Um instantâneo só fica disponível na sessão atual e é apagado automaticamente na reinicialização. O nome do instantâneo deve terminar com `.snapshot`.

Criar um instantâneo

```
> sudo systemctl snapshot MY_SNAPSHOT.snapshot
```

Apagar um instantâneo

```
> sudo systemctl delete MY_SNAPSHOT.snapshot
```

Ver um instantâneo

```
> sudo systemctl show MY_SNAPSHOT.snapshot
```

Ativar um instantâneo

```
> sudo systemctl isolate MY_SNAPSHOT.snapshot
```

19.6.4 Carregando módulos do kernel

Com o `systemd`, é possível carregar os módulos do kernel automaticamente no momento da inicialização, usando o arquivo de configuração em `/etc/modules-load.d`. O arquivo deve ser nomeado `MÓDULO.conf` e ter o seguinte conteúdo:

```
# load module MODULE at boot time
MODULE
```

Se um pacote instalar um arquivo de configuração para carregar um módulo do kernel, o arquivo será instalado em `/usr/lib/modules-load.d`. Se houver dois arquivos de configuração com o mesmo nome, aquele em `/etc/modules-load.d` terá precedência.

Para obter mais informações, consulte a página de manual de `modules-load.d(5)`.

19.6.5 Executando ações antes de carregar um serviço

Com o System V, as ações `init` que precisam ser executadas antes de carregar um serviço tinham que ser especificadas em `/etc/init.d/before.local`. Esse procedimento não é mais suportado com o `systemd`. Se você precisa executar ações antes de iniciar serviços, faça o seguinte:

Carregando módulos do kernel

Crie um arquivo drop-in no diretório `/etc/modules-load.d` (consulte `man modules-load.d` para ver a sintaxe)

Criando arquivos ou diretórios, limpando diretórios, mudando a propriedade

Crie um arquivo drop-in em `/etc/tmpfiles.d` (consulte `man tmpfiles.d` para ver a sintaxe)

Outras tarefas

Crie um arquivo de serviço de sistema, por exemplo `/etc/systemd/system/before.service`, com base no seguinte gabarito:

```
[Unit]
Before=NAME OF THE SERVICE YOU WANT THIS SERVICE TO BE STARTED BEFORE
[Service]
Type=oneshot
RemainAfterExit=true
ExecStart=YOUR_COMMAND
# beware, executable is run directly, not through a shell, check the man pages
# systemd.service and systemd.unit for full syntax
[Install]
# target in which to start the service
WantedBy=multi-user.target
#WantedBy=graphical.target
```

Quando o arquivo de serviço é criado, você deve executar os seguintes comandos (como root):

```
> sudo systemctl daemon-reload
> sudo systemctl enable before
```

Toda vez que você modifica o arquivo de serviço, deve executar:

```
> sudo systemctl daemon-reload
```

19.6.6 Grupos de controle (cgroups) do kernel

Em um sistema init tradicional do System V, nem sempre é possível atribuir claramente um processo ao serviço que o gerou. Alguns serviços, como o Apache, geram diversos processos de terceiros (por exemplo, processos CGI ou Java) que, por sua vez, geram mais processos. Isso dificulta ou até impossibilita uma atribuição clara. Além do mais, um serviço pode não terminar corretamente, deixando alguns filhos ativos.

O `systemd` resolve este problema colocando cada serviço em seu próprio grupo de controle (cgroup). Cgroups são recursos do kernel que possibilitam agregar processos e todos os seus filhos em grupos hierárquicos organizados. O `systemd` nomeia cada cgroup de acordo com seu serviço. Como um processo não privilegiado não pode “deixar” seu cgroup, essa é uma forma eficiente de rotular todos os processos gerados por um serviço com o nome do serviço.

Para listar todos os processos pertencentes a um serviço, use o comando `systemd-cgls`. O resultado será parecido com o seguinte exemplo (resumido):

EXEMPLO 19.3: LISTAR TODOS OS PROCESSOS PERTENCENTES A UM SERVIÇO

```
# systemd-cgls --no-pager
├─1 /usr/lib/systemd/systemd --switched-root --system --deserialize 20
├─user.slice
│   └─user-1000.slice
│       └─session-102.scope
│           ├──12426 gdm-session-worker [pam/gdm-password]
│           ├──15831 gdm-session-worker [pam/gdm-password]
│           ├──15839 gdm-session-worker [pam/gdm-password]
│           └─15858 /usr/lib/gnome-terminal-server
[...]
```



```
└─system.slice
    ├──systemd-hostnamed.service
    │   └─17616 /usr/lib/systemd/systemd-hostnamed
    ├──cron.service
    │   └─1689 /usr/sbin/cron -n
    ├──postfix.service
    │   ├──1676 /usr/lib/postfix/master -w
    │   ├──1679 qmgr -l -t fifo -u
    │   └─15590 pickup -l -t fifo -u
    ├──sshd.service
    │   └─1436 /usr/sbin/sshd -D
[...]
```

Consulte o Livro *“System Analysis and Tuning Guide”, Capítulo 10 “Kernel control groups”* para obter mais informações sobre os cgroups.

19.6.7 Terminando os serviços (enviando sinais)

Conforme explicado na [Seção 19.6.6, “Grupos de controle \(cgroups\) do kernel”](#), nem sempre é possível atribuir um processo a seu processo de serviço pai em um sistema init do System V. Isso dificulta terminar um serviço e todos os seus filhos. Os processos filhos que não forem terminados permanecerão como processos zumbis.

O conceito do systemd de confinar cada serviço em um cgroup possibilita identificar claramente todos os processos filho de um serviço e, portanto, permite enviar um sinal a cada um desses processos. Use **systemctl kill** para enviar sinais aos serviços. Para ver uma lista dos sinais disponíveis, consulte man 7 signals.

Enviando SIGTERM para um serviço

SIGTERM é o sinal padrão que é enviado.

```
> sudo systemctl kill MY_SERVICE
```

Enviando SIGNAL para um serviço

Use a opção -s para especificar o sinal que deve ser enviado.

```
> sudo systemctl kill -s SIGNAL MY_SERVICE
```

Selecionando processos

Por padrão, o comando **kill** envia o sinal para todos os processos do cgroup especificado. É possível restringi-lo ao processo control ou main. Este último, por exemplo, é útil para forçar um serviço a recarregar sua configuração enviando SIGHUP:

```
> sudo systemctl kill -s SIGHUP --kill-who=main MY_SERVICE
```

19.6.8 Notas importantes sobre o serviço D-Bus

O serviço D-BUS é o barramento de mensagem para comunicação entre clientes systemd e o gerenciador systemd que está sendo executado como pid 1. Embora o dbus seja um daemon independente, ele é parte integrante da infraestrutura do init.

Terminar ou reiniciar o dbus no sistema em execução é semelhante a uma tentativa de terminar ou reiniciar o pid 1. Isso interromperá a comunicação entre cliente e servidor systemd e inutilizará a maioria das funções do systemd.

Portanto, terminar ou reiniciar o dbus não é recomendado nem suportado.

A atualização do dbus ou dos pacotes relacionados ao dbus requer uma reinicialização. Quando estiver em dúvida se uma reinicialização é necessária, execute o comando **sudo zypper ps -s**. Se dbus aparecer entre os serviços listados, será necessário reinicializar o sistema.

Saiba que o dbus é atualizado mesmo quando as atualizações automáticas estão configuradas para ignorar os pacotes que exigem reinicialização.

19.6.9 Depurando serviços

Por padrão, o `systemd` não é muito verboso. Se um serviço for iniciado com êxito, nenhuma saída será gerada. Em caso de falha, uma breve mensagem de erro será exibida. Porém, o `systemctl status` oferece os meios de depurar a inicialização e operação de um serviço.

O `systemd` já vem com um mecanismo de registro (“The Journal” — O Diário) que registra as mensagens do sistema. Isso permite exibir as mensagens de serviço juntamente com as mensagens de status. O comando `status` funciona de forma parecida com o comando `tail` e também exibe as mensagens de registro em formatos diferentes, o que faz dele uma poderosa ferramenta de depuração.

Mostrar falha na inicialização de serviço

Sempre que houver falha ao iniciar um serviço, use `systemctl status MEU_SERVIÇO` para obter a mensagem de erro detalhada:

```
# systemctl start apache2
Job failed. See system journal and 'systemctl status' for details.
# systemctl status apache2
  Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled)
  Active: failed (Result: exit-code) since Mon, 04 Apr 2018 16:52:26 +0200; 29s ago
  Process: 3088 ExecStart=/usr/sbin/start_apache2 -D SYSTEMD -k start (code=exited,
  status=1/FAILURE)
  CGroup: name=systemd:/system/apache2.service

Apr 04 16:52:26 g144 start_apache2[3088]: httpd2-prefork: Syntax error on line
205 of /etc/apache2/httpd.conf: Syntax error on li...alHost>
```

Mostrar as últimas *n* mensagens de serviço

O comportamento padrão do subcomando `status` é exibir as dez últimas mensagens emitidas por um serviço. Para mudar o número de mensagens exibidas, use o parâmetro `--lines=N`:

```
> sudo systemctl status chronyd
> sudo systemctl --lines=20 status chronyd
```

Mostrar as mensagens de serviço no modo de anexação

Para exibir um “fluxo ao vivo” das mensagens de serviço, use a opção `--follow`, que funciona como o `tail -f`:

```
> sudo systemctl --follow status chronyd
```

Formato de saída das mensagens

O parâmetro `--output=MODO` permite mudar o formato de saída das mensagens de serviço. Os modos mais importantes disponíveis são:

short

O formato padrão. Mostra as mensagens de registro com uma marcação de horário legível.

verbose

Saída completa com todos os campos.

cat

Saída resumida sem marcações de horário.

19.7 Unidades do temporizador do `systemd`

Semelhante ao `cron`, as unidades do temporizador do `systemd` oferecem um mecanismo para programar tarefas no Linux. Embora as unidades do temporizador do `systemd` tenham a mesma finalidade que o `cron`, elas oferecem várias vantagens.

- As tarefas programadas usando uma unidade do temporizador podem depender de outros serviços do `systemd`.
- As unidades do temporizador são tratadas como serviços regulares do `systemd`, portanto, podem ser gerenciadas com o `systemctl`.
- Os temporizadores podem ser em tempo real e monotônicos.
- As unidades de tempo são registradas no diário do `systemd`, o que facilita o monitoramento e a solução de problemas.

As unidades do temporizador do `systemd` são identificadas pela extensão de nome de arquivo `.timer`.

19.7.1 Tipos de temporizador do `systemd`

As unidades do temporizador podem usar temporizadores monotônicos e em tempo real.

- Semelhante ao cron, os temporizadores em tempo real são acionados com base em eventos do calendário. Os temporizadores em tempo real são definidos usando a opção `OnCalendar`.
- Os temporizadores monotônicos são acionados em um tempo especificado decorrido a partir de um determinado ponto inicial. O último pode ser um evento de boot do sistema ou de ativação da unidade do sistema. Há várias opções para definir temporizadores monotônicos, incluindo `OnBootSec`, `OnUnitActiveSec` e `OnTypeSec`. Os temporizadores monotônicos não são persistentes e são redefinidos após cada reinicialização.

19.7.2 Temporizadores e unidades de serviço do `systemd`

Cada unidade do temporizador deve ter um arquivo de unidade do `systemd` correspondente que ela controla. Em outras palavras, o arquivo `.timer` ativa e gerencia o arquivo `.service` correspondente. Quando usado com um temporizador, o arquivo `.service` não requer uma seção `[Install]`, já que o serviço é gerenciado pelo temporizador.

19.7.3 Exemplo prático

Para entender os conceitos básicos das unidades do temporizador do `systemd`, configuramos um temporizador que aciona o script shell `foo.sh`.

A primeira etapa é criar uma unidade de serviço do `systemd` que controle o script shell. Para fazer isso, abra um novo arquivo de texto para edição e adicione a seguinte definição de unidade de serviço:

```
[Unit]
Description="Foo shell script"

[Service]
ExecStart=/usr/local/bin/foo.sh
```

Grave o arquivo com o nome `foo.service` no diretório `/etc/systemd/system/`.

Em seguida, abra um novo arquivo de texto para edição e adicione a seguinte definição do temporizador:

```
[Unit]
Description="Run foo shell script"
```



```
[Timer]
OnBootSec=5min
OnUnitActiveSec=24h
Unit=foo.service

[Install]
WantedBy=multi-user.target
```

A seção `[Timer]` no exemplo acima especifica qual serviço acionar (`foo.service`) e quando acioná-lo. Nesse caso, a opção `OnBootSec` especifica um temporizador monotônico que aciona o serviço cinco minutos após o boot do sistema, enquanto a opção `OnUnitActiveSec` aciona o serviço 24 horas após a ativação do serviço (ou seja, o temporizador acionará o serviço uma vez por dia). Por fim, a opção `WantedBy` especifica que o temporizador deve ser iniciado quando o sistema atingir o destino de multiusuários.

Em vez de um temporizador monotônico, você pode especificar um em tempo real usando a opção `OnCalendar`. A seguinte definição do temporizador em tempo real aciona a unidade de serviço relacionada uma vez por semana, começando na segunda-feira às 12:00.

```
[Timer]
OnCalendar=weekly
Persistent=true
```

A opção `Persistent=true` indica que o serviço será acionado logo após a ativação do temporizador, se o temporizador tiver perdido o último horário de início (por exemplo, porque o sistema estava desligado).

A opção `OnCalendar` também pode ser usada para definir horários e datas específicos para acionar um serviço usando o seguinte formato: `DiadaSemana Ano-Mês-Dia Hora:Minuto:Segundo`. O exemplo abaixo aciona um serviço às 5:00 todos os dias:

```
OnCalendar=*-*-* 5:00:00
```

Você pode usar um asterisco para especificar qualquer valor e vírgulas para listar os valores possíveis. Use dois valores separados por `..` para indicar uma faixa contígua. O exemplo a seguir aciona um serviço às 18:00 todas as sextas-feiras do mês:

```
OnCalendar=Fri *-*-1..7 18:00:00
```

Para acionar um serviço em horários diferentes, você pode especificar várias entradas `OnCalendar`:

```
OnCalendar=Mon..Fri 10:00
OnCalendar=Sat,Sun 22:00
```

No exemplo acima, um serviço é acionado às 10:00 nos dias da semana e às 22:00 nos fins de semana.

Quando você terminar de editar o arquivo de unidade do temporizador, grave-o com o nome `foo.timer` no diretório `/etc/systemd/system/`. Para verificar se os arquivos de unidade criados estão corretos, execute o seguinte comando:

```
> sudo systemd-analyze verify /etc/systemd/system/foo.*
```

Se o comando não retornar nenhuma saída, os arquivos foram aprovados na verificação.

Para iniciar o temporizador, use o comando `sudo systemctl start foo.timer`. Para habilitar o temporizador na inicialização, execute o comando `sudo systemctl enable foo.timer`.

19.7.4 Gerenciando temporizadores do systemd

Como os temporizadores são tratados como unidades regulares do `systemd`, você pode gerenciá-los usando o `systemctl`. Você pode iniciar um temporizador com `systemctl start`, habilitar um temporizador com `systemctl enable` e assim por diante. Além disso, você pode listar todos os temporizadores ativos usando o comando `systemctl list-timers`. Para listar todos os temporizadores, incluindo os inativos, execute o comando `systemctl list-timers --all`.

19.8 Mais informações

Para obter mais informações sobre o `systemd`, consulte os seguintes recursos online:

Home page

<http://www.freedesktop.org/wiki/Software/systemd> ↗

`systemd` para administradores

Lennart Pöttering, um dos criadores do `systemd`, escreveu uma série de entradas de blog (13 até o fechamento deste capítulo). Encontre-os em <http://0pointer.de/blog/projects> ↗.

III Sistema

- 20 Aplicativos de 32 bits e 64 bits em um ambiente de sistema de 64 bits **294**
- 21 **journalctl**: Consultar o diário do systemd **296**
- 22 **update-alternatives**: Gerenciando várias versões de comandos e arquivos **304**
- 23 Rede básica **312**
- 24 Operação da impressora **382**
- 25 Interface gráfica do usuário **397**
- 26 Acessando sistemas de arquivos com o FUSE **415**
- 27 Instalando várias versões do kernel **417**
- 28 Gerenciando módulos do kernel **424**
- 29 Gerenciamento dinâmico de dispositivos do kernel com udev **428**
- 30 Recursos especiais do sistema **441**
- 31 Usando o NetworkManager **453**

20 Aplicativos de 32 bits e 64 bits em um ambiente de sistema de 64 bits

O SUSE® Linux Enterprise Desktop está disponível para plataformas de 64 bits. Os desenvolvedores não portaram todos os aplicativos de 32 bits para os sistemas de 64 bits. Este capítulo apresenta uma breve visão geral da implementação do suporte a 32 bits em plataformas de 64 bits do SUSE Linux Enterprise Desktop.

O SUSE Linux Enterprise Desktop para plataformas de 64 bits AMD64 e Intel 64 foi desenvolvido para que os aplicativos de 32 bits existentes sejam executados no ambiente de 64 bits “out-of-the-box.” Este suporte significa que você pode continuar a usar os aplicativos de 32 bits de sua preferência sem esperar que uma porta de 64 bits correspondente se torne disponível.



Nota: Não há suporte para criação de aplicativos de 32 bits

O SUSE Linux Enterprise Desktop não suporta compilação de aplicativos de 32 bits. Ele apenas oferece suporte em tempo de execução para binários de 32 bits.

20.1 Suporte em tempo de execução



Importante: Conflitos entre versões de aplicativo

Se um aplicativo estiver disponível para ambos os ambientes de 32 e 64 bits, a instalação das duas versões poderá causar problemas. Nesses casos, escolha a versão que será instalada para evitar possíveis erros de tempo de execução.

Uma exceção a essa regra é o PAM (módulo de autenticação conectável). O SUSE Linux Enterprise Desktop usa o PAM no processo de autenticação como uma camada mediadora entre o usuário e o aplicativo. Sempre instale as duas versões do PAM em sistemas operacionais de 64 bits que também executam aplicativos de 32 bits.

Para a execução correta, cada aplicativo requer uma variedade de bibliotecas. Infelizmente, os nomes das versões de 32 e 64 bits dessas bibliotecas são idênticos. Eles devem ser diferenciados uns dos outros de outra forma.

Para manter a compatibilidade com as versões de 32 bits, as bibliotecas de 64 e 32 bits são armazenadas no mesmo local. A versão de 32 bits de `libc.so.6` está localizada em `/lib/libc.so.6` nos ambientes de 32 e 64 bits.

Todos os arquivos de objetos e todas as bibliotecas de 64 bits estão localizados em diretórios denominados `lib64`. Os arquivos de objeto de 64 bits que normalmente estão em `/lib` e em `/usr/lib`, agora estão em `/lib64` e em `/usr/lib64`. Isso significa que há espaço disponível para as bibliotecas de 32 bits em `/lib` e em `/usr/lib`, permitindo que o nome de arquivo de ambas as versões permaneça inalterado.

Se o conteúdo dos dados dos subdiretórios de 32 bits em `/lib` não depender do tamanho da palavra, ele não será movido. Este esquema está em conformidade com a LSB (Linux Standards Base — Base de Padrões Linux) e com o FHS (File System Hierarchy Standard — Padrão de Hierarquia de Sistema de Arquivos).

20.2 Especificações do kernel

Os kernels de 64 bits para AMD64/Intel 64 oferecem uma ABI (application binary interface – interface binária de aplicativo) de kernel de 32 e 64 bits. A de 64 bits é idêntica à ABI do kernel de 32 bits correspondente. Isso significa que a comunicação entre os aplicativos de 32 e 64 bits com kernels de 64 bits é idêntica.

A emulação de chamada do sistema de 32 bits para os kernels de 64 bits não suporta todas as APIs usadas pelos programas do sistema. Isso depende da plataforma. Por essa razão, alguns aplicativos, como `lspci`, devem ser compilados.

Um kernel de 64 bits apenas pode carregar módulos de kernel de 64 bits. Você deve compilar os módulos de 64 bits especificamente para os kernels de 64 bits. Não é possível usar módulos de kernel de 32 bits com kernels de 64 bits.



Dica: Módulos carregáveis pelo kernel

Alguns aplicativos requerem módulos separados carregáveis pelo kernel. Se você pretende usar um aplicativo de 32 bits em um ambiente de sistema de 64 bits, contate o provider do aplicativo e a SUSE. Verifique se a versão de 64 bits do módulo carregável pelo kernel e a versão compilada de 32 bits da API do kernel estão disponíveis para esse módulo.

21 **journalctl**: Consultar o diário do systemd

O `systemd` conta com um sistema de registro em diário próprio chamado *journal*. Não há necessidade de executar um serviço baseado no `syslog`, e todos os eventos do sistema são gravados no diário.

O próprio diário é um serviço do sistema gerenciado pelo `systemd`. Seu nome completo é `systemd-journald.service`. Ele coleta e armazena dados de registro mantendo diários indexados estruturados com base nas informações de registro recebidas do kernel, de processos dos usuários, da entrada padrão e de erros de serviços do sistema. Por padrão, o serviço `systemd-journald` está ativado:

```
> sudo systemctl status systemd-journald
systemd-journald.service - Journal Service
   Loaded: loaded (/usr/lib/systemd/system/systemd-journald.service; static)
   Active: active (running) since Mon 2014-05-26 08:36:59 EDT; 3 days ago
     Docs: man:systemd-journald.service(8)
           man:journald.conf(5)
  Main PID: 413 (systemd-journal)
    Status: "Processing requests..."
   CGroup: /system.slice/systemd-journald.service
           └─413 /usr/lib/systemd/systemd-journald
[...]
```

21.1 Tornando o diário persistente

Por padrão, o diário armazena os dados de registro em `/run/log/journal/`. Como o diretório `/run/` é volátil por natureza, os dados de registro são perdidos na reinicialização. Para torná-los persistentes, deve haver um diretório `/var/log/journal/` com propriedade e permissões corretas para o serviço `systemd-journald` armazenar seus dados. O `systemd` criará o diretório para você (e mudará o registro para persistente), se você fizer o seguinte:

1. Como `root`, abra o `/etc/systemd/journald.conf` para edição.

```
# vi /etc/systemd/journald.conf
```

2. Remova o comentário da linha com `Storage=` e mude-a para

```
[...]
[Journal]
Storage=persistent
```

```
#Compress=yes  
[...]
```

3. Grave o arquivo e reinicie o systemd-journald:

```
# systemctl restart systemd-journald
```

21.2 journalctl: Switches úteis

Esta seção apresenta várias opções comuns úteis para melhorar o comportamento padrão do **journalctl**. Todos os switches estão descritos na página de manual do **journalctl**: [man 1 journalctl](#).



Dica: Mensagens relacionadas a um executável específico

Para mostrar todas as mensagens do diário relacionadas a determinado executável, especifique o caminho completo para o executável:

```
> sudo journalctl /usr/lib/systemd/systemd
```

-f

Mostra apenas as mensagens mais recentes do diário e imprime novas entradas de registro à medida que são adicionadas ao diário.

Imprime as mensagens e pula para o fim do diário para que as entradas mais recentes fiquem visíveis no paginador.

-r

Imprime as mensagens do diário em ordem inversa para que as últimas entradas sejam listadas primeiro.

-k

Mostra apenas as mensagens do kernel. Equivale à correspondência de campo `_TRANSPORT=kernel` (consulte a [Seção 21.3.3, “Filtrando com base nos campos”](#)).

-u

Mostra apenas as mensagens da unidade `systemd` especificada. Equivale à correspondência de campo `_SYSTEMD_UNIT=UNIDADE` (consulte a [Seção 21.3.3, “Filtrando com base nos campos”](#)).

```
> sudo journalctl -u apache2
[...]  
Jun 03 10:07:11 pinkiepie systemd[1]: Starting The Apache Webserver...  
Jun 03 10:07:12 pinkiepie systemd[1]: Started The Apache Webserver.
```

21.3 Filtrando a saída do diário

Quando chamado sem switches, o **journalctl** mostra o conteúdo completo do diário, com as entradas mais antigas listadas primeiro. É possível filtrar a saída por switches e campos específicos.

21.3.1 Filtrando com base em um número de boot

O **journalctl** pode filtrar as mensagens com base em um boot do sistema específico. Para listar todos os boots disponíveis, execute

```
> sudo journalctl --list-boots  
-1 097ed2cd99124a2391d2cfffab1b566f0 Mon 2014-05-26 08:36:56 EDT-Fri 2014-05-30 05:33:44  
EDT  
0 156019a44a774a0bb0148a92df4af81b Fri 2014-05-30 05:34:09 EDT-Fri 2014-05-30 06:15:01  
EDT
```

A primeira coluna lista a diferença de boot: 0 para o boot atual, -1 para o boot anterior, -2 para o boot anterior a esse etc. A segunda coluna contém o ID do boot seguido das marcações de horário de limite do boot específico.

Mostrar todas as mensagens do boot atual:

```
> sudo journalctl -b
```

Se você precisa ver as mensagens de diário do boot anterior, adicione um parâmetro de diferença. O seguinte exemplo representa as mensagens do boot anterior:

```
> sudo journalctl -b -1
```

Uma outra maneira é listar as mensagens de boot com base no ID de boot. Para esta finalidade, use o campo **_BOOT_ID**:

```
> sudo journalctl _BOOT_ID=156019a44a774a0bb0148a92df4af81b
```


21.3.2 Filtrando com base no intervalo de tempo

É possível filtrar a saída do **journalctl** especificando a data de início e/ou de término. A especificação de data deve ser no formato "2014-06-30 9:17:16". Se a parte do horário for omitida, será considerada meia-noite. Se os segundos forem omitidos, será considerado ":00". Se a parte da data for omitida, será considerado o dia atual. Em vez da expressão numérica, você pode especificar as palavras-chave "ontem", "hoje" ou "amanhã". Elas se referem à meia-noite do dia anterior ao dia atual, ao dia atual ou ao dia após o dia atual. Se você especificar "agora", vai se referir ao horário atual. É possível também especificar horários com os prefixos **-** ou **+**, que se referem aos horários antes ou depois do horário atual.

Mostrar apenas novas mensagens a partir de agora e atualizar a saída continuamente:

```
> sudo journalctl --since "now" -f
```

Mostrar todas as mensagens desde meia-noite passada até às 3h20:

```
> sudo journalctl --since "today" --until "3:20"
```

21.3.3 Filtrando com base nos campos

É possível filtrar a saída do diário por campos específicos. A sintaxe de um campo para correspondência é **FIELD_NAME=MATCHED_VALUE**, como **_SYSTEMD_UNIT=httpd.service**. É possível especificar várias correspondências em uma única consulta para filtrar ainda mais as mensagens de saída. Consulte **man 7 systemd.journal-fields** para ver a lista de campos padrão.

Mostrar mensagens produzidas por um ID de processo específico:

```
> sudo journalctl _PID=1039
```

Mostrar mensagens que pertencem a determinado ID de usuário:

```
# journalctl _UID=1000
```

Mostrar mensagens do buffer de anel do kernel (as mesmas que o **dmesg** produz):

```
> sudo journalctl _TRANSPORT=kernel
```

Mostrar mensagens da saída padrão ou de erros do serviço:

```
> sudo journalctl _TRANSPORT=stdout
```

Mostrar mensagens produzidas apenas por determinado serviço:

```
> sudo journalctl _SYSTEMD_UNIT=avahi-daemon.service
```

Se dois campos diferentes forem especificados, apenas as entradas que corresponderem às duas expressões ao mesmo tempo serão mostradas:

```
> sudo journalctl _SYSTEMD_UNIT=avahi-daemon.service _PID=1488
```

Se duas correspondências fizerem referência ao mesmo campo, todas as entradas correspondentes a uma das expressões serão mostradas:

```
> sudo journalctl _SYSTEMD_UNIT=avahi-daemon.service _SYSTEMD_UNIT=dbus.service
```

É possível usar o separador "+" para combinar duas expressões em um "OR" lógico. O seguinte exemplo mostra todas as mensagens do processo do serviço Avahi com ID de processo 1480 juntamente com todas as mensagens do serviço D-Bus:

```
> sudo journalctl _SYSTEMD_UNIT=avahi-daemon.service _PID=1480 +  
_SYSTEMD_UNIT=dbus.service
```

21.4 Investigando erros do systemd

Esta seção apresenta um exemplo simples que ilustra como localizar e corrigir o erro relatado pelo `systemd` durante a inicialização do `apache2`.

1. Tentar iniciar o serviço `apache2`:

```
# systemctl start apache2  
Job for apache2.service failed. See 'systemctl status apache2' and 'journalctl -xn'  
for details.
```

2. Vejamos o que diz o status do serviço:

```
> sudo systemctl status apache2  
apache2.service - The Apache Webserver  
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled)  
   Active: failed (Result: exit-code) since Tue 2014-06-03 11:08:13 CEST; 7min ago  
  Process: 11026 ExecStop=/usr/sbin/start_apache2 -D SYSTEMD -DFOREGROUND \  
           -k graceful-stop (code=exited, status=1/FAILURE)
```

O ID do processo que causa a falha é 11026.

3. Mostrar a versão verbosa das mensagens relacionadas ao ID de processo 11026:

```
> sudo journalctl -o verbose _PID=11026
[...]  
MESSAGE=AH00526: Syntax error on line 6 of /etc/apache2/default-server.conf:  
[...]  
MESSAGE=Invalid command 'DocumenttRoot', perhaps misspelled or defined by a module  
[...]
```

4. Corrigir o erro de digitação em `/etc/apache2/default-server.conf`, iniciar o serviço `apache2` e imprimir seu status:

```
> sudo systemctl start apache2 && systemctl status apache2  
apache2.service - The Apache Webserver  
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled)  
   Active: active (running) since Tue 2014-06-03 11:26:24 CEST; 4ms ago  
 Process: 11026 ExecStop=/usr/sbin/start_apache2 -D SYSTEMD -DFOREGROUND  
         -k graceful-stop (code=exited, status=1/FAILURE)  
 Main PID: 11263 (httpd2-prefork)  
   Status: "Processing requests..."  
   CGroup: /system.slice/apache2.service  
           └─11263 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D [...]  
           └─11280 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D [...]  
           └─11281 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D [...]  
           └─11282 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D [...]  
           └─11283 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D [...]  
           └─11285 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D [...]
```

21.5 Configuração do journald

É possível ajustar o comportamento do serviço `systemd-journald` modificando `/etc/systemd/journald.conf`. Esta seção apresenta apenas as configurações de opção básicas. Para ver a descrição completa do arquivo, consulte [man 5 journald.conf](#). Observe que é necessário reiniciar o diário para que as mudanças entrem em vigor com

```
> sudo systemctl restart systemd-journald
```

21.5.1 Mudando o limite de tamanho do diário

Se os dados do registro em diário forem gravados em um local persistente (consulte a [Seção 21.1, “Tornando o diário persistente”](#)), eles usarão até 10% do sistema de arquivos no qual o `/var/log/journal` reside. Por exemplo, se `/var/log/journal` estiver em uma partição `/var` de 30 GB, o diário poderá usar até 3 GB de espaço em disco. Para mudar esse limite, altere (e remova o comentário) a opção `SystemMaxUse`:

```
SystemMaxUse=50M
```

21.5.2 Encaminhando o diário para `/dev/ttyX`

É possível encaminhar o diário para um dispositivo de terminal para você receber informações sobre mensagens do sistema na tela de terminal de sua preferência, por exemplo `/dev/tty12`. Mude as seguintes opções de `journald` para

```
ForwardToConsole=yes  
TTYPath=/dev/tty12
```

21.5.3 Encaminhando o diário para o recurso do syslog

O `Journald` é retroativamente compatível com as implementações tradicionais do syslog, como `rsyslog`. Verifique se as afirmativas a seguir são válidas:

- O `rsyslog` está instalado.

```
> sudo rpm -q rsyslog  
rsyslog-7.4.8-2.16.x86_64
```

- O serviço `rsyslog` está habilitado.

```
> sudo systemctl is-enabled rsyslog  
enabled
```

- O encaminhamento para syslog está habilitado em `/etc/systemd/journald.conf`.

```
ForwardToSyslog=yes
```

21.6 Usando o YaST para filtrar o diário do systemd

Uma forma fácil de filtrar o diário do systemd (sem ter que usar a sintaxe `journalctl`) é usar o módulo de diário do YaST. Após sua instalação por meio do `sudo zypper in yast2-journal`, inicie-o do YaST selecionando *Sistema > Systemd Journal* (Diário do Systemd). Se preferir, inicie-o da linha de comando digitando `sudo yast2 journal`.

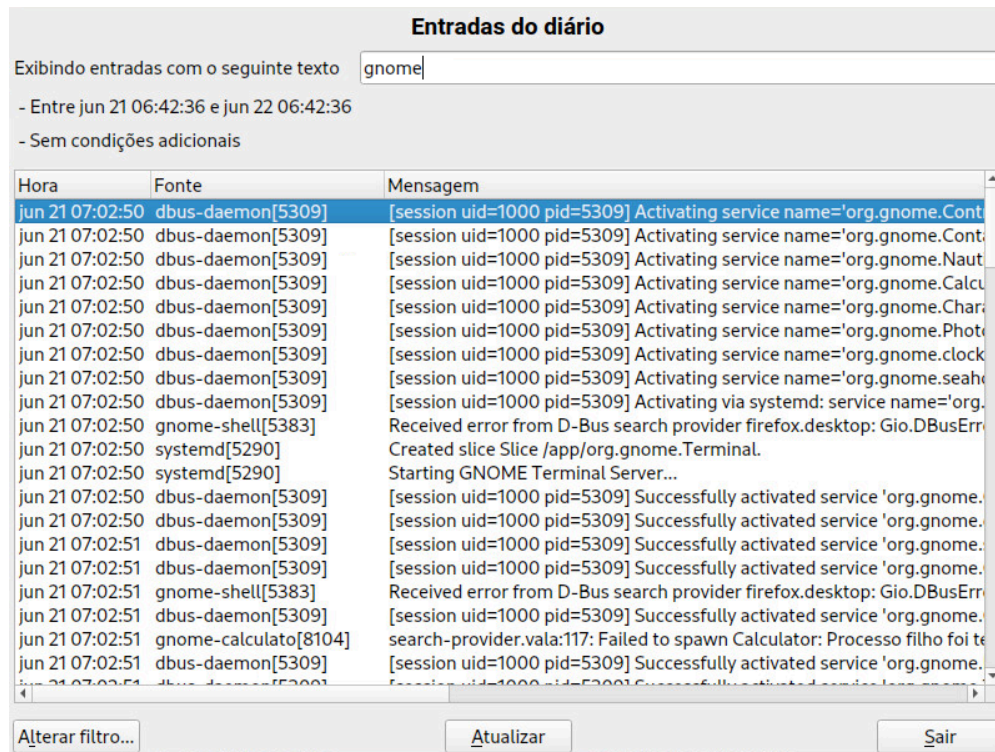


FIGURA 21.1: DIÁRIO DO SYSTEMD NO YAST

O módulo exibe as entradas de registro em uma tabela. A caixa de pesquisa na parte superior permite procurar as entradas que incluem determinados caracteres, semelhante ao `grep`. Para filtrar as entradas por data e horário, unidade, arquivo ou prioridade, clique em *Mudar filtro* e defina as respectivas opções.

21.7 Vendo registros no GNOME

Você pode ver o diário com *Registros do GNOME*. Inicie-o no menu do aplicativo. Para ver as mensagens de registro do sistema, ele precisa ser executado como root. Por exemplo, com `xdg-su gnome-logs`. Esse comando pode ser executado ao pressionar `Alt + F2`.

22 **update-alternatives**: Gerenciando várias versões de comandos e arquivos

Normalmente, há várias versões da mesma ferramenta instaladas em um sistema. Para que os administradores possam escolher e para possibilitar a instalação e o uso de versões diferentes lado a lado, o sistema de alternativas permite gerenciar as versões consistentemente.

22.1 Visão Geral

No SUSE Linux Enterprise Desktop, alguns programas executam tarefas iguais ou semelhantes. Por exemplo, se ambos Java 1.7 e Java 1.8 estiverem instalados no sistema, o script do sistema de alternativas (**update-alternatives**) será chamado do pacote RPM. Por padrão, o sistema de alternativas fará referência à versão 1.8: Versões superiores também têm maior prioridade. No entanto, o administrador pode mudar o padrão e apontar o nome genérico para a versão 1.7. A seguinte terminologia é usada neste capítulo:

TERMINOLOGIA

Diretório administrativo

O diretório padrão `/var/lib/rpm/alternatives` contém informações sobre o estado atual das alternativas.

Alternativa

O nome de um arquivo específico no sistema de arquivos, que pode tornar-se acessível por meio de um nome genérico usando o sistema de alternativas.

Diretório de alternativas

O diretório padrão `/etc/alternatives` que contém links simbólicos.

Nome genérico

Um nome (por exemplo, `/usr/bin/edit`) que se refere a um arquivo, dentre vários disponíveis, usando o sistema de alternativas.

Grupo de links

Um conjunto de links simbólicos relacionados que podem ser atualizados como um grupo.

Link master

O link, em um grupo de links, que determina como os outros links no grupo são configurados.

Link escravo

Um link, em um grupo de links, controlado pelo link master.

Link simbólico (symlink)

Um arquivo que é uma referência a outro arquivo no mesmo sistema de arquivos. O sistema de alternativas usa os links simbólicos no diretório de alternativas para alternar entre as versões de um arquivo.

Os links simbólicos no diretório de alternativas podem ser modificados pelo administrador por meio do comando **update-alternatives**.

O sistema de alternativas oferece o comando **update-alternatives** para criar, remover, manter e mostrar informações sobre os links simbólicos. Embora esses links simbólicos geralmente apontem para comandos, eles também podem apontar para arquivos JAR, páginas de manual e outros arquivos. Os exemplos neste capítulo usam comandos e páginas de manual, mas também podem ser aplicáveis a outros tipos de arquivos.

O sistema de alternativas usa o diretório de alternativas para coletar os links para possíveis alternativas. Quando um novo pacote com uma alternativa é instalado, a nova alternativa é adicionada ao sistema. Dependendo da prioridade e do modo definido, a nova alternativa do pacote será selecionada como padrão. Em geral, os pacotes com uma versão superior também têm maior prioridade. O sistema de alternativas pode operar em dois modos:

- **Modo automático.** Nesse modo, o sistema de alternativas garante que os links no grupo apontem para as alternativas de prioridade mais alta apropriadas ao grupo.
- **Modo manual.** Nesse modo, o sistema de alternativas não faz quaisquer mudanças nas configurações do administrador do sistema.

Por exemplo, o comando **java** tem a seguinte hierarquia de links no sistema de alternativas:

EXEMPLO 22.1: SISTEMA DE ALTERNATIVAS DO COMANDO **java**

```
/usr/bin/java ❶  
-> /etc/alternatives/java ❷  
-> /usr/lib64/jvm/jre-10-openjdk/bin/java ❸
```

- ❶ O nome genérico.

- ② O link simbólico no diretório de alternativas.
- ③ Uma das alternativas.

22.2 Casos de uso

Por padrão, o script **update-alternatives** é chamado de um pacote RPM. Quando um pacote é instalado ou removido, o script se encarrega de todos os seus links simbólicos. Porém, você pode executá-lo manualmente da linha de comando para:

- exibir as alternativas atuais para um nome genérico.
- mudar os padrões de uma alternativa.
- criar um conjunto de arquivos relacionados para uma alternativa.

22.3 Obtendo uma visão geral das alternativas

Para recuperar os nomes de todas as alternativas configuradas, use:

```
> ls /var/lib/alternatives
```

Para obter uma visão geral de todas as alternativas configuradas e os respectivos valores, use

```
> sudo update-alternatives --get-selections
asadmin                auto      /usr/bin/asadmin-2.7
awk                    auto      /usr/bin/gawk
chardetect              auto      /usr/bin/chardetect-3.6
dbus-launch             auto      /usr/bin/dbus-launch.x11
default-displaymanager auto      /usr/lib/X11/displaymanagers/gdm
[...]
```

22.4 Vendo detalhes das alternativas específicas

A maneira mais fácil de verificar as alternativas é seguir os links simbólicos do seu comando. Por exemplo, para saber a que o comando **java** se refere, execute o seguinte comando:

```
> readlink --canonicalize /usr/bin/java
/usr/lib64/jvm/jre-10-openjdk/bin/java
```


Se aparecer o mesmo caminho (em nosso exemplo, o caminho é `/usr/bin/java`), não haverá alternativas disponíveis para esse comando.

Para ver as alternativas completas (incluindo escravos), use a opção `--display`:

```
> sudo update-alternatives --display java
java - auto mode
link best version is /usr/lib64/jvm/jre-1.8.0-openjdk/bin/java
link currently points to /usr/lib64/jvm/jre-1.8.0-openjdk/bin/java
link java is /usr/bin/java
slave java.1.gz is /usr/share/man/man1/java.1.gz
slave jre is /usr/lib64/jvm/jre
slave jre_exports is /usr/lib64/jvm-exports/jre
slave keytool is /usr/bin/keytool
slave keytool.1.gz is /usr/share/man/man1/keytool.1.gz
slave orbd is /usr/bin/orbd
slave orbd.1.gz is /usr/share/man/man1/orbd.1.gz
[...]
```

22.5 Definindo a versão padrão das alternativas

Por padrão, os comandos em `/usr/bin` fazem referência ao diretório de alternativas com a prioridade mais alta. Por exemplo, por padrão, o comando `java` mostra o seguinte número da versão:

```
> java -version
openjdk version "10.0.1" 2018-04-17
OpenJDK Runtime Environment (build 10.0.1+10-suse-lp150.1.11-x8664)
OpenJDK 64-Bit Server VM (build 10.0.1+10-suse-lp150.1.11-x8664, mixed mode)
```

Para mudar o comando `java` padrão para fazer referência a uma versão anterior, execute:

```
> sudo update-alternatives --config java
root's password:
There are 2 choices for the alternative java (providing /usr/bin/java).

   Selection    Path                                                    Priority    Status
   -----
*  0             /usr/lib64/jvm/jre-10-openjdk/bin/java                2005       auto mode
    1             /usr/lib64/jvm/jre-1.8.0-openjdk/bin/java              1805       manual mode
    2             /usr/lib64/jvm/jre-10-openjdk/bin/java                2005       manual mode
    3             /usr/lib64/jvm/jre-11-openjdk/bin/java                  0          manual mode

Press <enter> to keep the current choice[*], or type selection number:
```

Dependendo do sistema e das versões instaladas, o número exato da versão do Java será diferente. Depois que você selecionar 1, o **java** mostrará o seguinte número da versão:

```
> java -version
java version "1.8.0_171"
OpenJDK Runtime Environment (IcedTea 3.8.0) (build 1.8.0_171-b11 suse-lp150.2.3.1-x86_64)
OpenJDK 64-Bit Server VM (build 25.171-b11, mixed mode)
```

Além disso, tenha em mente os seguintes pontos:

- Ao trabalhar no modo manual e instalar outra versão do Java, o sistema de alternativas não afeta os links nem muda o nome genérico.
- Ao trabalhar no modo automático e instalar outra versão do Java, o sistema de alternativas muda o link master do Java e todos os links escravos (como você pode ver na [Seção 22.4](#), “*Vendo detalhes das alternativas específicas*”). Para verificar os relacionamentos entre master e escravo, use:

```
> sudo update-alternatives --display java
```

22.6 Instalando alternativas personalizadas

Esta seção descreve como configurar alternativas personalizadas em um sistema. O exemplo faz as seguintes suposições:

- Há dois scripts, **foo-2** e **foo-3**, com funcionalidade semelhante.
- Os scripts são armazenados no diretório `/usr/local/bin` para evitar conflitos com as ferramentas do sistema em `/usr/bin`.
- Há um link master **foo** que aponta para **foo-2** ou **foo-3**.

Para oferecer alternativas no sistema, siga estas etapas:

1. Copie seus scripts para o diretório `/usr/local/bin`.
2. Torne os scripts executáveis:

```
> sudo chmod +x /usr/local/bin/foo-{2,3}
```

3. Execute **update-alternatives** para os dois scripts:

```
> sudo update-alternatives --install \
```

```

/usr/local/bin/foo ❶\
foo ❷\
/usr/local/bin/foo-2 ❸\
200 ❹
> sudo update-alternatives --install \
/usr/local/bin/foo ❶\
foo ❷\
/usr/local/bin/foo-3 ❸\
300 ❹

```

As opções após `--install` têm os seguintes significados:

- ❶ O nome genérico. Para evitar confusão, geralmente é o nome do script sem quaisquer números de versão.
- ❷ O nome do link master. Deve ser o mesmo.
- ❸ O caminho para o(s) script(s) original(is) localizado(s) em `/usr/local/bin/`.
- ❹ A prioridade. Especificamos para `foo-2` uma prioridade mais baixa do que para `foo-3`. É recomendável usar um aumento significativo de número para separar as prioridades. Por exemplo, uma prioridade de 200 para `foo-2` e de 300 para `foo-3`.

4. Verifique o link master:

```

> sudo update-alternatives --display foo
foo - auto mode
link best version is /usr/local/bin/foo-3
link currently points to /usr/local/bin/foo-3
link foo is /usr/local/bin/foo
/usr/local/bin/foo-2 - priority 200
/usr/local/bin/foo-3 - priority 300

```

Após concluir as etapas descritas, você poderá usar o link master `/usr/local/bin/foo`.

Se necessário, você poderá instalar outras alternativas. Para remover uma alternativa, use o seguinte comando:

```
> sudo update-alternatives --remove foo /usr/local/bin/foo-2
```

Depois que esse script for removido, o sistema de alternativas do grupo foo terá esta aparência:

```

> sudo update-alternatives --display foo
foo - auto mode
link best version is /usr/local/bin/foo-3
link currently points to /usr/local/bin/foo-3
link foo is /usr/local/bin/foo

```

22.7 Definindo alternativas dependentes

Se você tem alternativas, o próprio script não é suficiente. A maioria dos comandos não é completamente independente: Em geral, eles são fornecidos com arquivos adicionais, como extensões, configurações ou páginas de manual. Para criar alternativas que dependem de um link master, use as *alternativas de escravos*.

Vamos supor que desejamos estender nosso exemplo na [Seção 22.6, “Instalando alternativas personalizadas”](#) e fornecer páginas de manual e arquivos de configuração:

- Duas páginas de manual, `foo-2.1.gz` e `foo-3.1.gz`, armazenadas no diretório `/usr/local/man/man1`.
- Dois arquivos de configuração, `foo-2.conf` e `foo-3.conf`, armazenados em `/etc`.

Siga estas etapas para adicionar os outros arquivos às alternativas:

1. Copie os arquivos de configuração em `/etc`:

```
> sudo cp foo-{2,3}.conf /etc
```

2. Copie as páginas de manual para o diretório `/usr/local/man/man1`:

```
> sudo cp foo-{2,3}.1.gz /usr/local/man/man1/
```

3. Adicione os links escravos aos scripts principais com a opção `--slave`:

```
> sudo update-alternatives --install \  
  /usr/local/bin/foo foo /usr/local/bin/foo-2 200 \  
  --slave /usr/local/man/man1/foo.1.gz \  
  foo.1.gz \  
  /usr/local/man/man1/foo-2.1.gz \  
  --slave /etc/foo.conf \  
  foo.conf \  
  /etc/foo-2.conf  
> sudo update-alternatives --install \  
  /usr/local/bin/foo foo /usr/local/bin/foo-3 300 \  
  --slave /usr/local/man/man1/foo.1.gz \  
  foo.1.gz \  
  /usr/local/man/man1/foo-3.1.gz \  
  --slave /etc/foo.conf \  
  /etc/foo-3.conf
```

```
foo.conf \  
/etc/foo-3.conf
```

4. Verifique o link master:


```
foo - auto mode  
link best version is /usr/local/bin/foo-3  
link currently points to /usr/local/bin/foo-3  
link foo is /usr/local/bin/foo  
slave foo.1.gz is /usr/local/man/man1/foo.1.gz  
slave foo.conf is /etc/foo.conf  
/usr/local/bin/foo-2 - priority 200  
slave foo.1.gz: /usr/local/man/man1/foo-2.1.gz  
slave foo.conf: /etc/foo-2.conf  
/usr/local/bin/foo-3 - priority 300  
slave foo.1.gz: /usr/local/man/man1/foo-3.1.gz  
slave foo.conf: /etc/foo-3.conf
```

Se você mudar os links com **update-alternatives --config foo** para **foo-2**, todos os links escravos também serão mudados.

23 Rede básica

O Linux oferece os recursos e as ferramentas de rede necessários para a integração em todos os tipos de estruturas de rede. É possível configurar o acesso a rede usando uma placa de rede com o YaST. A configuração também pode ser feita manualmente. Neste capítulo são abordados apenas os mecanismos fundamentais e os arquivos de configuração de rede relevantes.

Linux e outros sistemas operacionais Unix usam o protocolo TCP/IP. Não é um protocolo de rede único, mas uma família de protocolos de rede que oferece vários serviços. Os protocolos listados na *Vários protocolos na família de protocolos TCP/IP* são oferecidos para trocar dados entre duas máquinas por meio do TCP/IP. As redes combinadas por TCP/IP compõem uma rede mundial também chamada de “Internet”.

RFC significa *Request for Comments*. Os RFCs são documentos que descrevem vários procedimentos de implementação e protocolos da Internet para o sistema operacional e seus aplicativos. Os documentos RFC descrevem a configuração dos protocolos da Internet. Para obter mais informações sobre RFCs, visite <https://datatracker.ietf.org/> .

VÁRIOS PROTOCOLOS NA FAMÍLIA DE PROTOCOLOS TCP/IP

TCP

Transmission Control Protocol: um protocolo seguro orientado por conexão. Os dados a serem transmitidos são enviados primeiramente pelo aplicativo como fluxo de dados e convertidos no formato adequado ao sistema operacional. Os dados chegam ao respectivo aplicativo no host de destino com o formato original de fluxo de dados no qual foram inicialmente enviados. O TCP determina se algum dado foi perdido ou embaralhado durante a transmissão. O TCP é implementado onde a sequência de dados for necessária.

UDP

User Datagram Protocol: um protocolo inseguro, não baseado em conexão. Os dados a serem transmitidos são enviados na forma de pacotes gerados pelo aplicativo. A ordem em que os dados chegam ao destinatário não é garantida, havendo possibilidade de perda dos dados. O UDP é adequado para aplicativos orientados por registro. Ele possui um período de latência menor que o TCP.

ICMP

Internet Control Message Protocol: Não se trata de um protocolo para o usuário final, mas de um protocolo de controle especial que emite relatórios de erros e pode controlar o comportamento de máquinas que participam da transferência de dados TCP/IP. Além disso, ele fornece um modo de eco especial, que pode ser visualizado usando o programa ping.

IGMP

Internet Group Management Protocol: esse protocolo controla o comportamento da máquina na implementação de multicast IP.

Conforme mostrado na *Figura 23.1, “Modelo simplificado de camadas para TCP/IP”*, a troca de dados ocorre em camadas diferentes. A camada de rede real é a transferência de dados insegura por IP (Internet protocol). Acima do IP, o TCP garante, até certo ponto, a segurança na transferência de dados. A camada IP é suportada pelo protocolo base dependente do hardware, como a Ethernet.

Modelo TCP/IP

Modelo OSI



FIGURA 23.1: MODELO SIMPLIFICADO DE CAMADAS PARA TCP/IP

O diagrama fornece um ou dois exemplos para cada camada. As camadas são organizadas de acordo com os *níveis de abstração*. A camada mais baixa fica muito próxima do hardware. A camada mais alta é quase completamente abstraída do hardware. Todas as camadas possuem suas funções especiais próprias. As funções especiais de cada camada, na maioria das vezes, estão implícitas em suas descrições. A vinculação de dados e as camadas físicas representam a rede física usada, como a Ethernet.

Quase todos os protocolos de hardware funcionam em uma base orientada por pacotes. Os dados a serem transmitidos são reunidos em *pacotes* (não podem ser enviados todos de uma vez). O tamanho máximo de um pacote TCP/IP é de aproximadamente 64 KB. Os pacotes são normalmente bem menores, já que o hardware da rede pode ser um fator de limitação. O tamanho máximo de um pacote de dados na Ethernet é de cerca de 1.500 bytes. O tamanho do pacote TCP/IP limita-se a esse valor quando os dados são enviados por Ethernet. Se mais dados forem transferidos, mais pacotes de dados precisarão ser enviados pelo sistema operacional.

Para que as camadas executem suas respectivas funções, informações adicionais referentes a cada uma delas devem ser gravadas no pacote de dados. Isso ocorre no *cabeçalho* do pacote. Todas as camadas anexam um pequeno bloco de dados, chamado cabeçalho do protocolo, à frente de cada pacote emergente. Veja uma demonstração de pacote de dados TCP/IP passando por um cabo Ethernet na [Figura 23.2, “Pacote Ethernet TCP/IP”](#). A soma de teste está localizada no final do pacote e não no início. Isso torna as coisas mais simples para o hardware de rede.



FIGURA 23.2: PACOTE ETHERNET TCP/IP

Quando um aplicativo envia dados por uma rede, eles passam por cada camada, todas implementadas no kernel do Linux, exceto a camada física. Cada camada é responsável pela preparação dos dados, para que eles possam passar para a camada seguinte. A camada mais baixa é a responsável pelo envio de dados. Todo o processo é invertido quando os dados são recebidos. Como camadas de uma cebola, em cada uma os cabeçalhos de protocolo são removidos dos dados transportados. Por fim, a camada de transporte é responsável por disponibilizar os dados para uso pelos aplicativos de destino. Dessa forma, cada camada se comunica somente com a camada diretamente acima ou abaixo dela. Para os aplicativos, é irrelevante se os dados são transmitidos por uma conexão com ou sem fio. Da mesma forma, é irrelevante para a linha de dados os tipos de dados transmitidos, contanto que os pacotes estejam no formato correto.

23.1 Endereços IP e roteamento

Esta seção limita-se à abordagem de redes IPv4. Para obter informações sobre o protocolo IPv6, sucessor do IPv4, consulte a [Seção 23.2, “IPv6: a Internet de última geração”](#).

23.1.1 Endereços IP

Todo computador na Internet possui um endereço de 32 bits exclusivo. Os 32 bits (ou 4 bytes) normalmente são gravados conforme ilustrado na segunda linha em [Exemplo 23.1, “Gravando endereços IP”](#).

EXEMPLO 23.1: GRAVANDO ENDEREÇOS IP

```
IP Address (binary): 11000000 10101000 00000000 00010100
IP Address (decimal): 192.      168.      0.      20
```

Na forma decimal, os quatro bytes são gravados no sistema de números decimais, separados por pontos. O endereço IP é designado a um host ou a uma interface de rede. Ele pode ser usado apenas uma vez em todo o mundo. Há exceções a essa regra, mas não são relevantes para as passagens a seguir.

Os pontos nos endereços IP indicam o sistema hierárquico. Até os anos 90, os endereços IP eram estritamente categorizados em classes. Entretanto, esse sistema demonstrou ser excessivamente inflexível e foi desativado. Agora, o *CIDR* (Classless Interdomain Routing — Roteamento Interdomínio sem Classes) é usado.

23.1.2 Máscaras de rede e roteamento

As máscaras de rede são usadas para definir a faixa de endereços de uma sub-rede. Se dois hosts estiverem na mesma sub-rede, eles poderão acessar um ao outro diretamente. Se não estiverem na mesma sub-rede, eles precisarão do endereço de um gateway que manipule todo o tráfego da sub-rede. Para verificar se dois endereços IP estão em uma mesma sub-rede, basta “E” os dois endereços com a máscara de rede. Se o resultado for idêntico, os dois endereços IP estarão na mesma rede local. Se houver diferenças, o endereço IP remoto e, portanto, a interface remota, só poderão ser localizados através de um gateway.

Para compreender como as máscaras de rede funcionam, consulte o *Exemplo 23.2, “Vinculando endereços IP à máscara de rede”*. A máscara de rede consiste em 32 bits que identificam o quanto um endereço IP pertence à rede. Todos os bits 1 marcam o bit correspondente no endereço IP como pertencente à rede. Todos os bits 0 marcam os bits dentro da sub-rede. Isso significa que quanto maior a quantidade de bits 1, menor será o tamanho da sub-rede. Como a máscara de rede sempre consiste em vários bits 1 sucessivos, também é possível contar o número de bits da máscara de rede. Na *Exemplo 23.2, “Vinculando endereços IP à máscara de rede”*, a primeira rede com 24 bits também pode ser gravada como 192.168.0.0/24.

EXEMPLO 23.2: VINCULANDO ENDEREÇOS IP À MÁSCARA DE REDE

```
IP address (192.168.0.20): 11000000 10101000 00000000 00010100
Netmask   (255.255.255.0): 11111111 11111111 11111111 00000000
-----
```

```

Result of the link:      11000000 10101000 00000000 00000000
In the decimal system:    192.      168.      0.      0

IP address (213.95.15.200): 11010101 10111111 00001111 11001000
Netmask (255.255.255.0): 11111111 11111111 11111111 00000000
-----
Result of the link:      11010101 10111111 00001111 00000000
In the decimal system:    213.      95.      15.      0

```

Para dar outro exemplo: todas as máquinas conectadas ao mesmo cabo Ethernet, normalmente, estão localizadas na mesma sub-rede e são diretamente acessíveis. Mesmo quando a sub-rede é dividida fisicamente por switches ou pontes, esses hosts ainda assim podem ser diretamente localizados.

Endereços IP fora da sub-rede local só poderão ser localizados se um gateway for configurado para a rede de destino. Nos casos mais comuns, há somente um gateway que controla todo o tráfego externo. Entretanto, também é possível configurar vários gateways para sub-redes diferentes.

Se um gateway tiver sido configurado, todos os pacotes IP externos serão enviados para o gateway apropriado. Esse gateway tentará então encaminhar os pacotes da mesma forma (de host para host) até acessar o host de destino ou até o TTL (time to live) do pacote expirar.

ENDEREÇOS ESPECÍFICOS

Endereço de Rede Base

Essa é a máscara de rede E qualquer endereço na rede, conforme mostrado no *Exemplo 23.2, “Vinculando endereços IP à máscara de rede”* em Resultado. Esse endereço não pode ser designado a nenhum host.

Endereço de broadcast

Isso pode ser parafraseado como: “Acessar todos os hosts nesta sub-rede.” Para gerar isso, a máscara de rede é invertida no formato binário e vinculada ao endereço de rede base com um OU lógico. Portanto, o exemplo acima resulta em 192.168.0.255. Esse endereço não pode ser atribuído a nenhum host.

Host Local

O endereço 127.0.0.1 é designado ao “dispositivo loopback” em cada host. Pode-se configurar uma conexão para a sua própria máquina com este endereço e com todos os endereços da rede de loopback completa 127.0.0.0/8, conforme definidos com o IPv4. Com o IPv6, existe apenas um endereço de loopback (::1).

Como os endereços IP precisam ser exclusivos em qualquer parte do mundo, não é possível selecionar endereços aleatoriamente. Há três domínios de endereços a serem usados para configurar uma rede baseada em IP privado. Eles não conseguem se conectar ao restante da Internet, pois não podem ser transmitidos através dela. Esses domínios de endereço são especificados no RFC 1597 e listados na *Tabela 23.1, “Domínios de endereços IP privados”*.

TABELA 23.1: DOMÍNIOS DE ENDEREÇOS IP PRIVADOS

Rede/máscara de rede	Domínio
<u>10.0.0.0 / 255.0.0.0</u>	<u>10.x.x.x</u>
<u>172.16.0.0 / 255.240.0.0</u>	<u>172.16.x.x – 172.31.x.x</u>
<u>192.168.0.0 / 255.255.0.0</u>	<u>192.168.x.x</u>

23.2 IPv6: a Internet de última geração

Devido ao surgimento da World Wide Web (WWW), a Internet teve um crescimento massivo com um número cada vez maior de computadores se comunicando por TCP/IP nos últimos 15 anos. Desde que Tim Berners-Lee da CERN (<http://public.web.cern.ch>) inventou a WWW em 1990, o número de hosts da Internet cresceu de poucos milhares para centenas de milhões deles. Conforme mencionado, um endereço IPv4 consiste em apenas 32 bits. Além disso, muitos endereços IP são perdidos, eles não podem ser usados devido à forma como as redes são organizadas. O número de endereços disponíveis na sua sub-rede é dois elevado à potência do número de bits, menos dois. Uma sub-rede tem, por exemplo, 2, 6 ou 14 endereços disponíveis. Para conectar 128 hosts à Internet, por exemplo, você precisa de uma sub-rede com 256 endereços IP, dos quais apenas 254 são utilizáveis, visto que são necessários dois endereços IP para a estrutura da própria sub-rede: o endereço de broadcast e o endereço de rede base.

No protocolo IPv4 atual, DHCP ou NAT (Network Address Translation — Conversão de Endereços de Rede) são os mecanismos comuns usados para contornar a grande falta de endereços. Combinado à convenção de manter endereços públicos e privados separados por espaços, esses métodos podem certamente reduzir a falta de endereços. O problema deles está em suas configurações, trabalhosas para configurar e difíceis de manter. Para configurar um host em uma rede IPv4, você precisa de vários itens de endereço, como o próprio endereço IP do host, a máscara de sub-rede, o endereço de gateway e talvez um endereço de servidor de nomes. Todos esses itens precisam ser conhecidos e não podem ser derivados de outro lugar.

Com o IPv6, tanto a falta de endereços quanto as configurações complicadas passariam a ser problemas do passado. As seções a seguir oferecem mais informações sobre os aprimoramentos e benefícios trazidos pelo IPv6 e sobre a transição do protocolo antigo para o novo.

23.2.1 Vantagens

A melhoria mais importante e visível oferecida pelo protocolo mais recente é a expansão enorme do espaço de endereço disponível. Um endereço IPv6 é composto por valores de 128 bits, em vez dos 32 bits tradicionais. Ele é capaz de fornecer 'quatrilhões' de endereços IP.

Entretanto, os endereços IPv6 não diferem de seus antecessores apenas em relação ao comprimento. Também possuem uma estrutura interna diferente, que pode conter mais informações específicas sobre os sistemas e as redes a que pertencem. Leia mais detalhes sobre eles na [Seção 23.2.2, “Estrutura e tipos de endereços”](#).

Veja a seguir uma lista de outras vantagens do protocolo mais recente:

Configuração automática

O IPv6 torna apto o “plug and play” da rede, o que significa que um sistema recém-configurado é integrado à rede (local) sem qualquer configuração manual. O novo host usa seu mecanismo de configuração automática para derivar seu próprio endereço a partir das informações disponibilizadas pelos roteadores vizinhos, com base em um protocolo chamado *ND* (Neighbor Discovery — descoberta de vizinho). Esse método não exige nenhuma intervenção por parte do administrador e não há necessidade de manter um servidor central para alocação de endereços; uma vantagem adicional em relação ao IPv4, cuja alocação automática de endereços exige um servidor DHCP.

No entanto, se houver um roteador conectado a um switch, ele deverá enviar anúncios periódicos com flags avisando os hosts de uma rede como eles devem interagir entre si. Para obter mais informações, consulte o RFC 2462, a página de manual do `radvd.conf(5)` e o RFC 3315.

Mobilidade

O IPv6 torna possível a atribuição de vários endereços a uma interface de rede ao mesmo tempo. Isso permite que usuários acessem várias redes facilmente, o que é comparado aos serviços de roaming internacionais oferecidos pelas empresas de celulares. Quando você viaja com seu celular, ele automaticamente se conecta a um serviço interurbano, ao entrar na área correspondente. Dessa forma, você pode ser localizado no mesmo número de celular em qualquer lugar e pode fazer ligações como se estivesse em sua cidade.

Comunicação segura

Com o IPv4, a segurança da rede é uma função adicional. O IPv6 inclui IPsec como um de seus recursos principais, permitindo que sistemas se comuniquem por um túnel seguro, para evitar a intromissão de estranhos na Internet.

Compatibilidade Retroativa

De forma realista, seria impossível mudar toda a Internet de IPv4 para IPv6 de uma só vez. Portanto, é essencial que ambos os protocolos possam coexistir na Internet, mas também em um sistema. Isso é garantido ao usar endereços compatíveis (endereços IPv4 podem facilmente ser convertidos em endereços IPv6) e vários túneis. Consulte a [Seção 23.2.3, “Coexistência de IPv4 e IPv6”](#). Da mesma forma, os sistemas podem se basear em uma técnica *IP de pilha dupla* para suportar os dois protocolos ao mesmo tempo, significando que possuem duas pilhas de rede completamente separadas, de tal forma que não há interferência entre as duas versões de protocolos.

Serviços adaptados e personalizados através de multicasting

Com o IPv4, alguns serviços, como SMB, precisam transmitir seus pacotes para todos os hosts na rede local. O IPv6 oferece uma abordagem muito mais refinada, permitindo que os servidores direcionem hosts por *multicasting*, ou seja, direcionando vários hosts como partes de um grupo. Esse procedimento é diferente de direcionar todos os hosts por meio de *broadcasting* ou cada host individualmente por *unicasting*. Os hosts enviados como grupos talvez dependam do aplicativo concreto. É possível enviar todos os servidores de nomes para alguns grupos predefinidos (o *grupo multicast de servidores de nomes*), por exemplo ou todos os roteadores (o *grupo multicast de todos os roteadores*).

23.2.2 Estrutura e tipos de endereços

Conforme mencionado, o protocolo IP atual tem duas limitações importantes: os endereços IP estão cada vez mais escassos, e a configuração de rede com manutenção de tabelas de rotina vem se tornando uma tarefa cada vez mais complexa e onerosa. O IPv6 soluciona o primeiro problema expandindo o espaço dos endereços para 128 bits. O segundo problema é amenizado com a introdução de uma estrutura hierárquica de endereços, combinada com técnicas sofisticadas para alocar endereços de rede e com *multihoming* (a capacidade de atribuir vários endereços a um dispositivo, concedendo acesso a diversas redes).

Ao utilizar o IPv6, é útil saber que há três tipos diferentes de endereços:

Unicast

Endereços desse tipo são associados com exatamente uma interface de rede. Pacotes com esse tipo de endereço são entregues em apenas um destino. Da mesma forma, os endereços unicast são usados para transferir pacotes para hosts individuais na rede local ou na Internet.

Multicast

Endereços desse tipo estão relacionados a um grupo de interfaces de rede. Pacotes com esse tipo de endereço são entregues a todos os destinos pertencentes ao grupo. Endereços multicast são usados, principalmente, por certos tipos de serviços de rede para se comunicarem com determinados grupos de host de forma bem direcionada.

Anycast

Endereços desse tipo estão relacionados a um grupo de interfaces. Pacotes com esse tipo de endereço são entregues ao membro do grupo mais próximo do remetente, de acordo com os princípios do protocolo de roteamento subjacente. Endereços anycast são usados para que hosts possam descobrir mais facilmente servidores que oferecem certos serviços na área da rede determinada. Todos os servidores do mesmo tipo possuem o mesmo endereço anycast. Sempre que um host solicita um serviço, ele recebe uma resposta do servidor com o local mais próximo, conforme determinado pelo protocolo de roteamento. Caso ocorra alguma falha com esse servidor, o protocolo selecionará automaticamente o segundo servidor mais próximo ou então o terceiro e assim por diante.

Um endereço IPv6 é constituído de oito campos de quatro dígitos, cada um representando 16 bits, gravados em notação hexadecimal. Eles são separados por dois-pontos (:). Quaisquer zero bytes iniciais em um determinado campo podem ser descartados, mas zeros dentro ou no final do campo não podem ser descartados. Outra convenção é a de que mais de quatro zero bytes consecutivos podem retornar como dois-pontos duplos. Entretanto, apenas um separador do tipo :: é permitido por endereço. Esse tipo de notação reduzida é mostrado no *Exemplo 23.3, "Amostra de endereço IPv6"*, em que todas as três linhas representam o mesmo endereço.

EXEMPLO 23.3: AMOSTRA DE ENDEREÇO IPV6

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                               : 10 : 1000 : 1a4
```

Cada parte de um endereço IPv6 possui uma função definida. Os primeiros bytes formam o prefixo e especificam o tipo de endereço. A parte central é a porção do endereço na rede, mas pode não ser utilizada. O final do endereço forma a parte do host. Com o IPv6, a máscara de rede é definida indicando o comprimento do prefixo depois de uma barra no final do endereço. Um endereço, como mostrado no *Exemplo 23.4, “Endereço IPv6 que especifica o comprimento do prefixo”*, contém as informações de que os primeiros 64 bits formam a parte da rede do endereço e que os últimos 64 formam a parte do host. Em outras palavras, 64 significa que a máscara de rede está preenchida com 64 valores de 1 bit a partir da esquerda. Como no IPv4, o endereço IP é combinado com E, com os valores da máscara de rede, para determinar se o host está localizado na mesma sub-rede ou em outra.

EXEMPLO 23.4: ENDEREÇO IPV6 QUE ESPECIFICA O COMPRIMENTO DO PREFIXO

```
fe80::10:1000:1a4/64
```

O IPv6 conhece vários tipos de prefixos predefinidos. Alguns deles são mostrados na *Vários prefixos IPv6*.

VÁRIOS PREFIXOS IPV6

00

Endereços IPv4 e endereços de compatibilidade de IPv4 sobre IPv6. Esses são usados para manter a compatibilidade com IPv4. O seu uso ainda exige um roteador capaz de converter pacotes IPv6 em pacotes IPv4. Vários endereços especiais, como o do dispositivo loopback, também possuem esse prefixo.

2 ou 3 como o primeiro dígito

Endereços unicast globais agregativos. Como no caso do IPv4, uma interface pode ser atribuída para fazer parte de determinada sub-rede. Atualmente, existem os seguintes espaços de endereço: 2001::/16 (espaço de endereço de qualidade de produção) e 2002::/16 (espaço de endereço 6to4).

fe80::/10

Endereços locais de links. Endereços com este prefixo não devem ser roteados e, portanto, só devem ser encontrados na mesma sub-rede.

fec0::/10

Endereços locais de sites. Esses podem ser roteados, mas somente na rede da organização a que pertencem. Na verdade, eles são o equivalente IPv6 do espaço de endereço de rede privada atual, como 10.x.x.x.

ff

Esses são endereços multicast.

Um endereço unicast consiste em três componentes básicos:

Topologia pública

A primeira parte (que também contém um dos prefixos mencionados acima) é usada para rotear pacotes através da Internet pública. Ela inclui informações sobre a empresa ou instituição que fornece o acesso à Internet.

Topologia do site

A segunda parte contém informações de roteamento sobre a sub-rede à qual o pacote deve ser entregue.

ID de interface

A terceira parte identifica a interface à qual o pacote deve ser entregue. Isso também permite que o MAC faça parte do endereço. Como MAC é um identificador fixo globalmente exclusivo codificado no dispositivo pelo fabricante do hardware, o procedimento de configuração é bastante simplificado. Na verdade, os primeiros 64 bits de endereço são consolidados para formar o token EUI-64, com os últimos 48 bits obtidos no MAC e os 24 bits restantes contendo informações especiais sobre o tipo de token. Isso também permite atribuir um token EUI-64 a interfaces que não tenham MAC, como aquelas baseadas em PPP.

No topo dessa estrutura básica, o IPv6 faz distinção entre cinco tipos de endereços unicast:

:: (não especificado)

Esse endereço é usado pelo host como seu endereço de origem durante a primeira inicialização da interface (momento em que o endereço ainda não pode ser determinado por outros meios).

:::1 (loopback)

O endereço do dispositivo loopback.

Endereços compatíveis com IPv4

O endereço IPv6 é formado pelo endereço IPv4 e um prefixo consistindo em 96 zero bits. Esse tipo de endereço de compatibilidade é usado para um túnel (consulte a [Seção 23.2.3, "Coexistência de IPv4 e IPv6"](#)) para permitir que os hosts IPv4 e IPv6 se comuniquem com outros que estejam operando em um ambiente IPv4 puro.

Endereços IPv4 mapeados para IPv6

Esse tipo de endereço especifica um endereço IPv4 puro em uma notação IPv6.

Endereços locais

Há dois tipos de endereços para uso local:

link-local

Este tipo de endereço só pode ser usado na sub-rede local. Pacotes com endereço de origem ou de destino desse tipo não devem ser roteados para a Internet nem para outras sub-redes. Esses endereços contêm um prefixo especial (`fe80::/10`) e o ID da interface da placa de rede, com a parte do meio consistindo em zero bytes. Endereços desse tipo são usados durante a configuração automática para se comunicarem com outros hosts pertencentes à mesma sub-rede.

site-local

Pacotes com este tipo de endereço podem ser roteados para outras sub-redes, mas não para a Internet mais ampla. Eles devem permanecer dentro da própria rede da organização. Tais endereços são usados para intranets e equivalem ao espaço de endereço privado definido pelo IPv4. Eles contêm um prefixo especial (`fec0::/10`), o ID da interface e um campo de 16 bits que especifica o ID da sub-rede. Novamente, o restante é preenchido com bytes zero.

Como um recurso completamente novo, introduzido com o IPv6, cada interface de rede normalmente obtém vários endereços IP, com a vantagem de que várias redes podem ser acessadas através da mesma interface. Uma dessas redes pode ser totalmente configurada de forma automática usando o MAC e um prefixo conhecido, resultando na possibilidade de todos os hosts na rede local serem encontrados quando o IPv6 é habilitado (usando o endereço link-local). Com o MAC fazendo parte disso, qualquer endereço IP usado no mundo será exclusivo. As únicas partes variáveis do endereço são aquelas que indicam a *topologia do site* e a *topologia pública*, dependendo da rede real na qual o host estiver operando no momento.

Para que um host avance e retroceda entre duas redes diferentes ele precisa de, pelo menos, dois endereços. Um deles, o *endereço pessoal*, contém não só o ID de interface, como também um identificador da rede doméstica a que ele normalmente pertence (e o prefixo correspondente). O endereço pessoal é um endereço estático e, portanto, normalmente não se modifica. Mesmo assim, todos os pacotes destinados ao host móvel podem ser entregues a ele, independentemente de ele operar na rede doméstica ou em outro local externo. Isso é possível devido aos recursos totalmente novos introduzidos com o IPv6, como *configuração automática sem estado* e *descoberta de vizinho*. Além do endereço residencial, um host móvel obtém um ou mais endereços adicionais

pertencentes às redes interurbanas com roaming. Eles são chamados endereços *care-of*. A rede doméstica tem um recurso que encaminha qualquer pacote destinado ao host quando ele está em roaming. Em um ambiente IPv6, essa tarefa é executada pelo *agente local*, que retransmite todos os pacotes destinados ao endereço residencial através de um túnel. Por outro lado, esses pacotes destinados ao endereço *care-of* são diretamente transferidos para o host móvel sem qualquer desvio especial.

23.2.3 Coexistência de IPv4 e IPv6

A migração de todos os hosts conectados à Internet do IPv4 para o IPv6 é um processo gradual. Os dois protocolos coexistirão durante algum tempo. A coexistência deles em um sistema é garantida onde houver uma implementação de *pilha dupla* de ambos os protocolos. Ainda resta a dúvida de como um host habilitado para IPv6 deve se comunicar com um host IPv4 e como os pacotes do IPv6 devem ser transportados pelas redes atuais, que são predominantemente baseadas no IPv4. As melhores soluções oferecem endereços de compatibilidade e túnel (consulte a [Seção 23.2.2, “Estrutura e tipos de endereços”](#)).

Os hosts IPv6 que estiverem mais ou menos isolados na rede IPv4 (mundial) podem se comunicar por túneis: os pacotes IPv6 são encapsulados como pacotes IPv4 para que sejam transmitidos por uma rede IPv4. Tal conexão entre dois hosts IPv4 é chamada de *túnel*. Para que isso ocorra, os pacotes devem incluir o endereço IPv6 de destino (ou o prefixo correspondente) e o endereço IPv4 do host remoto na extremidade de recepção do túnel. Um túnel básico pode ser configurado manualmente, de acordo com um contrato entre os administradores dos hosts. Também é chamado de *túnel estático*.

Entretanto, a configuração e manutenção de túneis estáticos é normalmente muito trabalhosa para ser usada diariamente em comunicações. Portanto, o IPv6 fornece três métodos de *túneis dinâmicos*:

6over4

Os pacotes IPv6 são automaticamente encapsulados como pacotes IPv4 e enviados por uma rede IPv4 com capacidade multicast. O IPv6 é induzido a considerar a rede inteira (Internet) como uma gigantesca rede local. Com isso, é possível determinar automaticamente o destino final do túnel IPv4. Entretanto, esse método não faz um dimensionamento muito bom e também é dificultado porque o multicasting IP não é tão difundido na Internet. Portanto, ele apenas fornece uma solução para redes corporativas ou institucionais menores, em que o multicast pode ser habilitado. As especificações para esse método estão descritas no RFC 2529.

6to4

Com esse método, os endereços IPv4 são automaticamente gerados a partir de endereços IPv6, habilitando a comunicação de hosts IPv6 isolados através de uma rede IPv4. Entretanto, vários problemas foram relatados em relação à comunicação entre esses hosts IPv6 isolados e a Internet. O método está descrito no RFC 3056.

Controlador do túnel IPv6

Esse método se baseia em servidores especiais que fornecem túneis dedicados para hosts IPv6. É descrito no RFC 3053.

23.2.4 Configurando o IPv6

Para configurar o IPv6, normalmente não é necessário fazer mudanças nas estações de trabalho individuais. O IPv6 é habilitado por padrão. Para desabilitar ou habilitar o IPv6 em um sistema instalado, use o módulo *Configurações de Rede* do YaST. Na guia *Opções Globais*, marque ou desmarque a opção *Habilitar IPv6* conforme necessário. Para habilitá-lo temporariamente até a próxima reinicialização, digite **modprobe -i ipv6** como **root**. É impossível descarregar o módulo IPv6 depois de carregado.

Devido ao conceito de configuração automática do IPv6, um endereço é designado à placa de rede na rede *link-local*. Normalmente, nenhum gerenciamento de tabela de roteamento é feito em uma estação de trabalho. Os roteadores de rede podem ser consultados pela estação de trabalho, usando o *protocolo de anúncios do roteador*, para o qual devem ser implementados um prefixo e gateways. O programa *radvd* pode ser usado para configurar um roteador IPv6. Esse programa informa às estações de trabalho o prefixo que deve ser usado para os endereços IPv6 e os roteadores. Outra opção é usar *zebra/quagga* para a configuração automática dos dois endereços e para roteamento.

Para obter informações sobre como configurar vários tipos de túneis usando os arquivos */etc/sysconfig/network*, consulte a página de manual de *ifcfg-tunnel* (**man ifcfg-tunnel**).

23.2.5 Mais informações

A visão geral acima não abrange totalmente o tópico do IPv6. Para obter informações mais detalhadas sobre o protocolo mais recente, consulte os livros e a documentação online a seguir:

<http://www.ipv6.org/> 

O ponto de partida para tudo relativo ao IPv6.

<http://www.ipv6day.org> ↗

Todas as informações necessárias para iniciar sua própria rede IPv6.

<http://www.ipv6-to-standard.org/> ↗

A lista de produtos habilitados para IPv6.

<http://www.bieringer.de/linux/IPv6/> ↗

Aqui, encontre o Linux IPv6-HOWTO e muitos links relacionados ao tópico.

RFC2460

Informações fundamentais do RFC sobre o IPv6.

IPv6 Essentials

Um livro que descreve todos os aspectos importantes do tópico é o *IPv6 Essentials* de Silvia Hagen (ISBN 0-596-00125-8).

23.3 Resolução de nome

O DNS ajuda na designação de um endereço IP a um ou mais nomes e na designação de um nome a um endereço IP. No Linux, essa conversão normalmente é executada por um tipo especial de software chamado bind. A máquina responsável por essa conversão é chamada de *servidor de nomes*. Os nomes criam um sistema hierárquico, no qual cada componente do nome é separado um ponto. A hierarquia de nomes é, entretanto, independente da hierarquia de endereços IP descrita acima.

Considere um nome completo, como jupiter.example.com, gravado no formato hostname.domain. Um nome completo, denominado *FQDN* (Fully Qualified Domain Name – Nome de Domínio Completo e Qualificado), consiste em um nome de host e um nome de domínio (example.com). O último também inclui o *TLD* (Top Level Domain — Domínio de Nível Superior) (com).

A designação TLD tornou-se bastante confusa por razões históricas. Tradicionalmente, nomes de domínio com três letras são usados nos EUA. No resto do mundo, os códigos nacionais ISO de duas letras são o padrão. Além disso, TLDs mais longos foram introduzidos em 2000, representando certas esferas de atividades (por exemplo, .info, .name, .museum).

No início da Internet (antes de 1990), o arquivo /etc/hosts era usado para armazenar os nomes de todas as máquinas representadas na Internet. Isso rapidamente se tornou impraticável, devido ao crescente número de computadores conectados à Internet. Por essa razão, um banco de dados descentralizado foi desenvolvido para armazenar nomes de host de uma forma amplamente

distribuída. Esse banco de dados, semelhante ao servidor de nomes, não possui os dados pertencentes a todos os hosts na Internet já disponíveis, mas pode encaminhar solicitações a outros servidores de nomes.

A parte superior da hierarquia é ocupada pelos *servidores de nomes raiz*. Esses servidores de nomes raiz gerenciam os domínios de nível superior e são executados pelo NIC (Network Information Center). Cada servidor de nomes raiz conhece os servidores de nomes responsáveis por um determinado domínio de nível superior. Para obter informações sobre NICs de domínio superior, vá para <http://www.internic.net>.

O DNS pode fazer mais do que resolver nomes de host. O servidor de nomes também distingue qual host recebe e-mails para um domínio inteiro: o *MX (servidor de correio)*.

Para sua máquina resolver um endereço IP, ela precisa pelo menos conhecer um servidor de nomes e seu respectivo endereço IP. Especifique facilmente esse tipo de servidor de nomes usando o YaST.

O protocolo `whois` está intimamente relacionado ao DNS. Com esse programa, é possível descobrir rapidamente o responsável por um domínio especificado.



Nota: MDNS e nomes de domínio `.local`

O domínio de nível superior `.local` é tratado como domínio link-local pelo resolver. As solicitações de DNS são enviadas como solicitações de DNS multicast, em vez de solicitações de DNS normal. Se você já usa o domínio `.local` em sua configuração de servidor de nomes, deverá desativar essa opção em `/etc/host.conf`. Para obter mais informações, consulte a página de manual `host.conf`.

Para desativar o MDNS durante a instalação, use `nomdns=1` como parâmetro de boot.

Para obter mais informações sobre DNS de multicast, consulte <http://www.multicastdns.org>.

23.4 Configurando uma conexão de rede com o YaST

Há muitos tipos de redes suportadas no Linux. A maioria delas usa nomes de dispositivos diferentes e os arquivos de configuração se espalham por vários locais no sistema de arquivos. Para obter uma visão geral detalhada dos aspectos da configuração manual de rede, consulte a [Seção 23.6, “Configurando uma conexão de rede manualmente”](#).

No SUSE Linux Enterprise Desktop, em que o NetworkManager está ativo por padrão, todas as placas de rede estão configuradas. Se o NetworkManager não estiver ativo, apenas a primeira interface com link ativo (com cabo de rede conectado) será configurada automaticamente. Hardwares adicionais podem ser configurados a qualquer momento no sistema instalado. As seguintes seções descrevem a configuração de rede para todos os tipos de conexões de rede suportadas pelo SUSE Linux Enterprise Desktop.

23.4.1 Configurando a placa de rede com o YaST

Para configurar a placa Ethernet ou Wi-Fi/Bluetooth no YaST, selecione *Sistema > Configurações de Rede*. Após iniciar o módulo, o YaST exibirá a caixa de diálogo *Configurações de Rede* com quatro guias: *Opções Globais*, *Visão Geral*, *Nome de host/DNS* e *Roteamento*.

A guia *Opções Globais* permite definir opções gerais de rede, como método de configuração de rede, IPv6 e opções gerais de DHCP. Para obter mais informações, consulte a [Seção 23.4.1.1, “Configurando as opções globais de rede”](#).

A guia *Visão Geral* contém informações sobre interfaces de rede instaladas e configurações. Ela lista os nomes de todas as placas de rede detectadas corretamente. Nessa caixa de diálogo, você pode configurar manualmente novas placas, bem como remover ou mudar suas configurações. Para configurar manualmente uma placa que não foi detectada automaticamente, consulte a [Seção 23.4.1.3, “Configurando uma placa de rede não detectada”](#). Para mudar a configuração de uma placa que já está configurada, consulte a [Seção 23.4.1.2, “Mudando a configuração de uma placa de rede”](#).

A guia *Nome de host/DNS* permite definir o nome de host da máquina e nomear os servidores que serão usados. Para obter mais informações, consulte a [Seção 23.4.1.4, “Configurando nome de host e DNS”](#).

A guia *Roteamento* é usada para a configuração do roteamento. Consulte a [Seção 23.4.1.5, “Configurando o roteamento”](#) para obter mais informações.

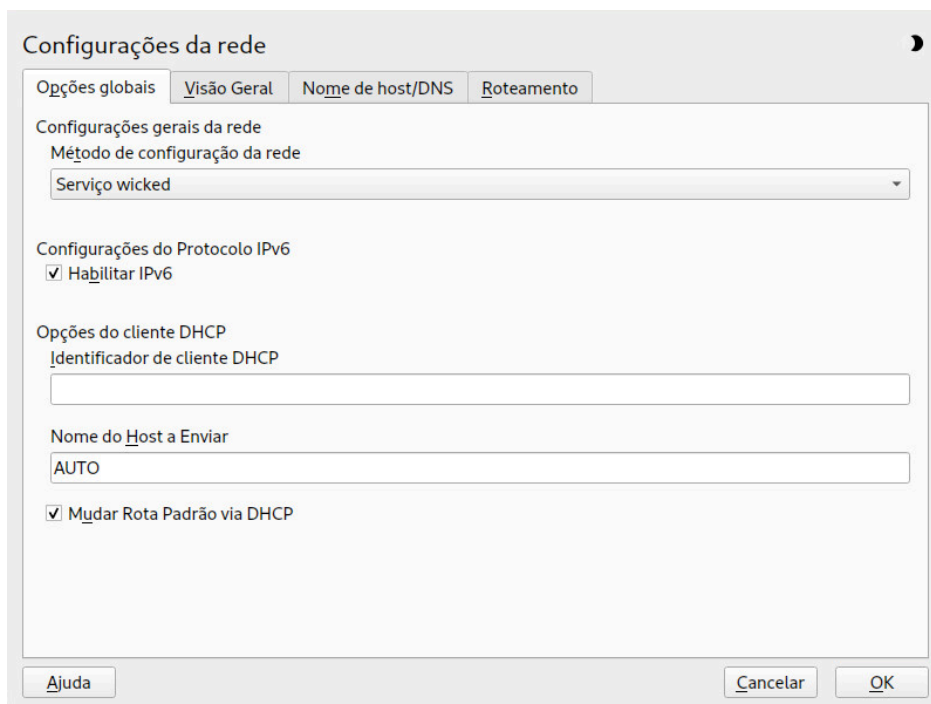


FIGURA 23.3: DEFININDO AS CONFIGURAÇÕES DE REDE

23.4.1.1 Configurando as opções globais de rede

A guia *Opções Globais* do módulo *Configurações de Rede* do YaST permite definir opções globais de rede importantes, como o uso do NetworkManager, o IPv6 e opções de cliente DHCP. Essas configurações são aplicáveis a todas as interfaces de rede.

Em *Método de Configuração da Rede*, escolha o modo como as conexões de rede são gerenciadas. Para que um applet de área de trabalho do NetworkManager gerencie as conexões de todas as interfaces, escolha *Serviço do NetworkManager*. O NetworkManager é ideal para alternar entre várias redes com fio e wireless. Se você não tem um ambiente de área de trabalho em execução, ou se o seu computador for um servidor Xen, um sistema virtual ou fornecer serviços de rede como DHCP ou DNS em sua rede, use o método *Serviço Wicked*. Se o NetworkManager for usado, o **nm-applet** deverá ser usado para configurar opções de rede, e as guias *Visão Geral*, *Nome de host/DNS* e *Roteamento* do módulo *Configurações de Rede* estarão desabilitadas. Para obter mais informações sobre o NetworkManager, consulte o [Capítulo 31, Usando o NetworkManager](#).

Em *Configurações do Protocolo IPv6*, escolha se é para usar o protocolo IPv6. É possível usar o IPv6 juntamente com o IPv4. Por padrão, IPv6 está habilitado. Contudo, nas redes que não usam o protocolo IPv6, os tempos de resposta podem ser acelerados com o protocolo IPv6 desabilitado. Para desabilitá-lo, desmarque *Habilitar IPv6*. Se o IPv6 for desabilitado, o kernel não carregará mais o módulo IPv6 automaticamente. Esta configuração será aplicada após a reinicialização.

Nas *Opções do Cliente DHCP*, configure as opções do cliente DHCP. O *Identificador de Cliente DHCP* deve ser diferente para cada cliente DHCP na mesma rede. Se ficar vazio, assumirá como padrão o endereço de hardware da interface da rede. Entretanto, se você tiver várias máquinas virtuais em execução na mesma interface de rede e, portanto, com o mesmo endereço de hardware, especifique aqui um identificador exclusivo.

O *Nome do Host a Enviar* especifica uma string usada no campo da opção de nome de host quando o cliente DHCP envia mensagens ao servidor DHCP. Alguns servidores DHCP atualizam as zonas do servidor de nomes (registros diretos e reversos) de acordo com esse nome de host (DNS Dinâmico). Além disso, alguns servidores DHCP exigem que o campo da opção *Nome do Host a Enviar* contenha uma string específica nas mensagens DHCP dos clientes. Mantenha AUTO para enviar o nome de host atual (ou seja, o que está definido em /etc/HOSTNAME). Deixe o campo da opção vazio para não enviar nenhum nome de host.

Para não mudar a rota padrão de acordo com as informações do DHCP, desmarque *Mudar Rota Padrão via DHCP*.

23.4.1.2 Mudando a configuração de uma placa de rede

Para mudar a configuração de uma placa de rede, selecione-a na lista de placas detectadas em *Configurações de Rede > Visão Geral* no YaST e clique em *Editar*. A caixa de diálogo *Configuração da Placa de Rede* é exibida, na qual é possível ajustar a configuração da placa usando as guias *Geral*, *Endereço* e *Hardware*.

23.4.1.2.1 Configurando endereços IP

Você pode definir o endereço IP da placa de rede ou o modo como seu endereço IP é determinado na guia *Endereço* da caixa de diálogo *Configuração da Placa de Rede*. Há suporte para endereços IPv4 e IPv6. A placa de rede pode ser *Sem Endereço IP* (útil para dispositivos de vinculação), ter um *Endereço IP Atribuído Estaticamente* (IPv4 ou IPv6) ou um *Endereço Dinâmico* atribuído por *DHCP*, *Zeroconf* ou ambos.

Ao usar um *Endereço Dinâmico*, selecione se deseja usar *Apenas DHCP Versão 4* (para IPv4), *Apenas DHCP Versão 6* (para IPv6) ou *DHCP Versões 4 e 6*.

Se possível, a primeira placa de rede com link que estiver disponível durante a instalação será configurada automaticamente para usar a configuração automática de endereço via DHCP. No SUSE Linux Enterprise Desktop, em que o NetworkManager está ativo por padrão, todas as placas de rede estão configuradas.

Também será necessário usar o DHCP se você estiver usando uma linha DSL sem nenhum IP estático atribuído pelo ISP (Internet Service Provider — Provedor de Serviços de Internet). Se você decidir usar o DHCP, configure os detalhes em *Opções do Cliente DHCP* na guia *Opções Globais* da caixa de diálogo *Configurações de Rede* do módulo de configuração de placa de rede do YaST. Se você tiver uma configuração de host virtual, em que hosts diferentes se comunicam pela mesma interface, será necessário um *Identificador de Cliente DHCP* para diferenciá-las.

O DHCP é uma boa opção para a configuração de clientes, mas não é a ideal para a configuração de servidores. Para definir um endereço IP estático, faça o seguinte:

1. Selecione uma placa na lista de placas detectadas na guia *Visão Geral* do módulo de configuração de placa de rede do YaST e clique em *Editar*.
2. Na guia *Endereço*, escolha *Endereço IP Atribuído Estaticamente*.
3. Digite o *Endereço IP*. Podem ser usados endereços IPv4 e IPv6. Digite a máscara de rede em *Máscara de Sub-rede*. Se for usado o endereço IPv6, use *Máscara de Sub-rede* para um comprimento do prefixo no formato `/64`.
Como opção, você pode digitar um *Nome de Host* completo para esse endereço, que será gravado no arquivo de configuração `/etc/hosts`.
4. Clique em *Avançar*.
5. Para ativar a configuração, clique em *OK*.



Nota: Ativação de interface e detecção de link

Durante a ativação de uma interface de rede, o **wicked** verifica a existência de uma operadora e apenas aplica a configuração de IP depois que um link foi detectado. Se você precisa aplicar a configuração independentemente do status do link (por exemplo, quando você deseja testar um serviço que escuta determinado endereço), pode ignorar a detecção de link adicionando a variável `LINK_REQUIRED=no` ao arquivo de configuração da interface em `/etc/sysconfig/network/ifcfg`.

Você também pode usar a variável `LINK_READY_WAIT=5` para especificar o tempo de espera de um link em segundos.

Para obter mais informações sobre os arquivos de configuração `ifcfg-*`, consulte a [Seção 23.6.2.5, “/etc/sysconfig/network/ifcfg-*”](#) e [man 5 ifcfg](#).

Se você usa o endereço estático, os servidores de nomes e o gateway padrão não são configurados automaticamente. Para configurar servidores de nomes, proceda conforme descrito na [Seção 23.4.1.4, “Configurando nome de host e DNS”](#). Para configurar um gateway, proceda conforme descrito na [Seção 23.4.1.5, “Configurando o roteamento”](#).

23.4.1.2.2 Configurando vários endereços

Um único dispositivo de rede pode ter vários endereços IP chamados *alias* ou *rótulos*.



Nota: *Alias* são um recurso de compatibilidade

Os *alias* ou *rótulos* funcionam apenas com IPv4. O uso de interfaces de rede `iproute2` torna possível ter um ou mais endereços.

Para definir mais endereços para sua placa de rede usando o YaST, faça o seguinte:

1. Selecione uma placa na lista de placas detectadas na guia *Visão Geral* da caixa de diálogo *Configurações de Rede* do YaST e clique em *Editar*.
2. Na guia *Endereço* > *Endereços Adicionais*, clique em *Adicionar*.
3. Digite o *Rótulo do Endereço IPv4*, o *Endereço IP* e a *Máscara de rede*. Observe que os *alias* de IP devem ser adicionados com a máscara de rede `/32`. Não inclua o nome da interface no nome do *alias*.
4. Para ativar a configuração, confirme as definições.

23.4.1.2.3 Mudando o nome de dispositivo e as regras de udev

É possível mudar o nome de dispositivo da placa de rede quando ela for usada. Também é possível determinar se a placa de rede deve ser identificada pelo udev usando o endereço (MAC) de hardware ou o ID do barramento. A última opção é preferencial em servidores grandes para simplificar o hotplug de placas. Para definir essas opções com o YaST, faça o seguinte:

1. Selecione uma placa na lista de placas detectadas na guia *Visão Geral* da caixa de diálogo *Configurações de Rede* do YaST e clique em *Editar*.
2. Vá até a guia *Geral*. O nome de dispositivo atual é mostrado em *Regras do Udev*. Clique em *Mudar*.
3. Selecione se o udev deve identificar a placa por seu *Endereço MAC* ou *ID do Bus*. O endereço MAC e o ID do barramento atuais da placa são mostrados na caixa de diálogo.
4. Para mudar o nome de dispositivo, marque a opção *Mudar Nome do Dispositivo* e edite o nome.
5. Para ativar a configuração, confirme as definições.

23.4.1.2.4 Mudando o driver do kernel da placa de rede

Para algumas placas de rede, pode haver vários drivers de kernel disponíveis. Se a placa já estiver configurada, o YaST permitirá selecionar um driver do Kernel para uso na lista de drivers compatíveis disponíveis. Também é possível especificar opções para o driver de kernel. Para definir essas opções com o YaST, faça o seguinte:

1. Selecione uma placa na lista de placas detectadas na guia *Visão Geral* do módulo *Configurações de Rede* do YaST e clique em *Editar*.
2. Vá até a guia *Hardware*.
3. Selecione o driver de kernel a ser usado em *Nome de Módulo*. Insira quaisquer opções para o driver selecionado em *Opções*, no formato `= VALOR`. Se forem usadas mais opções, elas deverão ser separadas por espaços.
4. Para ativar a configuração, confirme as definições.

23.4.1.2.5 Ativando o dispositivo de rede

Se você usar o método com o **wicked**, poderá configurar seu dispositivo para ser iniciado durante o boot, na conexão a cabo, ao detectar a placa, manualmente ou nunca. Para mudar a inicialização do dispositivo, faça o seguinte:

1. No YaST, selecione uma placa na lista de placas detectadas em *Sistema > Configurações de Rede* e clique em *Editar*.
2. Na guia *Geral*, selecione a entrada desejada em *Ativação de Dispositivo*.
Escolha *Em Tempo de Boot* para iniciar o dispositivo durante o boot do sistema. Com a opção *Em Conexão Cabo*, a interface é monitorada quanto a qualquer conexão física existente. Com a opção *Em Hotplug*, a interface é definida ao ficar disponível. Ela é semelhante à opção *Em Tempo de Boot*, a única diferença é que não ocorre nenhum erro quando a interface não está presente no momento da inicialização. Escolha *Manualmente* para controlar a interface manualmente com **ifup**. Escolha *Nunca* para não iniciar o dispositivo. A opção *Em NFSroot* é similar a *Em tempo de Boot*, mas a interface não é encerrada com o comando **systemctl stop network**. O serviço **network** também se encarregará do serviço **wicked** se o **wicked** estiver ativo. Use-a se você estiver usando um sistema de arquivos raiz NFS ou iSCSI.
3. Para ativar a configuração, confirme as definições.



Dica: NFS como sistema de arquivos raiz

Em sistemas (sem disco) nos quais a partição raiz é montada por rede como compartilhamento NFS, você precisa ter cuidado ao configurar o dispositivo de rede pelo qual o compartilhamento NFS pode ser acessado.

Ao encerrar ou reinicializar o sistema, a ordem de processamento padrão é desativar as conexões de rede e, na sequência, desmontar a partição raiz. Com a raiz NFS, essa ordem causa problemas, já que a partição raiz não pode ser completamente desmontada porque a conexão de rede com o compartilhamento NFS já não está ativada. Para impedir que o sistema desative o dispositivo de rede relevante, abra a guia de configuração do dispositivo de rede, conforme descrito na [Seção 23.4.1.2.5, “Ativando o dispositivo de rede”](#), e escolha *Em NFSroot* no painel *Ativação do Dispositivo*.

23.4.1.2.6 Configurando o tamanho da unidade máxima de transferência

Você pode definir uma unidade máxima de transferência (MTU) para a interface. A MTU refere-se ao maior tamanho de pacote permitido, em bytes. Uma MTU maior proporciona melhor eficiência da largura de banda. No entanto, pacotes grandes podem bloquear uma interface lenta por algum tempo, aumentando a latência dos pacotes seguintes.

1. No YaST, selecione uma placa na lista de placas detectadas em *Sistema > Configurações de Rede* e clique em *Editar*.
2. Na guia *Geral*, selecione a entrada desejada na lista *Definir MTU*.
3. Para ativar a configuração, confirme as definições.

23.4.1.2.7 Dispositivos multifuncionais PCIe

Dispositivos multifuncionais que suportam LAN, iSCSI e FCoE são permitidos. O cliente FCoE do YaST (**yast2 fcoe-client**) mostra flags particulares em colunas adicionais para permitir que o usuário selecione o dispositivo destinado ao FCoE. O módulo de rede do YaST (**yast2 lan**) exclui os “dispositivos apenas de armazenamento” da configuração de rede.

23.4.1.2.8 Configuração de InfiniBand para IP sobre InfiniBand (IPoIB)

1. No YaST, selecione o dispositivo InfiniBand em *Sistema > Configurações de Rede* e clique em *Editar*.
2. Na guia *Geral*, selecione um dos modos IPoIB (*IP-over-InfiniBand* – InfiniBand sobre IP): *connected* (conectado, que é o padrão) ou *datagram* (datagrama).
3. Para ativar a configuração, confirme as definições.

Para obter mais informações sobre o InfiniBand, consulte </usr/src/linux/Documentation/infiniband/ipoib.txt>.

23.4.1.2.9 Configurando o firewall

Sem precisar efetuar a configuração de firewall detalhada, como descrito na *Livro "Security and Hardening Guide", Capítulo 23 "Masquerading and firewalls", Seção 23.4 "firewalld"*, você pode determinar a configuração de firewall básica para seu dispositivo como parte da configuração dele. Proceda da seguinte maneira:

1. Abra o módulo *Sistema > Configurações de Rede* do YaST. Na guia *Visão Geral*, selecione uma placa na lista de placas detectadas e clique em *Editar*.
2. Acesse a guia *Geral* da caixa de diálogo *Configurações de Rede*.
3. Determine a *Zona de Firewall* à qual sua interface deve ser atribuída. As seguintes opções estão disponíveis:

Firewall Desabilitado

Essa opção estará disponível apenas se o firewall estiver desabilitado, sem entrar em execução. Use esta opção apenas se a sua máquina pertencer a uma rede maior protegida por um firewall externo.

Zona Atribuída Automaticamente

Essa opção fica disponível apenas quando o firewall está habilitado. O firewall está em execução e a interface é atribuída automaticamente a uma zona de firewall. Para uma interface como essa, será usada a zona que contiver a palavra-chave any ou a zona externa.

Zona Interna (Não Protegida)

O firewall está em execução, mas não assegura o uso obrigatório de nenhuma regra para proteger a interface. Use esta opção se a sua máquina pertencer a uma rede maior protegida por um firewall externo. Ela também é útil para as interfaces conectadas à rede interna, quando a máquina possui mais interfaces de rede.

Zona Desmilitarizada

Zona desmilitarizada é uma linha de defesa adicional situada na frente de uma rede interna e da Internet (hostil). Os hosts designados a essa zona podem ser acessados a partir da rede interna e a Internet, mas não podem acessar a rede interna.

Zona Externa

O firewall está em execução nesta interface e a protege totalmente contra outros tráfegos de rede (provavelmente hostis). Ela é a opção padrão.

4. Para ativar a configuração, confirme as definições.

23.4.1.3 Configurando uma placa de rede não detectada

Se uma placa de rede não for detectada corretamente, ela não será incluída na lista de placas detectadas. Se você tiver certeza de que o sistema contém um driver para sua placa, poderá configurá-la manualmente. Se for possível, configure também tipos especiais de dispositivos de rede, como ponte, ligação, TUN ou TAP. Para configurar uma placa de rede não detectada (ou um dispositivo especial), faça o seguinte:

1. Na caixa de diálogo *Sistema > Configurações de Rede > Visão Geral* no YaST, clique em *Adicionar*.
2. Na caixa de diálogo *Hardware*, defina o *Tipo de Dispositivo* da interface entre as opções disponíveis e o *Nome de Configuração*. Se a placa de rede for um dispositivo USB, ative a respectiva caixa de seleção e saia dessa caixa de diálogo clicando em *Avançar*. Caso contrário, você pode definir o *Nome de Módulo* do kernel para ser usado para a placa e as respectivas *Opções*, se necessário.

Em *Opções do Ethtool*, você pode definir as opções de **ethtool** usadas pelo **ifup** para a interface. Para obter informações sobre as opções disponíveis, consulte a página de manual do **ethtool**.

Se a string da opção começar com um `-` (por exemplo, `-K NOME_DA_INTERFACE rx on`), a segunda palavra na string será substituída pelo nome da interface atual. Do contrário (por exemplo, `autoneg off speed 10`), **ifup** adicionará `-s NOME_DA_INTERFACE` ao início.

3. Clique em *Avançar*.
4. Configure quaisquer opções que forem necessárias, como o endereço IP, a ativação do dispositivo ou a zona de firewall da interface nas guias *Geral*, *Endereço* e *Hardware*. Para obter mais informações sobre as opções de configuração, consulte [Seção 23.4.1.2, “Mudando a configuração de uma placa de rede”](#).
5. Se você selecionou *Wireless* como o tipo de dispositivo da interface, configure a conexão wireless na próxima caixa de diálogo.
6. Para ativar a nova configuração de rede, confirme as definições.

23.4.1.4 Configurando nome de host e DNS

Se você não mudou a configuração de rede durante a instalação e a placa Ethernet já estava disponível, um nome de host foi gerado automaticamente para o seu computador e o DHCP foi ativado. O mesmo se aplica às informações de serviço de nomes de que o host necessita para se integrar a um ambiente de rede. Se o DHCP for usado para a configuração de endereços de rede, a lista de servidores de nomes de domínio será preenchida automaticamente com os dados adequados. Se uma configuração estática for preferencial, defina esses valores manualmente.

Para mudar o nome do seu computador e ajustar a lista de pesquisa do servidor de nomes, faça o seguinte:

1. Vá para a guia *Configurações de Rede > Nome de host/DNS* no módulo *Sistema* no YaST.
2. Insira o *Nome de host*. Observe que o nome de host é global e aplica-se a todas as interfaces de rede.

Se você estiver usando o DHCP para obter um endereço IP, o nome de host do seu computador será definido automaticamente pelo servidor DHCP. Convém desabilitar esse comportamento se você se conecta a outras redes, já que elas podem atribuir nomes de host diferentes, e a mudança de nome de host em tempo de execução pode confundir a área de trabalho gráfica. Para desabilitar o uso do DHCP para obter um endereço IP, desmarque *Trocar Nome de Host via DHCP*.

3. Em *Modificar Configuração do DNS*, selecione o modo como a configuração do DNS (servidores de nomes, lista de pesquisa, conteúdo do arquivo `/run/netconfig/resolv.conf`) é modificada.

Se a opção *Usar Política Padrão* for selecionada, a configuração será gerenciada pelo script **netconfig**, que funde os dados definidos estaticamente (com o YaST ou nos arquivos de configuração) com os dados obtidos dinamicamente (do cliente DHCP ou do NetworkManager). Essa política padrão geralmente é suficiente.

Se a opção *Apenas Manualmente* for selecionada, **netconfig** não terá permissão para modificar o arquivo `/run/netconfig/resolv.conf`. Entretanto, esse arquivo pode ser editado manualmente.

Se a opção *Política Personalizada* for selecionada, deverá ser especificada uma string de *Regra de Política Personalizada* definindo a política de fusão. A string consiste em uma lista de nomes de interface separados por vírgula, considerada como fonte válida de configurações. Além dos nomes completos de interface, também são permitidos curingas básicos para corresponder a várias interfaces. Por exemplo, `eth* ppp?` primeiramente

encontrará todas as interfaces eth, depois, todas as interfaces de ppp0 a ppp9. Existem dois valores de política especiais que indicam como aplicar as configurações estáticas definidas no arquivo `/etc/sysconfig/network/config`:

STATIC

É necessário fundir as configurações estáticas com as configurações dinâmicas.

STATIC_FALLBACK

As configurações estáticas são usadas apenas quando não há nenhuma configuração dinâmica disponível.

Para obter mais informações, consulte a página de manual de **netconfig(8)** (**man 8 netconfig**).

4. Digite os *Servidores de Nome* e preencha a lista *Pesquisa de Domínio*. Servidores de nomes devem ser especificados por endereços IP, como 192.168.1.116, e não por nomes de host. Os nomes especificados na guia *Pesquisa de Domínio* são nomes de domínio usados para resolver nomes de host sem um domínio especificado. Se for usada mais de uma *Pesquisa de Domínio*, separe os domínios por vírgulas ou espaços.
5. Para ativar a configuração, confirme as definições.

É possível também editar o nome de host usando o YaST da linha de comando. As mudanças feitas pelo YaST entram em vigor imediatamente (o que não acontece quando se edita o arquivo `/etc/HOSTNAME` manualmente). Para mudar o nome de host, use o seguinte comando:

```
# yast dns edit hostname=HOSTNAME
```

Para mudar os servidores de nomes, use os seguintes comandos:

```
# yast dns edit nameserver1=192.168.1.116
# yast dns edit nameserver2=192.168.1.117
# yast dns edit nameserver3=192.168.1.118
```

23.4.1.5 Configurando o roteamento

Para que sua máquina se comunique com outras máquinas e redes, é necessário fornecer informações de roteamento para que o tráfego de rede siga o caminho correto. Se o DHCP for usado, essas informações serão fornecidas automaticamente. Se uma configuração estática for usada, esses dados deverão ser adicionados manualmente.

1. No YaST, vá para *Configurações de Rede > Roteamento*.
2. Digite o endereço IP do *Gateway Padrão* (IPv4 e IPv6, se necessário). O gateway padrão corresponde a todos os destinos possíveis, mas se houver uma entrada da tabela de roteamento que corresponda ao endereço exigido, ela será usada no lugar da rota padrão, pelo Gateway Padrão.
3. É possível digitar mais entradas na *Tabela de Roteamento*. Digite o endereço IP do *Destino*, o endereço IP do *Gateway* e a *Máscara de Rede*. Selecione o *Dispositivo* pelo qual será roteado o tráfego para a rede definida (o sinal de menos significa qualquer dispositivo). Para omitir qualquer um desses valores, use o sinal de menos `-`. Para digitar um gateway padrão na tabela, use padrão no campo *Destino*.



Nota: Priorização de rota

Se forem usadas mais rotas padrão, será possível especificar a opção métrica para determinar qual rota possui a prioridade mais alta. Para especificar a opção métrica, digite `- metric NÚMERO` em *Opções*. A menor métrica possível é 0. A rota com a menor métrica tem a prioridade mais alta e é usada como padrão. Se o dispositivo de rede for desconectado, sua rota será removida e o dispositivo seguinte será usado.

4. Se o sistema for um roteador, habilite *Encaminhamento IPv4* e *Encaminhamento IPv6* em *Configurações de Rede*, conforme necessário.
5. Para ativar a configuração, confirme as definições.

23.5 NetworkManager

O NetworkManager é a solução ideal para laptops e outros computadores portáteis. Com o NetworkManager, não é necessário preocupar-se em configurar interfaces de rede e alternar entre redes quando você estiver em trânsito.



Importante:

O NetworkManager é suportado apenas pelo SUSE para cargas de trabalho de desktop com SLED ou a Workstation Extension. Todas as certificações de servidor são feitas com o **wicked** como a ferramenta de configuração de rede, e o uso do NetworkManager pode invalidá-las. O NetworkManager não é suportado pelo SUSE para cargas de trabalho de servidor.

23.5.1 NetworkManager e wicked

Entretanto, como o NetworkManager não é uma solução adequada para todos os casos, você ainda pode escolher entre o método de gerenciamento de conexões de rede controlado pelo **wicked** e o NetworkManager. Para gerenciar sua conexão de rede com o NetworkManager, habilite-o no módulo Configurações de Rede do YaST, conforme descrito na [Seção 31.2, “Habilitando ou desabilitando o NetworkManager”](#), e configure suas conexões de rede com o NetworkManager. Para ver uma lista dos casos de uso e uma descrição detalhada de como configurar e usar o NetworkManager, consulte o [Capítulo 31, Usando o NetworkManager](#).

Algumas diferenças entre o wicked e o NetworkManager:

Privilégios de root

Se você usa o NetworkManager para configurar a rede, poderá alternar, parar ou iniciar com facilidade a conexão de rede, a qualquer momento, de dentro do ambiente de área de trabalho usando um applet. O NetworkManager também permite mudar e configurar conexões de placa wireless sem exigir privilégios de root. Por esse motivo, o NetworkManager é a solução ideal para uma estação de trabalho móvel.

O **wicked** também oferece algumas maneiras de alternar, parar ou iniciar a conexão com ou sem a intervenção do usuário, como os dispositivos gerenciados pelo usuário. No entanto, privilégios de root sempre são exigidos para mudar ou configurar um dispositivo de rede. Isso normalmente é um problema para a computação móvel, na qual não é possível pré-configurar todas as possibilidades de conexão.

Tipos de conexões de rede

Tanto o **wicked** quanto o NetworkManager podem gerenciar conexões de rede com uma rede wireless (com acesso WEP, WPA-PSK e WPA-Enterprise) e redes com fio usando a configuração DHCP e estática. Eles também suportam conexão por discagem e VPN. Com o NetworkManager, é possível também conectar um modem de banda larga móvel (3G) ou configurar uma conexão DSL, o que não é possível com a configuração tradicional.

O NetworkManager tenta manter o computador conectado o tempo todo usando a melhor conexão disponível. Se o cabo da rede for desconectado por acidente, ele tentará reconectar. Ele é capaz de localizar a rede que tiver a melhor intensidade de sinal na lista de conexões wireless e usá-la automaticamente para uma conexão. Para obter a mesma funcionalidade com o **wicked**, são necessárias mais configurações.

23.5.2 Funcionalidade e arquivos de configuração do NetworkManager

As configurações individuais de conexão de rede criadas com o NetworkManager são armazenadas em perfis de configuração. As conexões do *sistema* configuradas com o NetworkManager ou o YaST são gravadas em `/etc/NetworkManager/system-connections/*` ou em `/etc/sysconfig/network/ifcfg-*`. No GNOME, todas as conexões definidas pelo usuário são armazenadas no GConf.

Caso não haja nenhum perfil configurado, o NetworkManager criará um automaticamente com o nome `Auto $INTERFACE-NAME`. Isso é uma tentativa de fazer funcionar sem qualquer configuração para tantos casos quanto forem possíveis (com segurança). Se os perfis criados automaticamente não atenderem às suas necessidades, use as caixas de diálogo de configuração da conexão de rede, fornecidas pelo GNOME, para modificá-los conforme desejado. Para obter mais informações, consulte a [Seção 31.3, “Configurando conexões de rede”](#).

23.5.3 Controlando e bloqueando recursos do NetworkManager

Em máquinas administradas centralmente, determinados recursos do NetworkManager poderão ser controlados ou desabilitados com o PolKit, por exemplo, se um usuário tiver permissão para modificar as conexões definidas pelo administrador ou para definir suas próprias configurações de rede. Para ver ou mudar as respectivas políticas do NetworkManager, inicie a ferramenta gráfica *Autorizações* para o PolKit. Na árvore do lado esquerdo, elas se encontram abaixo

da entrada *network-manager-settings*. Para ver uma introdução sobre o PolKit e detalhes de como usá-lo, consulte o Livro *“Security and Hardening Guide”, Capítulo 18 “The Polkit authentication framework”*.

23.6 Configurando uma conexão de rede manualmente

A configuração manual do software de rede deve ser a última alternativa. É recomendável usar o YaST. Entretanto, essas informações de base sobre a configuração de rede também podem ajudar você na utilização do YaST.

23.6.1 Configuração de rede com **wicked**

A ferramenta e biblioteca chamada **wicked** dispõe de uma nova estrutura para configuração de rede.

Um dos desafios do gerenciamento de interface de rede tradicional é que as diferentes camadas de gerenciamento de rede são misturadas desorganizadamente em um único script ou, no máximo, em dois scripts diferentes. Esses scripts interagem entre si de maneira mal definida. Isso leva a problemas imprevisíveis, restrições e convenções obscuras etc. Várias camadas de hacks especiais para diversos cenários aumentam as despesas gerais de manutenção. Estão sendo usados protocolos de configuração de endereço que são implementados por meio de daemons como o *dhcpcd*, que pouco se interagem com o restante da infraestrutura. Esquemas de nomeação de interface ruins que exigem suporte pesado a *udev* são introduzidos para obter identificação persistente das interfaces.

A ideia do **wicked** é analisar o problema de várias maneiras. Nenhuma delas é totalmente inovadora, mas esperamos que, ao tentar reunir ideias de diferentes projetos, seja criada uma solução global melhor.

Uma abordagem é usar um modelo de cliente/servidor. Dessa forma, o **wicked** pode definir recursos padronizados para ações como configuração de endereço que se integrem bem à estrutura geral. Por exemplo, ao usar a configuração de um endereço específico, o administrador pode solicitar que uma interface seja configurada por DHCP ou IPv4 zeroconf. Nesse caso, o serviço de configuração de endereço simplesmente obtém o aluguel do servidor e o transfere para o processo do servidor **wicked**, que instala os endereços e as rotas solicitados.

A outra abordagem para analisar o problema é impor o aspecto de organização em camadas. Para qualquer tipo de interface de rede, é possível definir um serviço dbus que configure a camada do dispositivo da interface de rede: VLAN, ponte, ligação ou dispositivo paravirtualizado. Uma funcionalidade comum, como a configuração de endereço, é implementada por serviços de junção, que são colocados em camadas sobre esses serviços específicos do dispositivo, sem ter que implementá-los especificamente.

A estrutura do wicked implementa esses dois aspectos usando uma variedade de serviços dbus, que são anexados a uma interface de rede de acordo com o seu tipo. Veja a seguir uma visão geral simples da hierarquia de objeto no wicked.

Cada interface de rede é representada por um objeto filho de `/org/opensuse/Network/Interfaces`. O nome do objeto filho é dado por seu ifindex. Por exemplo, a interface de loopback, que geralmente tem ifindex 1, é `/org/opensuse/Network/Interfaces/1`, a primeira interface Ethernet registrada é `/org/opensuse/Network/Interfaces/2`.

Cada interface de rede tem uma “classe” associada, que é usada para selecionar as interfaces dbus suportadas. Por padrão, cada interface de rede pertence à classe `netif`, e o `wickedd` anexa automaticamente todas as interfaces compatíveis com essa classe. Na implementação atual, isso inclui as seguintes interfaces:

`org.opensuse.Network.Interface`

Funções de interface de rede genéricas, como mover o link para cima ou para baixo, atribuir uma MTU, etc

`org.opensuse.Network.Addrconf.ipv4.dhcp`,
`org.opensuse.Network.Addrconf.ipv6.dhcp`,
`org.opensuse.Network.Addrconf.ipv4.auto`

Serviços de configuração de endereço para DHCP, IPv4 zeroconf, etc

Além disso, as interfaces de rede podem exigir ou oferecer mecanismos de configuração especiais. Para um dispositivo Ethernet, por exemplo, você deve controlar a velocidade do link, descarregar o checksum etc. Para fazer isso, os dispositivos Ethernet têm uma classe própria chamada `netif-ethernet`, que é uma subclasse de `netif`. Como consequência, as interfaces dbus atribuídas a uma interface Ethernet incluem todos os serviços relacionados anteriormente e mais o `org.opensuse.Network.Ethernet`, um serviço disponível apenas para os objetos pertencentes à classe `netif-ethernet`.

Semelhantemente, existem classes para tipos de interface como pontes, VLANs, ligações ou infinibands.

Como você interage com uma interface do tipo da VLAN (que é realmente uma interface de rede virtual sobre um dispositivo Ethernet) que precisa ser criada pela primeira vez? Para isso, o `wicked` define interfaces de fábrica, como `org.opensuse.Network.VLAN.Factory`. Esse tipo de interface de fábrica oferece uma única função que permite criar uma interface do tipo solicitado. Essas interfaces de fábrica são anexadas ao nó da lista `/org/opensuse/Network/Interfaces`.

23.6.1.1 Arquitetura e recursos do `wicked`

O serviço `wicked` é composto por várias partes, conforme mostrado em *Figura 23.4, “Arquitetura do `wicked`”*.

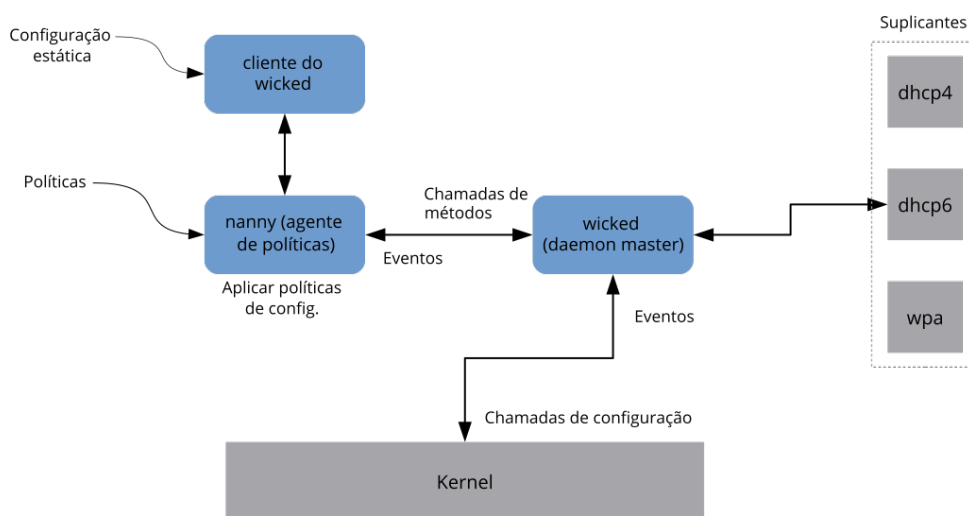


FIGURA 23.4: ARQUITETURA DO `wicked`

O `wicked` suporta o seguinte:

- Back ends de arquivo de configuração para analisar os arquivos `/etc/sysconfig/network` no estilo SUSE.
- Um back end de configuração interno para representar a configuração da interface de rede em XML.
- Ativação e encerramento de interfaces de rede “normais”, como Ethernet ou InfiniBand, VLAN, ponte, ligações, tun, tap, dummy, macvlan, macvtap, hsi, qeth, iucv e dispositivos wireless (com limite de uma rede wpa-psk/eap).
- Um cliente DHCPv4 e um cliente DHCPv6 incorporados.

- O daemon nanny (habilitado por padrão) ajuda a ativar automaticamente as interfaces configuradas quando o dispositivo está disponível (hot plug de interface) e definir a configuração de IP quando um link (operadora) é detectado. Consulte a [Seção 23.6.1.3, “Nanny”](#) para obter mais informações.
- O wicked foi implementado como um grupo de serviços DBus que estão integrados ao systemd. Dessa forma, os comandos comuns do systemctl são aplicados ao wicked.

23.6.1.2 Usando o wicked

No SUSE Linux Enterprise, o wicked é executado por padrão. Para saber o que está habilitado no momento e se está em execução, chame:

```
systemctl status network
```

Se o wicked estiver habilitado, você verá alguma indicação nestas linhas:

```
wicked.service - wicked managed network interfaces
  Loaded: loaded (/usr/lib/systemd/system/wicked.service; enabled)
  ...
```

Se algo diferente estiver em execução (por exemplo, o NetworkManager) e você quiser alterar para o wicked, primeiro interrompa o que estiver em execução e, em seguida, habilite o wicked:

```
systemctl is-active network && \
systemctl stop      network
systemctl enable --force wicked
```

Isso habilita os serviços do wicked, cria o link do alias network.service com o alias wicked.service e inicia a rede na próxima inicialização.

Iniciando o processo do servidor:

```
systemctl start wickedd
```

Esse procedimento inicia o wickedd (o servidor principal) e os suplicantes associados:

```
/usr/lib/wicked/bin/wickedd-auto4 --systemd --foreground
/usr/lib/wicked/bin/wickedd-dhcp4  --systemd --foreground
/usr/lib/wicked/bin/wickedd-dhcp6  --systemd --foreground
/usr/sbin/wickedd --systemd --foreground
/usr/sbin/wickedd-nanny --systemd --foreground
```

Em seguida, ative a rede:

```
systemctl start wicked
```

Se preferir, use o álias `network.service`:

```
systemctl start network
```

Estes comandos usam as fontes de configuraço padro ou do sistema, conforme definido em `/etc/wicked/client.xml`.

Para habilitar a depuraço, defina `WICKED_DEBUG` em `/etc/sysconfig/network/config`, por exemplo:

```
WICKED_DEBUG="all"
```

Ou para omiti-la:

```
WICKED_DEBUG="all,-dbus,-objectmodel,-xpath,-xml"
```

Use o utilitrio cliente para exibir as informaçes de todas as interfaces ou da interface especificada com `IFNAME`:

```
wicked show all  
wicked show IFNAME
```

Na sada XML:

```
wicked show-xml all  
wicked show-xml IFNAME
```

Ativando uma interface:

```
wicked ifup eth0  
wicked ifup wlan0  
...
```

Como no h nenhuma fonte de configuraço especificada, o cliente do wicked verifica suas fontes de configuraço padro definidas em `/etc/wicked/client.xml`:

1. firmware: iBFT (iSCSI Boot Firmware Table)
2. Arquivos compat: `ifcfg`, implementados para compatibilidade

O que o `wicked` obtiver destas fontes para determinada interface ser aplicado. A ordem de importncia desejada  firmware e depois compat, o que pode ser mudado no futuro.

Para obter mais informaçes, consulte a pgina de manual de wicked.

23.6.1.3 Nanny

Nanny é um daemon orientado por eventos e políticas que é responsável por cenários assíncronos ou não solicitados, como dispositivos de hot plug. Portanto, o daemon nanny ajuda a iniciar ou reiniciar dispositivos atrasados ou temporariamente ausentes. O Nanny monitora as mudanças em dispositivos e links e integra novos dispositivos definidos pelo conjunto de políticas atual. O Nanny continua a configuração, mesmo que o **ifup** já tenha saído por causa das restrições de tempo de espera especificadas.

Por padrão, o daemon nanny está ativo no sistema. Ele é habilitado no arquivo de configuração `/etc/wicked/common.xml`:

```
<config>
  ...
  <use-nanny>true</use-nanny>
</config>
```

Essa configuração faz com que o ifup e o ifreload apliquem uma política com a configuração efetiva ao daemon nanny; em seguida, o nanny configura o `wickedd` e, dessa forma, garante o suporte a hot plug. Ele aguarda por eventos ou mudanças (como novos dispositivos ou ativação de operadora) em segundo plano.

23.6.1.4 Ativando várias interfaces

Para ligações e pontes, convém definir a topologia inteira do dispositivo em um arquivo (`ifcfg-bondX`) e ativá-la de uma vez. Na sequência, o wicked poderá ativar a configuração inteira, se você especificar os nomes das interfaces de nível superior (da ponte ou da ligação):

```
wicked ifup br0
```

Esse comando configura automaticamente a ponte e suas dependências na ordem apropriada, sem a necessidade de listar as dependências (portas ou outras) separadamente.

Para ativar várias interfaces em um comando:

```
wicked ifup bond0 br0 br1 br2
```

Ou também todas as interfaces:

```
wicked ifup all
```

23.6.1.5 Usando túneis com o wicked

O `TUNNEL_DEVICE` é usado quando você precisa utilizar túneis com Wicked. Ele permite especificar um nome de dispositivo opcional para vincular o túnel ao dispositivo. Os pacotes tunneled apenas são roteados por meio desse dispositivo.

Para obter mais informações, consulte `man 5 ifcfg-tunnel`.

23.6.1.6 Processando mudanças incrementais

Com o **wicked**, não há necessidade de desativar uma interface para reconfigurá-la (exceto se exigido pelo kernel). Por exemplo, para adicionar outro endereço IP ou rota a uma interface de rede estaticamente configurada, adicione o endereço IP à definição da interface e execute outra operação “ifup”. O servidor tentará de tudo para atualizar apenas as configurações que foram mudadas. Isso vale para as opções no nível do link, como a MTU do dispositivo ou o endereço MAC, e para as configurações no nível da rede, como endereços, rotas ou até mesmo o modo de configuração de endereço (por exemplo, ao mover de uma configuração estática para DHCP).

Claro que as coisas se tornam mais complicadas quando há interfaces virtuais combinadas a vários dispositivos reais, como pontes ou ligações. Para dispositivos acoplados, é impossível mudar determinados parâmetros enquanto o dispositivo está ativado. Se você fizer isso, haverá erro.

No entanto, o que ainda deve funcionar é a adição ou remoção dos dispositivos filho de uma ligação ou ponte, ou a escolha de uma interface principal da ligação.

23.6.1.7 Extensões do wicked: configuração de endereço

O **wicked** foi desenvolvido para ser extensível com scripts shell. É possível definir as extensões no arquivo `config.xml`.

Atualmente, há várias classes de extensões suportadas:

- configuração de link: são scripts responsáveis por configurar a camada de link do dispositivo de acordo com a configuração fornecida pelo cliente e por desconfigurá-la novamente.
- configuração de endereço: são scripts responsáveis por gerenciar a configuração de endereço de um dispositivo. Geralmente, a configuração de endereço e o DHCP são gerenciados pelo próprio **wicked**, mas podem ser implementados por meio de extensões.
- extensão de firewall: estes scripts podem aplicar regras de firewall.

Normalmente, as extensões possuem um comando de início e parada, um “arquivo pid” opcional e um conjunto de variáveis de ambiente que são passadas para o script.

Para ilustrar como isso deve funcionar, observe a extensão de firewall definida em etc/server.xml:

```
<dbus-service interface="org.opensuse.Network.Firewall">
  <action name="firewallUp"    command="/etc/wicked/extensions/firewall up"/>
  <action name="firewallDown"  command="/etc/wicked/extensions/firewall down"/>

  <!-- default environment for all calls to this extension script -->
  <putenv name="WICKED_OBJECT_PATH" value="$object-path"/>
  <putenv name="WICKED_INTERFACE_NAME" value="$property:name"/>
  <putenv name="WICKED_INTERFACE_INDEX" value="$property:index"/>
</dbus-service>
```

A extensão está anexada à tag <dbus-service> e define os comandos que serão executados para as ações dessa interface. Além disso, a declaração pode definir e inicializar as variáveis de ambiente passadas para as ações.

23.6.1.8 Extensões do wicked: arquivos de configuração

É possível estender a administração de arquivos de configuração também com scripts. Por exemplo, as atualizações DNS dos aluguéis são definitivamente administradas pelo script extensions/resolver, com o comportamento configurado em server.xml:

```
<system-updater name="resolver">
  <action name="backup"    command="/etc/wicked/extensions/resolver backup"/>
  <action name="restore"   command="/etc/wicked/extensions/resolver restore"/>
  <action name="install"   command="/etc/wicked/extensions/resolver install"/>
</system-updater>
```

```
<action name="remove" command="/etc/wicked/extensions/resolver remove"/>
</system-updater>
```

Quando uma atualização chega ao `wickedd`, as rotinas do atualizador do sistema analisam o aluguel e chamam os comandos apropriados (`backup`, `install` etc.) no script do resolver. Isso, por sua vez, define as configurações de DNS usando `/sbin/netconfig` ou manualmente, gravando `/run/netconfig/resolv.conf` como fallback.

23.6.2 Arquivos de configuração

Esta seção fornece uma visão geral dos arquivos de configuração de rede e explica sua finalidade e formato usado.

23.6.2.1 `/etc/wicked/common.xml`

O arquivo `/etc/wicked/common.xml` inclui definições comuns que devem ser usadas por todos os aplicativos. Ele é originado/incluído por outros arquivos de configuração nesse diretório. Embora você possa usar esse arquivo para habilitar a depuração em todos os componentes do `wicked`, recomendamos usar o arquivo `/etc/wicked/local.xml` para essa finalidade. Você poderá perder suas mudanças após a aplicação de atualizações de manutenção, pois o `/etc/wicked/common.xml` talvez seja sobregravado. O arquivo `/etc/wicked/common.xml` inclui o `/etc/wicked/local.xml` na instalação padrão, portanto, você normalmente não precisa modificar o `/etc/wicked/common.xml`.

Para desabilitar o `nanny` definindo `<use-nanny>` como `false`, reinicie o `wickedd.service` e execute o seguinte comando para aplicar todas as configurações e políticas:

```
> sudo wicked ifup all
```



Nota: Arquivos de configuração

Os programas `wickedd`, `wicked` ou `nanny` tentarão ler o `/etc/wicked/common.xml` se não tiverem seu próprio arquivo de configuração.

23.6.2.2 `/etc/wicked/server.xml`

O arquivo `/etc/wicked/server.xml` é lido pelo processo de servidor `wickedd` na inicialização. O arquivo armazena as extensões no `/etc/wicked/common.xml`. Além do mais, esse arquivo configura a manipulação de um resolver e o recebimento de informações dos suplicantes `addrconf`, por exemplo, DHCP.

É recomendável adicionar as mudanças necessárias nesse arquivo a um arquivo `/etc/wicked/server-local.xml` separado, que é incluído por `/etc/wicked/server.xml`. Usando um arquivo separado, você evita sobregravar as mudanças feitas durante as atualizações de manutenção.

23.6.2.3 `/etc/wicked/client.xml`

O `/etc/wicked/client.xml` é usado pelo comando `wicked`. O arquivo especifica o local de um script usado durante a descoberta de dispositivos gerenciados pelo `ibft` e define os locais das configurações de interface de rede.

É recomendável adicionar as mudanças necessárias nesse arquivo a um arquivo `/etc/wicked/client-local.xml` separado, que é incluído por `/etc/wicked/server.xml`. Usando um arquivo separado, você evita sobregravar as mudanças feitas durante as atualizações de manutenção.

23.6.2.4 `/etc/wicked/nanny.xml`

O `/etc/wicked/nanny.xml` configura tipos de camadas de link. É recomendável adicionar a configuração específica a um arquivo `/etc/wicked/nanny-local.xml` separado para evitar perda das mudanças durante as atualizações de manutenção.

23.6.2.5 `/etc/sysconfig/network/ifcfg-*`

Estes arquivos contêm as configurações tradicionais das interfaces de rede.



Nota: **wicked** e os arquivos `ifcfg-*`

O **wicked** lerá esses arquivos se você especificar o prefixo `compat:`. De acordo com a configuração padrão do SUSE Linux Enterprise Desktop no `/etc/wicked/client.xml`, o **wicked** testa esses arquivos antes dos arquivos de configuração XML em `/etc/wicked/ifconfig`.

O switch `--ifconfig` é fornecido sobretudo para fins de teste. Se especificado, as fontes de configuração padrão definidas em `/etc/wicked/ifconfig` não serão aplicadas.

Os arquivos `ifcfg-*` incluem informações, como o modo de início e o endereço IP. Os parâmetros possíveis são descritos na página de manual de `ifup`. Além disso, a maioria das variáveis dos arquivos `dhcp` e `wireless` poderá ser usada nos arquivos `ifcfg-*` se uma configuração geral for usada para apenas uma interface. Entretanto, a maioria das variáveis de `/etc/sysconfig/network/config` é global e não pode ser anulada nos arquivos `ifcfg`. Por exemplo, as variáveis `NETCONFIG_*` são globais.

Para configurar as interfaces `macvlan` e `macvtap`, consulte as páginas de manual de `ifcfg-macvlan` e `ifcfg-macvtap`. Por exemplo, para a interface `macvlan`, insira `ifcfg-macvlan0` com as seguintes configurações:

```
STARTMODE='auto'
MACVLAN_DEVICE='eth0'
#MACVLAN_MODE='vepa'
#LLADDR=02:03:04:05:06:aa
```

Para saber sobre o `ifcfg.template`, consulte [Seção 23.6.2.6, “/etc/sysconfig/network/config, /etc/sysconfig/network/dhcp e /etc/sysconfig/network/wireless”](#).

23.6.2.6 `/etc/sysconfig/network/config, /etc/sysconfig/network/dhcp e /etc/sysconfig/network/wireless`

O arquivo `config` contém configurações gerais para o comportamento de `ifup`, `ifdown` e `ifstatus`. O `dhcp` contém configurações para DHCP, e o `wireless` para placas LAN wireless. Nos três arquivos de configuração, as variáveis estão em forma de comentário. Algumas variáveis de `/etc/sysconfig/network/config` também podem ser usadas nos arquivos `ifcfg-*`, nos quais recebem prioridade mais alta. O arquivo `/etc/sysconfig/network/ifcfg.template` lista as variáveis que podem ser especificadas para cada interface. Entretanto, a maioria das variáveis de `/etc/sysconfig/network/config` é global e não pode ser anulada em arquivos `ifcfg`. Por exemplo, as variáveis `NETWORKMANAGER` ou `NETCONFIG_*` são globais.



Nota: Usando o DHCPv6

No SUSE Linux Enterprise 11, o DHCPv6 costumava funcionar mesmo nas redes em que os RAs (Router Advertisements – Anúncios de Roteador) IPv6 não estavam configurados apropriadamente. A partir do SUSE Linux Enterprise 12, o DHCPv6 exige que pelo menos um dos roteadores na rede envie RAs indicando que a rede é gerenciada por DHCPv6.

Para as redes nas quais o roteador não pode ser configurado corretamente, a opção `ifcfg` permite ao usuário anular esse comportamento especificando `DHCLIENT6_MODE='managed'` no arquivo `ifcfg`. É possível também ativar essa correção alternativa com um parâmetro de boot no sistema de instalação:

```
ifcfg=eth0=dhcp6,DHCLIENT6_MODE=managed
```

23.6.2.7 `/etc/sysconfig/network/routes` e `/etc/sysconfig/network/ifroute-*`

O roteamento estático dos pacotes TCP/IP é determinado pelos arquivos `/etc/sysconfig/network/routes` e `/etc/sysconfig/network/ifroute-*`. Todas as rotas estáticas exigidas pelas várias tarefas do sistema podem ser especificadas em `/etc/sysconfig/network/routes`: rotas para um host, rotas para um host via gateway e rotas para uma rede. Para cada interface que precisa de roteamento individual, defina um arquivo de configuração adicional: `/etc/sysconfig/network/ifroute-*`. Substitua o curinga (*) pelo nome da interface. As entradas nos arquivos de configuração de roteamento terão esta aparência:

#	Destination	Gateway	Netmask	Interface	Options
---	-------------	---------	---------	-----------	---------

O destino da rota está na primeira coluna. Essa coluna pode conter o endereço IP de uma rede ou host ou, no caso de servidores de nomes *acessíveis*, o nome completo da rede ou do host. A rede deve ser gravada em notação CIDR (endereço com o comprimento do prefixo de roteamento associado), como 10.10.0.0/16 para rotas IPv4 ou fc00::/7 para rotas IPv6. A palavra-chave `default` indica que a rota é o gateway padrão na mesma família de endereços do gateway. Para dispositivos sem gateway, use destinos explícitos 0.0.0.0/0 ou ::/0.

A segunda coluna contém o gateway padrão ou um gateway por meio do qual um host ou uma rede podem ser acessados.

A terceira coluna foi descontinuada; ela antes incluía a máscara de rede IPv4 do destino. Para rotas IPv6, rota padrão ou ao usar o comprimento do prefixo (notação CIDR) na primeira coluna, digite um traço (-) aqui.

A quarta coluna contém o nome da interface. Se você a deixar vazia usando um traço (-), poderá provocar um comportamento não intencional em `/etc/sysconfig/network/routes`. Para obter mais informações, consulte a página de manual de `routes`.

Uma quinta coluna (opcional) pode ser usada para inserir opções especiais. Para obter detalhes, consulte a página de manual de `routes`.

EXEMPLO 23.5: INTERFACES DE REDE COMUNS E ALGUMAS ROTAS ESTÁTICAS

```
# --- IPv4 routes in CIDR prefix notation:
# Destination      [Gateway]      -      Interface
127.0.0.0/8        -              -      lo
204.127.235.0/24   -              -      eth0
default            204.127.235.41 -      eth0
207.68.156.51/32   207.68.145.45 -      eth1
192.168.0.0/16     207.68.156.51 -      eth1

# --- IPv4 routes in deprecated netmask notation"
# Destination      [Dummy/Gateway]  Netmask      Interface
#
127.0.0.0          0.0.0.0          255.255.255.0 lo
204.127.235.0      0.0.0.0          255.255.255.0 eth0
default            204.127.235.41   0.0.0.0      eth0
207.68.156.51      207.68.145.45    255.255.255.255 eth1
192.168.0.0        207.68.156.51    255.255.0.0   eth1

# --- IPv6 routes are always using CIDR notation:
# Destination      [Gateway]      -      Interface
2001:DB8:100::/64 -              -      eth0
2001:DB8:100::/32 fe80::216:3eff:fe6d:c042 -      eth0
```

23.6.2.8 `/var/run/netconfig/resolv.conf`

O domínio ao qual o host pertence está especificado em `/var/run/netconfig/resolv.conf` (palavra-chave `search`). É possível especificar até seis domínios com um total de 256 caracteres com a opção `search`. Durante a resolução de um nome incompleto, uma tentativa de gerar um nome será feita anexando as entradas de `search` individuais. É possível especificar até três

servidores de nomes com a opção `nameserver`, cada um em sua própria linha. Os comentários são precedidos por cerquilha ou ponto-e-vírgula (`#` ou `;`). Como um exemplo, consulte o [Exemplo 23.6, “/var/run/netconfig/resolv.conf”](#).

Entretanto, o `/etc/resolv.conf` não deve ser editado manualmente. Ele será gerado pelo script **netconfig** e é um link simbólico para `/run/netconfig/resolv.conf`. Para definir configurações DNS estáticas sem usar o YaST, edite as variáveis apropriadas manualmente no arquivo `/etc/sysconfig/network/config`:

NETCONFIG_DNS_STATIC_SEARCHLIST

lista de nomes de domínios DNS usados para pesquisa de nomes de host

NETCONFIG_DNS_STATIC_SERVERS

lista de endereços IP de servidor de nomes usados para pesquisa de nomes de host

NETCONFIG_DNS_FORWARDER

o nome do encaminhador de DNS que precisa ser configurado, por exemplo `bind` ou `resolver`

NETCONFIG_DNS_RESOLVER_OPTIONS

opções arbitrárias que serão gravadas em `/var/run/netconfig/resolv.conf`, por exemplo:

```
debug attempts:1 timeout:10
```

Para obter mais informações, consulte a página de manual de `resolv.conf`.

NETCONFIG_DNS_RESOLVER_SORTLIST

lista com até 10 itens, por exemplo:

```
130.155.160.0/255.255.240.0 130.155.0.0
```

Para obter mais informações, consulte a página de manual de `resolv.conf`.

Para desabilitar a configuração do DNS usando o `netconfig`, defina `NETCONFIG_DNS_POLICY=''`. Para obter mais informações sobre o **netconfig**, consulte a página de manual do `netconfig(8)` (**man 8 netconfig**).

EXEMPLO 23.6: `/var/run/netconfig/resolv.conf`

```
# Our domain
search example.com
#
# We use dns.example.com (192.168.1.116) as nameserver
nameserver 192.168.1.116
```

23.6.2.9 /sbin/netconfig

O **netconfig** é uma ferramenta modular destinada a gerenciar configurações de rede adicionais. Ele funde as configurações definidas estaticamente com as configurações fornecidas pelos mecanismos de configuração automática, como DHCP ou PPP, de acordo com uma política predefinida. As mudanças necessárias são aplicadas ao sistema chamando-se os módulos do netconfig responsáveis pela modificação de um arquivo de configuração e pela reinicialização de um serviço ou uma ação semelhante.

O **netconfig** reconhece três ações principais. Os comandos **netconfig modify** e **netconfig remove** são usados por daemons, como DHCP ou PPP, para fornecer ou remover configurações do netconfig. Apenas o comando **netconfig update** está disponível para o usuário:

modify

O comando **netconfig modify** modifica as configurações dinâmicas específicas de interface e serviço, além de atualizar a configuração da rede. O netconfig lê as configurações da entrada padrão ou de um arquivo especificado pela opção **--lease-file NOME_DE_ARQUIVO** e as armazena internamente até a próxima reinicialização do sistema (ou a próxima ação modify ou remove). As configurações que já existirem para a mesma combinação de interface e serviço serão sobregravadas. A interface é especificada pelo parâmetro **-i NOME_DA_INTERFACE**. O serviço é especificado pelo parâmetro **-s NOME_DO_SERVIÇO**.

remove

O comando **netconfig remove** remove as configurações dinâmicas fornecidas por uma ação de edição para a combinação de interface e serviço especificada e atualiza a configuração da rede. A interface é especificada pelo parâmetro **-i NOME_DA_INTERFACE**. O serviço é especificado pelo parâmetro **-s NOME_DO_SERVIÇO**.

update

O comando **netconfig update** atualiza a configuração da rede usando as configurações atuais. Isso é útil quando a política ou a configuração estática é mudada. Use o parâmetro **-m TIPO_DE_MÓDULO** para atualizar apenas um serviço especificado (**dns**, **nis** ou **ntp**).

A política do netconfig e as configurações estáticas são definidas manualmente ou por meio do YaST no arquivo **/etc/sysconfig/network/config**. As configurações dinâmicas fornecidas pelas ferramentas de configuração automática, como DHCP ou PPP, são entregues diretamente por essas ferramentas com as ações **netconfig modify** e **netconfig remove**. Quando o NetworkManager está habilitado, o netconfig (no modo de política **auto**) usa apenas as

configurações do NetworkManager, ignorando as configurações de qualquer outra interface configurada pelo método tradicional ifup. Se o NetworkManager não fornecer nenhuma configuração, as configurações estáticas serão usadas como fallback. Não há suporte para a utilização mista do NetworkManager nem para o método wicked.

Para obter mais informações sobre o netconfig, consulte man 8 netconfig.

23.6.2.10 /etc/hosts

Neste arquivo, mostrado em *Exemplo 23.7, “/etc/hosts”*, os endereços IP foram atribuídos a nomes de host. Se nenhum servidor de nomes for implementado, todos os hosts nos quais uma conexão IP for configurada precisarão ser listados aqui. Para cada host, digite uma linha no arquivo com o endereço IP, o nome completo do host e o nome de host. O endereço IP precisa estar no início da linha e as entradas separadas por espaços vazios e guias. Comentários são sempre precedidos pelo sinal #.

EXEMPLO 23.7: /etc/hosts

```
127.0.0.1 localhost
192.168.2.100 jupiter.example.com jupiter
192.168.2.101 venus.example.com venus
```

23.6.2.11 /etc/networks

Aqui, os nomes de rede são convertidos em endereços de rede. O formato é semelhante ao do arquivo hosts, exceto que os nomes de rede precedem os endereços. Consulte a *Exemplo 23.8, “/etc/networks”*.

EXEMPLO 23.8: /etc/networks

```
loopback    127.0.0.0
localnet    192.168.0.0
```

23.6.2.12 /etc/host.conf

Resolução de nomes — a conversão de nomes de host e de rede através da biblioteca *resolver* é controlada por esse arquivo. Esse arquivo é usado somente para programas vinculados a libc4 ou libc5. Para programas glibc atuais, consulte as configurações em /etc/nsswitch.conf. Cada

parâmetro deve ser sempre digitado em uma linha separada. Os comentários são precedidos pelo sinal `#`. [Tabela 23.2, “Parâmetros para `/etc/host.conf`”](#) mostra os parâmetros disponíveis. Uma amostra de `/etc/host.conf` é mostrada no [Exemplo 23.9, “`/etc/host.conf`”](#).

TABELA 23.2: PARÂMETROS PARA `/ETC/HOST.CONF`

<code>order hosts, bind</code>	Especifica em que ordem os serviços são acessados para a resolução de nomes. Os argumentos disponíveis são (separados por espaços vazios ou vírgulas):
	<code>hosts</code> : pesquisa o arquivo <code>/etc/hosts</code>
	<code>bind</code> : acessa um servidor de nomes
	<code>nis</code> : usa o NIS
<code>multi on/off</code>	Define se um host digitado em <code>/etc/hosts</code> pode ter vários endereços IP.
<code>nospoof on spoofalert on/off</code>	Esses parâmetros influenciam o <code>spoof</code> do servidor de nomes, mas não exercem qualquer influência na configuração da rede.
<code>trim domainname</code>	O nome de domínio especificado será separado do nome de host após a resolução de nome de host (desde que o nome de host inclua o nome de domínio). Essa opção é útil apenas quando os nomes do domínio local estão no arquivo <code>/etc/hosts</code> , mas ainda devem ser reconhecidos com os nomes de domínio anexados.

EXEMPLO 23.9: `/etc/host.conf`

```
# We have named running
order hosts bind
# Allow multiple address
multi on
```

23.6.2.13 `/etc/nsswitch.conf`

O lançamento do GNU C Library 2.0 foi acompanhado pelo lançamento do NSS (Name Service Switch). Consulte a página de manual do `nsswitch.conf(5)` e o *The GNU C Library Reference Manual* (Manual de Referência da Biblioteca GNU C) para obter mais detalhes.

A ordem das consultas é definida no arquivo `/etc/nsswitch.conf`. Uma amostra do `nsswitch.conf` é mostrada no *Exemplo 23.10, “/etc/nsswitch.conf”*. Comentários são precedidos pelo sinal `#`. Nesse exemplo, a entrada no banco de dados `hosts` significa que uma solicitação foi enviada para `/etc/hosts` (*arquivos*) através do DNS.

EXEMPLO 23.10: `/etc/nsswitch.conf`

```
passwd:    compat
group:     compat

hosts:     files dns
networks:  files dns

services:  db files
protocols: db files
rpc:       files
ethers:    files
netmasks: files
netgroup:  files nis
publickey: files

bootparams: files
automount:  files nis
aliases:    files nis
shadow:     compat
```

Os “bancos de dados” disponíveis em NSS estão listados na *Tabela 23.3, “Bancos de dados disponíveis por `/etc/nsswitch.conf`”*. As opções de configuração para bancos de dados NSS estão listadas na *Tabela 23.4, “Opções de configuração para “bancos de dados” NSS”*.

TABELA 23.3: BANCOS DE DADOS DISPONÍVEIS POR `/ETC/NSSWITCH.CONF`

<u>aliases</u>	Álias de correio implementados por <code>sendmail</code> ; consulte <code>man 5 aliases</code> .
<u>ethers</u>	Endereços de Ethernet.
<u>netmasks</u>	Lista de redes e suas máscaras de sub-rede. Apenas necessário quando se usa sub-redes.

<u>group</u>	Grupos de usuários utilizados por <u>getgrent</u> . Consulte também a página de manual para <u>group</u> .
<u>hosts</u>	Nomes de host e endereços IP usados por <u>gethostbyname</u> e funções similares.
<u>netgroup</u>	Listas de usuários e hosts válidos na rede para controlar permissões de acesso. Consulte a página de manual do <u>netgroup(5)</u> .
<u>networks</u>	Nomes e endereços de redes, usados por <u>getnetent</u> .
<u>publickey</u>	Chaves públicas e secretas de Secure_RPC usadas pelo NFS e NIS+.
<u>passwd</u>	Senhas de usuários usadas por <u>getpwent</u> . Consulte a página de manual do <u>passwd(5)</u> .
<u>protocols</u>	Protocolos de rede usados por <u>getprotoent</u> . Consulte a página de manual do <u>protocols(5)</u> .
<u>rpc</u>	Nomes e endereços de RPC (Remote Procedure Call) usados por <u>getrpcbyname</u> e funções similares.
<u>serviços</u>	Serviços de rede, usados por <u>getservent</u> .
<u>shadow</u>	Senhas transitórias de usuários, usadas por <u>getspnam</u> ; consulte a página de manual do <u>shadow(5)</u> .

TABELA 23.4: OPÇÕES DE CONFIGURAÇÃO PARA “BANCOS DE DADOS” NSS

<u>files</u>	arquivos de acesso direto, por exemplo, <u>/etc/aliases</u>
--------------	---

<u>db</u>	acesso através de um banco de dados
<u>nis</u> , <u>nisplus</u>	NIS, consulte também o <i>Livro "Security and Hardening Guide", Capítulo 3 "Using NIS"</i>
<u>dns</u>	só pode ser usada como extensão de <u>hosts</u> e <u>networks</u>
<u>compat</u>	só pode ser usada como extensão de <u>passwd</u> , <u>shadow</u> e <u>group</u>

23.6.2.14 `/etc/nscd.conf`

Esse arquivo é usado para configurar o `nscd` (name service cache daemon). Consulte as páginas de manual de `nscd(8)` e `nscd.conf(5)`. Por padrão, as entradas do sistema de `passwd`, `groups` e `hosts` são armazenadas em cache pelo `nscd`. Isso é importante para o desempenho dos serviços de diretório, como NIS e LDAP; pois, do contrário, a conexão de rede precisará ser usada para todo acesso a nomes, grupos ou hosts.

Se o armazenamento em cache de `passwd` estiver ativado, normalmente levará quinze segundos para que um usuário local recentemente adicionado seja reconhecido. Reduza este tempo de espera reiniciando o `nscd` com:

```
> sudo systemctl restart nscd
```

23.6.2.15 `/etc/HOSTNAME`

`/etc/HOSTNAME` contém o FQHN (fully qualified host name – nome completo do host). O nome completo do host é o nome de host com o nome de domínio anexado. Este arquivo deve incluir apenas uma linha (na qual o nome de host é definido). Ele é lido durante a inicialização da máquina.

23.6.3 Testando a configuração

Antes de gravar sua configuração nos arquivos de configuração, você pode testá-la. Para definir uma configuração de teste, use o comando `ip`. Para testar a conexão, use o comando `ping`.

O comando **ip** muda a configuração de rede diretamente, sem gravá-la no arquivo de configuração. A menos que você insira a configuração nos arquivos de configuração corretos, a configuração de rede mudada será perdida na reinicialização.



Nota: **ifconfig** e **route** são obsoletos

As ferramentas **ifconfig** e **route** estão obsoletas. Em vez disso, use **ip**. O **ifconfig**, por exemplo, limita os nomes de interface a 9 caracteres.

23.6.3.1 Configurando uma interface de rede com **ip**

ip é uma ferramenta para mostrar e configurar dispositivos de rede, roteamentos, roteamento de políticas e túneis.

ip é uma ferramenta muito complexa. Sua sintaxe comum é **ip** *OPÇÕES* *OBJETO* *COMANDO*. Você pode trabalhar com os seguintes objetos:

link

Este objeto representa um dispositivo de rede.

address

Este objeto representa o endereço IP do dispositivo.

neighbor

Este objeto representa uma entrada de cache ARP ou NDISC.

route

Este objeto representa a entrada da tabela de roteamento.

rule

Este objeto representa uma regra no banco de dados de políticas de roteamento.

maddress

Este objeto representa um endereço multicast.

mroute

Este objeto representa uma entrada de cache de roteamento multicast.

tunnel

Este objeto representa um túnel sobre IP.

Se nenhum comando for fornecido, será usado o comando padrão (normalmente **list**).

Mude o estado de um dispositivo com o comando:

```
> sudo ip link set DEV_NAME
```

Por exemplo, para desativar o dispositivo , digite eth0

```
> sudo ip link set eth0 down
```

Para ativá-lo novamente, use

```
> sudo ip link set eth0 up
```



Dica: Desconectando o dispositivo NIC

Se você desativar um dispositivo com

```
> sudo ip link set DEV_NAME down
```

a interface de rede será desabilitada no nível do software.

Para simular a perda do link como se o cabo Ethernet estivesse desconectado ou o switch conectado estivesse desligado, execute

```
> sudo ip link set DEV_NAME carrier off
```

Por exemplo, enquanto `ip link set DEV_NAME down` descarta todas as rotas que usam `DEV_NAME`, `ip link set DEV carrier off` não. Saiba que `carrier off` requer suporte do driver do dispositivo de rede.

Para reconectar o dispositivo à rede física, execute

```
> sudo ip link set DEV_NAME carrier on
```

Após ativar um dispositivo, você poderá configurá-lo. Para definir o endereço IP, use

```
> sudo ip addr add IP_ADDRESS + dev DEV_NAME
```

Por exemplo, para definir o endereço da interface eth0 como 192.168.12.154/30 com o broadcast padrão (opção `brd`), digite

```
> sudo ip addr add 192.168.12.154/30 brd + dev eth0
```

Para ter uma conexão ativa, você também precisa configurar o gateway padrão. Para definir um gateway para seu sistema, digite

```
> sudo ip route add default via gateway_ip_address
```

Para exibir todos os dispositivos, use

```
> sudo ip link ls
```

Para exibir apenas as interfaces em execução, use

```
> sudo ip link ls up
```

Para imprimir as estatísticas de interface de um dispositivo, digite

```
> sudo ip -s link ls DEV_NAME
```

Para ver mais informações úteis, especificamente sobre dispositivos de rede virtuais, digite

```
> sudo ip -d link ls DEV_NAME
```

Além disso, para ver os endereços de camada de rede (IPv4, IPv6) dos dispositivos, digite

```
> sudo ip addr
```

Na saída, você pode encontrar informações sobre os endereços MAC dos dispositivos. Para mostrar todas as rotas, use

```
> sudo ip route show
```

Para obter mais informações sobre como usar o **ip**, digite **ip help** ou consulte a página de manual **man 8 ip**. A opção **help** também está disponível para todos os subcomandos **ip**, como:

```
> sudo ip addr help
```

Encontre o manual do **ip** em </usr/share/doc/packages/iproute2/ip-cref.pdf>.

23.6.3.2 Testando uma conexão com o comando ping

O comando **ping** é a ferramenta padrão para testar o funcionamento de uma conexão TCP/IP. Ele usa o protocolo ICMP para enviar um pequeno pacote de dados, o datagrama ECHO_REQUEST, para o host de destino, solicitando uma resposta imediata. Se isso funcionar, o **ping** exibirá uma mensagem nesse sentido. Isso indica que o link da rede está funcionando.

O **ping** vai além de simplesmente testar a função da conexão entre dois computadores; ele também fornece algumas informações básicas sobre a qualidade da conexão. No *Exemplo 23.11, “Saída do comando ping”*, você pode ver um exemplo da saída do **ping**. A penúltima linha contém informações sobre o número de pacotes transmitidos, o número de pacotes perdidos e o tempo total da execução do **ping**.

Como destino, é possível usar um nome de host ou endereço IP, por exemplo, **ping** example.com ou **ping** 192.168.3.100. O programa enviará pacotes até que você pressione **Ctrl-C**.

Se você só precisar verificar a funcionalidade da conexão, poderá limitar o número dos pacotes com a opção **-c**. Por exemplo, para limitar o ping a três pacotes, digite **ping -c 3** example.com.

EXEMPLO 23.11: SAÍDA DO COMANDO PING

```
ping -c 3 example.com
PING example.com (192.168.3.100) 56(84) bytes of data.
64 bytes from example.com (192.168.3.100): icmp_seq=1 ttl=49 time=188 ms
64 bytes from example.com (192.168.3.100): icmp_seq=2 ttl=49 time=184 ms
64 bytes from example.com (192.168.3.100): icmp_seq=3 ttl=49 time=183 ms
--- example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 183.417/185.447/188.259/2.052 ms
```

O intervalo padrão entre dois pacotes é um segundo. Para mudar o intervalo, o ping fornece a opção **-i**. Por exemplo, para aumentar o intervalo do ping para dez segundos, digite **ping -i 10** example.com.

Em um sistema com vários dispositivos de rede, às vezes é útil enviar o ping através de um endereço de interface específico. Para isso, use a opção **-I** com o nome do dispositivo selecionado, por exemplo, **ping -I wlan1** example.com.

Para obter mais opções e informações sobre como usar o ping, digite **ping -h** ou consulte a página de manual do ping (8).



Dica: Executando ping de endereços IPv6

Para endereços IPv6, use o comando **ping6**. Observe que, para executar ping em endereços locais de link, deve-se especificar a interface com **-I**. O comando a seguir funcionará se o endereço for acessível via eth1:

```
ping6 -I eth1 fe80::117:21ff:feda:a425
```

23.6.4 Arquivos unit e scripts de inicialização

Além dos arquivos de configuração descritos anteriormente, há os arquivos unit do systemd e vários scripts que carregam os serviços de rede durante a inicialização da máquina. Eles são iniciados quando o sistema é alternado para o destino `multi-user.target`. Alguns desses arquivos unit e scripts estão descritos em *Alguns arquivos unit e scripts de inicialização para programas de rede*. Para obter mais informações sobre o `systemd`, consulte o *Capítulo 19, Daemon systemd*, e para obter mais informações sobre os destinos do `systemd`, consulte a página de manual do `systemd.special` (`man systemd.special`).

ALGUNS ARQUIVOS UNIT E SCRIPTS DE INICIALIZAÇÃO PARA PROGRAMAS DE REDE

`network.target`

`network.target` é o destino do systemd para projeto de rede, mas seu significado depende das configurações fornecidas pelo administrador do sistema.

Para obter mais informações, consulte o <http://www.freedesktop.org/wiki/Software/systemd/NetworkTarget/>.

`multi-user.target`

`multi-user.target` é o destino do systemd para um sistema multiusuário com todos os serviços de rede necessários.

`rpcbind`

Inicia o utilitário `rpcbind`, que converte os números de programa RPC em endereços universais. Necessário para os serviços RPC, como um servidor NFS.

`ypserv`

Inicia o servidor NIS.

`ypbind`

Inicia o cliente NIS.

`/etc/init.d/nfsserver`

Inicia o servidor NFS.

`/etc/init.d/postfix`

Controla o processo de postfix.

23.7 Configurando dispositivos de ligação

Em alguns sistemas, existe a necessidade de implementar conexões de rede compatíveis com outros requisitos além dos padrões de disponibilidade ou segurança de dados de um dispositivo Ethernet comum. Nesses casos, vários dispositivos Ethernet podem ser agregados a um único dispositivo de ligação.

A configuração do dispositivo de ligação é feita através das opções dos módulos de ligação. O comportamento é afetado principalmente pelo modo do dispositivo de ligação. Por padrão, o modo é `active-backup`, o que significa que uma porta de ligação diferente se tornará ativa se houver falha na porta ativa. Os seguintes modos de ligação estão disponíveis:

0 (balance-rr)

Os pacotes são transmitidos em round-robin da primeira para a última interface disponível. Fornece tolerância a falhas e equilíbrio de carga.

1 (active-backup)

Apenas uma interface de rede está ativa. Se ela falhar, uma interface diferente se tornará ativa. Essa é a configuração padrão para o SUSE Linux Enterprise Desktop. Fornece tolerância a falhas.

2 (balance-xor)

O tráfego é dividido entre todas as interfaces disponíveis com base no número de dispositivos incluídos na ligação. Esse procedimento requer suporte do switch. Fornece tolerância a falhas e equilíbrio de carga.

3 (broadcast)

Todo o tráfego é transmitido em todas as interfaces. Requer suporte do switch. Fornece tolerância a falhas.

4 (802.3ad)

Agrega as interfaces em grupos que compartilham as mesmas configurações de velocidade e duplex. Requer suporte a `ethtool` nos drivers de interface e um switch com suporte e configuração para Agregação de link dinâmico IEEE 802.3ad. Fornece tolerância a falhas e equilíbrio de carga.

5 (balance-tlb)

Equilíbrio de carga de transmissão adaptativa. Requer suporte a `ethtool` nos drivers de interface, mas não suporte a switch. Fornece tolerância a falhas e equilíbrio de carga.

6 (balance-alb)

Equilíbrio de carga adaptativo. Requer suporte a **ethtool** nos drivers de interface, mas não suporte a switch. Fornece tolerância a falhas e equilíbrio de carga.

Para obter uma descrição mais detalhada dos modos, consulte <https://www.kernel.org/doc/Documentation/networking/bonding.txt>.



Dica: Ligação e Xen

O uso de dispositivos de ligação só é interessante para máquinas que tenham várias placas de rede reais disponíveis. Na maioria das configurações, isso significa que você deve usar a configuração de ligação apenas no Dom0. Somente se você tiver várias placas de rede atribuídas a um sistema Convidado VM é que também poderá ser útil configurar a ligação em um Convidado VM.



Nota: IBM POWER: Modos de ligação 5 e 6 (balance-tlb/balance-alb) não suportados pelo ibmveth

Há um conflito com a configuração de ligação tlb/alb e o firmware do Power. Em resumo, o driver de ligação no modo tlb/alb envia pacotes de Loopback Ethernet com os dois endereços MAC de origem e destino listados como o endereço MAC Ethernet Virtual. Esses pacotes não são suportados pelo firmware do Power. Portanto, os modos de ligação 5 e 6 não são suportados pelo ibmveth.

Para configurar um dispositivo de ligação, siga este procedimento:

1. Execute *YaST* > *Sistema* > *Configurações de Rede*.
2. Use *Adicionar* e mude o *Tipo de Dispositivo* para *Ligação*. Continue com *Próximo*.

3. Escolha como vai atribuir o endereço IP ao dispositivo de ligação. Há três métodos à sua disposição:

- Nenhum Endereço IP
- Endereço Dinâmico (com DHCP ou Zeroconf)
- Endereço IP atribuído estaticamente

Use o método mais apropriado ao seu ambiente.

4. Na guia *Portas de ligação*, selecione os dispositivos Ethernet que devem ser incluídos na ligação ativando as caixas de seleção relacionadas.
5. Edite as *Opções do Driver de Vinculação* e escolha um modo de ligação.
6. Verifique se o parâmetro `miimon=100` foi adicionado às *Opções do Driver de Vinculação*. Sem esse parâmetro, a integridade dos dados não é verificada regularmente.
7. Clique em *Avançar* e saia do YaST clicando em *OK* para criar o dispositivo.

23.7.1 Hotplug de portas de ligação

Em ambientes de rede específicos (como os de Alta Disponibilidade), há casos em que você precisa substituir uma interface de porta de ligação por outra. O motivo pode ser uma falha constante no dispositivo de rede. A solução é configurar o hotplug das portas de ligação.

A ligação é configurada como de costume (de acordo com [man 5 ifcfg-bonding](#)), por exemplo:

```
ifcfg-bond0
    STARTMODE='auto' # or 'onboot'
    BOOTPROTO='static'
    IPADDR='192.168.0.1/24'
    BONDING_MASTER='yes'
    BONDING_SLAVE_0='eth0'
    BONDING_SLAVE_1='eth1'
    BONDING_MODULE_OPTS='mode=active-backup miimon=100'
```

As portas de ligação são especificadas com [STARTMODE=hotplug](#) e [BOOTPROTO=none](#):

```
ifcfg-eth0
    STARTMODE='hotplug'
    BOOTPROTO='none'

ifcfg-eth1
    STARTMODE='hotplug'
    BOOTPROTO='none'
```

[BOOTPROTO=none](#) usa as opções de `ethtool` (quando fornecidas), mas não define o link ativo no **ifup eth0**. O motivo é que a interface da porta de ligação é controlada pelo dispositivo de ligação.

[STARTMODE=hotplug](#) faz com que a interface da porta de ligação se una à ligação automaticamente quando ela estiver disponível.

As regras do `udev` em `/etc/udev/rules.d/70-persistent-net.rules` precisam ser modificadas para corresponder ao dispositivo por ID de barramento (palavra-chave `KERNELS` do `udev` igual a "SysFS BusID" conforme visível em `hwinfo --netcard`), em vez do endereço MAC. Isso permite a substituição de hardware com defeito (uma placa de rede no mesmo slot, mas com MAC diferente) e evita confusão quando a ligação muda o endereço MAC de todas as suas portas.

Por exemplo:

```
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="*",
KERNELS=="0000:00:19.0", ATTR{dev_id}=="0x0", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0"
```

No momento da inicialização, o `network.service` do `systemd` não espera o hotplug das portas de ligação, mas sim a ligação ficar pronta, o que requer no mínimo uma porta de ligação disponível. Quando uma das interfaces de porta de ligação é removida (desvinculação do driver NIC, `rmmmod` do driver NIC ou remoção verdadeira do hotplug do PCI) do sistema, o kernel a remove automaticamente da ligação. Quando uma nova placa é adicionada ao sistema (substituição do hardware no slot), o `udev` a renomeia usando a regra de nome persistente baseada em barramento com o nome da porta de ligação e chama o `ifup` para ela. A chamada do `ifup` une-a automaticamente à ligação.

23.8 Configurando dispositivos de equipe para agrupamento de rede

“Agregação de link” é o termo geral que descreve a combinação (ou agregação) de uma conexão de rede para fornecer uma camada lógica. Você pode encontrar os termos “agrupamento de canal”, “ligação de Ethernet”, “truncamento de porta” etc., que são sinônimos e se referem ao mesmo conceito.

Esse conceito é bastante conhecido como “ligação” e foi originalmente integrado ao kernel do Linux (consulte a [Seção 23.7, “Configurando dispositivos de ligação”](#) para ver a implementação original). O termo *Agrupamento de Rede* é usado para fazer referência à nova implementação desse conceito.

A principal diferença entre a ligação e o Agrupamento de Rede é que o agrupamento dispõe de um conjunto de pequenos módulos do kernel responsáveis pelo fornecimento de uma interface para instâncias do `teamd`. Todo o restante é executado no espaço do usuário. Isso é diferente da implementação de ligação original que inclui todas as suas funcionalidades exclusivamente no kernel. Para ver uma comparação, consulte a [Tabela 23.5, “Comparação de recursos entre ligação e agrupamento”](#).

TABELA 23.5: COMPARAÇÃO DE RECURSOS ENTRE LIGAÇÃO E AGRUPAMENTO

Recurso	Vínculo	Equipe
broadcast, política TX round-robin	sim	sim
política TX ativa-backup	sim	sim
Suporte a LACP (802.3ad)	sim	sim

Recurso	Vínculo	Equipe
política TX baseada em hash	sim	sim
usuário pode definir função de hash	não	sim
Suporte a balanceamento de carga TX (TLB)	sim	sim
Suporte a balanceamento de carga TX para LACP	não	sim
Monitoramento de link Ethtool	sim	sim
Monitoramento de link ARP	sim	sim
Monitoramento de link NS/NA (IPV6)	não	sim
Bloqueio de RCU em caminhos TX/RX	não	sim
porta prio e adesão	não	sim
configuração de monitoramento de link separado por porta	não	sim
configuração de monitoramento de links múltiplos	limitado	sim
Suporte a VLAN	sim	sim
empilhamento de vários dispositivos	sim	sim
Fonte: http://libteam.org/files/teamdev.pp.pdf 		

Ambas as implementações, ligação e Agrupamento de Rede, podem ser usadas em paralelo. O Agrupamento de Rede é uma alternativa à implementação de ligação existente. Ele não a substitui.

É possível usar o Agrupamento de Rede em diversos casos de uso. Os dois casos de uso mais importantes são explicados mais adiante e envolvem:

- Equilíbrio de carga entre dispositivos de rede diferentes.
- Failover de um dispositivo de rede para outro em caso de falha em um dos dispositivos.

No momento, não há nenhum módulo do YaST que suporte a criação de dispositivo do agrupamento. Você precisa configurar o Agrupamento de Rede manualmente. O procedimento geral é mostrado a seguir e pode ser aplicado a todas as suas configurações de Agrupamento de Rede:

PROCEDIMENTO 23.1: PROCEDIMENTO GERAL

1. Verifique se que você possui todos os pacotes necessários instalados. Instale os pacotes `libteam-tools`, `libteamctl0` e `python-libteam`.
2. Crie um arquivo de configuração em `/etc/sysconfig/network/`. Normalmente, esse arquivo é `ifcfg-team0`. Se você precisar de mais de um dispositivo de Agrupamento de Rede, numere-os em ordem crescente.
Esse arquivo de configuração contém diversas variáveis que são explicadas nas páginas de manual (consulte `man ifcfg` e `man ifcfg-team`). Há um exemplo de configuração em seu sistema no arquivo `/etc/sysconfig/network/ifcfg.template`.
3. Remova os arquivos de configuração das interfaces que serão usadas com o dispositivo de agrupamento (geralmente, `ifcfg-eth0` e `ifcfg-eth1`).
É recomendável fazer um backup e remover os dois arquivos. O Wicked recriará os arquivos de configuração com os parâmetros necessários para o agrupamento.
4. Opcionalmente, verifique se tudo está incluído no arquivo de configuração do Wicked:

```
> sudo wicked show-config
```

5. Inicie o dispositivo de Agrupamento de Rede `team0`:

```
> sudo wicked ifup all team0
```

Se você precisar de informações adicionais sobre depuração, use a opção `--debug all` após o subcomando `all`.

6. Verifique o status do dispositivo de Agrupamento de Rede. Para fazer isso, execute os seguintes comandos:

- Obtenha o estado da instância do teamd do Wicked:

```
> sudo wicked ifstatus --verbose team0
```

- Obtenha o estado de toda a instância:

```
> sudo teamdctl team0 state
```

- Obtenha o estado do systemd da instância do teamd:

```
> sudo systemctl status teamd@team0
```

Cada um deles mostra uma tela um pouco diferente, dependendo das suas necessidades.

7. Se você precisar mudar algo no arquivo `ifcfg-team0` posteriormente, recarregue sua configuração com:

```
> sudo wicked ifreload team0
```

Não use `systemctl` para iniciar ou parar o dispositivo de agrupamento! Em vez disso, use o comando `wicked` conforme mostrado acima.

Para remover completamente o dispositivo de equipe, siga este procedimento:

PROCEDIMENTO 23.2: REMOVENDO UM DISPOSITIVO DE AGRUPAMENTO

1. Pare o dispositivo de Agrupamento de Rede `team0`:

```
> sudo wicked ifdown team0
```

2. Renomeie o arquivo `/etc/sysconfig/network/ifcfg-team0` para `/etc/sysconfig/network/.ifcfg-team0`. Insira um ponto na frente do nome do arquivo para torná-lo “invisível” ao wicked. Se você realmente não precisa mais da configuração, também pode remover o arquivo.

3. Recarregue a configuração:

```
> sudo wicked ifreload all
```

23.8.1 Caso de uso: equilíbrio de carga com agrupamento de rede

O equilíbrio de carga é usado para melhorar a largura de banda. Use o seguinte arquivo de configuração para criar um dispositivo de Agrupamento de Rede com recursos de equilíbrio de carga. prossiga com *Procedimento 23.1, "Procedimento geral"* para configurar o dispositivo. Verifique a saída com `teamdctl`.

EXEMPLO 23.12: CONFIGURAÇÃO PARA EQUILÍBRIO DE CARGA COM AGRUPAMENTO DE REDE

```
STARTMODE=auto ❶
BOOTPROTO=static ❷
IPADDRESS="192.168.1.1/24" ❷
IPADDR6="fd00:deca:fbad:50::1/64" ❷

TEAM_RUNNER="loadbalance" ❸
TEAM_LB_TX_HASH="ipv4,ipv6,eth,vlan"
TEAM_LB_TX_BALANCER_NAME="basic"
TEAM_LB_TX_BALANCER_INTERVAL="100"

TEAM_PORT_DEVICE_0="eth0" ❹
TEAM_PORT_DEVICE_1="eth1" ❹

TEAM_LW_NAME="ethtool" ❺
TEAM_LW_ETHTOOL_DELAY_UP="10" ❻
TEAM_LW_ETHTOOL_DELAY_DOWN="10" ❻
```

- ❶ Controla a inicialização do dispositivo de agrupamento. O valor de `auto` significa que a interface será configurada quando o serviço de rede estiver disponível e será iniciada automaticamente a cada reinicialização.

Caso você mesmo tenha necessidade de controlar o dispositivo (e impedir que ele seja iniciado automaticamente), defina `STARTMODE` como `manual`.

- ❷ Define o endereço IP estático (neste caso, `192.168.1.1` para IPv4 e `fd00:deca:fbad:50::1` para IPv6).

Se o dispositivo de Agrupamento de Rede tiver que usar um endereço IP dinâmico, defina `BOOTPROTO="dhcp"` e remova (ou comente) a linha com `IPADDRESS` e `IPADDR6`.

- ❸ Define `TEAM_RUNNER` como `loadbalance` para ativar o modo de equilíbrio de carga.

- ❹ Especifica um ou mais dispositivos que devem ser agregados para criar o dispositivo de Agrupamento de Rede.

- 5 Define um monitor de link para monitorar o estado dos dispositivos subordinados. O valor padrão `ethtool` verifica apenas se o dispositivo está ativo e é acessível. Isso torna essa verificação rápida o suficiente. No entanto, ele não verifica se o dispositivo pode realmente enviar ou receber pacotes.
Se você precisar de mais confiança na conexão, use a opção `arp_ping`. Ela envia pings a um host arbitrário (configurado na variável `TEAM_LW_ARP_PING_TARGET_HOST`). O dispositivo de Agrupamento de Rede é considerado ativo apenas quando as respostas são recebidas.
- 6 Define o atraso em milissegundos entre o link ficar ativo (ou inativo) e o executor ser notificado.

23.8.2 Caso de uso: failover com agrupamento de rede

O failover é usado para garantir alta disponibilidade de um dispositivo de Agrupamento de Rede crítico envolvendo um dispositivo de rede de backup paralelo. O dispositivo de rede de backup é executado o tempo todo e entra em ação em caso de falha no dispositivo principal.

Use o seguinte arquivo de configuração para criar um dispositivo de Agrupamento de Rede com recursos de failover. prossiga com *Procedimento 23.1, "Procedimento geral"* para configurar o dispositivo. Verifique a saída com `teamdctl`.

EXEMPLO 23.13: CONFIGURAÇÃO DO DISPOSITIVO DE AGRUPAMENTO DE REDE DHCP

```
STARTMODE=auto ①
BOOTPROTO=static ②
IPADDR="192.168.1.2/24" ②
IPADDR6="fd00:deca:fbad:50::2/64" ②

TEAM_RUNNER=activebackup ③
TEAM_PORT_DEVICE_0="eth0" ④
TEAM_PORT_DEVICE_1="eth1" ④

TEAM_LW_NAME=ethtool ⑤
TEAM_LW_ETHTOOL_DELAY_UP="10" ⑥
TEAM_LW_ETHTOOL_DELAY_DOWN="10" ⑥
```

- 1 Controla a inicialização do dispositivo de agrupamento. O valor de `auto` significa que a interface será configurada quando o serviço de rede estiver disponível e será iniciada automaticamente a cada reinicialização.
Caso você mesmo tenha necessidade de controlar o dispositivo (e impedir que ele seja iniciado automaticamente), defina `STARTMODE` como `manual`.

- ② Define o endereço IP estático (neste caso, 192.168.1.2 para IPv4 e fd00:deca:fbad:50::2 para IPv6).
Se o dispositivo de Agrupamento de Rede tiver que usar um endereço IP dinâmico, defina B00TPR0T0="dhcp" e remova (ou comente) a linha com IPADDRESS e IPADDR6.
- ③ Define TEAM_RUNNER como activebackup para ativar o modo de failover.
- ④ Especifica um ou mais dispositivos que devem ser agregados para criar o dispositivo de Agrupamento de Rede.
- ⑤ Define um monitor de link para monitorar o estado dos dispositivos subordinados. O valor padrão ethtool verifica apenas se o dispositivo está ativo e é acessível. Isso torna essa verificação rápida o suficiente. No entanto, ele não verifica se o dispositivo pode realmente enviar ou receber pacotes.
Se você precisar de mais confiança na conexão, use a opção arp_ping. Ela envia pings a um host arbitrário (configurado na variável TEAM_LW_ARP_PING_TARGET_HOST). Apenas se as respostas forem recebidas, o dispositivo de Agrupamento de Rede será considerado ativo.
- ⑥ Define o atraso em milissegundos entre o link ficar ativo (ou inativo) e o executor ser notificado.

23.8.3 Caso de uso: VLAN em dispositivo de agrupamento

VLAN é a abreviação de *Virtual Local Area Network* (Rede Local Virtual). Ela permite a execução de várias Ethernets *lógicas* (virtuais) em uma única Ethernet física. Ela divide logicamente a rede em diferentes domínios de broadcast para que os pacotes sejam trocados apenas entre portas que são designadas para a mesma VLAN.

O seguinte caso de uso cria duas VLANs estáticas na parte superior de um dispositivo de equipe:

- vlan0, vinculada ao endereço IP 192.168.10.1
- vlan1, vinculada ao endereço IP 192.168.20.1

Proceda da seguinte maneira:

1. Habilite as tags VLAN no switch. Para usar o equilíbrio de carga em seu dispositivo de equipe, o switch precisa ser compatível com LACP (*Link Aggregation Control Protocol – Protocolo de Controle de Agregação de Links*) (802.3 ad). Consulte os detalhes no manual do seu hardware.

2. Decida se você deseja usar equilíbrio de carga ou failover em seu dispositivo de equipe. Configure o dispositivo de equipe conforme descrito na [Seção 23.8.1, “Caso de uso: equilíbrio de carga com agrupamento de rede”](#) ou na [Seção 23.8.2, “Caso de uso: failover com agrupamento de rede”](#).

3. Em `/etc/sysconfig/network`, crie um arquivo `ifcfg-vlan0` com o seguinte conteúdo:

```
STARTMODE="auto"  
BOOTPROTO="static" ❶  
IPADDR='192.168.10.1/24' ❷  
ETHERDEVICE="team0" ❸  
VLAN_ID="0" ❹  
VLAN='yes'
```

- ❶ Define um endereço IP fixo, especificado em `IPADDR`.
 - ❷ Define o endereço IP, aqui com sua máscara de rede.
 - ❸ Contém a interface real para usar para a interface VLAN, aqui nosso dispositivo de equipe (`team0`).
 - ❹ Especifica um ID exclusivo para a VLAN. Preferencialmente, o nome do arquivo e a variável `VLAN_ID` correspondem ao nome `ifcfg-vlanVLAN_ID`. No nosso caso, `VLAN_ID` é `0`, que leva ao nome de arquivo `ifcfg-vlan0`.
4. Copie o arquivo `/etc/sysconfig/network/ifcfg-vlan0` para `/etc/sysconfig/network/ifcfg-vlan1` e mude os seguintes valores:
- `IPADDR` de `192.168.10.1/24` para `192.168.20.1/24`.
 - `VLAN_ID` de `0` para `1`.

5. Inicie as duas VLANs:

```
# wicked ifup vlan0 vlan1
```

6. Verifique a saída de `ifconfig`:

```
# ifconfig -a  
[...]  
vlan0      Link encap:Ethernet  HWaddr 08:00:27:DC:43:98  
            inet addr:192.168.10.1 Bcast:192.168.10.255 Mask:255.255.255.0  
            inet6 addr: fe80::a00:27ff:fedc:4398/64 Scope:Link  
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
```

```
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 b) TX bytes:816 (816.0 b)

vlan1    Link encap:Ethernet  HWaddr 08:00:27:DC:43:98
          inet addr:192.168.20.1 Bcast:192.168.20.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fedc:4398/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b) TX bytes:816 (816.0 b)
```

24 Operação da impressora

O SUSE® Linux Enterprise Desktop suporta a impressão com muitos tipos de impressoras, incluindo impressoras de rede remotas. É possível configurar as impressoras manualmente ou com o YaST. Para obter instruções de configuração, consulte a [Capítulo 34, Configurando uma impressora](#). Os utilitários gráficos e de linha de comando estão disponíveis para iniciar e gerenciar serviços de impressão. Se a sua impressora não funcionar como se esperava, consulte a [Seção 24.8, “Solução de problemas”](#).

CUPS (Common Unix Printing System) é o sistema de impressão padrão no SUSE Linux Enterprise Desktop.

As impressoras podem ser distinguidas pela interface, como USB ou rede, e pela linguagem de impressão. Ao comprar uma impressora, verifique se a sua interface é suportada (USB, Ethernet ou Wi-Fi) e se a sua linguagem é adequada. As impressoras podem ser categorizadas com base em três classes de linguagem:

Impressoras PostScript

PostScript é a linguagem de impressora na qual a maior parte dos serviços de impressão em Linux e Unix são gerados e processados pelo sistema de impressão interno. Se documentos PostScript puderem ser diretamente processados pela impressora e não precisarem ser convertidos em estágios adicionais do sistema de impressão, o número de origens de erro potenciais será reduzido.

Atualmente, o PostScript vem sendo substituído pelo PDF como o formato padrão dos serviços de impressão. Já existem impressoras PostScript + PDF que imprimem diretamente em PDF (e também em PostScript). Para as impressoras PostScript tradicionais, é necessário converter de PDF em PostScript no workflow de impressão.

Impressoras padrão (linguagens como PCL e ESC/P)

No caso de linguagens de impressora conhecidas, o sistema de impressão pode converter serviços PostScript na respectiva linguagem de impressão com o Ghostscript. Esta fase do processamento é chamada de interpretação. As linguagens mais conhecidas são PCL (mais usada pelas impressoras HP e seus clones) e ESC/P (utilizada nas impressoras Epson). Geralmente, essas linguagens são suportadas no Linux e produzem um resultado de impressão adequado. O Linux pode não conseguir realizar algumas funções especiais da impressora. Com exceção da HP e da Epson, não há fabricantes de impressoras que desenvolvem e disponibilizam drivers de Linux a distribuidores Linux sob uma licença de código-fonte aberto.

Impressoras proprietárias (também denominadas impressoras GDI)

Essas impressoras não suportam nenhuma das linguagens de impressora comuns. Elas usam suas próprias linguagens de impressora não documentadas, que ficam sujeitas a mudanças quando é lançada uma edição nova de um modelo. Geralmente, apenas os drivers do Windows estão disponíveis para essas impressoras. Consulte a [Seção 24.8.1, “Impressoras sem suporte de linguagem de impressora padrão”](#) para obter mais informações.

Antes de comprar uma nova impressora, consulte as seguintes fontes para verificar a abrangência do suporte ao equipamento pretendido:

<http://www.openprinting.org/printers> 

A home page OpenPrinting com o banco de dados de impressão. O banco de dados mostra o status mais recente de suporte do Linux. No entanto, a distribuição do Linux só pode integrar os drivers disponíveis no momento da produção. Da mesma forma, uma impressora atualmente classificada como “perfeitamente suportada” talvez não apresentasse esse status quando a versão mais recente do SUSE Linux Enterprise Desktop foi lançada. Assim, os bancos de dados não indicarão necessariamente o status correto, mas apenas uma informação aproximada.

<http://pages.cs.wisc.edu/~ghost/> 

Página do Ghostscript na Web.

</usr/share/doc/packages/ghostscript/catalog.devices>

Lista de drivers Ghostscript incorporados.

24.1 O workflow do CUPS


O usuário cria um serviço de impressão. O serviço de impressão consiste nos dados que serão impressos mais as informações do spooler. Isso inclui o nome da impressora ou o nome da fila de impressão e, opcionalmente, as informações do filtro (por exemplo, as opções específicas da impressora).

Existe pelo menos uma fila de impressão dedicada para cada impressora. O spooler mantém o serviço de impressão em fila até que a impressora desejada esteja pronta para receber dados. Uma vez pronta, o spooler envia os dados pelo filtro, tendo a impressora como back end.

O filtro converte os dados gerados pelo aplicativo que está imprimindo (geralmente PostScript ou PDF, mas também ASCII, JPEG etc.) em dados específicos da impressora (PostScript, PCL, ESC/P etc.). Os recursos da impressora são descritos nos arquivos PPD. O arquivo PPD contém opções da impressora com os parâmetros necessários para habilitá-los. O sistema de filtros verifica se as opções selecionadas pelo usuário foram habilitadas.

Se você usa uma impressora PostScript, o sistema de filtros converte os dados em PostScript específico da impressora. Isso não exige um driver de impressora. Se você usa uma impressora não PostScript, o sistema de filtros converte os dados em dados específicos da impressora. Isso exige um driver adequado à sua impressora. O back end recebe do filtro os dados específicos da impressora e os repassa a ela.

24.2 Métodos e protocolos de conexão de impressoras

Existem várias possibilidades para conectar uma impressora ao sistema. A configuração do CUPS não faz distinção entre uma impressora local e uma impressora conectada ao sistema pela rede. Para obter mais informações sobre a conexão de impressoras, leia o artigo *CUPS in a Nutshell* (CUPS numa Casca de Noz) em https://en.opensuse.org/SDB:CUPS_in_a_Nutshell .



Atenção: Mudando as conexões de cabo em um sistema em execução

Ao conectar a impressora à máquina, não esqueça de que apenas dispositivos USB podem ser conectados ou desconectados durante a operação. Para evitar danos ao sistema ou à impressora, encerre o sistema antes de mudar qualquer conexão que não seja USB.

24.3 Instalando o software

PPD (descrição de impressora PostScript) é a linguagem de computador que descreve as propriedades, como resolução, e as opções, como disponibilidade de uma unidade duplex. Essas descrições são necessárias para o uso de várias opções de impressora no CUPS. Sem um arquivo PPD, os dados de impressão seriam encaminhados à impressora em estado “bruto”, o que normalmente não é desejado.

Para configurar uma impressora PostScript, a melhor opção é obter um arquivo PPD adequado. Muitos arquivos PPD estão disponíveis nos pacotes `manufacturer-PPDs` e `OpenPrintingPPDs-postscript`. Consulte a [Seção 24.7.3, “Arquivos PPD em vários pacotes”](#) e a [Seção 24.8.2, “Nenhum arquivo PPD adequado disponível para impressora PostScript”](#).

É possível armazenar novos arquivos PPD no diretório `/usr/share/cups/model/` ou adicioná-los ao sistema de impressão com o YaST, conforme descrito na [Seção 34.1.1, “Adicionando drivers com o YaST”](#). Na sequência, é possível selecionar o arquivo PPD durante a configuração da impressora.

Observe se o fabricante da impressora requer que você instale pacotes inteiros de software. Esse tipo de instalação pode resultar na perda do suporte oferecido pelo SUSE Linux Enterprise Desktop. Além disso, os comandos de impressão podem funcionar de forma diferente, e o sistema talvez não possa mais processar dispositivos de outros fabricantes. Por isso, não recomendamos instalar o software do fabricante.

24.4 Impressoras de rede

Uma impressora de rede pode suportar vários protocolos, alguns deles até simultaneamente. Embora a maioria dos protocolos suportados seja padronizada, alguns fabricantes modificam o padrão. Os fabricantes então fornecem drivers apenas para alguns sistemas operacionais. Infelizmente, raros são os drivers para Linux. Na situação atual, não é possível agir como se todos os protocolos funcionassem perfeitamente no Linux. Portanto, talvez seja necessário testar várias opções para chegar a uma configuração funcional.

O CUPS suporta os protocolos `socket`, `LPD`, `IPP` e `smb`.

`socket`

Socket refere-se a uma conexão em que os dados de impressão simples são enviados diretamente a um soquete TCP. Alguns números de portas de soquete normalmente usados são `9100` ou `35`. A sintaxe do URI (Uniform Resource Identifier) do dispositivo é: `socket://IP.DA.IMPRESSORA:PORTA`. Por exemplo: `socket://192.168.2.202:9100/`.

`LPD (daemon de impressora de linha)`

O protocolo LPD está descrito no RFC 1179. Nesse protocolo, alguns dados relacionados ao serviço, como o ID da fila de impressão, são enviados antes dos dados da impressão propriamente ditos. Portanto, a fila de impressão deve ser especificada no momento da configuração do protocolo LPD. As implementações de fabricantes de impressoras diferentes são flexíveis o suficiente para aceitar qualquer nome como a fila de impressão.

Se necessário, o manual da impressora indicará o nome a ser usado. Geralmente se usa LPT, LPT1, LP1 ou nomes semelhantes. O número de porta para o serviço LPD é 515. Um exemplo de URI de dispositivo é lpd://192.168.2.202/LPT1.

IPP (protocolo de impressão de Internet)

O IPP é baseado no protocolo HTTP. Com o IPP, mais dados referentes à tarefa são transmitidos. O CUPS usa o IPP em transmissões internas de dados. É necessário indicar o nome da fila de impressão para que o IPP seja configurado corretamente. A porta padrão do IPP é 631. Exemplos de URIs de dispositivo são ipp://192.168.2.202/ps e ipp://192.168.2.202/printers/ps.

SMB (compartilhamento Windows)

O CUPS também suporta a impressão em impressoras conectadas a compartilhamentos Windows. O protocolo usado para essa finalidade é o SMB. O SMB usa os números de porta 137, 138 e 139. Exemplos de URIs de dispositivo são smb://user:password@workgroup/smb.example.com/printer, smb://user:password@smb.example.com/printer e smb://smb.example.com/printer.

O protocolo suportado pela impressora deve ser determinado antes da configuração. Se o fabricante não fornecer as informações necessárias, o comando nmap (que vem com o pacote nmap) pode ser usado para verificar o protocolo. O nmap verifica se há portas abertas em um host. Por exemplo:

```
> nmap -p 35,137-139,515,631,9100-10000 IP.OF.THE.PRINTER
```

24.5 Configurando o CUPS com ferramentas de linha de comando

É possível configurar o CUPS com ferramentas de linha de comando, como lpinfo, lpadmin e lpoptions. Você precisa de um URI de dispositivo composto por um back end, como USB, e parâmetros. Para determinar os URIs de dispositivo válidos no sistema, use o comando lpinfo -v | grep "":"/:

```
> sudo lpinfo -v | grep "":"/
direct usb://ACME/FunPrinter%20XL
network socket://192.168.2.253
```


Com o **lpadmin**, o administrador do servidor CUPS pode adicionar, remover ou gerenciar filas de impressão. Para adicionar uma fila de impressão, use a seguinte sintaxe:

```
> sudo lpadmin -p QUEUE -v DEVICE-URI -P PPD-FILE -E
```

Em seguida, o dispositivo (-v) fica disponível como FILA (-p), usando o arquivo PPD especificado (-P). Isso significa que você precisa saber qual é o arquivo PPD e o URI de dispositivo para configurar a impressora manualmente.

Não use -E como primeira opção. Em todos os comandos CUPS, -E como primeiro argumento define o uso de uma conexão criptografada. Para habilitar a impressora, -E deve ser usado como mostrado no seguinte exemplo:

```
> sudo lpadmin -p ps -v usb://ACME/FunPrinter%20XL -P \
/usr/share/cups/model/Postscript.ppd.gz -E
```

O seguinte exemplo configura uma impressora de rede:

```
> sudo lpadmin -p ps -v socket://192.168.2.202:9100/ -P \
/usr/share/cups/model/Postscript-level1.ppd.gz -E
```

Para conhecer mais opções de **lpadmin**, consulte a página de manual do **lpadmin(8)**.

Durante a configuração da impressora, algumas opções são definidas como padrão. Essas opções podem ser modificadas para cada serviço de impressão (dependendo da ferramenta de impressão utilizada). Também é possível modificar essas opções padrão com o YaST. Usando ferramentas de linha de comando, defina opções padrão da seguinte forma:

1. Primeiro, liste todas as opções:

```
> sudo lpoptions -p QUEUE -l
```

Exemplo:

```
Resolution/Output Resolution: 150dpi *300dpi 600dpi
```

A opção padrão ativada é identificada por um asterisco na frente (*).

2. Mude a opção com **lpadmin**:

```
> sudo lpadmin -p QUEUE -o Resolution=600dpi
```

3. Verifique a nova configuração:

```
> sudo lpoptions -p QUEUE -l
```

```
Resolution/Output Resolution: 150dpi 300dpi *600dpi
```

Quando um usuário comum executa **lpoptions**, as configurações são gravadas em ~/.cups/lpoptions. Porém, as configurações de root são gravadas em /etc/cups/lpoptions.

24.6 Imprimindo pela linha de comando

Para imprimir da linha de comando, digite **lp -d *NOMEDAFILA* *NOMEDOARQUIVO***, substituindo *NOMEDAFILA* e *NOMEDOARQUIVO* pelos nomes correspondentes.

Alguns aplicativos dependem do comando **lp** para imprimir. Neste caso, digite o comando correto na caixa de diálogo do aplicativo, normalmente sem especificar *NOMEDOARQUIVO*. Por exemplo, **lp -d *NOMEDAFILA***.

24.7 Recursos especiais no SUSE Linux Enterprise Desktop

Vários recursos do CUPS foram adaptados para o SUSE Linux Enterprise Desktop. Algumas das mudanças mais importantes são abordadas aqui.

24.7.1 CUPS e firewall

Após realizar a instalação padrão do SUSE Linux Enterprise Desktop, o firewalld estará ativo, e as interfaces de rede serão configuradas para ficarem na zona pública, que bloqueia o tráfego de entrada.

Quando o firewalld está ativo, pode ser necessário configurá-lo para permitir que os clientes procurem impressoras de rede com a permissão de mdns e ipp pela zona de rede interna. A zona pública nunca deve expor as filas da impressora.

(Há mais informações sobre a configuração do firewalld disponíveis no *Livro "Security and Hardening Guide"*, Capítulo 23 "*Masquerading and firewalls*", Seção 23.4 "*firewalld*" e em https://en.opensuse.org/SDB:CUPS_and_SANE_Firewall_settings.)

24.7.1.1 Cliente CUPS

Normalmente, um cliente CUPS é executado em uma estação de trabalho comum, localizada em um ambiente de rede confiável protegido por firewall. Neste caso, é recomendável configurar a interface de rede para ficar na Zona Interna, de modo que a estação de trabalho possa ser alcançada de dentro da rede.

24.7.1.2 Servidor CUPS

Se o servidor CUPS fizer parte de um ambiente de rede confiável, protegido por um firewall, a interface de rede deverá ser configurada para ficar na Zona Interna do firewall. Não é recomendado configurar um servidor CUPS em um ambiente de rede não confiável, a menos que você garanta que ele seja protegido por regras especiais de firewall e opções seguras na configuração do CUPS.

24.7.2 Procurando impressoras de rede

Os servidores CUPS anunciam regularmente as informações sobre disponibilidade e status das impressoras compartilhadas na rede. Os clientes podem acessar essas informações para exibir uma lista de impressoras disponíveis nas caixas de diálogo de impressão, por exemplo. Isso se chama “procurar”.

Os servidores CUPS anunciam suas filas de impressão pela rede usando o protocolo de procura tradicional do CUPS ou o Bonjour/DNS-SD. Para habilitar a procura de filas de impressão de rede, o serviço `cups-browsed` precisa ser executado em todos os clientes que imprimem por meio de servidores CUPS. O `cups-browsed` não é iniciado por padrão. Para iniciá-lo na sessão ativa, use **`sudo systemctl start cups-browsed`**. Para assegurar que ele seja iniciado automaticamente após a inicialização, habilite-o com **`sudo systemctl enable cups-browsed`** em todos os clientes.

Caso a pesquisa não funcione depois de iniciar `cups-browsed`, o(s) servidor(es) CUPS provavelmente anunciará(ão) as filas de impressão de rede pelo Bonjour/DNS-SD. Neste caso, é necessário instalar também o pacote `avahi` e iniciar o serviço associado ao **`sudo systemctl start avahi-daemon`** em todos os clientes.

Consulte a [Seção 24.7.1, “CUPS e firewall”](#) para obter informações sobre como permitir a procura de impressoras por meio do `firewalld`.

24.7.3 Arquivos PPD em vários pacotes

A configuração de impressora do YaST define as filas do CUPS usando os arquivos PPD instalados em `/usr/share/cups/model`. Para localizar os arquivos PPD adequados ao modelo da impressora, o YaST compara o fornecedor e o modelo determinados durante a detecção de hardware com os fornecedores e modelos em todos os arquivos PPD. Para isso, a configuração de impressora do YaST gera um banco de dados com as informações de fabricante e modelo extraídas dos arquivos PPD.

A configuração com apenas arquivos PPD e nenhuma outra fonte de informação tem a vantagem de permitir a livre modificação de arquivos PPD em `/usr/share/cups/model/`. Por exemplo, se você possui impressoras PostScript, será possível copiar os arquivos PPD diretamente para `/usr/share/cups/model` (se ainda não existirem nos pacotes `manufacturer-PPDs` ou `OpenPrintingPPDs-postscript`) para atingir a configuração ideal para as suas impressoras.

Os arquivos PPD adicionais são fornecidos pelos seguintes pacotes:

- `gutenprint`: o driver Gutenprint e seus PPDs correspondentes
- `splix`: o driver SpliX e seus PPDs correspondentes
- `OpenPrintingPPDs-ghostscript`: os PPDs para os drivers Ghostscript incorporados
- `OpenPrintingPPDs-hpijs`: PPDs para o driver HPIJS para impressoras não HP

24.8 Solução de problemas

As seções a seguir abordam alguns dos problemas mais encontrados em relação a hardware e software de impressora, bem como formas de solucionar ou superar esses problemas. Os tópicos abordados incluem impressoras GDI, arquivos PPD e configuração de porta. Problemas comuns de impressoras de rede, impressões com defeito e gerenciamento de filas também são tratados.

24.8.1 Impressoras sem suporte de linguagem de impressora padrão

Essas impressoras não suportam nenhuma linguagem de impressora comum, podendo apenas ser tratadas com sequências especiais de controle proprietário. Portanto, elas só funcionam com as versões de sistema operacional para as quais o fabricante fornece driver. GDI é uma interface de

programação desenvolvida pela Microsoft* para dispositivos gráficos. Geralmente o fabricante fornece drivers apenas para Windows e, com o driver do Windows usa a interface GDI, essas impressoras também são chamadas de *impressoras GDI*. O verdadeiro problema não é a interface de programação, mas o fato de que essas impressoras apenas podem ser reconhecidas com a linguagem de impressora proprietária do respectivo modelo da impressora.

Algumas impressoras GDI podem ser ajustadas para funcionar no modo GDI ou em uma das linguagens de impressora padrão. Consulte o manual da impressora para saber se isso é possível. Alguns modelos exigem software especial do Windows para fazer o ajuste (observe que o driver de impressora do Windows pode sempre retornar a impressora para o modo GDI quando se imprime do Windows). Para outras impressoras GDI, existem módulos de extensão disponíveis para uma linguagem de impressora padrão.

Alguns fabricantes oferecem drivers proprietários para suas impressoras. A desvantagem dos drivers de impressora proprietários é que não há garantia de que vão funcionar com o sistema de impressão instalado ou de que sejam adequados para as diferentes plataformas de hardware. Em contraste, impressoras que suportam uma linguagem de impressora padrão não dependem de uma versão do sistema de impressão especial ou de plataforma de hardware especial.

Em vez de perder tempo tentando fazer funcionar um driver de Linux proprietário, a compra de uma impressora que suporte a linguagem padrão de impressora (preferencialmente PostScript) pode ter melhor custo-benefício. Isso soluciona o problema do driver de uma vez por todas, eliminando a necessidade de instalar e configurar software de driver especial e obter atualizações de driver que talvez fossem necessárias por causa de novos avanços no sistema de impressão.

24.8.2 Nenhum arquivo PPD adequado disponível para impressora PostScript

Se o pacote `manufacturer-PPDs` ou `OpenPrintingPPDs-postscript` não incluir o arquivo PPD adequado para uma impressora PostScript, será possível utilizar o arquivo PPD do CD do driver do fabricante da impressora ou fazer download de um arquivo PPD adequado da página do fabricante da impressora na Web.

Se o arquivo PPD for fornecido como arquivo compactado (.zip) ou arquivo compactado de autoextração (.exe), faça a descompactação com `unzip`. Primeiro, reveja os termos de licença do arquivo PPD. Em seguida, use o utilitário `cupstestppd` para verificar se o arquivo PPD atende à “Especificação de Formato de Arquivo PPD (PostScript Printer Description — Descrição de Impressora PostScript) da Adobe, versão 4.3”. Se o utilitário retornar “FAIL”, significa que

os erros nos arquivos PPD são graves e provavelmente causam os principais problemas. Os problemas reportados pelo `cupstestppd` devem ser eliminados. Se necessário, peça o arquivo PPD adequado ao fabricante da impressora.

24.8.3 Conexões da impressora de rede

Identificação de problemas de rede

Conecte a impressora diretamente ao computador. Para fins de teste, configure-a como impressora local. Se isso funcionar, o problema está na rede.

Verificando a rede TCP/IP

A rede TCP/IP e a resolução de nomes devem ser funcionais.

Verificando um `lpd` remoto

Use o comando a seguir para testar o estabelecimento de uma conexão TCP com `lpd` (porta 515) no `HOST`:

```
> netcat -z HOST 515 && echo ok || echo failed
```

Se a conexão com `lpd` não for estabelecida, o `lpd` pode não estar ativo ou pode haver problemas básicos de rede.

Desde que o respectivo `lpd` esteja ativo e o host aceite consultas, execute o seguinte comando como `root` para consultar um relatório de status para `FILA` no `HOST` remoto:

```
# echo -e "\004queue" \  
| netcat -w 2 -p 722 HOST 515
```

Se o `lpd` não responder, ele pode não estar ativo ou pode haver problemas básicos de rede.

Se o `lpd` responder, a resposta deverá mostrar por que não é possível imprimir na `fila` do `host`. Se você receber uma resposta como esta, mostrada no *Exemplo 24.1, “Mensagem de erro do `lpd`”*, significa que o problema está sendo causado pelo `lpd` remoto.

EXEMPLO 24.1: MENSAGEM DE ERRO DO `lpd`

```
lpd: your host does not have line printer access  
lpd: queue does not exist  
printer: spooling disabled  
printer: printing disabled
```

Verificando um `cupsd` remoto

Um servidor de rede CUPS pode transmitir suas filas por padrão a cada 30 segundos na porta UDP `631`. Conforme apresentado, os seguintes comandos podem ser usados para testar se existe um servidor de rede CUPS de broadcasting na rede. Não deixe de parar seu daemon CUPS local antes de executar o comando.

```
> netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Se existir um servidor de rede CUPS de transmissão, a saída aparecerá conforme mostrado no *Exemplo 24.2, “Transmissão do servidor de rede CUPS”*.

EXEMPLO 24.2: TRANSMISSÃO DO SERVIDOR DE REDE CUPS

```
ipp://192.168.2.202:631/printers/queue
```

Use o comando a seguir para testar o estabelecimento de uma conexão TCP com `cupsd` (porta `631`) no `HOST`:

```
> netcat -z HOST 631 && echo ok || echo failed
```

Se a conexão com `cupsd` não for estabelecida, o `cupsd` poderá não estar ativo ou talvez haja problemas básicos de rede. `lpstat -h HOST -l -t` retorna um relatório de status (possivelmente muito extenso) para todas as filas no `HOST`, desde que o respectivo `cupsd` esteja ativo e o host aceite consultas.

O próximo comando pode ser usado para testar se a `FILA` no `HOST` aceita um serviço de impressão que consiste em um único caractere de retorno de carro. Nada será impresso. Possivelmente, será ejetada uma página em branco.

```
> echo -en "\r" \  
| lp -d queue -h HOST
```

Solução de problemas na impressora de rede ou na máquina do servidor de impressão

Algumas vezes, spoolers executados na máquina do servidor de impressão causam problemas quando precisam processar vários serviços de impressão. Como esse problema é causado pelo spooler na máquina do servidor de impressão, ele não tem solução. Como medida alternativa, desvie o spooler na máquina do servidor de impressão endereçando a impressora conectada à máquina diretamente com o soquete TCP. Consulte a *Seção 24.4, “Impressoras de rede”*.

Dessa forma, a máquina do servidor de impressão é reduzida a um conversor entre as várias formas de transferência de dados (conexão de rede TCP/IP e impressora local). Para usar esse método, você precisa saber a porta TCP da máquina do servidor de impressão.

Se a impressora estiver conectada à máquina do servidor de impressão e ligada, essa porta TCP poderá ser determinada normalmente com o utilitário `nmap` do pacote `nmap`, algum tempo depois que a máquina for ligada. Por exemplo, `nmap endereço-IP` pode resultar na seguinte saída para a máquina do servidor de impressão:

Port	State	Service
23/tcp	open	telnet
80/tcp	open	http
515/tcp	open	printer
631/tcp	open	cups
9100/tcp	open	jetdirect

Essa saída indica que a impressora conectada à máquina do servidor de impressão pode ser endereçada via soquete TCP na porta `9100`. Por padrão, `nmap` verifica somente algumas portas mais conhecidas listadas em `/usr/share/nmap/nmap-services`. Para verificar todas as portas possíveis, use o comando `nmap -p PORTA_DE_ORIGEM-PORTA_DE_DESTINO ENDEREÇO_IP`. O processo pode levar algum tempo. Para obter mais informações, consulte a página de manual de `nmap`.

Digite um comando como

```
> echo -en "\rHello\r\n" | netcat -w 1 IP-address port
cat file | netcat -w 1 IP-address port
```

para enviar strings de caracteres ou arquivos diretamente à respectiva porta para testar se a impressora pode ser endereçada dessa porta.

24.8.4 Defeitos na impressão sem mensagem de erro

Para o sistema de impressão, o serviço de impressão é concluído quando o back end do CUPS conclui a transferência de dados ao destinatário (impressora). Se houver falha no processamento posterior no destinatário (por exemplo, se a impressora não imprimir seus próprios dados específicos), o sistema de impressão não notará. Se a impressora não puder imprimir seus dados específicos, selecione um arquivo PPD mais adequado à impressora.

24.8.5 Filas desabilitadas

Se a transferência de dados para o destinatário falhar completamente após várias tentativas, o back end do CUPS, como `USB` ou `socket`, reportará um erro ao sistema de impressão (ao `cupsd`). O back end determina quantas tentativas malsucedidas são necessárias para que a

transferência de dados seja considerada impossível. Visto que as tentativas posteriores serão inúteis, o **cupsd** desabilita a impressão da fila correspondente. Após resolver a causa do problema, o administrador do sistema deve reabilitar a impressão com o comando **cupsenable**.

24.8.6 Navegação do CUPS: apagando serviços de impressão

Se um servidor de rede CUPS transmitir suas filas aos hosts de clientes via navegação e um **cupsd** local adequado estiver ativo nos hosts de clientes, o **cupsd** de cliente aceitará serviços de impressão de aplicativos e os encaminhará ao **cupsd** no servidor. Quando **cupsd** no servidor aceitar um serviço de impressão, ele receberá um novo número de serviço. Portanto, o número da tarefa no host cliente é diferente do número da tarefa no servidor. Como geralmente um serviço de impressão é encaminhado de imediato, não é possível apagá-lo com o número de serviço do host cliente, porque o **cupsd** do cliente considera o serviço de impressão concluído quando ele é encaminhado ao **cupsd** do servidor.

Para apagar o serviço de impressão do servidor, use um comando como **lpstat -h cups.example.com -o** para determinar o número do serviço no servidor. Esse procedimento assume que o servidor ainda não tenha concluído o serviço de impressão (isto é, enviado-o completamente para a impressora). Use o número de serviço obtido para apagar o serviço de impressão do servidor da seguinte maneira:

```
> cancel -h cups.example.com QUEUE-JOBNUMBER
```

24.8.7 Serviços de impressão com defeito e erros de transferência de dados

Se você desligar a impressora ou encerrar o computador durante o processo de impressão, o serviço de impressão permanecerá na fila. A impressão continua quando o computador (ou a impressora) é ligado novamente. Os serviços de impressão com defeito devem ser removidos da fila com **cancel**.

Se um serviço de impressão estiver corrompido ou se ocorrer um erro na comunicação entre o host e a impressora, a impressora não poderá processar os dados corretamente e imprimirá várias folhas de papel com caracteres ininteligíveis. Para corrigir o problema, siga estas etapas:

1. Para interromper a impressão, remova todo o papel das bandejas da impressora jato de tinta ou laser. Impressoras de alta qualidade têm um botão de cancelamento da impressão.

2. O serviço de impressão pode ainda estar na fila, já que os serviços apenas são removidos depois de inteiramente enviados à impressora. Use `lpstat -o` ou `lpstat -h cups.example.com -o` para verificar a fila que está sendo impressa. Apague o serviço de impressão com `cancel FILA-NÚMERODOSESRVIÇO` ou `cancel -h cups.example.com FILA-NÚMERODOSESRVIÇO`.
3. Alguns dados podem ainda ser transferidos à impressora mesmo que o serviço tenha sido apagado da fila. Verifique se há um processo back end do CUPS em execução para a fila respectiva e termine-o.
4. Reinicialize a impressora completamente deixando-a desligada por um tempo. Em seguida, insira o papel e ligue a impressora.

24.8.8 Depurando o CUPS

Use o seguinte procedimento genérico para localizar problemas no CUPS:

1. Defina `LogLevel debug` em `/etc/cups/cupsd.conf`.
2. Pare o `cupsd`.
3. Remova `/var/log/cups/error_log*` para não precisar procurar em arquivos de registro muito grandes.
4. Inicie o `cupsd`.
5. Repita a ação que causou o problema.
6. Verifique as mensagens em `/var/log/cups/error_log*` para identificar a causa do problema.

24.8.9 Mais informações

Há informações detalhadas sobre impressão no SUSE Linux Enterprise Desktop no Banco de Dados de Suporte do openSUSE em <https://en.opensuse.org/Portal:Printing>. Há soluções para vários problemas específicos no SUSE Knowledgebase (<https://www.suse.com/support/>). Localize os artigos relevantes com uma pesquisa pelo texto `CUPS`.

25 Interface gráfica do usuário

O SUSE Linux Enterprise Desktop inclui o servidor X.org, o Wayland e a área de trabalho do GNOME. Este capítulo descreve a configuração da interface gráfica do usuário para todos os usuários.

25.1 Sistema X Window

O servidor X.org é o padrão de fato para implementação do protocolo X11. O X é baseado em rede, permitindo que aplicativos iniciados em um host sejam exibidos em outro host conectado em qualquer tipo de rede (LAN ou Internet).

Em geral, o Sistema X Window não requer configuração. O hardware é detectado dinamicamente durante a inicialização do X. Portanto, o uso do `xorg.conf` foi descontinuado. Se você ainda tiver que especificar opções personalizadas para mudar o comportamento do X, poderá modificar os arquivos de configuração em `/etc/X11/xorg.conf.d/`.

No SUSE Linux Enterprise Desktop 15 SP4, o Wayland é incluído como uma alternativa ao servidor X.org. É possível selecioná-lo durante a instalação.

Instale os pacotes `xorg-docs` para obter informações mais detalhadas sobre o X11. O **man 5 `xorg.conf`** apresenta mais informações sobre o formato da configuração manual (se necessário). Mais informações sobre o desenvolvimento do X11 podem ser encontradas na home page do projeto, em <http://www.x.org>.

Os drivers estão nos pacotes `xf86-video-*`, por exemplo, `xf86-video-ati`. Muitos dos drivers incluídos nesses pacotes estão descritos em detalhes na página de manual relacionada. Por exemplo, se você usa o driver `ati`, encontra mais informações sobre ele em **man 4 `ati`**.

As informações sobre os drivers de terceiros estão disponíveis em `/usr/share/doc/packages/<nome_do_pacote>`. Por exemplo, a documentação de `x11-video-nvidiaG03` estará disponível em `/usr/share/doc/packages/x11-video-nvidiaG04` após a instalação do pacote.

Instale o pacote `xrdp` em um servidor e use o software cliente RDP para acessar o servidor por meio do protocolo de área de trabalho remota.

25.2 Instalando e configurando fontes

É possível categorizar as fontes no Linux em duas partes:

Fontes geométricas ou vetoriais

Apresenta uma descrição matemática; por exemplo, instruções sobre como desenhar a forma de um glifo. Dessa forma, cada glifo pode ser dimensionado a tamanhos arbitrários sem perder a qualidade. Antes de usar a fonte (ou glifo), as descrições matemáticas devem ser transformadas em raster (grade). Este processo é denominado *rasterização de fonte*. As *dicas de fonte* (embutidas na fonte) melhoram e otimizam o resultado da renderização de determinado tamanho. A rasterização e as dicas são feitas com a biblioteca FreeType.

Os formatos comuns no Linux são PostScript Type 1 e Type 2, TrueType e OpenType.

Fontes de bitmap ou raster


Compostas por uma matriz de pixels designados para um tamanho de fonte específico. As fontes de bitmap são extremamente rápidas e simples de se renderizar. Porém, em comparação com as fontes vetoriais, as fontes de bitmap não podem ser dimensionadas sem perda de qualidade. Sendo assim, essas fontes são normalmente distribuídas em tamanhos diferentes. Atualmente, as fontes de bitmap ainda são usadas no console do Linux e, algumas vezes, em terminais.


No Linux, o Portable Compiled Format (PCF) ou Glyph Bitmap Distribution Format (BDF) são os formatos mais comuns.



A aparência dessas fontes pode ser influenciada por dois aspectos principais:

- a escolha de uma família de fontes adequada e
- a renderização da fonte com um algoritmo que atinja resultados agradáveis aos olhos do receptor.

O último ponto só será relevante no caso de fontes vetoriais. Embora os dois pontos acima sejam altamente subjetivos, alguns padrões devem ser criados.

Os sistemas de renderização de fonte do Linux são compostos por várias bibliotecas com relações diferentes. A biblioteca básica de renderização de fonte é a [FreeType \(http://www.freetype.org/\)](http://www.freetype.org/) , que converte glifos de fonte de formatos suportados em glifos de bitmap otimizados. O processo de renderização é controlado por um algoritmo e seus parâmetros (que podem estar sujeitos a questões de patente).

Cada programa ou biblioteca que usa FreeType deve consultar a biblioteca [Fontconfig](http://www.fontconfig.org/). (<http://www.fontconfig.org/>)  Essa biblioteca combina a configuração da fonte dos usuários e do sistema. Quando um usuário muda a configuração de Fontconfig, essa mudança resulta em aplicativos com reconhecimento de Fontconfig.

A forma OpenType mais sofisticada, necessária para scripts como Arabic, Han ou Phags-Pa e outro tipo de processamento de texto de nível mais elevado, fica por conta do [Harfbuzz](http://www.harfbuzz.org/) (<http://www.harfbuzz.org/>)  ou do [Pango](http://www.pango.org/) (<http://www.pango.org/>) .

25.2.1 Mostrando as fontes instaladas

Para ter uma visão geral sobre as fontes que estão instaladas no sistema, execute os comandos `rpm` ou `fc-list`. Os dois apresentam uma boa resposta, mas podem retornar uma lista diferente, dependendo do sistema e da configuração do usuário:

`rpm`

Chame `rpm` para ver quais pacotes de software com fontes estão instalados no sistema:

```
> rpm -qa '*fonts*'
```

Cada pacote de fontes deve satisfazer essa expressão. No entanto, o comando pode retornar alguns falsos positivos, como `fonts-config` (que não é uma fonte e nem inclui fontes).

`fc-list`

Chame `fc-list` para ter uma visão geral sobre as famílias de fontes que podem ser acessadas e saber se elas estão instaladas no sistema ou no diretório pessoal:


```
> fc-list ':' family
```



Nota: Comando `fc-list`

O comando `fc-list` é um agrupador da biblioteca Fontconfig. É possível consultar uma variedade de informações interessantes do Fontconfig ou, para ser mais preciso, de seu cache. Consulte `man 1 fc-list` para obter mais detalhes.

25.2.2 Vendo fontes

Para saber a aparência de uma família de fontes instalada, use o comando **ftview** (pacote **ft2demos**) ou visite <http://fontinfo.opensuse.org/> . Por exemplo, para exibir a fonte FreeMono no ponto 14, use **ftview** da seguinte forma:

```
> ftview 14 /usr/share/fonts/truetype/FreeMono.ttf
```

Se precisar de mais informações, acesse <http://fontinfo.opensuse.org/>  para saber quais estilos (regular, negrito, itálico etc.) e idiomas são suportados.

25.2.3 Consultando fontes

Para consultar a fonte que será usada quando determinado padrão for especificado, use o comando **fc-match**.

Por exemplo, se o padrão já tiver uma fonte instalada, o **fc-match** retornará o nome do arquivo, a família de fontes e o estilo:

```
> fc-match 'Liberation Serif'
LiberationSerif-Regular.ttf: "Liberation Serif" "Regular"
```

Se a fonte desejada não existir no sistema, as regras de correspondência da Fontconfig serão aplicadas para tentar encontrar as fontes disponíveis mais parecidas. Ou seja, a sua solicitação é substituída:

```
> fc-match 'Foo Family'
DejaVuSans.ttf: "DejaVu Sans" "Book"
```

A Fontconfig suporta *álises*: um nome é substituído por outro nome de família. Um exemplo comum é com nomes genéricos, como “sans-serif”, “serif” e “monospace”. Esses nomes de alias podem ser substituídos por nomes reais de família ou até mesmo por uma lista preferencial de nomes de família:

```
> for font in serif sans mono; do fc-match "$font" ; done
DejaVuSerif.ttf: "DejaVu Serif" "Book"
DejaVuSans.ttf: "DejaVu Sans" "Book"
DejaVuSansMono.ttf: "DejaVu Sans Mono" "Book"
```

O resultado pode variar no sistema de acordo com as fontes que estão instaladas.



Nota: Regras de similaridade segundo a Fontconfig

A Fontconfig *sempre* retorna uma família real (se pelo menos uma estiver instalada) de acordo com a solicitação especificada, a mais parecida possível. A “similaridade” depende das métricas internas da Fontconfig e das configurações de usuário ou administrador da Fontconfig.

25.2.4 Instalando fontes

Para instalar uma nova fonte, os seguintes métodos principais estão disponíveis:

1. Instalar manualmente os arquivos de fonte, como `*.ttf` ou `*.otf`, em um diretório de fontes conhecido. Se precisar ser um diretório de todo o sistema, use o padrão `/usr/share/fonts`. Para instalação em seu diretório pessoal, use `~/.config/fonts`. Para sair dos padrões, a Fontconfig permite escolher um diretório diferente. Informe a Fontconfig usando o elemento `<dir>`. Consulte a [Seção 25.2.5.2, “Conhecendo o XML da Fontconfig”](#) para obter os detalhes.
2. Instalar as fontes usando o **zypper**. Muitas fontes já estão disponíveis como um pacote, seja em sua distribuição do SUSE ou no repositório `M17N:fonts`. (<http://download.opensuse.org/repositories/M17N:/fonts/>) ➦ Adicione o repositório à sua lista usando o seguinte comando. Por exemplo, para adicionar um repositório para o SUSE Linux Enterprise Desktop 15 SP4:

```
> sudo zypper ar
    https://download.opensuse.org/repositories/M17N:/fonts/SLE_15/
```

Para procurar o `NOME_DA_FAMÍLIA_DE_FONTES` use este comando:

```
> zypper se 'FONT_FAMILY_NAME*fonts'
```

25.2.5 Configurando a aparência das fontes

Dependendo do meio de renderização e do tamanho da fonte, o resultado pode não ser satisfatório. Por exemplo, um monitor médio atual possui resolução de 100 dpi que torna os pixels grandes demais e os glifos pesados.

Há diversos algoritmos disponíveis para lidar com resoluções baixas, como suavização (atenuação da escala de cinzas), dicas (ajuste à grade) ou renderização de subpixel (triplicação da resolução em uma direção). Esses algoritmos também podem ser diferentes entre um formato de fonte e outro.



Importante: Questões de patentes com a renderização de subpixel

A renderização de subpixel não é usada em distribuições do SUSE. Embora a FreeType2 suporte esse algoritmo, ele envolve várias patentes que vencem no fim do ano de 2019. Portanto, a configuração das opções de renderização de subpixel na Fontconfig não terá nenhum efeito, exceto se o sistema tiver a biblioteca FreeType2 com a renderização de subpixel compilada.

Pela Fontconfig, é possível selecionar um algoritmo de renderização para cada fonte separadamente ou para um conjunto de fontes.

25.2.5.1 Configurando fontes pelo `sysconfig`

O SUSE Linux Enterprise Desktop vem com uma camada do `sysconfig` acima do Fontconfig. Este é um ótimo ponto de partida para testar a configuração da fonte. Para mudar as configurações padrão, edite o arquivo de configuração `/etc/sysconfig/fonts-config`. (ou use o módulo `sysconfig` do YaST). Após editar o arquivo, execute **`fonts-config`**:

```
> sudo /usr/sbin/fonts-config
```

Reinicie o aplicativo para tornar o efeito visível. Lembre-se das seguintes questões:

- Alguns aplicativos precisam ser reiniciados. Por exemplo, o Firefox sempre lê a configuração de Fontconfig de tempos em tempos. As guias recém-criadas ou recarregadas acessam as novas configurações de fontes posteriormente.
- O script **`fonts-config`** é chamado automaticamente após cada instalação ou remoção de pacote (do contrário, trata-se de um bug do pacote de software de fontes).
- É possível substituir temporariamente cada variável `sysconfig` pela opção de linha de comando **`fonts-config`**. Consulte **`fonts-config --help`** para obter os detalhes.

Há diversas variáveis `sysconfig` que podem ser alteradas. Consulte [`man 1 fonts-config`](#) ou a página de ajuda do módulo `sysconfig` do YaST. As seguintes variáveis são alguns exemplos:

Uso de algoritmos de renderização

Considere `FORCE_HINTSTYLE`, `FORCE_AUTOHINT`, `FORCE_BW`, `FORCE_BW_MONOSPACE`, `USE_EMBEDDED_BITMAPS` e `EMBEDDED_BITMAP_LANGAGES`

Listas preferenciais de alíases genéricos

Use `PREFER_SANS_FAMILIES`, `PREFER_SERIF_FAMILIES`, `PREFER_MONO_FAMILIES` e `SEARCH_METRIC_COMPATIBLE`

A lista a seguir mostra alguns exemplos de configuração, começando das fontes “mais legíveis” (mais contraste) até as fontes “mais bonitas” (mais suavizadas).

Fontes de bitmap

Dê preferência às fontes de bitmap por meio das variáveis `PREFER_*_FAMILIES`. Siga o exemplo na seção de Ajuda dessas variáveis. Observe que essas fontes são renderizadas em preto e branco, e não suavizadas, e que as fontes de bitmap estão disponíveis em vários tamanhos. Considere usar

```
SEARCH_METRIC_COMPATIBLE="no"
```

para desabilitar as substituições de nome de família orientadas por compatibilidade de métrica.

Fontes escaláveis renderizadas em preto e branco

As fontes escaláveis renderizadas sem suavização podem produzir resultados parecidos com as fontes de bitmap, enquanto mantêm a escalabilidade da fonte. Use fontes com dicas bem elaboradas, como as famílias Liberation. Não há muitas opções de fontes com dicas bem elaboradas. Defina a seguinte variável para forçar este método:

```
FORCE_BW="yes"
```

Fontes monoespaçadas renderizadas em preto e branco

Somente renderize fontes monoespaçadas sem suavização, do contrário, use as configurações padrão:

```
FORCE_BW_MONOSPACE="yes"
```

Configurações padrão

Todas as fontes são renderizadas com suavização. As fontes com dicas bem elaboradas serão renderizadas com o BCI (*byte code interpreter* — intérprete de código de byte), e o restante com o autohinter (`hintstyle=hintslight`). Deixe todas as variáveis `sysconfig` relevantes com a configuração padrão.

Fontes CFF

Use as fontes no formato CFF. Elas também podem ser consideradas mais legíveis do que as fontes TrueType padrão, por causa das atuais melhorias na FreeType2. Faça um teste com elas seguindo o exemplo de `PREFER_*_FAMILIES`. É possível torná-las mais escuras e colocá-las em negrito com:

```
SEARCH_METRIC_COMPATIBLE="no"
```

já que são renderizadas por `hintstyle=hintslight`, por padrão. Considere usar também:

```
SEARCH_METRIC_COMPATIBLE="no"
```

Autohinter exclusivamente

Mesmo para uma fonte com dicas bem elaboradas, use o autohinter da FreeType2. Isso pode gerar formas de letras mais grossas, às vezes mais confusas, com contraste menor. Defina a seguinte variável para ativá-lo:

```
FORCE_AUTOHINTER="yes"
```

Use `FORCE_HINTSTYLE` para controlar o nível de dicas.

25.2.5.2 Conhecendo o XML da Fontconfig

O formato de configuração da Fontconfig é o *eXtensible Markup Language* (XML). Estes exemplos não são uma referência completa, e sim uma visão geral. Você encontra detalhes e outras inspirações no **man 5 fonts-conf** ou em `/etc/fonts/conf.d/`.

O arquivo de configuração central do Fontconfig é `/etc/fonts/fonts.conf`, que, além de outras coisas, inclui todo o diretório `/etc/fonts/conf.d/`. Para personalizar a Fontconfig, há dois lugares para você fazer as mudanças:

ARQUIVOS DE CONFIGURAÇÃO DA FONTCONFIG

1. **Mudanças de todo o sistema.** Edite o arquivo `/etc/fonts/local.conf` (por padrão, ele inclui um elemento `fontconfig` vazio).
2. **Mudanças específicas do usuário.** Edite o arquivo `~/.config/fontconfig/fonts.conf`. Coloque os arquivos de configuração da Fontconfig no diretório `~/.config/fontconfig/conf.d/`.

As mudanças específicas do usuário sobregravam qualquer configuração de todo o sistema.



Nota: Arquivo de configuração do usuário descontinuado

O arquivo `~/.fonts.conf` está marcado como descontinuado e não deve mais ser usado. Use agora o `~/.config/fontconfig/fonts.conf`.

Cada arquivo de configuração precisa ter um elemento `fontconfig`. Dessa forma, o arquivo mínimo terá a seguinte aparência:

```
<?xml version="1.0"?>
  <!DOCTYPE fontconfig SYSTEM "fonts.dtd">
  <fontconfig>
    <!-- Insert your changes here -->
  </fontconfig>
```

Se os diretórios padrão não forem suficientes, insira o elemento `dir` com o respectivo diretório:

```
<dir>/usr/share/fonts2</dir>
```

A Fontconfig procura as fontes *repetidamente*.

É possível escolher os algoritmos de renderização de fonte com o seguinte trecho da Fontconfig (consulte o [Exemplo 25.1, "Especificando algoritmos de renderização"](#)):

EXEMPLO 25.1: ESPECIFICANDO ALGORITMOS DE RENDERIZAÇÃO

```
<match target="font">
  <test name="family">
```

```

    <string>FAMILY_NAME</string>
  </test>
  <edit name="antialias" mode="assign">
    <bool>true</bool>
  </edit>
  <edit name="hinting" mode="assign">
    <bool>true</bool>
  </edit>
  <edit name="autohint" mode="assign">
    <bool>false</bool>
  </edit>
  <edit name="hintstyle" mode="assign">
    <const>hintfull</const>
  </edit>
</match>

```

É possível testar várias propriedades de fontes. Por exemplo, o elemento `<test>` pode testar a família de fontes (conforme mostrado no exemplo), o intervalo de tamanhos, o espaçamento, o formato da fonte, etc. Quando `<test>` é completamente abandonado, todos os elementos `<edit>` são aplicados a cada fonte (mudança global).

EXEMPLO 25.2: SUBSTITUIÇÕES DE ÁLIAS E NOME DE FAMÍLIA

Regra 1

```

<alias>
  <family>Alegreya SC</family>
  <default>
    <family>serif</family>
  </default>
</alias>

```

Regra 2

```

<alias>
  <family>serif</family>
  <prefer>
    <family>Droid Serif</family>
  </prefer>
</alias>

```

Regra 3

```

<alias>

```

```

<family>serif</family>
<accept>
  <family>STIXGeneral</family>
</accept>
</alias>

```

As regras do [Exemplo 25.2, “Substituições de alias e nome de família”](#) criam uma PFL (*prioritized family list* — lista prioritária de famílias). Dependendo do elemento, são executadas ações diferentes:

<default> da [Regra 1](#)

Esta regra adiciona um nome da família serif *ao fim* da PFL.

<prefer> da [Regra 2](#)

Essa regra adiciona “Droid Serif” *logo antes* da primeira ocorrência de serif na PFL, sempre que Alegreya SC está presente na PFL.

<accept> da [Regra 3](#)

Esta regra adiciona o nome da família “STIXGeneral” *logo depois da* primeira ocorrência do nome da família serif na PFL.

Juntando tudo isso, quando os trechos ocorrem na ordem [Regra 1](#), [Regra 2](#) e [Regra 3](#) e o usuário solicita “Alegreya SC”, a PFL é criada conforme mostrado na [Tabela 25.1, “Gerando a PFL com base nas regras da Fontconfig”](#).

TABELA 25.1: GERANDO A PFL COM BASE NAS REGRAS DA FONTCONFIG

Ordem	PFL atual
Solicitação	<u>Alegreya SC</u>
Regra 1	<u>Alegreya SC</u> , <u>serif</u>
Regra 2	<u>Alegreya SC</u> , <u>Droid Serif</u> , <u>serif</u>
Regra 3	<u>Alegreya SC</u> , <u>Droid Serif</u> , <u>serif</u> , <u>STIXGeneral</u>

Nas métricas da Fontconfig, o nome da família tem a maior prioridade sobre outros padrões, como estilo, tamanho etc. A Fontconfig verifica qual família está instalada no sistema. Se “Alegreya SC” estiver instalada, a Fontconfig a retornará. Do contrário, ela solicitará “Droid Serif”, etc

Tenha cuidado. Quando a ordem dos trechos da Fontconfig é modificada, a Fontconfig poderá retornar resultados diferentes, conforme mostrado na *Tabela 25.2, “Resultados da geração da PFL com base nas regras da Fontconfig com a ordem modificada”*.

TABELA 25.2: RESULTADOS DA GERAÇÃO DA PFL COM BASE NAS REGRAS DA FONTCONFIG COM A ORDEM MODIFICADA

Ordem	PFL atual	Nota
Solicitação	<u>Alegreya SC</u>	Mesma solicitação efetuada.
<i>Regra 2</i>	<u>Alegreya SC</u>	<u>serif</u> não está na PFL; nada é substituído
<i>Regra 3</i>	<u>Alegreya SC</u>	<u>serif</u> não está na PFL; nada é substituído
<i>Regra 1</i>	<u>Alegreya SC</u> , <u>serif</u>	<u>Alegreya SC</u> presente na PFL; a substituição é realizada



Nota: Implicação

Pense no alias <default> como uma classificação ou inclusão deste grupo (se não estiver instalado). Conforme mostrado no exemplo, <default> sempre deve preceder os aliases <prefer> e <accept> deste grupo.

A classificação <default> não se limita aos aliases genéricos serif, sans-serif e monospace. Consulte /usr/share/fontconfig/conf.avail/30-metric-aliases.conf para ver um exemplo complexo.

O seguinte trecho da Fontconfig no *Exemplo 25.3, “Substituições de alias e nome de família”* cria um grupo serif. Cada família desse grupo poderá substituir outras famílias, caso ainda não exista uma fonte instalada.

EXEMPLO 25.3: SUBSTITUIÇÕES DE ÁLIAS E NOME DE FAMÍLIA

```
<alias>
<family>Alegreya SC</family>
<default>
  <family>serif</family>
</default>
```

```

</alias>
<alias>
  <family>Droid Serif</family>
  <default>
    <family>serif</family>
  </default>
</alias>
<alias>
  <family>STIXGeneral</family>
  <default>
    <family>serif</family>
  </default>
</alias>
<alias>
  <family>serif</family>
  <accept>
    <family>Droid Serif</family>
    <family>STIXGeneral</family>
    <family>Alegreya SC</family>
  </accept>
</alias>

```

A prioridade é aplicada seguindo a ordem do álías `<accept>`. Da mesma forma, é possível usar os álíases `<prefer>` mais fortes.

O *Exemplo 25.2, “Substituições de álías e nome de família”* é expandido pelo *Exemplo 25.4, “Substituições de álías e nome de família”*.

EXEMPLO 25.4: SUBSTITUIÇÕES DE ÁLIAS E NOME DE FAMÍLIA

Regra 4

```

<alias>
  <family>serif</family>
  <accept>
    <family>Liberation Serif</family>
  </accept>
</alias>

```

Regra 5

```

<alias>
  <family>serif</family>
  <prefer>
    <family>DejaVu Serif</family>
  </prefer>
</alias>

```

A configuração expandida do *Exemplo 25.4, “Substituições de alias e nome de família”* leva à seguinte evolução da PFL:

TABELA 25.3: RESULTADOS DA GERAÇÃO DA PFL COM BASE NAS REGRAS DA FONTCONFIG

Ordem	PFL atual
Solicitação	<u>Alegreya SC</u>
<i>Regra 1</i>	<u>Alegreya SC, serif</u>
<i>Regra 2</i>	<u>Alegreya SC, Droid Serif, serif</u>
<i>Regra 3</i>	<u>Alegreya SC, Droid Serif, serif, STIXGeneral</u>
<i>Regra 4</i>	<u>Alegreya SC, Droid Serif, serif, Liberation Serif, STIXGeneral</u>
<i>Regra 5</i>	<u>Alegreya SC, Droid Serif, DejaVu Serif, serif, Liberation Serif, STIXGeneral</u>



Nota: Implicações.

- Caso haja várias declarações <accept> para o mesmo nome genérico, a declaração que for analisada por último “vencerá”. Se possível, não use <accept> **após** o usuário (/etc/fonts/conf.d/*-user.conf) ao criar uma configuração de todo o sistema.
- Caso haja várias declarações <prefer> para o mesmo nome genérico, a declaração que for analisada por último “vencerá”. Se possível, não use <prefer> **antes** do usuário na configuração de todo o sistema.
- Cada declaração <prefer> sobregrava as declarações <accept> para o mesmo nome genérico. Se o administrador deseja permitir que o usuário utilize <accept>, e não apenas <prefer>, ele não deverá usar <prefer> na configuração de todo o sistema. Por outro lado, como os usuários costumam utilizar mais <prefer>, isso não deve ter nenhum efeito negativo. Observamos também o uso de <prefer> nas configurações de todo o sistema.

25.3 Configuração do GNOME para administradores

25.3.1 Sistema dconf

da área de trabalho do GNOME é gerenciada com `dconf`. Trata-se de um banco de dados hierarquicamente estruturado ou um registro que permite que os usuários modifiquem suas configurações pessoais e os administradores de sistema definam valores padrão ou obrigatórios para todos os usuários. O `dconf` substitui o sistema `gconf` do GNOME 2.

Use o **`dconf-editor`** para ver as opções do `dconf` com uma interface gráfica do usuário. Use o **`dconf`** para acessar e modificar as opções de configuração com a linha de comando.

A ferramenta **Ajustes** do GNOME oferece uma interface do usuário fácil de usar para opções de configuração adicionais, além da configuração normal do GNOME. A ferramenta pode ser iniciada no menu de aplicativos do GNOME ou por linha de comando com **`gnome-tweak-tool`**.

25.3.2 Configuração de todo o sistema

É possível definir os parâmetros globais de configuração do `dconf` no diretório `/etc/dconf/db/`. Isso inclui a configuração do GDM ou o bloqueio de determinadas opções de configuração para os usuários.

Siga o procedimento abaixo como exemplo para criar uma configuração de todo o sistema:

1. Crie um novo diretório que termine com `.d` em `/etc/dconf/db/`. Esse diretório pode conter uma quantidade arbitrária de arquivos de texto com opções de configuração. Para este exemplo, crie o arquivo `/etc/dconf/db/network.d/00-proxy` com o seguinte conteúdo:

```
# This is a comment
[system/proxy/http]
host='10.0.0.1'
enabled=true
```

2. Analise as novas diretivas de configuração em relação ao formato de banco de dados `dconf`:

```
> sudo dconf update
```

3. Adicione o novo banco de dados de configuração de rede ao perfil de usuário padrão criando o arquivo /etc/dconf/profiles/user. Em seguida, adicione o conteúdo abaixo:

```
system-db:network
```

O arquivo /etc/dconf/profiles/user é um padrão do GNOME que será usado. Outros perfis podem ser definidos na variável de ambiente DCONF_PROFILE.

4. Opcional: Para bloquear a configuração de proxy aos usuários, crie o arquivo /etc/dconf/db/network/locks/proxy. Em seguida, adicione uma linha a esse arquivo com as chaves que não podem ser mudadas:

```
/system/proxy/http/host  
/system/proxy/http/enabled
```

Você pode usar o **dconf-editor** gráfico para criar um perfil com um usuário e, em seguida, usar **dconf dump /** para listar todas as opções de configuração. Depois disso, as opções de configuração poderão ser armazenadas em um perfil global.

Uma descrição detalhada da configuração global está disponível em <https://wiki.gnome.org/Projects/dconf/SystemAdministrators> [↗](#).

25.3.3 Mais informações

Para obter mais informações, consulte a <http://help.gnome.org/admin/> [↗](#).

25.4 Alternando entre as GPUs Intel e NVIDIA Optimus com o SUSE Prime

O SUSE Prime é uma ferramenta para alternar entre as Unidades de Processamento Gráfico (GPUs, Graphical Processing Units) Intel e as GPUs NVIDIA equipadas com a tecnologia Optimus de "gráficos comutáveis" da NVIDIA. O Optimus oferece um mecanismo para alternar facilmente entre uma GPU Intel integrada e uma GPU NVIDIA separada. Ele foi projetado para executar um laptop no modo de economia de energia ou com desempenho máximo: use a GPU Intel para economizar energia e a GPU NVIDIA para aplicativos 3D.

O SUSE Prime faz parte da SUSE Linux Enterprise Workstation Extension para SUSE Linux Enterprise 15 SP4.

O SUSE Prime funciona apenas em sistemas com o X11, não o Wayland. Se o seu sistema tem o Wayland, você deve desabilitá-lo e efetuar fallback para o X11, se quiser usar o SUSE Prime (consulte a [Seção 25.4.1, “Pré-requisitos”](#)).

25.4.1 Pré-requisitos

Você deve ter uma GPU NVIDIA Optimus configurada e ativa que usa os drivers NVIDIA incluídos no SUSE Linux Enterprise 15 SP4 (consulte a [Seção 25.4.3, “Instalando drivers NVIDIA”](#)) e uma GPU Intel integrada. O Bumblebee, a ferramenta de comutação mais antiga do NVIDIA Optimus, não deve ser instalado.

Não deve haver um arquivo `/etc/X11/xorg.conf` e nenhum arquivo de configuração com as seções "ServerLayout", "Device" ou "Screen" ativas no diretório `/etc/X11/xorg.conf.d`.

O SUSE Prime funciona apenas com o X11. Use o comando `loginctl` para verificar se o seu sistema usa o X11 ou o Wayland:

```
> loginctl
  SESSION      UID USER      SEAT      TTY
          2      1000 tux        seat0
> loginctl show-session 2|grep Type
Type=x11
```

Se ele usar o Wayland, desabilite-o editando o `/etc/gdm/custom.conf` e removendo o comentário `WaylandEnable=false`. Em seguida, reinicialize-o.

25.4.2 Instalando e usando o SUSE Prime

Sua placa de vídeo NVIDIA já deve estar instalada e funcionando. Se não estiver, consulte a [Seção 25.4.3, “Instalando drivers NVIDIA”](#).

Instale o pacote `suse-prime`:

```
> sudo zypper install suse-prime
```

Para alternar sua GPU, execute um dos seguintes comandos, efetue logout e login novamente:

```
> sudo prime-select intel
> sudo prime-select intel2
> sudo prime-select nvidia
```

Use o driver **intel** quando ele for o driver modesetting. O **intel2** é para sistemas que usam o driver **xf86-video-intel**. Você pode obter essa informação instalando e executando o **inxi**:

```
> inxi -G
Graphics: Device-1: Intel Xeon E3-1200 v3/4th Gen Core Processor Integrated Graphics
Controller
Display Server: x11(X.org 1.20.1 ) drivers: modesetting (unloaded: fbdev, vesa)
Resolution: 1920x1080@60.00hz
OpenGL: renderer: Mesa DRI Intel Haswell Desktop version: 4.5 Mesa 18.2.8
```

Qual GPU está ativa no momento?

```
> sudo /usr/sbin/prime-select get-current
Driver configured: intel
```

25.4.3 Instalando drivers NVIDIA

Se você precisa identificar sua placa NVIDIA para saber qual driver usar, execute o seguinte comando:

```
> /sbin/lspci | grep VGA
```

Siga estas etapas para instalar os drivers com o Zypper.

Liste os pacotes de driver disponíveis:

```
> sudo zypper se nvidia
```

Em seguida, instale os drivers para sua placa de vídeo NVIDIA:

```
> sudo zypper se packagename
```

26 Acessando sistemas de arquivos com o FUSE

FUSE é o acrônimo de *file system in user space* (sistema de arquivos no espaço do usuário). Isso significa que você pode configurar e montar um sistema de arquivos como um usuário sem privilégios. Normalmente, você precisa ser o root para executar esta tarefa. O FUSE, isoladamente, é um módulo de kernel. Combinado a plug-ins, ele permite estender o FUSE para acessar quase todos os sistemas de arquivos, como conexões SSH remotas, imagens ISO, etc.

26.1 Configurando o FUSE

Antes de usar o FUSE, é necessário instalar o pacote fuse. Dependendo do sistema de arquivos que você deseja usar, serão necessários plug-ins adicionais, disponíveis em pacotes separados. Em geral, não é necessário configurar o FUSE. Mas vale a pena criar um diretório com todos os pontos de montagem combinados. Por exemplo, você pode criar um diretório ~/mounts e inserir nele subdiretórios para os diferentes sistemas de arquivo.

26.2 Montando uma partição NTFS

NTFS, *New Technology File System*, é o sistema de arquivos padrão do Windows. Em circunstâncias normais, como o usuário sem privilégio não pode montar dispositivos de blocos NTFS usando a biblioteca FUSE externa, o processo de montagem de uma partição do Windows descrito a seguir requer privilégios de root. A montagem de partições NTFS é suportada apenas no SUSE Linux Enterprise Server e no SUSE Linux Enterprise Desktop com SUSE Linux Enterprise Workstation Extension.

1. Torne-se root e instale o pacote ntfs-3g. Ele está disponível na SUSE Linux Enterprise Workstation Extension.
2. Crie um diretório para ser usado como ponto de montagem, por exemplo, ~/mounts/windows.

3. Descubra de qual partição do Windows você precisa. Use o YaST e inicie o módulo particionador para saber qual partição pertence ao Windows, mas não modifique nada. Como alternativa, torne-se `root` e execute `/sbin/fdisk -l`. Procure as partições com o tipo `HPFS/NTFS`.
4. Monte a partição no modo leitura-gravação. Substitua o marcador `DISPOSITIVO` pela sua partição do Windows correspondente:

```
> ntfs-3g /dev/DEVICE MOUNT POINT
```

Para usar a partição do Windows no modo apenas leitura, anexe `-o ro`:

```
> ntfs-3g /dev/DEVICE MOUNT POINT -o ro
```

O comando `ntfs-3g` usa o usuário (UID) e o grupo (GID) atual para montar o dispositivo especificado. Para definir permissões de gravação para outro usuário, use o comando `id` `USUÁRIO` para obter a saída dos valores de UID e GID. Defina-a com:

```
# id tux
uid=1000(tux) gid=100(users) groups=100(users),16(dialout),33(video)
ntfs-3g /dev/DEVICE MOUNT POINT -o uid=1000,gid=100
```

Há mais opções disponíveis na página de manual.

Para desmontar um recurso, execute `fusermount -u PONTO DE MONTAGEM`.

26.3 Mais informações

Para obter mais informações, consulte a home page do FUSE em <https://github.com/libfuse/libfuse>.

27 Instalando várias versões do kernel

O SUSE Linux Enterprise Desktop suporta a instalação paralela de várias versões do kernel. Ao instalar um segundo kernel, uma entrada de boot e um initrd são automaticamente criados, dessa forma, nenhuma outra configuração manual é necessária. Ao reiniciar a máquina, o kernel recém-adicionado fica disponível como mais um parâmetro de boot.

Usando esta funcionalidade, você pode testar as atualizações do kernel com segurança e sempre realizar fallback para o kernel anterior comprovado. Para isso, não use as ferramentas de atualização (como a Atualização Online do YaST ou o applet de atualização). Em vez disso, siga o processo descrito neste capítulo.



Atenção: Direito a suporte

Fique ciente de que você perde todo o seu direito a suporte para a máquina ao instalar um kernel autocompilado ou de terceiros. Somente os kernels distribuídos com o SUSE Linux Enterprise Desktop e os kernels disponibilizados pelos canais de atualização oficiais do SUSE Linux Enterprise Desktop são suportados.



Dica: Verificar o kernel de configuração do carregador de boot

É recomendável verificar a configuração do carregador de boot após a instalação de outro kernel para definir a entrada de boot padrão de sua escolha. Consulte a [Seção 18.3, “Configurando o carregador de boot com o YaST”](#) para obter mais informações.

27.1 Habilitando e configurando suporte multiversão

A instalação de várias versões de um pacote de software (suporte multiversão) está habilitada por padrão a partir do SUSE Linux Enterprise Server 12. Para verificar essa configuração, faça o seguinte:

1. Abra `/etc/zypp/zypp.conf` como `root` no editor de sua escolha.

2. Pesquise pela string `multiversion` (multiversão). Se a multiversão estiver habilitada para todos os pacotes do kernel compatíveis com esse recurso, a seguinte linha aparecerá sem comentários:

```
multiversion = provides:multiversion(kernel)
```

3. Para restringir o suporte multiversão a determinados tipos de kernel, adicione os nomes dos pacotes como uma lista separada por vírgula à opção `multiversion` em `/etc/zypp/zypp.conf`, por exemplo

```
multiversion = kernel-default,kernel-default-base,kernel-source
```

4. Grave as mudanças feitas.



Atenção: Pacotes de módulos do kernel (KMP)

Verifique se os módulos do kernel necessários (Pacotes de Módulos do Kernel) distribuídos pelo fornecedor também foram instalados para o novo kernel atualizado. O processo de atualização do kernel não avisa sobre eventuais módulos do kernel que estiverem faltando, porque os requisitos do pacote ainda estão sendo atendidos pelo kernel antigo mantido no sistema.

27.1.1 Apagando kernels não usados automaticamente

Quando novos kernels são testados com frequência com o suporte multiversão habilitado, o menu de boot torna-se rapidamente confuso. Como a partição `/boot` normalmente tem espaço limitado, você também pode ter problemas com overflow de `/boot`. Embora seja possível apagar as versões não usadas do kernel manualmente com o YaST ou o Zypper (conforme descrito a seguir), você também pode configurar o `libzypp` para apagar automaticamente os kernels que não são mais usados. Por padrão, nenhum kernel é apagado.

1. Abra `/etc/zypp/zypp.conf` como `root` no editor de sua escolha.
2. Pesquise pela string `multiversion.kernels` e ative esta opção removendo o comentário da linha. Esta opção usa uma lista separada por vírgula dos seguintes valores:

5.3.18-53.3: manter o kernel com o número de versão especificado

mais recente: manter o kernel com o número de versão mais alto

latest-N: manter o kernel com o Nth número de versão mais alto

em execução: manter o kernel em execução

oldest: manter o kernel com o número de versão mais baixo (o número originalmente incluído no SUSE Linux Enterprise Desktop)

oldest+N: manter o kernel com o Nth número de versão mais baixo

Veja a seguir alguns exemplos

multiversion.kernels = latest,running

Manter o kernel mais recente e o que estiver em execução. Isso é o mesmo que não habilitar o recurso multiversão, com a exceção de que o kernel antigo será removido *após a próxima reinicialização*, e não logo após a instalação.

multiversion.kernels = latest,latest-1,running

Manter os dois últimos kernels e o que estiver em execução.

multiversion.kernels = latest,running,5.3.18-53.3

Manter o kernel mais recente, o que estiver em execução e 5.3.18-53.3.



Dica: Manter o kernel em execução

Exceto se você usa uma configuração especial, sempre mantenha o kernel marcado como running (em execução).

Se você não fizer isso, ele será apagado durante a atualização. Por sua vez, isso significa que todos os módulos do kernel em execução também serão apagados e não poderão mais ser carregados.

Se você decidir não manter o kernel em execução, sempre reinicialize logo após um upgrade do kernel para evitar problemas com os módulos.

27.1.2 Caso de uso: Apagando um kernel antigo apenas depois da reinicialização

É importante garantir que o kernel antigo seja apagado apenas depois que o sistema é reinicializado com êxito com o novo kernel.

Mude a seguinte linha em `/etc/zypp/zypp.conf`:

```
multiversion.kernels = latest,running
```

Os parâmetros anteriores pedem para o sistema manter o kernel mais recente e o que está em execução apenas se eles forem diferentes.

27.1.3 Caso de uso: Mantendo kernels mais antigos como fallback

Convém manter uma ou mais versões de kernel para ter um ou mais kernels “sobressalentes”.

Isso pode ser útil se você precisa de kernels para testes. Se alguma coisa der errado (por exemplo, sua máquina não for inicializada), você ainda poderá usar uma ou mais versões de kernel reconhecidamente boas.

Mude a seguinte linha em `/etc/zypp/zypp.conf`:

```
multiversion.kernels = latest,latest-1,latest-2,running
```

Quando você reinicializa o sistema após a instalação de um novo kernel, o sistema mantém três kernels: o atual (configurado como `latest,running`) e os dois antecessores imediatos (configurados como `latest-1` e `latest-2`).

27.1.4 Caso de uso: Mantendo uma versão específica do kernel

Você faz atualizações de sistema regulares e instala novas versões de kernel. Porém, você também está compilando sua própria versão do kernel e deseja garantir que o sistema a mantenha.

Mude a seguinte linha em `/etc/zypp/zypp.conf`:

```
multiversion.kernels = latest,5.3.18-53.3,running
```

Quando você reinicializa o sistema após a instalação de um novo kernel, o sistema mantém dois kernels: o kernel novo em execução (configurado como `latest,running`) e o seu próprio kernel compilado (configurado como `5.3.18-53.3`).

27.2 Instalando/Removendo várias versões do kernel com o YaST

Você pode instalar ou remover vários kernels com YaST:

1. Inicie o YaST e abra o gerenciador de software em *Software > Gerenciamento de Software*.
2. Liste todos os pacotes capazes de fornecer várias versões escolhendo *Ver > Classificação do pacote > Pacotes com várias versões*.

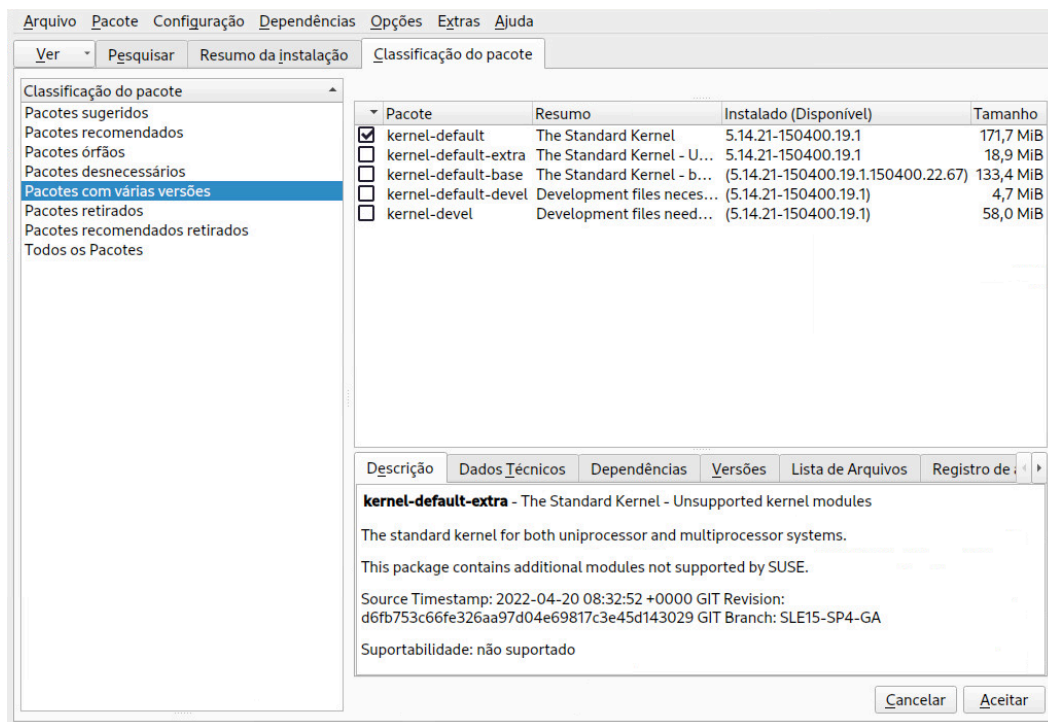


FIGURA 27.1: GERENCIADOR DE SOFTWARE DO YAST: EXIBIÇÃO MULTIVERSÃO

3. Selecione um pacote e abra a guia *Versão* no painel inferior à esquerda.
4. Para instalar um pacote, clique na caixa de seleção ao lado dele. Uma marca de seleção verde indica que ele está selecionado para instalação.
Para remover um pacote já instalado (indicado com uma marca de seleção branca), clique na caixa de seleção ao lado dele até um X vermelho indicar que ele está selecionado para remoção.
5. Clique em *Aceitar* para iniciar a instalação.

27.3 Instalando/Removendo várias versões do kernel com o Zypper

Você pode instalar ou remover vários kernels com o **zypper**:

1. Use o comando **zypper se -s 'kernel*'** para exibir uma lista de todos os pacotes de kernel disponíveis:

S	Name	Type	Version	Arch	Repository
i+	kernel-default	package	5.14.21-150400.6.3	x86_64	SLE-Module-Basesystem15-SP4-Pool
	kernel-default-base	package	5.14.21-150400.6.3.150400.22.27	x86_64	SLE-Module-Basesystem15-SP4-Pool
	kernel-default-devel	package	5.14.21-150400.6.3	x86_64	SLE-Module-Basesystem15-SP4-Pool
	kernel-devel	package	5.14.21-150400.6.4	noarch	SLE-Module-Basesystem15-SP4-Pool
i	kernel-firmware-all	package	20220119-150400.1.1	noarch	SLE-Module-Basesystem15-SP4-Pool
i	kernel-firmware-amdgpu	package	20220119-150400.1.1	noarch	SLE-Module-Basesystem15-SP4-Pool
i	kernel-firmware-ath10k	package	20220119-150400.1.1	noarch	SLE-Module-Basesystem15-SP4-Pool
i	kernel-firmware-ath11k	package	20220119-150400.1.1	noarch	SLE-Module-Basesystem15-SP4-Pool
i	kernel-firmware-atheros	package	20220119-150400.1.1	noarch	SLE-Module-Basesystem15-SP4-Pool
i	kernel-firmware-bluetooth	package	20220119-150400.1.1	noarch	SLE-Module-Basesystem15-SP4-Pool
i	kernel-firmware-bnx2	package	20220119-150400.1.1	noarch	SLE-Module-Basesystem15-SP4-Pool
i	kernel-firmware-brcm	package	20220119-150400.1.1	noarch	SLE-Module-Basesystem15-SP4-Pool
i	kernel-firmware-chelsio	package	20220119-150400.1.1	noarch	SLE-Module-Basesystem15-SP4-Pool
i	kernel-firmware-dpaa2	package	20220119-150400.1.1	noarch	SLE-Module-Basesystem15-SP4-Pool
i	kernel-firmware-i915	package	20220119-150400.1.1	noarch	SLE-Module-Basesystem15-SP4-Pool
i	kernel-firmware-intel	package	20220119-150400.1.1	noarch	SLE-Module-Basesystem15-SP4-Pool
i	kernel-firmware-iwlwifi	package	20220119-150400.1.1	noarch	SLE-Module-Basesystem15-SP4-Pool
i	kernel-firmware-liquidio	package	20220119-150400.1.1	noarch	SLE-Module-Basesystem15-SP4-Pool
i	kernel-firmware-marvell	package	20220119-150400.1.1	noarch	SLE-Module-Basesystem15-SP4-Pool
i	kernel-firmware-media	package	20220119-150400.1.1	noarch	SLE-Module-Basesystem15-SP4-Pool
i	kernel-firmware-mediatek	package	20220119-150400.1.1	noarch	SLE-Module-Basesystem15-SP4-Pool

i	kernel-firmware-mellanox	package	20220119-150400.1.1	noarch	SLE-Module-
Basesystem15-SP4-Pool					
i	kernel-firmware-mwifiex	package	20220119-150400.1.1	noarch	SLE-Module-
Basesystem15-SP4-Pool					
i	kernel-firmware-network	package	20220119-150400.1.1	noarch	SLE-Module-
Basesystem15-SP4-Pool					
i	kernel-firmware-nfp	package	20220119-150400.1.1	noarch	SLE-Module-
Basesystem15-SP4-Pool					
i	kernel-firmware-nvidia	package	20220119-150400.1.1	noarch	SLE-Module-
Basesystem15-SP4-Pool					
i	kernel-firmware-platform	package	20220119-150400.1.1	noarch	SLE-Module-
Basesystem15-SP4-Pool					
i	kernel-firmware-prestera	package	20220119-150400.1.1	noarch	SLE-Module-
Basesystem15-SP4-Pool					
i	kernel-firmware-qcom	package	20220119-150400.1.1	noarch	SLE-Module-
Basesystem15-SP4-Pool					
i	kernel-firmware-qlogic	package	20220119-150400.1.1	noarch	SLE-Module-
Basesystem15-SP4-Pool					
i	kernel-firmware-radeon	package	20220119-150400.1.1	noarch	SLE-Module-
Basesystem15-SP4-Pool					
i	kernel-firmware-realtek	package	20220119-150400.1.1	noarch	SLE-Module-
Basesystem15-SP4-Pool					
i	kernel-firmware-serial	package	20220119-150400.1.1	noarch	SLE-Module-
Basesystem15-SP4-Pool					
i	kernel-firmware-sound	package	20220119-150400.1.1	noarch	SLE-Module-
Basesystem15-SP4-Pool					
i	kernel-firmware-ti	package	20220119-150400.1.1	noarch	SLE-Module-
Basesystem15-SP4-Pool					
i	kernel-firmware-ueagle	package	20220119-150400.1.1	noarch	SLE-Module-
Basesystem15-SP4-Pool					
i	kernel-firmware-usb-network	package	20220119-150400.1.1	noarch	SLE-Module-
Basesystem15-SP4-Pool					
	kernel-macros	package	5.14.21-150400.6.4	noarch	SLE-Module-
Basesystem15-SP4-Pool					

2. Especifique a versão exata ao instalar:

```
> sudo zypper in kernel-default-5.3.18-53.3
```

3. Ao desinstalar um kernel, use os comandos **zypper se -s 'kernel*'** para listar todos os kernels instalados e o **zypper rm NOMEDOPACOTE-VERSÃO** para remover o pacote.

28 Gerenciando módulos do kernel

Embora o Linux seja um kernel monolítico, ele pode ser ampliado usando módulos do kernel. Esses são objetos especiais que podem ser inseridos no kernel e removidos sob demanda. Em termos práticos, os módulos do kernel tornam possível adicionar e remover drivers e interfaces que não estão incluídos no próprio kernel. O Linux dispõe de vários comandos para gerenciar módulos do kernel.

28.1 Listando módulos carregados com lsmod e modinfo

Use o comando **lsmod** para ver os módulos do kernel que estão carregados no momento. A saída do comando pode ter a seguinte aparência:

```
> lsmod
Module                Size  Used by
snd_usb_audio         188416  2
snd_usbmidi_lib        36864  1 snd_usb_audio
hid_plantronics        16384  0
snd_rawmidi            36864  1 snd_usbmidi_lib
snd_seq_device         16384  1 snd_rawmidi
fuse                   106496  3
nfsv3                   45056  1
nfs_acl                16384  1 nfsv3
```

A saída é dividida em três colunas. A coluna Module (Módulo) lista os nomes dos módulos carregados, enquanto a coluna Size (Tamanho) exibe o tamanho de cada módulo. A coluna Used by (Usado por) mostra o número de módulos de referência e seus nomes. Observe que essa lista pode estar incompleta.

Para ver informações detalhadas sobre um módulo do kernel específico, use o comando **modinfo** *NOME_DO_MÓDULO*, em que *NOME_DO_MÓDULO* é o nome do módulo do kernel desejado. Observe que o binário **modinfo** reside no diretório */sbin*, que não está na variável de ambiente *PATH* do usuário. Isso significa que você deve especificar o caminho completo para o binário ao executar o comando **modinfo** como um usuário comum:

```
> /sbin/modinfo kvm
filename:      /lib/modules/5.3.18-57-default/kernel/arch/x86/kvm/kvm.ko.xz
license:      GPL
author:       Qumranet
suserelease:  SLE15-SP3
```

```
srcversion:      3D8FBA9060D4537359A06FC
depends:          irqbypass
supported:       yes
retpoline:       Y
intree:          Y
name:            kvm
vermagic:        5.3.18-57-default SMP mod_unload modversions
```

28.2 Adicionando e removendo módulos do kernel

Embora seja possível usar `insmod` e `rmmod` para adicionar e remover módulos do kernel, em vez disso, é recomendável usar a ferramenta `modprobe`. `modprobe` oferece diversas vantagens importantes, incluindo a resolução automática de dependências e a criação de lista negra.

Quando usado sem parâmetros, o comando `modprobe` instala um módulo do kernel especificado. O `modprobe` deve ser executado com privilégios de root:

```
> sudo modprobe acpi
```

Para remover um módulo do kernel, use o parâmetro `-r`:

```
> sudo modprobe -r acpi
```

28.2.1 Carregando módulos do kernel automaticamente na inicialização

Em vez de carregar os módulos do kernel manualmente, você pode carregá-los automaticamente durante o processo de boot usando o serviço `system-modules-load.service`. Para habilitar um módulo do kernel, adicione um arquivo `.conf` ao diretório `/etc/modules-load.d/`. Convém dar ao arquivo de configuração o mesmo nome do módulo. Por exemplo:

```
/etc/modules-load.d/rt2800usb.conf
```

O arquivo de configuração deve conter o nome do módulo do kernel desejado (por exemplo, `rt2800usb`).

A técnica descrita permite que você carregue os módulos do kernel sem parâmetros. Se você precisar carregar um módulo do kernel com opções específicas, em vez disso, adicione um arquivo de configuração ao diretório `/etc/modprobe.d/`. O arquivo deve ter a extensão `.conf`. O nome do arquivo deve cumprir a seguinte convenção de nomeação: `prioridade-nomedomódulo.conf`. Por exemplo: `50-thinkfan.conf`. O arquivo de configuração deve conter

o nome do módulo do kernel e os parâmetros desejados. Você pode usar o comando de exemplo a seguir para criar um arquivo de configuração com o nome do módulo do kernel e seus parâmetros:

```
> echo "options thinkpad_acpi fan_control=1" | sudo tee /etc/modprobe.d/thinkfan.conf
```



Nota: Carregando módulos do kernel

A maioria dos módulos do kernel é carregada pelo sistema automaticamente quando um dispositivo é detectado ou o espaço do usuário requer funcionalidades específicas. Portanto, a adição manual de módulos a `/etc/modules-load.d/` raramente é necessária.

28.2.2 Adicionando módulos do kernel à lista negra com modprobe

A adição de um módulo do kernel à lista negra o impede de ser carregado durante o processo de boot. Isso pode ser útil quando você deseja desabilitar um módulo que você suspeita ser a causa de problemas no sistema. Você ainda pode carregar manualmente os módulos do kernel que constam na lista negra usando as ferramentas `insmod` ou `modprobe`.

Para adicionar um módulo à lista negra, crie um arquivo `/etc/modprobe.d/60-blacklist-MODULE_NAME.conf` com o seguinte conteúdo:

```
blacklist MODULE_NAME
```

Execute o comando `dracut` como root para gerar uma nova imagem do `initrd` e reinicialize sua máquina (substitua `NAME` pelo nome do `initrd` atual e `KERNELVERSION` pelo kernel que está em execução):

```
> su
echo "blacklist nouveau" >> /etc/modprobe.d/60-blacklist-nouveau.conf
/usr/bin/dracut --logfile /var/log/YaST2/mkinitrd.log --force /boot/$initrd-NAME
$KERNELVERSION
reboot
```

Para desabilitar um módulo do kernel apenas temporariamente, inclua-o na lista negra diretamente durante a inicialização. Para fazer isso, pressione a tecla **E** quando aparecer a tela de boot. Essa ação direciona você para um editor mínimo que permite modificar os parâmetros de boot. Localize a linha que tem a seguinte aparência:

```
linux /boot/vmlinuz...splash= silent quiet showopts
```


Adicione o comando **`modprobe.blacklist=NOME_DO_MÓDULO`** ao fim da linha. Por exemplo:

```
linux /boot/vmlinuz...splash= silent quiet showopts modprobe.blacklist=nouveau
```

Pressione **F10** ou **Ctrl + X** para inicializar com a configuração especificada.

Para adicionar um módulo do kernel à lista negra permanentemente pelo GRUB, abra o arquivo `/etc/default/grub` para edição e adicione a opção **`modprobe.blacklist=NOME_DO_MÓDULO`** ao comando **`GRUB_CMD_LINUX`**. Em seguida, execute o comando **`sudo grub2-mkconfig -o /boot/grub2/grub.cfg`** para habilitar as mudanças.

29 Gerenciamento dinâmico de dispositivos do kernel com udev

O kernel pode adicionar ou remover praticamente qualquer dispositivo em um sistema em execução. Mudanças no estado do dispositivo (se um dispositivo foi conectado ou removido) precisam ser propagadas ao espaço do usuário. Os dispositivos precisam ser configurados no momento em que são conectados e reconhecidos. Os usuários de um determinado dispositivo precisam ser informados sobre qualquer mudança no estado reconhecido desse dispositivo. O `udev` fornece a infraestrutura necessária para manter dinamicamente os arquivos dos nós de dispositivo e os links simbólicos no diretório `/dev`. As regras do `udev` fornecem uma maneira de conectar ferramentas externas ao processamento de evento do dispositivo de kernel. Dessa forma, você pode personalizar o gerenciamento de dispositivos do `udev`, adicionando determinados scripts para execução como parte do gerenciamento de dispositivos do kernel, ou solicitar e importar dados adicionais para avaliar durante o gerenciamento de dispositivos.

29.1 Diretório `/dev`

Os nós de dispositivo no diretório `/dev` fornecem acesso aos dispositivos de kernel correspondentes. Com `udev`, o diretório `/dev` reflete o estado atual do kernel. Cada dispositivo de kernel tem um arquivo de dispositivo correspondente. Se um dispositivo for desconectado do sistema, o nó de dispositivo será removido.

O conteúdo do diretório `/dev` será mantido em um sistema de arquivos temporário, e todos os arquivos serão renderizados a cada inicialização do sistema. Arquivos criados ou modificados manualmente por definição não resistem a uma reinicialização. Os diretórios e arquivos estáticos que sempre devem estar no diretório `/dev`, independentemente do estado do dispositivo de kernel correspondente, podem ser criados com `systemd-tmpfiles`. Os arquivos de configuração estão em `/usr/lib/tmpfiles.d/` e `/etc/tmpfiles.d/`. Para obter mais informações, consulte a página de manual do `systemd-tmpfiles(8)`.

29.2 Kernel `uevents` e `udev`

As informações de dispositivo necessárias são exportadas pelo sistema de arquivos `sysfs`. Para cada dispositivo detectado e inicializado pelo kernel, um diretório com o nome do dispositivo é criado. Ele contém arquivos de atributos com propriedades específicas do dispositivo.

Sempre que um dispositivo é adicionado ou removido, o kernel envia um uevent para notificar o `udev` sobre a mudança. O daemon `udev` lê e analisa todas as regras dos arquivos `/usr/lib/udev/rules.d/*.rules` e `/etc/udev/rules.d/*.rules` na inicialização e as mantém na memória. Se os arquivos de regras forem mudados, adicionados ou removidos, o daemon poderá recarregar sua representação na memória com o comando `udevadm control --reload`. Para obter mais detalhes sobre as regras do `udev` e sua sintaxe, consulte a [Seção 29.6, “Influenciando o gerenciamento de eventos de dispositivo do kernel com as regras do udev”](#).

Cada evento recebido é comparado com o conjunto de regras fornecido. As regras podem adicionar ou modificar chaves de ambiente de eventos, solicitar um nome específico a ser criado pelo nó do dispositivo, adicionar links simbólicos apontando para o nó ou adicionar programas a serem executados após a criação do nó do dispositivo. Os `uevents` de núcleo do driver são recebidos de um soquete netlink do kernel.

29.3 Drivers, módulos do kernel e dispositivos

Os drivers de barramento de kernel pesquisam dispositivos. Para cada dispositivo detectado, o kernel cria uma estrutura de dispositivo interna enquanto o núcleo do driver envia um uevent ao daemon `udev`. Dispositivos de barramento se identificam através de um ID formatado especialmente, que informa o tipo de dispositivo. Geralmente esses IDs consistem em IDs de produto e fornecedor, além de outros valores específicos do subsistema. Cada barramento tem seu próprio esquema para esses IDs, chamados `MODALIAS`. O kernel toma as informações do dispositivo, compõe uma string de ID `MODALIAS` a partir dele e envia essa string junto com o evento. Para um mouse USB, a string tem a seguinte aparência:

```
MODALIAS=usb:v046DpC03Ed2000dc00dsc00dp00ic03isc01ip02
```

Cada driver de dispositivo carrega uma lista de aliases conhecidos para os dispositivos que pode tratar. A lista está contida no próprio arquivo de módulo de kernel. O programa `depmod` lê as listas de ID e cria o arquivo `modules.alias` no diretório `/lib/modules` do kernel para todos os módulos disponíveis atualmente. Com essa infraestrutura, carregar o módulo é fácil como chamar `modprobe` para cada evento com uma chave `MODALIAS`. Se `modprobe $MODALIAS` for chamado, ele corresponderá o alias do dispositivo composto para o dispositivo com os aliases fornecidos pelos módulos. Se uma entrada correspondente for encontrada, o módulo será carregado. Tudo isso é acionado automaticamente pelo `udev`.

29.4 Inicialização e configuração do dispositivo inicial

Todos os eventos de dispositivo que ocorrem durante o processo de boot antes da execução do daemon `udev` são perdidos, pois a infraestrutura para gerenciar esses eventos reside no sistema de arquivos raiz e não está disponível naquele momento. Para cobrir essa perda, o kernel fornece um arquivo `uevent` localizado no diretório de dispositivo de cada dispositivo no sistema de arquivos `sysfs`. Ao gravar `add` para esse arquivo, o kernel envia novamente o mesmo evento como o evento perdido durante a inicialização. Um loop simples em todos os arquivos `uevent` em `/sys` aciona todos os eventos novamente para criar os nós de dispositivo e executar a configuração do dispositivo.

Por exemplo, durante o boot, um mouse USB talvez não seja inicializado pela lógica de boot anterior, pois o driver não está disponível nesse momento. O evento para a descoberta do dispositivo foi perdido e não encontrou um módulo de kernel para o dispositivo. Em vez de pesquisar manualmente os dispositivos conectados, o `udev` solicita todos os eventos de dispositivo do kernel após a disponibilização do sistema de arquivos raiz. Dessa forma, o evento para o dispositivo de mouse USB é executado novamente. Então ele encontra o módulo de kernel no sistema de arquivos raiz montado e o mouse USB pode ser inicializado.

No espaço do usuário, não há diferença visível entre a sequência `coldplug` do dispositivo e a descoberta de dispositivo durante o tempo de execução. Em ambos os casos, as mesmas regras são usadas para correspondência e os mesmos programas configurados são executados.

29.5 Monitorando o daemon udev em execução

O programa `udevadm monitor` pode ser usado para visualizar os eventos centrais do driver e a temporização dos processos de eventos do `udev`.

```
UEVENT[1185238505.276660] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1 (usb)
UDEV [1185238505.279198] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1 (usb)
UEVENT[1185238505.279527] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UDEV [1185238505.285573] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UEVENT[1185238505.298878] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/
input10 (input)
UDEV [1185238505.305026] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/
input10 (input)
UEVENT[1185238505.305442] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/
input10/mouse2 (input)
UEVENT[1185238505.306440] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/
input10/event4 (input)
```

```
UDEV [1185238505.325384] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/
input10/event4 (input)
UDEV [1185238505.342257] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/
input10/mouse2 (input)
```

As linhas `UEVENT` mostram os eventos que o kernel enviou através de netlink. As linhas `UDEV` mostram os handlers de evento do `udev` concluídos. A temporização é impressa em microssegundos. O tempo entre `UEVENT` e `UDEV` é o tempo que o `udev` levou para processar esse evento ou que o daemon `udev` atrasou sua execução para sincronizar esse evento com eventos relacionados e já em execução. Por exemplo, eventos para partições de disco rígido sempre esperam pela conclusão do evento do dispositivo de disco principal, pois os eventos de partição podem se basear nos dados que o evento de disco principal consultou do hardware.

`udevadm monitor --env` mostra o ambiente de evento completo:

```
ACTION=add
DEVPATH=/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10
SUBSYSTEM=input
SEQNUM=1181
NAME="Logitech USB-PS/2 Optical Mouse"
PHYS="usb-0000:00:1d.2-1/input0"
UNIQ=""
EV=7
KEY=70000 0 0 0 0
REL=103
MODALIAS=input:b0003v046DpC03Ee0110-e0,1,2,k110,111,112,r0,1,8,amlsfw
```

O `udev` também envia mensagens para o syslog. A prioridade syslog padrão que controla as mensagens que são enviadas ao syslog é especificada no arquivo de configuração do `udev` `/etc/udev/udev.conf`. A prioridade de registro do daemon em execução pode ser modificada com `udevadm control --log_priority= NÍVEL/NÚMERO`.

29.6 Influenciando o gerenciamento de eventos de dispositivo do kernel com as regras do udev

Uma regra do `udev` pode corresponder a qualquer propriedade que o kernel adiciona ao evento propriamente dito ou a qualquer informação que o kernel exporta para `sysfs`. A regra também pode solicitar informações adicionais de programas externos. Os eventos são comparados com todas as regras incluídas nos diretórios `/usr/lib/udev/rules.d/` (para regras padrão) e `/etc/udev/rules.d` (configuração específica do sistema).

Cada linha no arquivo de regras contém pelo menos um par de valores de chave. Há dois tipos de chaves, de atribuição e correspondência. Se todas as chaves de correspondência corresponderem aos valores, a regra será aplicada e as chaves de atribuição serão atribuídas ao valor especificado. Uma regra correspondente pode especificar o nome do nó do dispositivo, adicionar links simbólicos apontando para o nó ou executar um programa especificado como parte do gerenciamento de eventos. Se nenhuma regra de correspondência for encontrada, o nome do nó de dispositivo padrão será usado para criar o nó de dispositivo. As informações detalhadas sobre a sintaxe da regra e as chaves fornecidas para corresponder ou importar os dados estão descritas na página de manual do `udev`. As regras de exemplo a seguir apresentam uma introdução básica à sintaxe da regra do `udev`. As regras de exemplo são todas extraídas do conjunto de regras padrão do `udev` `/usr/lib/udev/rules.d/50-udev-default.rules`.

EXEMPLO 29.1: REGRAS `udev` DE EXEMPLO

```
# console
KERNEL=="console", MODE="0600", OPTIONS="last_rule"

# serial devices
KERNEL=="ttyUSB*", ATTRS{product}=="[Pp]alm*Handheld*", SYMLINK+="pilot"

# printer
SUBSYSTEM=="usb", KERNEL=="lp*", NAME="usb/%k", SYMLINK+="usb%k", GROUP="lp"

# kernel firmware loader
SUBSYSTEM=="firmware", ACTION=="add", RUN+="firmware.sh"
```

A regra do `console` consiste em três chaves: uma chave de correspondência (`KERNEL`) e duas chaves de atribuição (`MODE`, `OPTIONS`). A regra de correspondência `KERNEL` pesquisa qualquer item do tipo `console` na lista de dispositivos. Apenas correspondências exatas são válidas e acionam essa regra para que seja executada. A chave `MODE` atribui permissões especiais ao nó de dispositivo, neste caso, permissões de leitura e gravação apenas ao proprietário desse dispositivo. A chave `OPTIONS` torna esta a última regra a ser aplicada a qualquer dispositivo desse tipo. Qualquer regra posterior que corresponda a esse tipo de dispositivo em particular não terá nenhum efeito.

A regra dos `serial devices` não está mais disponível em `50-udev-default.rules`, mas ainda vale a pena ser considerada. Consiste em duas chaves de correspondência (`KERNEL` e `ATTRS`) e uma de atribuição (`SYMLINK`). A chave `KERNEL` procura todos os dispositivos do tipo `ttyUSB`. Usando o curinga `*`, essa chave corresponde a diversos desses dispositivos. A segunda chave de correspondência, `ATTRS`, verifica se o arquivo de atribuição do `produto` em `sysfs` para

qualquer dispositivo `ttyUSB` contém uma determinada string. A chave de atribuição (`SYMLINK`) aciona a adição de um link simbólico para esse dispositivo em `/dev/pilot`. O operador usado nessa chave (`+=`) diz ao para executar essa ação adicionalmente, mesmo se regras anteriores ou posteriores adicionarem outros links simbólicos. `udev` Como essa regra contém duas chaves de correspondência, ela é aplicada apenas se ambas as condições são cumpridas.

A regra da `printer` lida com impressoras USB e contém duas chaves de correspondência que devem ser aplicadas para que a regra inteira seja aplicada (`SUBSYSTEM` e `KERNEL`). Três chaves de atribuição lidam com a nomeação desse tipo de dispositivo (`NAME`), a criação dos links de dispositivo simbólicos (`SYMLINK`) e a participação no grupo desse tipo de dispositivo (`GROUP`). O uso do curinga `*` na chave `KERNEL` faz com que ela corresponda a diversos dispositivos de impressora `lp`. Substituições são usadas pelo nome do dispositivo interno tanto na chave `NAME` quanto na `SYMLINK` para estender essas strings. Por exemplo, o link simbólico para a primeira impressora USB `lp` seria `/dev/usb/lp0`.

A regra do `kernel firmware loader` faz com que o `udev` carregue um firmware adicional por um script de assistente externo durante o tempo de execução. A chave de correspondência `SUBSYSTEM` procura o subsistema de `firmware`. A chave `ACTION` verifica se algum dispositivo pertencente ao subsistema de `firmware` foi adicionado. A chave `RUN+=` aciona a execução do script `firmware.sh` para localizar o firmware a ser carregado.

Algumas características são comuns a todas as regras:

- Cada regra é composta por um ou mais pares de valores de chaves separados por vírgula.
- A operação de uma chave é determinada pelo operador. As regras do `udev` suportam diversos operadores.
- Cada valor dado deve estar entre aspas.
- Cada linha do arquivo de regras representa uma regra. Se a regra for maior do que uma linha, use `\` para unir as linhas diferentes como se faz na sintaxe do shell.
- As regras do `udev` suportam um padrão no estilo do shell que corresponde aos padrões de `*`, `?` e `[]`.
- As regras do `udev` suportam substituições.

29.6.1 Usando operadores nas regras do udev

Ao criar chaves, você pode escolher dentre vários operadores, dependendo do tipo de chave que deseja criar. Normalmente, as chaves de correspondência são usadas para localizar um valor que corresponda ou explicitamente não corresponda ao valor da pesquisa. As chaves de correspondência contêm um dos seguintes operadores:

==

Comparar para igualdade. Se a chave contém um padrão de pesquisa, todos os resultados correspondentes a esse padrão são válidos.

!=

Comparar para não igualdade. Se a chave contém um padrão de pesquisa, todos os resultados correspondentes a esse padrão são válidos.

Qualquer um dos operadores a seguir também pode ser usado com chaves de atribuição:

=

Atribuir um valor a uma chave. Se a chave consistia anteriormente em uma lista de valores, ela é redefinida e apenas o valor único é atribuído.

+=

Adicionar um valor a uma chave que contenha uma lista de entradas.

:=

Atribuir um valor final. Não permitir nenhuma mudança posterior por regras posteriores.

29.6.2 Usando substituições nas regras do udev

As regras do udev suportam o uso de marcadores e substituições. Use-as como faria em qualquer outro script. É possível usar as seguintes substituições com as regras do udev:

%r, \$root

O diretório do dispositivo, /dev por padrão.

%p, \$devpath

O valor de DEVPATH.

%k, \$kernel

O valor de KERNEL ou o nome do dispositivo interno.

%n, \$number

O nome do dispositivo.

%N, \$tempnode

O nome temporário do arquivo de dispositivo.

%M, \$major

O número maior do dispositivo.

%m, \$minor

O número menor do dispositivo.

%s{ATRIBUTO}, \$attr{ATRIBUTO}

O valor de um atributo sysfs (especificado por ATRIBUTO).

%E{VARIÁVEL}, \$env{VARIÁVEL}

O valor de uma variável de ambiente (especificado por VARIÁVEL).

%c, \$result

A saída de PROGRAM.

%%

O caractere %.

\$\$

O caractere \$.

29.6.3 Usando as chaves de correspondência do udev

As chaves de correspondência descrevem as condições que devem ser atendidas para aplicar uma regra do udev. As seguintes chaves de correspondência estão disponíveis:

ACTION

O nome da ação do evento, por exemplo, add ou remove na adição ou remoção de um dispositivo.

DEVPATH

O caminho do dispositivo do evento, por exemplo, DEVPATH=/bus/pci/drivers/ipw3945 para procurar todos os eventos relacionados ao driver ipw3945.

KERNEL

O nome interno (do kernel) do dispositivo do evento.

SUBSYSTEM

O subsistema do dispositivo do evento, por exemplo, SUBSYSTEM=usb para todos os eventos relacionados a dispositivos USB.

ATTR{NOMEDEARQUIVO}

Atributos sysfs do dispositivo do evento. Para corresponder a uma string contida no nome de arquivo do atributo vendor, você poderia usar ATTR{vendor}=="On[sS]tream", por exemplo.

KERNELS

Permite que o udev pesquise o caminho do dispositivo para encontrar um nome de dispositivo correspondente.

SUBSYSTEMS

Permite que o udev pesquise o caminho do dispositivo para encontrar um nome de subsistema do dispositivo correspondente.

DRIVERS

Permite que o udev pesquise o caminho do dispositivo para encontrar um nome de driver do dispositivo correspondente.

ATTRS{NOMEDEARQUIVO}

Permite que o udev pesquise o caminho do dispositivo para encontrar um com valores de atributo sysfs correspondentes.

ENV{CHAVE}

O valor de uma variável de ambiente, por exemplo, ENV{ID_BUS}="ieee1394" para procurar todos os eventos relacionados ao ID do barramento FireWire.

PROGRAM

Permite que o udev execute um programa externo. Para ser bem-sucedido, o programa deve retornar com código de saída zero. A saída do programa, impressa em STDOUT, está disponível para a chave RESULT.

RESULT

Corresponder à string de saída da última chamada de PROGRAM. Incluir esta chave na mesma regra que a chave PROGRAM ou em uma posterior.

29.6.4 Usando as chaves de atribuição do udev

Em contraste com as chaves de correspondência descritas anteriormente, as chaves de atribuição não descrevem condições que devem ser cumpridas. Elas atribuem valores, nomes e ações aos nós do dispositivo mantidos pelo udev.

NOME

O nome do nó de dispositivo a ser criado. Depois que uma regra definir o nome de um nó, todas as outras regras com a chave NAME referente a esse nó serão ignoradas.

SYMLINK

O nome de um link simbólico relacionado ao nó a ser criado. Várias regras de correspondência podem adicionar links simbólicos a serem criados com o nó do dispositivo. Você também pode especificar vários links simbólicos para um nó em uma regra usando o caractere de espaço para separar os nomes dos links simbólicos.

OWNER, GROUP, MODE

As permissões do novo nó de dispositivo. Os valores especificados aqui sobregravam qualquer coisa que tenha sido compilada.

ATTR{CHAVE}

Especifica um valor para ser gravado no atributo sysfs do dispositivo de evento. Se o operador == é usado, essa chave também é usada para corresponder com o valor de um atributo sysfs.

ENV{CHAVE}

Indica ao udev para exportar uma variável para o ambiente. Se o operador == é usado, essa chave também é usada para corresponder com uma variável de ambiente.

RUN

Indica ao udev para adicionar um programa à lista de programas a serem executados neste dispositivo. Lembre-se de restringir isso a tarefas muito curtas, a fim de evitar o bloqueio de outros eventos para esse dispositivo.

LABEL

Adicionar um rótulo para onde um GOTO possa ir.

GOTO

Indicar ao udev para ignorar várias regras e continuar com uma que inclua o rótulo citado pela chave GOTO.

IMPORT{TIPO}

Carregar variáveis para o ambiente do evento, como a saída de um programa externo. O udev importa variáveis de diversos tipos. Se nenhum tipo for especificado, o udev tentará determinar o tipo sozinho, com base na parte executável das permissões do arquivo.

- program diz ao udev para executar um programa externo e importar sua saída.
- file diz ao udev para importar um arquivo texto.
- parent diz ao udev para importar as chaves armazenadas do dispositivo pai.

WAIT_FOR_SYSFS

Indica ao udev para aguardar a criação do arquivo sysfs especificado para determinado dispositivo. Por exemplo, WAIT_FOR_SYSFS="ioerr_cnt" informa o udev para aguardar até que o arquivo ioerr_cnt seja criado.

OPTIONS

A chave OPTION pode ter vários valores:

- last_rule diz ao udev para ignorar todas as regras posteriores.
- ignore_device diz ao udev para ignorar esse evento completamente.
- ignore_remove diz ao udev para ignorar todos os eventos de remoção posteriores para o dispositivo.
- all_partitions diz ao udev para criar nós de dispositivo para todas as partições disponíveis em um dispositivo de bloco.

29.7 Nomeação persistente de dispositivos

O diretório do dispositivo dinâmico e a infraestrutura de regras do udev possibilitam especificar nomes estáveis para todos os dispositivos de disco, independentemente da ordem de reconhecimento ou da conexão usada para o dispositivo. Cada dispositivo de bloco apropriado criado pelo kernel é examinado por ferramentas com conhecimento especial sobre determinados barramentos, tipos de unidade ou sistemas de arquivos. Com o nome do nó do dispositivo fornecido pelo kernel dinâmico, o udev mantém as classes de links persistentes apontando para o dispositivo:

```
/dev/disk
```

```

|-- by-id
| |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B -> ../../sda
| |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part1 -> ../../sda1
| |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part6 -> ../../sda6
| |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part7 -> ../../sda7
| |-- usb-Generic_STORAGE_DEVICE_02773 -> ../../sdd
| `-- usb-Generic_STORAGE_DEVICE_02773-part1 -> ../../sdd1
|-- by-label
| |-- Photos -> ../../sdd1
| |-- SUSE10 -> ../../sda7
| `-- devel -> ../../sda6
|-- by-path
| |-- pci-0000:00:1f.2-scsi-0:0:0:0 -> ../../sda
| |-- pci-0000:00:1f.2-scsi-0:0:0:0-part1 -> ../../sda1
| |-- pci-0000:00:1f.2-scsi-0:0:0:0-part6 -> ../../sda6
| |-- pci-0000:00:1f.2-scsi-0:0:0:0-part7 -> ../../sda7
| |-- pci-0000:00:1f.2-scsi-1:0:0:0 -> ../../sr0
| |-- usb-02773:0:0:2 -> ../../sdd
| |-- usb-02773:0:0:2-part1 -> ../../sdd1
`-- by-uuid
    |-- 159a47a4-e6e6-40be-a757-a629991479ae -> ../../sda7
    |-- 3e999973-00c9-4917-9442-b7633bd95b9e -> ../../sda6
    `-- 4210-8F8C -> ../../sdd1

```

29.8 Arquivos usados pelo udev

/sys/*

Sistema de arquivos virtual fornecido pelo kernel do Linux, exportando todos os dispositivos conhecidos atualmente. Essas informações são usadas pelo udev para criar nós de dispositivo em /dev.

/dev/*

Nós de dispositivo criados dinamicamente e conteúdo estático criado com systemd-tmpfiles. Para obter mais informações, consulte a página de manual do systemd-tmpfiles(8).

Os arquivos e os diretórios a seguir incluem elementos cruciais da infraestrutura do udev:

/etc/udev/udev.conf

Arquivo de configuração principal do udev.

/etc/udev/rules.d/*

Regras de correspondência de eventos do udev específicas do sistema. Aqui, é possível adicionar regras personalizadas para modificar ou anular as regras padrão do /usr/lib/udev/rules.d/*.

Os arquivos são analisados em ordem alfanumérica. As regras dos arquivos com prioridade mais alta modificam ou anulam as regras com prioridade mais baixa. Quanto menor o número, maior a prioridade.

/usr/lib/udev/rules.d/*

Regras de correspondência de eventos do udev padrão. Os arquivos nesse diretório são de propriedade dos pacotes e serão sobregravados pelas atualizações. Não adicione, remova ou edite esses arquivos; em vez disso, use o /etc/udev/rules.d.

/usr/lib/udev/*

Programas ajudantes chamados de regras do udev.

/usr/lib/tmpfiles.d/ e /etc/tmpfiles.d/

Responsáveis pelo conteúdo do /dev estático.

29.9 Mais informações

Para obter mais informações sobre a infraestrutura do udev, consulte as seguintes páginas de manual:

udev

Informações importantes sobre udev, chaves, regras e outras questões essenciais de configuração.

udevadm

É possível usar o udevadm para controlar o comportamento de tempo de execução do udev, solicitar eventos do kernel, gerenciar a fila de eventos e fornecer mecanismos simples de depuração.

udev

Informações sobre o daemon de gerenciamento de eventos do udev.

30 Recursos especiais do sistema

Este capítulo começa com informações sobre vários pacotes de software, os consoles virtuais e o layout do teclado. Falamos sobre os componentes de software, como bash, cron e logrotate, porque eles foram mudados ou aperfeiçoados durante os últimos ciclos de lançamento. Mesmo que eles sejam pequenos ou considerados de menor importância, os usuários devem mudar o seu comportamento padrão, porque esses componentes muitas vezes estão estreitamente ligados ao sistema. O capítulo termina com uma seção sobre configurações específicas de país e idioma (I18N e L10N).

30.1 Informações sobre pacotes de software especiais

O capítulo a seguir apresenta informações básicas sobre as seguintes ferramentas: bash, cron, logrotate, locate, ulimit e free.

30.1.1 Pacote bash e /etc/profile

Bash é o shell de sistema padrão. Quando usado com um shell de login, ele lê vários arquivos de inicialização. O Bash os processa na ordem em que são exibidos na lista:

1. /etc/profile
2. ~/.profile
3. /etc/bash.bashrc
4. ~/.bashrc

Faça configurações personalizadas em ~/.profile ou ~/.bashrc. Para assegurar o processamento correto desses arquivos, é necessário copiar as configurações básicas de /etc/skel/.profile ou /etc/skel/.bashrc no diretório pessoal do usuário. É recomendável copiar as configurações de /etc/skel após uma atualização. Execute os seguintes comandos de shell para evitar a perda de ajustes pessoais:

```
> mv ~/.bashrc ~/.bashrc.old
```

```
> cp /etc/skel/.bashrc ~/.bashrc
> mv ~/.profile ~/.profile.old
> cp /etc/skel/.profile ~/.profile
```

Em seguida, copie os ajustes pessoais novamente dos arquivos `*.old`.

30.1.2 Pacote cron

Use o `cron` para executar comandos em segundo plano automaticamente em horários predefinidos. O `cron` usa tabelas de horários especialmente formatadas, e a ferramenta inclui várias tabelas padrão. Os usuários também podem especificar tabelas personalizadas, se necessário.

As tabelas cron estão localizadas em `/var/spool/cron/tabs`. `/etc/crontab` atua como uma tabela cron para todo o sistema. Digite o nome de usuário para executar o comando diretamente após a tabela de tempo e antes do comando. No [Exemplo 30.1, “Entrada in /etc/crontab”](#), `root` foi inserido. Tabelas específicas de pacote, localizadas em `/etc/cron.d`, possuem o mesmo formato. Consulte a página de manual do `cron` (`man cron`).

EXEMPLO 30.1: ENTRADA IN /ETC/CRONTAB

```
1-59/5 * * * * root test -x /usr/sbin/atrun && /usr/sbin/atrun
```

Você não pode editar `/etc/crontab` chamando o comando `crontab -e`. Esse arquivo deve ser carregado diretamente em um editor, modificado e gravado.

Vários pacotes instalam scripts de shell nos diretórios `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` e `/etc/cron.monthly`, cuja execução é controlada por `/usr/lib/cron/run-crons`. `/usr/lib/cron/run-crons` é executado a cada 15 minutos da tabela principal (`/etc/crontab`). Isso garante que os processos que tenham sido negligenciados possam ser executados no momento adequado.

Para executar os scripts de manutenção por hora, por dia ou outros scripts de manutenção periódica em horários personalizados, remova os arquivos de marcação de horário regularmente, utilizando as entradas `/etc/crontab` (consulte o [Exemplo 30.2, “/etc/crontab: remover arquivos de marcação de horário”](#), que remove a opção por hora antes de cada hora cheia, a opção por dia uma vez ao dia às 2:14, etc).

EXEMPLO 30.2: /ETC/CRONTAB: REMOVER ARQUIVOS DE MARCAÇÃO DE HORÁRIO

```
59 * * * * root rm -f /var/spool/cron/lastrun/cron.hourly
14 2 * * * root rm -f /var/spool/cron/lastrun/cron.daily
29 2 * * 6 root rm -f /var/spool/cron/lastrun/cron.weekly
```



```
44 2 1 * * root rm -f /var/spool/cron/lastrun/cron.monthly
```

Se preferir, defina `DAILY_TIME` em `/etc/sysconfig/cron` como o horário de início de `cron.daily`. A configuração de `MAX_NOT_RUN` garante que as tarefas diárias sejam acionadas para execução, mesmo se o usuário não ligou o computador no `DAILY_TIME` especificado por um período mais longo. O valor máximo de `MAX_NOT_RUN` é 14 dias.

Os trabalhos de manutenção diária de sistema são distribuídos a vários scripts por motivos de clareza. Eles estão contidos no pacote `aaa_base`. `/etc/cron.daily` contém, por exemplo, os componentes `suse.de-backup-rpmbd`, `suse.de-clean-tmp` ou `suse.de-cron-local`.

30.1.3 Parando mensagens de status do Cron

Para evitar o excesso de emails causado pelas mensagens de status do Cron, o valor padrão de `SEND_MAIL_ON_NO_ERROR` em `/etc/sysconfig/cron` está definido como "no" nas novas instalações. Mesmo com essa configuração definida como "no", a saída de dados do Cron ainda será enviada para o endereço `MAILTO`, conforme documentado na página de manual do Cron. Em caso de atualização, é recomendado definir esses valores de acordo com as suas necessidades.

30.1.4 Arquivos de registro: pacote logrotate

Há vários serviços de sistema (*daemons*) que, juntamente com o próprio kernel, gravam regularmente o status do sistema e eventos específicos em arquivos de registro. Dessa maneira, o administrador pode verificar regularmente o status do sistema em um determinado momento, reconhecer erros ou funções defeituosas e solucioná-los com total precisão. Esses arquivos de registro são normalmente armazenados em `/var/log`, como especificado pelo FHS, e crescem diariamente. O pacote `logrotate` ajuda a controlar o crescimento desses arquivos. Para obter mais detalhes, consulte o Livro *"System Analysis and Tuning Guide"*, Capítulo 3 *"System log files"*, Seção 3.3 *"Managing log files with logrotate"*.

30.1.5 Comando locate

`locate`, um comando para localização rápida de arquivos, não está incluído no escopo padrão do software instalado. Se desejado, instale o pacote `mlocate`, o sucessor do pacote `findutils-locate`. O processo `updatedb` é iniciado automaticamente todas as noites ou aproximadamente 15 minutos após a inicialização do sistema.

30.1.6 Comando **ulimit**

Com o comando **ulimit** (*limites do usuário*), é possível definir limites para o uso dos recursos do sistema e fazer com que sejam exibidos. O **ulimit** é especialmente útil para limitar a memória disponível para os aplicativos. Com isso, um aplicativo pode ser impedido de absorver recursos em demasia do sistema e deixar o sistema operacional lento ou até travá-lo.

O comando **ulimit** pode ser usado com várias opções. Para limitar o uso da memória, use as opções listadas na *Tabela 30.1, “ulimit: definindo recursos para o usuário”*.

TABELA 30.1: **ulimit: DEFININDO RECURSOS PARA O USUÁRIO**

<u>-m</u>	O tamanho máximo do conjunto residente
<u>-v</u>	A quantidade máxima de memória virtual disponível para o shell
<u>-s</u>	O tamanho máximo da pilha
<u>-c</u>	O tamanho máximo dos arquivos básicos criados
<u>-a</u>	Todos os limites atuais são informados

As entradas padrão de todo o sistema estão definidas em /etc/profile. Não é recomendado editar esse arquivo diretamente, pois as mudanças serão sobregravadas durante os upgrades do sistema. Para personalizar as configurações de perfil de todo o sistema, use /etc/profile.local. Convém efetuar as configurações por usuário em ~USER/.perfil.

EXEMPLO 30.3: **ulimit: CONFIGURAÇÕES EM ~/.bashrc**

```
# Limits maximum resident set size (physical memory):
ulimit -m 98304

# Limits of virtual memory:
ulimit -v 98304
```

As alocações de memória devem ser especificadas em KB. Para obter informações mais detalhadas, consulte man bash.

! Importante: Suporte a **ulimit**

Nem todos os shells suportam as diretivas **ulimit**. O PAM (por exemplo, `pam_limits`) oferece uma infinidade de possibilidades de ajustes como alternativa ao **ulimit**.

30.1.7 Comando **free**

O comando **free** exibe a quantidade total de memória física livre e utilizada e o espaço de troca (swap) no sistema e os buffers e o cache consumidos pelo kernel. O conceito de *RAM disponível* surgiu antes da época do gerenciamento unificado de memória. O slogan *memória livre é memória ruim* se aplica bem ao Linux. Como resultado, o Linux sempre se esforçou para equilibrar caches externos sem realmente permitir memória livre ou sem uso.

O kernel não tem conhecimento direto de nenhum aplicativo ou dados de usuário. Em vez disso, ele gerencia aplicativos e dados de usuário em um *cache de página*. Se a memória diminuir, partes dele serão gravadas na partição de troca ou em arquivos, dos quais poderão ser lidas inicialmente com o comando **mmap** (consulte `man mmap`).

O kernel também contém outros caches, como o *cache slab*, onde os caches usados para acesso a rede são armazenados. Isso pode explicar as diferenças entre os contadores em `/proc/meminfo`. A maioria deles (mas não todos) pode ser acessada via `/proc/slabinfo`.

No entanto, se o seu objetivo for descobrir quanta RAM está em uso, encontre essa informação em `/proc/meminfo`.

30.1.8 Páginas de manual e de informações

Para alguns aplicativos GNU (como o tar), as páginas de manuais não são mais mantidas. Para esses comandos, use a opção `--help` para obter uma visão geral rápida das páginas de informações, que apresentam instruções mais detalhadas. Info é um sistema de hipertexto do GNU. Leia uma introdução sobre esse sistema digitando `info info`. As páginas de informações podem ser exibidas com Emacs digitando `emacs -f info` ou diretamente em um console, com `info`. Também é possível usar `tkinfo`, `xinfo` ou o sistema de ajuda do para exibir as páginas de informações.

30.1.9 Selecionando páginas de manual usando o comando `man`

Para ler a página de manual, digite `man PÁGINA_DE_MANUAL`. Se existir uma página de manual com o mesmo nome em seções diferentes, elas serão listadas com os números da seção correspondentes. Selecione uma para exibir. Se você não digitar um número de seção em alguns segundos, a primeira página de manual será exibida.

Para mudar desse comportamento para o padrão do sistema, defina `MAN_POSIXLY_CORRECT=1` em um arquivo de inicialização de shell, como `~/.bashrc`.

30.1.10 Configurações para GNU Emacs

O GNU Emacs é um complexo ambiente de trabalho. As seções a seguir descrevem os arquivos de configuração processados quando o GNU Emacs é iniciado. Há mais informações em <http://www.gnu.org/software/emacs/>.

Na inicialização, o Emacs lê vários arquivos que contêm as configurações do usuário, administrador do sistema e distribuidor para personalização ou pré-configuração. O arquivo de inicialização `~/.emacs` é instalado nos diretórios pessoais dos usuários individuais por meio de `/etc/skel`. O `.emacs`, por sua vez, lê o arquivo `/etc/skel/.gnu-emacs`. Para personalizar o programa, copie o arquivo `.gnu-emacs` para o diretório pessoal (com `cp /etc/skel/.gnu-emacs ~/.gnu-emacs`) e faça as configurações desejadas nesse diretório.

O `.gnu-emacs` define o arquivo `~/.gnu-emacs-custom` como arquivo personalizado. Se os usuários tiverem feito as configurações com as opções `personalizar` no Emacs, as configurações serão gravadas no arquivo `~/.gnu-emacs-custom`.

Com o SUSE Linux Enterprise Desktop, o pacote `emacs` instala o arquivo `site-start.el` no diretório `/usr/share/emacs/site-lisp`. O arquivo `site-start.el` é carregado antes do arquivo de inicialização `~/.emacs`. Entre outras coisas, o arquivo `site-start.el` assegura que os arquivos de configuração especial distribuídos com os pacotes de expansão do Emacs, como o `psgml`, sejam carregados automaticamente. Os arquivos de configuração deste tipo também estão localizados em `/usr/share/emacs/site-lisp`, e sempre começam com o nome `suse-start-`. O administrador do sistema local pode especificar configurações globais do sistema no arquivo `default.el`.

Mais informações sobre esses arquivos estão disponíveis no arquivo de informações do Emacs em *Init File*: `info:/emacs/InitFile`. Informações sobre como desabilitar o carregamento desses arquivos, se necessário, também são fornecidas neste local.

Os componentes do Emacs são divididos em vários pacotes:

- O pacote base `emacs`.
- `emacs-x11` (geralmente instalado): o programa *com* suporte para X11.
- `emacs-nox`: o programa *sem* suporte para X11.
- `emacs-info`: documentação online em formato info.
- `emacs-el`: os arquivos de biblioteca não compilados em Emacs Lisp. Eles não são necessários em tempo de execução.
- Numerosos pacotes complementares podem ser instalados se necessário: `emacs-auctex` (LaTeX), `psgml` (SGML e XML), `gnuserv` (operação cliente e servidor) e outros.

30.2 Consoles virtuais

O Linux é um sistema multiusuário e multitarefa. As vantagens desses recursos podem ser apreciadas mesmo em um sistema de PC independente. No modo de texto, existem seis consoles virtuais disponíveis. Alterne entre eles utilizando as teclas de `Alt - F1` até `Alt - F6`. O sétimo console é reservado para X e o décimo console mostra as mensagens do kernel.

Para alternar para um console de X sem o fechar, use a combinação de teclas de `Ctrl - Alt - F1` até `Ctrl - Alt - F6`. Para voltar para X, pressione `Alt - F7`.

30.3 Mapeamento de teclado

Para padronizar o mapeamento de teclado de programas, foram feitas mudanças nos seguintes arquivos:

```
/etc/inputrc
/etc/X11/Xmodmap
/etc/skel/.emacs
/etc/skel/.gnu-emacs
/etc/skel/.vimrc
/etc/csh.cshrc
/etc/termcap
/usr/share/terminfo/x/xterm
/usr/share/X11/app-defaults/XTerm
```

```
/usr/share/emacs/VERSION/site-lisp/term/*.el
```

Essas mudanças afetam apenas os aplicativos que usam as entradas **terminfo** ou que têm arquivos de configuração que são modificados diretamente (**vi**, **emacs**, etc). Os aplicativos que não acompanham o sistema devem ser adaptados a esses padrões.

Em X, a tecla Compose (multitecla) pode ser habilitada conforme explicado em [/etc/X11/Xmodmap](#).

Outras configurações são possíveis utilizando-se a Extensão de Teclado X (XKB).



Dica: Mais informações

Há informações sobre o XKB disponíveis nos documentos listados em [/usr/share/doc/packages/xkeyboard-config](#) (parte do pacote [xkeyboard-config](#)).

30.4 Configurações de idioma e específicas de país

O sistema é, em uma extensão bastante ampla, internacionalizado e pode ser modificado de acordo com as necessidades locais. A internacionalização (*I18N*) permite a localização específica (*L10N*). As abreviações *I18N* e *L10N* são derivadas das primeiras e últimas letras das palavras e, no meio, está o número de letras omitidas.

As configurações são feitas com variáveis **LC_** definidas no arquivo [/etc/sysconfig/language](#). Elas referem-se não somente ao *suporte ao idioma nativo*, mas também às categorias *Mensagens* (Idioma), *Conjunto de Caracteres*, *Ordem de Classificação*, *Hora e Data*, *Números* e *Moeda*. Cada uma dessas categorias pode ser definida diretamente com sua própria variável ou indiretamente com uma variável master no arquivo [language](#) (consulte a página de manual **locale**).

LISTA DE VARIÁVEIS

RC_LC_MESSAGES, **RC_LC_CTYPE**, **RC_LC_COLLATE**, **RC_LC_TIME**, **RC_LC_NUMERIC**, **RC_LC_MONETARY**

Essas variáveis são passadas para o shell sem o prefixo **RC_** e representam as categorias listadas. Os perfis shell de referência estão listados abaixo. A configuração atual pode ser exibida com o comando **locale**.

RC_LC_ALL

Essa variável, se definida, sobregrava os valores das variáveis já mencionadas.

RC_LANG

Se nenhuma das variáveis anteriores for definida, esse é o fallback. Por padrão, apenas RC_LANG está definida. Isso facilita o processo para que os usuários informem seus próprios valores.

ROOT_USES_LANG

É possível definir essa variável como yes ou ctype (padrão). Se definida como yes, o root usará as configurações específicas de idioma e país; do contrário, o administrador do sistema sempre trabalhará em um ambiente POSIX.

As variáveis podem ser definidas com o editor `sysconfig` do YaST. O valor dessa variável contém o código do idioma, código do país, codificação e modificador. Os componentes individuais são unidos por caracteres especiais:

```
LANG=<language>[_<COUNTRY>].<Encoding>[@<Modifier>]
```

30.4.1 Configurações de idioma de todo o sistema

O `systemd` lê o `/etc/locale.conf` no início do boot. As configurações de idioma definidas nesse arquivo são herdadas por cada serviço ou usuário, a menos que haja configurações individuais.



Nota: Comportamento dos arquivos de configuração mais antigos no SUSE Linux Enterprise Desktop

As versões anteriores do SUSE Linux Enterprise Desktop liam as configurações de idioma de `/etc/sysconfig/language`, `/etc/sysconfig/keyboard` e `/etc/sysconfig/console`. A partir do SUSE Linux Enterprise Desktop 15 GA, esses arquivos são considerados obsoletos. O `systemd` não lê mais as configurações desses arquivos. Em vez disso, o `systemd` lê de `/etc/locale.conf`.

No entanto, as variáveis definidas no `/etc/sysconfig/language` ainda serão usadas: elas anulam o idioma de todo o sistema e podem ser usadas para definir configurações de idioma diferentes para os shells de usuário (consulte a [Seção 30.4.2, “Alguns exemplos”](#)).

Para definir o idioma de todo o sistema, você pode:

- Gravar as configurações no `/etc/locale.conf`. Cada linha é uma atribuição de variável como um ambiente (consulte **man 5 locale.conf** para ver uma lista de variáveis):

```
LANG=de_DE.UTF-8
```

Para ajustar as configurações, você pode adicionar outras variáveis, uma por linha.

- Usar o comando **localectl**:

```
# localectl set-locale LANG=de_DE.UTF-8
```

Neste caso, você também pode especificar mais variáveis após o comando **localectl set-locale**.

Para manter a compatibilidade retroativa com sistemas antigos durante a atualização do pacote `systemd`, todas as variáveis mencionadas serão migradas do `sysconfig` para seus destinos finais, se ainda não estiverem definidas nesse local.

30.4.2 Alguns exemplos

Você deve sempre definir os códigos do idioma e do país juntos. As configurações do idioma seguem o padrão ISO 639 disponível em <http://www.evertype.com/standards/iso639/iso639-en.html> e <http://www.loc.gov/standards/iso639-2/>. Os códigos de país estão listados em ISO 3166, consulte http://en.wikipedia.org/wiki/ISO_3166.

Só faz sentido definir valores para os quais os arquivos de descrição utilizáveis podem ser encontrados em `/usr/lib/locale`. Arquivos de descrição adicionais podem ser criados de arquivos em `/usr/share/i18n` utilizando o comando **localedef**. Os arquivos de descrição fazem parte do pacote `glibc-i18ndata`. Um arquivo de descrição para `en_US.UTF-8` (para inglês e Estados Unidos) pode ser criado com:

```
localedef -i en_US -f UTF-8 en_US.UTF-8
```

```
LANG=en_US.UTF-8
```

Essa é a configuração padrão se Inglês americano for selecionado durante a instalação. Se você tiver selecionado outro idioma, ele será habilitado, mas ainda terá o UTF-8 como codificação de caractere.

LANG=en_US.ISO-8859-1

Define o idioma como inglês, o país como Estados Unidos e o conjunto de caracteres como ISO-8859-1. Essa definição de caractere não suporta o sinal de Euro, mas às vezes pode ser útil para programas que não foram atualizados para suportar UTF-8. A string que define o conjunto de caracteres (ISO-8859-1 nesse caso) é então avaliada por programas como o Emacs.

LANG=en_IE@euro

O exemplo acima inclui explicitamente o sinal de Euro em uma configuração de idioma. Essa configuração está obsoleta agora, pois o UTF-8 também abrange o símbolo do Euro. Será útil apenas se um aplicativo suportar ISO-8859-15 e não UTF-8.

As mudanças em /etc/sysconfig/language são ativadas pela seguinte cadeia de processo:

- Para Bash: /etc/profile lê /etc/profile.d/lang.sh que, por sua vez, analisa /etc/sysconfig/language.
- Para tcsh: No login, /etc/csh.login lê /etc/profile.d/lang.csh que, por sua vez, analisa /etc/sysconfig/language.

Isso garante que toda mudança em /etc/sysconfig/language fique disponível no próximo login para o respectivo shell, sem ter que ativá-la manualmente.

Os usuários anular os padrões do sistema editando o seu ~/ .bashrc da maneira adequada. Por exemplo, se você não deseja usar en_US em todo o sistema para mensagens de programa, em vez disso, inclua LC_MESSAGES=es_ES para exibir as mensagens em espanhol.

30.4.3 Configurações de idioma em ~/ .i18n

Se não estiver satisfeito com os padrões do sistema local, mude as configurações em ~/ .i18n de acordo com a sintaxe de script Bash. As entradas em ~/ .i18n substituem os padrões do sistema de /etc/sysconfig/language. Use os mesmos nomes de variáveis, mas sem os prefixos de namespace RC_. Por exemplo, use LANG em vez de RC_LANG:

```
LANG=cs_CZ.UTF-8
LC_COLLATE=C
```

30.4.4 Configurações de suporte de idioma

Arquivos na categoria *Mensagens* são, via de regra, armazenados somente no diretório do idioma correspondente (como `en`) para ter um fallback. Se você definir `LANG` para `en_US` e o arquivo de mensagem em `/usr/share/locale/en_US/LC_MESSAGES` não existir, ele voltará para `/usr/share/locale/en/LC_MESSAGES`.

Uma cadeia de fallback também pode ser definida, por exemplo, para bretão para francês ou galego para espanhol para português:

```
LANGUAGE="br_FR:fr_FR"
```

```
LANGUAGE="gl_ES:es_ES:pt_PT"
```

Se desejar, use as variantes norueguesas Nynorsk e Bokmål (com fallback adicional para `no`):

```
LANG="nn_NO"
```

```
LANGUAGE="nn_NO:nb_NO:no"
```

ou

```
LANG="nb_NO"
```

```
LANGUAGE="nb_NO:nn_NO:no"
```

Observe que em norueguês, `LC_TIME` também é tratado de maneira diferente.

Um problema que pode surgir é um separador usado para delimitar grupos de dígitos não ser reconhecido corretamente. Isso acontece se `LANG` for definido para um código de idioma com somente duas letras, como `de`, mas o arquivo de definição que o glibc utiliza estiver localizado em `/usr/share/lib/de_DE/LC_NUMERIC`. Por isso, `LC_NUMERIC` deve ser definido como `de_DE` para tornar a definição de separador visível para o sistema.

30.4.5 Mais informações

- *The GNU C Library Reference Manual*, Capítulo “Locales and Internationalization”. Ele está incluído no pacote `glibc-info`.
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, atualmente em <https://www.cl.cam.ac.uk/~mgk25/unicode.html>.

31 Usando o NetworkManager

O NetworkManager é a solução ideal para laptops e outros computadores portáteis. Ele suporta tipos e padrões de criptografia avançados para conexões de rede, incluindo conexões com rede protegidas por 802.1X. 802.1X é o “Padrão IEEE para Redes Locais e de Área Metropolitana — Controle de Acesso a Rede Baseado na Porta”. Com o NetworkManager, você não precisa se preocupar em configurar interfaces de rede nem em alternar entre redes wireless ou com fio quando estiver em trânsito. O NetworkManager pode conectar-se automaticamente a redes wireless conhecidas ou gerenciar várias conexões de rede paralelamente, caso em que a conexão mais rápida é usada como padrão. Além disso, você pode alternar manualmente entre as redes disponíveis e gerenciar sua conexão de rede usando um applet na bandeja do sistema.

Várias conexões podem estar ativas simultaneamente, em vez de apenas uma. Isso lhe permite desplugar o laptop de uma Ethernet e permanecer conectado por uma conexão wireless.



Importante:

O NetworkManager é suportado apenas pelo SUSE para cargas de trabalho de desktop com SLED ou a Workstation Extension. Todas as certificações de servidor são feitas com o **wicked** como a ferramenta de configuração de rede, e o uso do NetworkManager pode invalidá-las. O NetworkManager não é suportado pelo SUSE para cargas de trabalho de servidor.

31.1 Casos de uso do NetworkManager

O NetworkManager dispõe de uma interface do usuário sofisticada e intuitiva, que permite aos usuários alternar facilmente seu ambiente de rede. Contudo, o NetworkManager não é uma solução adequada nos seguintes casos:

- O computador fornece serviços de rede para outros computadores de sua rede, por exemplo, se ele for um servidor DHCP ou DNS.
- Seu computador é um servidor Xen ou seu sistema é um sistema virtual dentro do Xen.

31.2 Habilitando ou desabilitando o NetworkManager

Em computadores desktop e laptop, o NetworkManager está habilitado por padrão. Você pode desabilitá-lo e habilitá-lo a qualquer momento usando o módulo Configurações de Rede no YaST.

1. Execute o YaST e vá para *Sistema > Configurações de Rede*.
2. A caixa de diálogo *Configurações de Rede* é aberta. Vá até a guia *Opções Globais*.
3. Para configurar e gerenciar suas conexões de rede com o NetworkManager:
 - a. No campo *Método de Configuração da Rede*, selecione *Controlado por Usuário com o NetworkManager*.
 - b. Clique em *OK* e feche o YaST.
 - c. Configure as conexões de rede com o NetworkManager, conforme descrito na [Seção 31.3, "Configurando conexões de rede"](#).
4. Para desativar o NetworkManager e controlar a rede com sua própria configuração:
 - a. No campo *Método de Configuração da Rede*, escolha *Controlled by wicked* (Controlado pelo wicked).
 - b. Clique em *OK*.
 - c. Configure a placa de rede com o YaST usando a configuração automática através do DHCP ou de um endereço IP estático.
Há uma descrição detalhada da configuração de rede com o YaST na [Seção 23.4, "Configurando uma conexão de rede com o YaST"](#).

31.3 Configurando conexões de rede

Após habilitar o NetworkManager no YaST, configure suas conexões de rede com o front end do NetworkManager disponível no GNOME. Ele mostra guias para todos os tipos de conexões de rede; por exemplo, conexões com fio, wireless, de banda larga móvel, DSL e VPN.



Dica: Editor de Conexão do NetworkManager

Nas versões anteriores do SUSE Linux Enterprise Desktop, as conexões de rede eram configuradas usando um aplicativo chamado *Editor de Conexão do NetworkManager*. Ele não é mais instalado por padrão, pois o *GNOME Control Center* substituiu totalmente seus recursos de configuração.

Se você ainda precisa usar o Editor de Conexão do NetworkManager para configurar conexões de rede, instale o pacote `NetworkManager-connection-editor` manualmente:

```
> sudo zypper install NetworkManager-connection-editor
```

Para abrir a caixa de diálogo de configuração de rede no GNOME, abra o menu de configurações, pelo menu de status, e clique na entrada *Rede*.



Nota: Disponibilidade de opções

Dependendo da configuração de seu sistema, talvez não seja permitido configurar conexões. Em um ambiente seguro, talvez algumas opções estejam bloqueadas ou exijam permissão de `root`. Consulte o administrador do sistema para obter os detalhes.

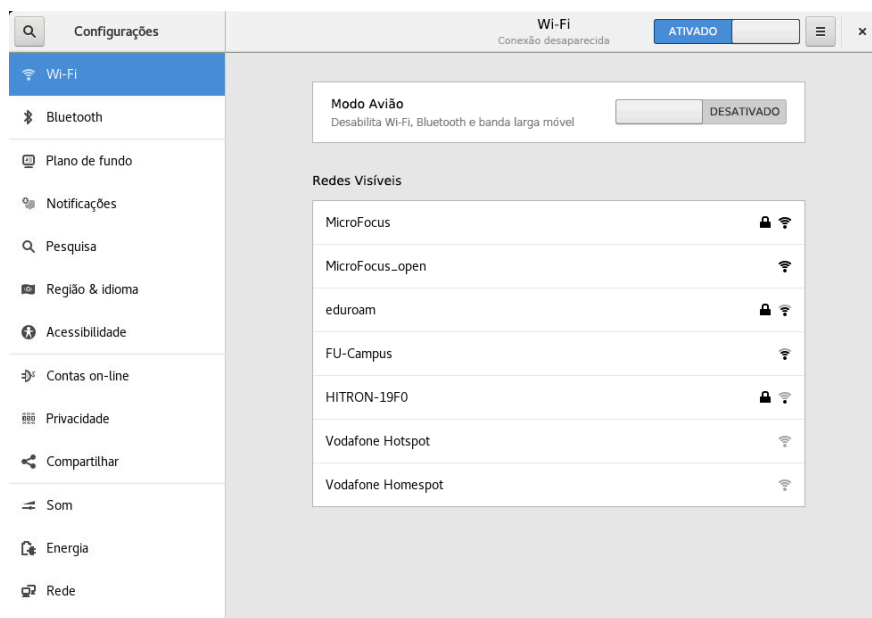


FIGURA 31.1: CAIXA DE DIÁLOGO CONEXÕES DE REDE DO GNOME

1. Abra a caixa de diálogo de configuração do NetworkManager.
2. Para adicionar uma conexão:
 - a. Clique no ícone de + no canto inferior esquerdo.
 - b. Selecione o tipo de conexão preferencial e siga as instruções.
 - c. Ao concluir, clique em *Adicionar*.
 - d. Depois que você confirmar suas mudanças, a conexão de rede recém-configurada será exibida na lista de redes disponíveis no menu Status.
3. Para editar uma conexão:
 - a. Selecione a entrada para editar.
 - b. Clique no ícone de engrenagem para abrir a caixa de diálogo *Configurações da Conexão*.
 - c. Faça as mudanças e clique em *Aplicar* para gravá-las.
 - d. Para disponibilizá-la como conexão do sistema, vá para a guia *Identidade* e marque a caixa de seleção *Disponibilizar para outros usuários*. Para obter mais informações sobre conexões de usuário e sistema, consulte a [Seção 31.4.1, "Conexões de usuário e sistema"](#).

31.3.1 Gerenciando conexões de rede com fio

Se o seu computador estiver conectado a uma rede com fio, use o applet do NetworkManager para gerenciar a conexão.

1. Abra o Menu de Status e clique em *Com fio* para mudar os detalhes da conexão ou desligá-la.
2. Para mudar as configurações, clique em *Configurações com Fio* e clique no ícone de engrenagem.
3. Para desligar todas as conexões de rede, ative a configuração *Airplane Mode* (Modo Avião).

31.3.2 Gerenciando conexões de rede wireless

As redes wireless visíveis estão listadas no menu do applet do NetworkManager do GNOME em *Redes Wireless*. A força do sinal de cada rede também é mostrada no menu. Redes wireless criptografadas são marcadas com um ícone de escudo.

PROCEDIMENTO 31.2: CONECTANDO-SE A UMA REDE WIRELESS VISÍVEL

1. Para conectar-se a uma rede wireless visível, abra o Menu de Status e clique em *Wi-Fi*.
2. Clique em *Turn On* (Ativar) para habilitá-la.
3. Clique em *Select Network* (Selecionar Rede), selecione a Rede Wi-Fi e clique em *Conectar*.
4. Se a rede estiver criptografada, será aberta uma caixa de diálogo de configuração. Ela mostra o tipo de criptografia que a rede usa e as caixas de texto para digitar as credenciais de login.

PROCEDIMENTO 31.3: CONECTANDO-SE A UMA REDE WIRELESS INVISÍVEL

1. Para conectar-se a uma rede que não transmite seu identificador SSID ou ESSID e, portanto, não pode ser detectada automaticamente, abra o Menu de Status e clique em *Wi-Fi*.
2. Clique em *Configurações Wi-Fi* para abrir o menu de configurações detalhadas.
3. Verifique se o seu Wi-Fi está habilitado e clique em *Conectar a uma Rede Oculta*.
4. Na caixa de diálogo aberta, digite o SSID ou o ESSID em *Nome de Rede* e defina os parâmetros de criptografia, se necessário.

Uma rede wireless escolhida explicitamente permanecerá conectada o máximo de tempo possível. Se houver um cabo de rede conectado durante esse período, todas as conexões definidas como *Stay connected when possible* (Permanecer conectado quando possível) ficarão conectadas enquanto a conexão wireless continuar ativa.

31.3.3 Habilitando detecção de portal cativo wireless

Na conexão inicial, muitos pontos ativos wireless públicos forçam os usuários a visitarem uma landing page (o *portal cativo*). Antes de você efetuar login ou concordar com os termos e condições, todas as suas solicitações HTTP são redirecionadas ao portal cativo do provedor.

Durante a conexão a uma rede wireless com um portal cativo, o NetworkManager e o GNOME mostram automaticamente a página de login como parte do processo de conexão. Isso garante que você sempre saiba quando está conectado e ajuda a concluir a configuração o mais rápido possível sem usar o browser para efetuar login.

Para habilitar esse recurso, instale o pacote `NetworkManager-branding-SLE` e reinicie o NetworkManager com:

```
> sudo systemctl restart network
```

Sempre que você se conectar a uma rede com um portal cativo, o NetworkManager (ou o GNOME) abre a página de login do portal cativo para você. Efetue login com suas credenciais para acessar a Internet.

31.3.4 Configurando a placa Wi-Fi/Bluetooth como ponto de acesso

Se a placa Wi-Fi/Bluetooth suportar o modo de ponto de acesso, você poderá usar o NetworkManager para a configuração.

1. Abra o Menu de Status e clique em *Wi-Fi*.
2. Clique em *Configurações Wi-Fi* para abrir o menu de configurações detalhadas.
3. Clique em *Usar como Ponto Ativo...* e siga as instruções.
4. Use as credenciais mostradas na caixa de diálogo resultante para conectar-se ao ponto ativo de uma máquina remota.

31.3.5 NetworkManager e VPN

O NetworkManager suporta várias tecnologias de VPN (Virtual Private Network). Para cada tecnologia, o SUSE Linux Enterprise Desktop possui um pacote básico com suporte genérico ao NetworkManager. Além disso, você também precisa instalar o respectivo pacote específico da área de trabalho para o seu applet.

OpenVPN

Para usar esta tecnologia VPN, instale:

- [NetworkManager-openvpn](#)
- [NetworkManager-openvpn-gnome](#)

OpenConnect

Para usar esta tecnologia VPN, instale:

- [NetworkManager-openconnect](#)
- [NetworkManager-openconnect-gnome](#)

PPTP (Point-to-Point Tunneling Protocol)

Para usar esta tecnologia VPN, instale:

- [NetworkManager-pptp](#)
- [NetworkManager-pptp-gnome](#)

O procedimento a seguir descreve como configurar o computador como um cliente OpenVPN usando o NetworkManager. A configuração de outros tipos de VPN é semelhante.

Antes de começar, verifique se o pacote [NetworkManager-openvpn-gnome](#) está instalado e se todas as dependências foram resolvidas.

PROCEDIMENTO 31.4: CONFIGURANDO O OPENVPN COM O NETWORKMANAGER

1. Abra o aplicativo de *Configurações* clicando nos ícones de status na extremidade direita do painel e clicando no ícone de *chave inglesa e chave de fenda*. Na janela *Todas as Configurações*, escolha *Rede*.
2. Clique no ícone *+*.
3. Selecione *VPN* e, em seguida, *OpenVPN*.
4. Escolha o tipo *Autenticação*. Dependendo da configuração do seu servidor OpenVPN, escolha *Certificados (TLS)* ou *Senha com Certificados (TLS)*.
5. Insira os valores necessários nas respectivas caixas de texto. Para nossa configuração de exemplo, os valores são:

<i>Gateway</i>	O endpoint remoto do servidor VPN
----------------	-----------------------------------

<i>Nome de usuário</i>	O usuário (disponível apenas quando você seleciona <i>Senha com Certificados (TLS)</i>)
<i>Senha</i>	A senha do usuário (disponível apenas quando você seleciona <i>Senha com Certificados (TLS)</i>)
<i>Certificado de Usuário</i>	<u>/etc/ovpn/client1.crt</u>
<i>Certificado de CA</i>	<u>/etc/ovpn/ca.crt</u>
<i>Chave privada</i>	<u>/etc/ovpn/client1.key</u>

6. Concluir a configuração com *Adicionar*.
7. Para habilitar a conexão, no painel *Rede* do aplicativo de *Configurações*, clique no botão de alternância. Se preferir, clique nos ícones de status na extremidade direita do painel, clique no nome da VPN e, em seguida, *Conectar*.

31.4 NetworkManager e segurança

O NetworkManager distingue dois tipos de conexões wireless: confiáveis e não confiáveis. Uma conexão confiável é qualquer rede selecionada explicitamente no passado. Todas as outras são não confiáveis. As conexões confiáveis são identificadas pelo nome e pelo endereço MAC do ponto de acesso. O uso do endereço MAC garante que você não possa usar um ponto de acesso diferente com o nome da conexão confiável.

O NetworkManager faz uma exploração periódica de redes wireless disponíveis. Se forem encontradas várias redes confiáveis, a usada mais recentemente será selecionada automaticamente. O NetworkManager aguarda a sua seleção caso nenhuma das redes seja confiável.

Se a configuração de criptografia mudar, mas o nome e o endereço MAC continuarem os mesmos, o NetworkManager tentará se conectar, mas primeiro você será solicitado a confirmar as novas configurações de criptografia e fornecer atualizações, como uma nova chave.

Se você mudar da conexão wireless para o modo offline, o NetworkManager deixará o SSID ou o ESSID em branco. Isso garante que a placa seja desconectada.

31.4.1 Conexões de usuário e sistema

O NetworkManager conhece dois tipos de conexões: conexões de usuário e sistema.

As conexões de usuário requerem que todos os usuários façam a autenticação no NetworkManager, que armazena as credenciais deles no respectivo chaveiro do GNOME local para que não precisem digitá-las novamente sempre que se conectarem.

As conexões do sistema estão disponíveis a todos os usuários automaticamente. O primeiro usuário que cria a conexão digita as credenciais necessárias e, depois disso, todos os demais usuários terão acesso sem precisar saber as credenciais. A diferença entre a configuração de uma conexão de usuário ou de sistema é uma única caixa de seleção: *Disponibilizar para outros usuários*. Para obter informações sobre como configurar conexões de usuário ou de sistema com o NetworkManager, consulte a [Seção 31.3, “Configurando conexões de rede”](#).

31.4.2 Armazenando senhas e credenciais

Para não ter que digitar suas credenciais toda vez que se conectar a uma rede criptografada, você pode usar o Gerenciador de Chaveiros do GNOME para armazenar as credenciais criptografadas no disco, protegidas por uma senha master.

31.4.3 Zonas do firewall

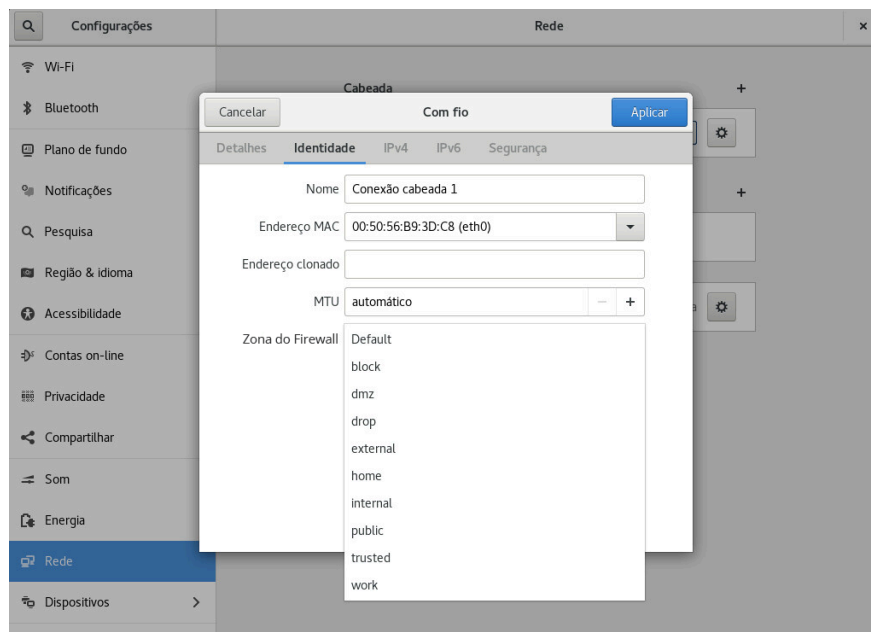


FIGURA 31.2: ZONAS firewall NO NETWORKMANAGER

As zonas do firewall definem as regras gerais sobre as conexões de rede que são permitidas. Para configurar a zona de *firewalld* para uma conexão com fio, acesse a guia *Identidade* das configurações de conexão. Para configurar a zona de *firewalld* para uma conexão Wi-Fi, acesse a guia *Segurança* das configurações de conexão.

Se você está em sua rede doméstica, use a zona home. Para redes wireless públicas, alterne para public. Se você está em um ambiente seguro e deseja permitir todas as conexões, use a zona trusted.

Para obter detalhes sobre o *firewalld*, consulte o Livro *“Security and Hardening Guide”, Capítulo 23 “Masquerading and firewalls”, Seção 23.4 “firewalld”*.

31.5 Perguntas frequentes

Veja a seguir algumas perguntas frequentes sobre a configuração de opções de rede especiais com o NetworkManager.

1. Como vincular uma conexão a um dispositivo específico?

Por padrão, as conexões no NetworkManager são específicas ao tipo de dispositivo: elas se aplicam a todos os dispositivos físicos do mesmo tipo. Se houver mais de um dispositivo físico disponível por tipo de conexão (por exemplo, quando a máquina está equipada com duas placas Ethernet), você poderá vincular uma conexão a determinado dispositivo.

Para fazer isso no GNOME, primeiro procure o endereço MAC do seu dispositivo (use as *Informações da Conexão* disponíveis no applet ou use a saída das ferramentas de linha de comando, como **nm-tool** ou **wicked show all**). Em seguida, inicie a caixa de diálogo para configurar conexões de rede e escolher a conexão que você deseja modificar. Na guia *Com fio* ou *Wireless*, digite o *Endereço MAC* do dispositivo e confirme suas mudanças.

2. Como especificar um determinado ponto de acesso caso sejam detectados vários pontos de acesso com o mesmo ESSID?

Quando há vários pontos de acesso disponíveis com bandas wireless diferentes (a/b/g/n), o ponto de acesso com o sinal mais forte é automaticamente escolhido por padrão. Para anular isso, use o campo *BSSID* ao configurar conexões wireless.

O BSSID (Basic Service Set Identifier) identifica de forma exclusiva cada Conjunto de Serviços Básicos. Em um Conjunto de Serviços Básicos de infraestrutura, o BSSID é o endereço MAC do ponto de acesso wireless. Em um Conjunto de Serviços Básicos independente (ad-hoc), o BSSID é um endereço MAC administrado localmente, gerado de um número aleatório de 46 bits.

Inicie a caixa de diálogo para configurar conexões de rede conforme descrito na [Seção 31.3, “Configurando conexões de rede”](#). Escolha a conexão wireless que você deseja modificar e clique em *Editar*. Na guia *Wireless*, digite o BSSID.

3. *Como compartilhar conexões de rede com outros computadores?*

O dispositivo principal (que está conectado à Internet) não precisa de nenhuma configuração especial. Entretanto, você deve configurar o dispositivo que está conectado ao barramento local ou à máquina, conforme a seguir:

1. Inicie a caixa de diálogo para configurar conexões de rede conforme descrito na [Seção 31.3, “Configurando conexões de rede”](#). Escolha a conexão que você deseja modificar e clique em *Editar*. Alterne para a guia *Configurações IPv4* e, na caixa suspensa *Método*, ative *Compartilhado com outros computadores*. Isso habilitará o encaminhamento de tráfego IP e executar um servidor DHCP no dispositivo. Confirme suas mudanças no NetworkManager.
2. Como o servidor DHCP utiliza a porta 67, verifique se ela não está bloqueada pelo firewall: Na máquina que compartilha as conexões, inicie o YaST e selecione *Segurança e Usuários* > *Firewall*. Alterne para a categoria *Serviços Permitidos*. Se o *Servidor DHCP* ainda não for exibido como *Serviço Permitido*, selecione *Servidor DHCP* em *Serviços a Permitir* e clique em *Adicionar*. Confirme as mudanças no YaST.

4. *Como fornecer informações de DNS estático com endereços automáticos (DHCP, PPP, VPN)?*

Caso um servidor DHCP forneça informações (e/ou rotas) inválidas de DNS, você pode anulá-las. Inicie a caixa de diálogo para configurar conexões de rede conforme descrito na [Seção 31.3, “Configurando conexões de rede”](#). Escolha a conexão que você deseja modificar e clique em *Editar*. Alterne para a guia *Configurações IPv4* e, na caixa suspensa *Método*, ative *Somente endereços (DHCP) automáticos*. Digite as informações de DNS nos campos *Servidores DNS* e *Domínios de Pesquisa*. Para *Ignorar automaticamente rotas obtidas*, clique em *Rotas* e ative a respectiva caixa de seleção. Confirme as mudanças.

5. *Como fazer o NetworkManager conectar-se a redes protegidas por senha antes que um usuário efetue login?*

Defina uma conexão do sistema que possa ser usada para esse fim. Para obter mais informações, consulte a [Seção 31.4.1, “Conexões de usuário e sistema”](#).

31.6 Solução de problemas

Podem ocorrer problemas de conexão. Alguns problemas comuns relacionados ao NetworkManager são: o applet não é iniciado ou opção ausente na VPN. Métodos para resolver e evitar esses problemas dependem da ferramenta usada.

O applet da área de trabalho do NetworkManager não é iniciado

Os applets serão iniciados automaticamente se a rede for configurada para controle do NetworkManager. Se o applet não for iniciado, verifique se o NetworkManager está habilitado no YaST, conforme descrito na [Seção 31.2, “Habilitando ou desabilitando o NetworkManager”](#). Em seguida, verifique se o pacote NetworkManager-gnome também está instalado.

Se o applet de área de trabalho estiver instalado, mas não estiver em execução por algum motivo, inicie-o manualmente com o comando **nm-applet**.

O applet do NetworkManager não inclui a opção VPN

O suporte a NetworkManager, applets e VPN para NetworkManager é distribuído em pacotes separados. Se o applet NetworkManager não incluir a opção VPN, verifique se os pacotes com suporte ao NetworkManager referentes à sua tecnologia VPN estão instalados. Para obter mais informações, consulte a [Seção 31.3.5, “NetworkManager e VPN”](#).

Nenhuma conexão de rede disponível

Se você configurou a conexão de rede corretamente e todos os outros componentes da conexão de rede (roteador etc.) também estão ativos e em execução, às vezes é útil reiniciar as interfaces de rede no computador. Para isso, efetue login em uma linha de comando como root e execute **systemctl restart wickeds**.

31.7 Mais informações

Você encontra mais informações sobre o NetworkManager nos seguintes sites na Web e diretórios:

página de projeto do NetworkManager

<https://gitlab.freedesktop.org/NetworkManager/NetworkManager> ↗

Documentação do pacote

Consulte também o conteúdo dos seguintes diretórios para obter as informações mais recentes sobre o NetworkManager e o applet do GNOME:

- [/usr/share/doc/packages/NetworkManager/](#),
- [/usr/share/doc/packages/NetworkManager-gnome/](#).

IV Configuração de hardware

- 32 Configurando o layout do teclado do sistema **467**
- 33 Configurando placas de som **468**
- 34 Configurando uma impressora **471**
- 35 Configurando um scanner **478**
- 36 Gerenciamento de energia **480**
- 37 Memória persistente **487**

32 Configurando o layout do teclado do sistema

O módulo *Layout do Teclado do Sistema* do YaST permite definir o layout do teclado padrão do sistema (também usado para o console). Os usuários podem modificar o layout do teclado nas sessões X individuais, usando as ferramentas da área de trabalho.


1. Inicie a caixa de diálogo *Configuração do Teclado do Sistema* do YaST clicando em *Hardware > System Keyboard Layout* (Layout do Teclado do Sistema) no YaST. Se preferir, inicie o módulo pela linha de comando com `sudo yast2 keyboard`.
2. Selecione o *Layout do Teclado* desejado na lista.
3. Teste o layout do teclado selecionado na caixa de texto *Testar*.
4. Se o resultado for o esperado, confirme as mudanças e feche a caixa de diálogo.
5. O resultado é armazenado nos arquivos `/etc/vconsole.conf` (para consoles de texto) e `/etc/X11/xorg.conf.d/00-keyboard.conf` (para X11).
6. As configurações avançadas do teclado podem ser definidas em *Sistema > Editor do Sysconfig > Hardware > Teclado*. Nesse local, você pode especificar as configurações de taxa e atraso do teclado e habilitar ou desabilitar NumLock, CapsLock e ScrollLock. Essas configurações são armazenadas em `/etc/sysconfig/keyboard`.

33 Configurando placas de som

O YaST detecta a maioria das placas de som automaticamente e as configura com os valores apropriados. Para mudar as configurações padrão ou configurar uma placa de som que não pôde ser configurada automaticamente, use o módulo de som do YaST. Nele, é possível também configurar placas de som adicionais ou mudar sua ordem.

Para iniciar o módulo de som, inicie o YaST e clique em *Hardware* > *Som*. Se preferir, inicie a caixa de diálogo *Configuração de Som* diretamente, executando **yast2 sound &** como usuário root por uma linha de comando. Se o módulo de som não estiver disponível, instale-o usando o comando **sudo zypper install yast2-sound**.

PROCEDIMENTO 33.1: CONFIGURANDO PLACAS DE SOM

Se você adicionou uma nova placa de som ou se o YaST não pôde configurar automaticamente uma placa de som existente, siga as etapas abaixo. Para configurar uma nova placa de som, você deve saber o fornecedor e o modelo dela. Em caso de dúvida, consulte a documentação da placa de som para ver as informações necessárias. Para acessar uma lista de referência de placas de som suportadas pelo ALSA com seus respectivos módulos de som, acesse <http://www.alsa-project.org/main/index.php/Matrix:Main> .

Durante a configuração, é possível escolher entre as seguintes opções de configuração:

Configuração automática rápida

Não é necessário executar nenhuma das outras etapas de configuração, a placa de som é configurada automaticamente. É possível definir o volume ou qualquer opção que deseja mudar posteriormente.

Configuração normal

Permite ajustar o volume de saída e reproduzir um som de teste durante a configuração.

Configuração avançada com possibilidade de mudar opções

Somente para especialistas. Permite personalizar todos os parâmetros da placa de som.



Importante: Configuração avançada

Use essa opção apenas se souber exatamente o que está fazendo. Do contrário, não mexa nos parâmetros e use as opções de configuração normal ou automática.

1. Inicie o módulo de som do YaST.
2. Para configurar uma placa de som detectada, mas *Não Configurada*, selecione a respectiva entrada na lista e clique em *Editar*.
Para configurar uma nova placa de som, clique em *Adicionar*. Selecione o fornecedor e modelo da sua placa de som e clique em *Avançar*.
3. Escolha uma das opções de configuração e clique em *Avançar*.
4. Se você escolheu *Configuração normal*, poderá agora *Testar* a configuração de som e fazer ajustes no volume. Você deve iniciar com um volume de aproximadamente 10% para evitar danos aos ouvidos e alto-falantes.
5. Se todas as opções estiverem definidas conforme o desejado, clique em *Próximo*.
A caixa de diálogo *Configuração de Som* mostra a placa de som recém-configurada ou modificada.
6. Para remover uma configuração de placa de som desnecessária, selecione a respectiva entrada e clique em *Apagar*.
7. Clique em *OK* para gravar as mudanças e sair do módulo de som do YaST.

PROCEDIMENTO 33.2: MODIFICANDO AS CONFIGURAÇÕES DA PLACA DE SOM

1. Para mudar a configuração de uma placa de som individual (somente para especialistas!), selecione a entrada da placa de som na caixa de diálogo *Configuração de Som* e clique em *Editar*.
Isso leva você até as *Opções Avançadas para Placa de Som*, onde é possível ajustar vários parâmetros. Para obter mais informações, clique em *Ajuda*.
2. Para ajustar o volume de uma placa de som já configurada ou testar a placa de som, selecione a entrada da placa de som na caixa de diálogo *Configuração de Som* e clique em *Outros*. Selecione o respectivo item de menu.



Nota: Mixer do YaST

As configurações do mixer do YaST oferecem apenas opções básicas. Sua meta é solucionar problemas (por exemplo, se o teste de som não for audível). Acesse as configurações do mixer do YaST em *Outros > Volume*. Para uso diário e ajuste das opções de som, use o applet de mixer fornecido pelo seu desktop ou a ferramenta de linha de comando **alsasound**.

3. Para a reprodução de arquivos MIDI, selecione *Outros > Iniciar Sequenciador*.
4. Quando uma placa de som suportada é detectada, você pode instalar o SoundFonts para reprodução de arquivos MIDI:
 - a. Insira o CD-ROM do driver original na unidade de CD ou DVD.
 - b. Selecione *Outros > Instalar Soundfonts* para copiar as SoundFonts™ SF2 para o seu disco rígido. As SoundFonts são gravadas no diretório /usr/share/sfbank/creative/.
5. Se você configurou mais de uma placa de som no sistema, poderá ajustar a ordem delas. Para definir uma placa de som como dispositivo principal, selecione a placa de som em *Configuração de Som* e clique em *Outros > Definir como Placa Principal*. O dispositivo de som com índice 0 é o padrão e, portanto, usado pelo sistema e pelos aplicativos.
6. Por padrão, o SUSE Linux Enterprise Desktop usa o sistema de som PulseAudio. Trata-se de uma camada de abstração que faz a mixagem de vários fluxos de áudio, ignorando quaisquer restrições que o hardware possa ter. Para habilitar ou desabilitar o sistema de som PulseAudio, clique em *Outros > Configuração do PulseAudio*. Se habilitado, o daemon do PulseAudio é usado para reproduzir sons. Desabilite o *Suporte ao PulseAudio* para usar algum outro recurso em todo o sistema.

O volume e a configuração de todas as placas de som são gravados quando você clica em *OK* e sai do módulo de som do YaST. As configurações do mixer são gravadas no arquivo /etc/asound.state. Os dados de configuração do ALSA são anexados ao fim do arquivo /etc/modprobe.d/sound e gravados em /etc/sysconfig/sound.

34 Configurando uma impressora

É possível usar o YaST para configurar uma impressora local conectada à máquina por USB e definir a impressão com impressoras de rede. É possível também compartilhar impressoras na rede. Há mais informações disponíveis sobre impressão (informações gerais, detalhes técnicos e solução de problemas) no [Capítulo 24, Operação da impressora](#).

No YaST, clique em *Hardware* > *Impressora* para iniciar o módulo de impressora. Por padrão, ele é aberto na tela *Configurações da Impressora*, exibindo uma lista de todas as impressoras disponíveis e configuradas. Isso é especialmente útil quando se tem acesso a inúmeras impressoras na rede. Deste ponto, é possível também *Imprimir uma Página de Teste* e configurar impressoras.



Nota: Iniciando o CUPS

Para imprimir do seu sistema, o CUPS deve estar em execução. Se ele não estiver em execução, será solicitado para que seja iniciado. Responda com *Sim*, do contrário, não será possível configurar a impressão. Caso o CUPS não seja iniciado no momento da inicialização, também será solicitado para você habilitar esse recurso. É recomendado especificar *Sim*, do contrário, o CUPS terá de ser iniciado manualmente após cada reinicialização.

34.1 Configurando impressoras

Normalmente, uma impressora USB é automaticamente detectada. Há dois motivos possíveis para ela não ser detectada automaticamente:

- A impressora USB está desligada.
- A comunicação entre a impressora e o computador não é possível. Verifique o cabo e os plugues para se certificar de que a impressora esteja corretamente conectada. Se este for o caso, o problema poderá não estar relacionado à impressora, mas sim ao USB.

A configuração de uma impressora é um processo de três etapas: especificar o tipo de conexão, escolher um driver e dar um nome à fila de impressão para esta configuração.

Há vários drivers disponíveis para diversos modelos de impressora. Ao configurar a impressora, o YaST usa como padrão os drivers marcados com recommended (recomendados) como regra geral. Normalmente, não é necessário mudar o driver. Entretanto, para que uma impressora

colorida imprima apenas em preto e branco, você pode usar um driver que não suporte impressão colorida. Se você tiver problemas de desempenho com uma impressora PostScript para imprimir gráficos, tente alternar de um driver PostScript para um driver PCL (contanto que sua impressora reconheça PCL).

Se o driver de sua impressora não aparecer na lista, tente selecionar um driver genérico com uma linguagem padrão apropriada na lista. Consulte a documentação da sua impressora para saber qual linguagem (o conjunto de comandos que controlam a impressora) é entendida por sua impressora. Se isso não funcionar, consulte a [Seção 34.1.1, “Adicionando drivers com o YaST”](#) para obter outra solução possível.

A impressora nunca é usada diretamente, mas sempre por meio de uma fila de impressão. Dessa forma, as tarefas simultâneas poderão ser enfileiradas e processadas em sequência. Cada fila de impressão recebe um driver específico, e uma impressora pode ter várias filas. Isso possibilita configurar uma segunda fila em uma impressora colorida que imprima somente em preto e branco, por exemplo. Consulte a [Seção 24.1, “O workflow do CUPS”](#) para obter mais informações sobre filas de impressão.

PROCEDIMENTO 34.1: ADICIONANDO UMA NOVA IMPRESSORA

1. Inicie o módulo de impressora do YaST em *Hardware > Impressora*.
2. Na tela *Configurações da Impressora*, clique em *Adicionar*.
3. Se a impressora já estiver na lista em Especificar a Conexão, vá para a próxima etapa. Do contrário, tente *Detect More* (Detectar Mais) ou inicie o *Assistente de Conexão*.
4. Na caixa de texto em Find and Assign a Driver (Localizar e Atribuir um Driver), digite o nome do fornecedor e do modelo e clique em *Procurar por*.
5. Escolha um driver que corresponda à impressora. É recomendado escolher o primeiro driver da lista. Se nenhum driver adequado for exibido:
 - a. Verifique o termo de pesquisa.
 - b. Amplie a pesquisa clicando em *Localizar Mais*.
 - c. Adicione o driver conforme descrito na [Seção 34.1.1, “Adicionando drivers com o YaST”](#).
6. Especifique o Tamanho padrão do papel.
7. No campo *Set Arbitrary Name* (Definir Nome Arbitrário), digite um nome exclusivo para a fila de impressão.

8. A impressora agora está definida com as configurações padrão e pronta para ser usada. Clique em *OK* para retornar à tela *Configurações da Impressora*. A impressora recém-configurada agora aparece na lista de impressoras.

34.1.1 Adicionando drivers com o YaST

Nem todos os drivers de impressora disponíveis para o SUSE Linux Enterprise Desktop são instalados por padrão. Se nenhum driver adequado estiver disponível na caixa de diálogo *Find and Assign a Driver* ao adicionar uma nova impressora, instale um pacote que tenha os drivers para a sua impressora:

PROCEDIMENTO 34.2: INSTALANDO PACOTES DE DRIVERS ADICIONAIS

1. Inicie o módulo de impressora do YaST em *Hardware > Impressora*.
2. Na tela *Configurações da Impressora*, clique em *Adicionar*.
3. Na seção *Find and Assign a Driver*, clique em *Pacotes de Drivers*.
4. Escolha um ou mais pacotes de drivers adequados na lista. Não especifique o caminho para um arquivo de descrição da impressora.
5. Escolha *OK* e confirme a instalação do pacote.
6. Para usar os drivers diretamente, proceda conforme descrito no *Procedimento 34.1, "Adicionando uma nova impressora"*.

As impressoras PostScript não precisam de software de driver de impressora. As impressoras PostScript só precisam de um arquivo PPD (PostScript Printer Description) correspondente ao modelo em particular. Os arquivos PPD são fornecidos pelo fabricante da impressora.

Se não houver nenhum arquivo PPD adequado disponível na caixa de diálogo *Localizar e Atribuir um Driver* ao adicionar uma impressora PostScript, instale um arquivo PPD para sua impressora:

Há várias fontes de arquivos PPD disponíveis. A recomendação é primeiro tentar outros pacotes de drivers que façam parte do SUSE Linux Enterprise Desktop, mas que não são instalados por padrão (veja a seguir as instruções de instalação). Se esses pacotes não incluírem os drivers adequados para a sua impressora, obtenha os arquivos PPD diretamente do fornecedor da impressora ou do CD do driver de uma impressora PostScript. Para obter os detalhes, consulte a *Seção 24.8.2, "Nenhum arquivo PPD adequado disponível para impressora PostScript"*. Se preferir, localize os arquivos PPD em <http://www.linuxfoundation.org/collaborate/workgroups/>

[openprinting/database/databaseintro](https://openprinting.org/database/databaseintro), o “banco de dados de impressoras do OpenPrinting.org”. Ao fazer download dos arquivos PPD do OpenPrinting, lembre-se de que o status do suporte do Linux mais recente é sempre mostrado, que não é necessariamente igual ao do SUSE Linux Enterprise Desktop.

PROCEDIMENTO 34.3: ADICIONANDO UM ARQUIVO PPD PARA IMPRESSORAS POSTSCRIPT

1. Inicie o módulo de impressora do YaST em *Hardware > Impressora*.
2. Na tela *Configurações da Impressora*, clique em *Adicionar*.
3. Na seção Find and Assign a Driver, clique em *Pacotes de Drivers*.
4. Insira o caminho completo para o arquivo PPD na caixa de texto em Disponibilizar um Arquivo de Descrição de Impressora.
5. Clique em *OK* para retornar à tela Adicionar Nova Configuração de Impressora.
6. Para usar diretamente esse arquivo PPD, proceda conforme descrito no *Procedimento 34.1, “Adicionando uma nova impressora”*.

34.1.2 Editando a configuração da impressora local

Ao editar uma configuração existente de uma impressora, é possível mudar as configurações básicas, como o tipo de conexão e o driver. Também é possível ajustar as configurações padrão de tamanho de papel, resolução, fonte de mídia etc. Você pode mudar os identificadores da impressora alterando a descrição ou o local da impressora.

1. Inicie o módulo de impressora do YaST em *Hardware > Impressora*.
2. Na tela *Configurações da Impressora*, escolha a configuração da impressora local na lista e clique em *Editar*.
3. Mude o tipo de conexão ou o driver conforme descrito no *Procedimento 34.1, “Adicionando uma nova impressora”*. Isso será necessário apenas se houver problemas com a configuração atual.
4. Se preferir, defina a impressora como padrão marcando *Impressora Padrão*.
5. Ajuste as configurações padrão clicando em *Todas as Opções do Driver Atual*. Para mudar uma configuração, expanda a lista de opções clicando no sinal de + relacionado. Mude o padrão clicando em uma opção. Aplique suas mudanças com *OK*.

34.2 Configurando a impressão pela rede com o YaST

As impressoras de rede não são detectadas automaticamente. Elas devem ser configuradas manualmente usando o módulo de impressora do YaST. Dependendo de sua configuração de rede, você poderá imprimir em um servidor de impressão (CUPS, LPD, SMB ou IPX) ou diretamente em uma impressora de rede (de preferência, via TCP). Acesse a tela de configuração para impressão de rede escolhendo *Impressão pela Rede* no painel esquerdo do módulo de impressora do YaST.

34.2.1 Usando CUPS

Em um ambiente Linux, o CUPS é geralmente usado para imprimir pela rede. A configuração mais simples consiste em imprimir apenas por um único servidor CUPS que possa ser diretamente acessado por todos os clientes. A impressão por mais de um servidor CUPS requer um daemon local do CUPS em execução que se comunique com os servidores CUPS remotos.



Importante: Pesquisando filas de impressão de rede

Os servidores CUPS anunciam suas filas de impressão pela rede usando o protocolo de pesquisa tradicional do CUPS ou o Bonjour/DNS-SD. Os clientes precisam navegar pelas listas para que os usuários possam selecionar as impressoras específicas às quais enviar seus serviços de impressão. Para navegar em filas de impressão de rede, o serviço `cups-browsed` incluído no pacote `cups-filters-cups-browsed` deve ser executado em todos os clientes que imprimem usando servidores CUPS. O `cups-browsed` é iniciado automaticamente quando a impressão de rede é configurada com o YaST.

Caso a pesquisa não funcione depois de iniciar `cups-browsed`, o(s) servidor(es) CUPS provavelmente anunciará(ão) as filas de impressão de rede pelo Bonjour/DNS-SD. Neste caso, é necessário instalar também o pacote `avahi` e iniciar o serviço associado ao **`sudo systemctl start avahi-daemon`** em todos os clientes.

PROCEDIMENTO 34.4: IMPRIMINDO POR UM ÚNICO SERVIDOR CUPS

1. Inicie o módulo de impressora do YaST em *Hardware > Impressora*.
2. No painel esquerdo, inicie a tela *Imprimir pela Rede*.

3. Marque *Do All Your Printing Directly via One Single CUPS Server* (Realizar Toda a Impressão Diretamente via um Único Servidor CUPS) e especifique o nome ou endereço IP do servidor.
4. Clique em *Testar Servidor* para verificar se você escolheu o nome ou endereço IP correto.
5. Clique em *OK* para retornar à tela *Configurações da Impressora*. Todas as impressoras disponíveis pelo servidor CUPS são listadas.

PROCEDIMENTO 34.5: IMPRIMINDO POR VÁRIOS SERVIDORES CUPS

1. Inicie o módulo de impressora do YaST em *Hardware > Impressora*.
2. No painel esquerdo, inicie a tela *Imprimir pela Rede*.
3. Marque *Accept Printer Announcements from CUPS Servers* (Aceitar Anúncios de Impressora de Servidores CUPS).
4. Em *Configurações Gerais*, especifique quais servidores serão usados. É possível aceitar conexões de todas as redes disponíveis ou de hosts específicos. Se você escolher a última opção, deverá especificar os nomes de host ou endereços IP.
5. Clique em *OK* para confirmar e depois em *Sim* quando for solicitado a iniciar um servidor CUPS local. Após a inicialização do servidor, o YaST retornará para a tela *Configurações da Impressora*. Clique em *Lista de Atualização* para ver as impressoras detectadas até o momento. Clique nesse botão mais uma vez, caso haja mais impressoras disponíveis.

34.2.2 Usando servidores de impressão diferentes do CUPS

Se a sua rede oferecer serviços de impressão por servidores de impressão diferentes do CUPS, inicie o módulo de impressora do YaST clicando em *Hardware > Impressora* e inicie a tela *Imprimir pela Rede* pelo painel esquerdo. Inicie o *Assistente de Conexão* e escolha o *Tipo de Conexão*. Solicite mais informações ao administrador da rede sobre como configurar uma impressora de rede em seu ambiente.

34.3 Compartilhando impressoras pela rede

As impressoras gerenciadas por um daemon CUPS local podem ser compartilhadas pela rede, portanto, transforme sua máquina em um servidor CUPS. Normalmente, você compartilha uma impressora habilitando o chamado “modo de navegação” no CUPS. Se a pesquisa estiver

habilitada, as filas de impressão locais serão disponibilizadas na rede para escutar os daemons remotos do CUPS. Também é possível configurar um servidor CUPS dedicado que gerencie todas as filas de impressão e possa ser acessado diretamente pelos clientes remotos. Nesse caso, não é necessário habilitar a navegação.

PROCEDIMENTO 34.6: **COMPARTILHANDO IMPRESSORAS**

1. Inicie o módulo de impressora do YaST em *Hardware > Impressora*.
2. Inicie a tela *Compartilhar Impressoras* no painel esquerdo.
3. Selecione *Permitir acesso remoto*. Marque também *Para computadores dentro da rede local* e habilite o modo de pesquisa marcando *Publicar impressoras por padrão dentro da rede local*.
4. Clique em *OK* para reiniciar o servidor CUPS e retornar à tela *Configurações da Impressora*.
5. Para saber sobre as configurações do CUPS e de firewall, acesse o site https://en.opensuse.org/SDB:CUPS_and_SANE_Firewall_settings ↗.

35 Configurando um scanner

É possível configurar um scanner USB ou SCSI com o YaST. O pacote `sane-backends` inclui drivers de hardware e outros itens essenciais necessários para usar o scanner. Se você tiver um dispositivo multifuncional HP, consulte a [Seção 35.1, “Configurando um dispositivo multifuncional HP”](#), as instruções sobre como configurar um scanner de rede estão disponíveis na [Seção 35.3, “Digitalizando pela rede”](#).

PROCEDIMENTO 35.1: CONFIGURANDO UM SCANNER USB OU SCSI

1. Conecte o scanner USB ou SCSI ao computador e ligue-o.
2. Inicie o YaST e selecione *Hardware > Scanner*. O YaST cria o banco de dados de scanner e tenta detectar seu modelo de scanner automaticamente.
Se um scanner USB ou SCSI não for corretamente detectado, tente *Outros > Reiniciar Detecção*.
3. Para ativar o scanner, selecione-o na lista de scanners detectados e clique em *Editar*.
4. Escolha o modelo na lista e clique em *Avançar* e em *Concluir*.
5. Use *Outros > Testar* para verificar se você escolheu o driver correto.
6. Saia da tela de configuração clicando em *OK*.

35.1 Configurando um dispositivo multifuncional HP

É possível configurar um dispositivo Multifuncional HP com o YaST, mesmo que ele esteja disponibilizado na rede. Se tiver um dispositivo multifuncional HP USB, inicie a configuração conforme descrito no [Procedimento 35.1, “Configurando um scanner USB ou SCSI”](#). Se for detectado apropriadamente e o *Teste* for bem-sucedido, estará pronto para uso.

Se o dispositivo USB não for detectado apropriadamente ou o dispositivo multifuncional HP estiver conectado à rede, execute o Gerenciador de Dispositivos HP:

1. Inicie o YaST e selecione *Hardware > Scanner*. O YaST carrega o banco de dados de scanner.
2. Inicie o Gerenciador de Dispositivos HP clicando em *Outros > Executar hp-setup* e siga as instruções na tela. Após concluir o Gerenciador de Dispositivos HP, o módulo de scanner do YaST reiniciará automaticamente a detecção automática.

3. Teste-o clicando em *Outros* > *Testar*.
4. Saia da tela de configuração clicando em *OK*.

35.2 Compartilhando um scanner pela rede

O SUSE Linux Enterprise Desktop permite compartilhar um scanner na rede. Para isso, configure o scanner da seguinte forma:

1. Configure o scanner conforme descrito no *Capítulo 35, Configurando um scanner*.
2. Escolha *Outros* > *Digitalização via Rede*.
3. Digite os nomes de host dos clientes (separados por vírgula) que devem ter permissão para usar o scanner em *Configurações do Servidor* > *Clientes Permitidos para saned* e clique em *OK* para sair da caixa de diálogo de configuração.

35.3 Digitalizando pela rede

Para usar um scanner compartilhado pela rede, faça o seguinte:

1. Inicie o YaST e selecione *Hardware* > *Scanner*.
2. Abra o menu de configuração do scanner de rede clicando em *Outros* > *Digitalização via Rede*.
3. Digite o nome de host da máquina à qual o scanner está conectado em *Configurações do Cliente* > *Servidores Usados para net Metadriver*.
4. Saia com *OK*. O scanner de rede está agora listado na janela *Configuração do Scanner* e pronto para uso.

36 Gerenciamento de energia

O gerenciamento de energia é especialmente importante em laptops, mas também é útil em outros sistemas. A ACPI (Advanced Configuration and Power Interface — Interface de Energia e Configuração Avançada) está disponível em todos os computadores modernos (laptops, desktops e servidores). As tecnologias de gerenciamento de energia exigem hardware adequado e rotinas BIOS. A maioria dos laptops e muitos desktops e servidores modernos atendem a esses requisitos. Também é possível controlar a escala de frequência de CPU para economizar energia ou reduzir o ruído.

36.1 Funções de economia de energia

As funções de economia de energia não são significativas apenas para o uso móvel de laptops, como também para sistemas desktop. As funções principais e respectivas utilizações na ACPI são:

Standby

Não suportado.

Suspend (para a memória)

Este modo grava todo o estado do sistema na memória RAM. Em seguida, todo o sistema é colocado em repouso, salvo a memória RAM. Neste estado, o computador consome pouquíssima energia. A vantagem desse estado é a possibilidade de reiniciar o trabalho no mesmo ponto em alguns segundos sem precisar inicializar e reiniciar os aplicativos. Essa função corresponde ao estado da ACPI S3.

Hibernação (suspend para disco)

Neste modo operacional, o estado do sistema inteiro é gravado no disco rígido e o sistema é desligado. Deve existir uma partição de troca pelo menos tão grande quanto a RAM para gravar todos os dados ativos. A reativação desse estado leva de 30 a 90 segundos. O estado anterior ao suspenso é restaurado. Alguns fabricantes oferecem variantes híbridas desse modo, como RediSafe em Thinkpads da IBM. O estado correspondente da ACPI é S4. No Linux, a suspensão para disco é desempenhada pelas rotinas de kernel, que são independentes de ACPI.



Nota: UUID modificado para partições de troca (swap) ao formatar com **mkswap**

Não reformate as partições de troca (swap) existentes com **mkswap**, se possível. A reformatação com **mkswap** muda o valor do UUID da partição de troca (swap). Reformate usando o YaST (o que atualizará o `/etc/fstab`) ou ajuste o `/etc/fstab` manualmente.

Monitor de bateria

A ACPI verifica o status da carga da bateria e fornece informações correspondentes. Além disso, ela coordena as ações a serem desempenhadas quando um status de carga crítico é atingido.

Desligamento automático

Após um encerramento, o computador é desligado. Isto é especialmente importante quando um encerramento automático é realizado pouco antes da bateria esgotar-se.

Controle de velocidade do processador

Em conexão com a CPU, é possível economizar energia de três maneiras diferentes: escala de frequência e voltagem (também conhecida como PowerNow! ou Speedstep), throttling e adormecimento do processador (C-states). Dependendo do modo operacional do computador, esses métodos também podem ser combinados.

36.2 Advanced Configuration and Power Interface (ACPI)

A ACPI foi desenvolvida para habilitar o sistema operacional a configurar e controlar cada componente de hardware. A ACPI substitui tanto o Plug and Play (PnP) de Gerenciamento de Energia quanto o Gerenciamento Avançado de Energia (APM). Ela envia informações sobre a bateria, o adaptador de CA, a temperatura, o ventilador e eventos do sistema, como “fechar tampa” ou “bateria fraca”.

O BIOS fornece tabelas que contém informações sobre os componentes individuais e métodos de acesso ao hardware. O sistema operacional usa essas informações para tarefas como atribuir interrupções ou ativar e desativar componentes. Como o sistema operacional executa comandos armazenados no BIOS, a funcionalidade depende da implementação do BIOS. As tabelas que a ACPI pode detectar e carregar estão relatadas em `journalctl`. Consulte o [Capítulo 21, `journalctl`](#):

Consultar o *diário do systemd* para obter mais informações sobre como ver as mensagens de registro do diário. Consulte a *Seção 36.2.2, “Solução de problemas”* para obter mais informações sobre solução de problemas da ACPI.

36.2.1 Controlando o desempenho da CPU

A CPU pode economizar energia de três maneiras:

- Escala de frequência e voltagem
- Obstruindo a frequência do relógio (T-states)
- Adormecendo o processador (C-states)

Dependendo do modo operacional do computador, estes métodos também podem ser combinados. Economizar energia também significa que o sistema esquenta menos e os ventiladores são ativados com menos frequência.

Expansão e throttling de frequência são relevantes apenas quando o processador está ocupado, pois o C-state mais econômico é aplicado de qualquer maneira quando o processador fica ocioso. Se a CPU estiver ocupada, a escala da frequência é o método recomendado para economia de energia. Em geral o processador só trabalha com carga parcial. Neste caso, pode ser executado com uma frequência inferior. Normalmente, a expansão da frequência dinâmica controlada pelo regulador sob demanda do kernel é a melhor abordagem.

Throttling deve ser usado como última alternativa, por exemplo, para ampliar o tempo de operação da bateria, apesar de uma alta carga do sistema. Contudo, alguns sistemas não são executados suavemente quando ocorrem throttlings em excesso. Ademais, o throttling da CPU não faz sentido se a CPU tem pouco a fazer.

Para obter informações mais detalhadas, consulte o Livro *“System Analysis and Tuning Guide”*, Capítulo 12 *“Power management”*.

36.2.2 Solução de problemas

Há dois tipos de problemas. De um lado, o código ACPI do kernel pode conter erros que não foram detectados em tempo útil. Neste caso, uma solução estará disponível para download. O mais comum é que os problemas sejam causados pelo BIOS. Às vezes, desvios da especificação da ACPI são propositalmente integrados ao BIOS para contornar erros na implementação da

ACPI em outros sistemas operacionais amplamente utilizados. Componentes de hardware que têm erros sérios na implementação da ACPI são gravados em uma lista negra que impede que o kernel do Linux use a ACPI para esses componentes.

A primeira ação a ser tomada quando problemas forem detectados, é atualizar o BIOS. Se o computador não inicializar, um dos seguintes parâmetros de boot poderá ser útil:

pci=noacpi

Não usar ACPI para configurar os dispositivos PCI.

acpi=ht

Realizar apenas uma configuração com recursos simples. Não usar a ACPI para outros fins.

acpi=off

Desabilitar a ACPI.



Atenção: Problemas de boot sem ACPI

Algumas máquinas mais novas (especialmente os sistemas SMP e AMD64) precisam de ACPI para configurar o hardware corretamente. Nestas máquinas, desabilitar a ACPI pode causar problemas.

Às vezes a máquina é confundida pelo hardware conectado por USB ou FireWire. Se uma máquina se recusa a inicializar, desconecte todos os itens de hardware desnecessários e tente novamente.

Monitore as mensagens de boot do sistema com o comando `dmesg -T | grep -2i acpi` (ou todas as mensagens, porque o problema pode não ser causado pela ACPI) após a inicialização. Se ocorrer um erro ao analisar uma tabela ACPI, a tabela mais importante, a DSDT (*Differentiated System Description Table*), poderá ser substituída por uma versão aprimorada. Neste caso, a DSDT defeituosa do BIOS é ignorada. O procedimento está descrito na [Seção 36.4, “Solução de problemas”](#).

Na configuração do kernel, há um switch para ativar as mensagens de depuração da ACPI. Se houver um kernel com depuração ACPI compilado e instalado, serão emitidas informações detalhadas.

Se você tiver problemas com BIOS ou hardware, é sempre recomendável entrar em contato com os fabricantes. Especialmente se eles nem sempre derem assistência ao Linux, devem ser indagados em caso de problemas. Os fabricantes só levarão a questão a sério se compreenderem que um número satisfatório de seus clientes usa Linux.

36.2.2.1 Mais informações

- <https://tldp.org/HOWTO/ACPI-HOWTO/> (ACPI HOWTO detalhado, contém patches DSDT)
- <https://uefi.org/specifications> (Configuração Avançada e Especificação da Interface de Energia)

36.3 Inatividade do disco rígido

No Linux, o disco rígido pode ser colocado em repouso total se não estiver em uso e pode ser executado em modo mais econômico ou silencioso. Nos laptops modernos, não é necessário desativar o disco rígido manualmente, porque entram automaticamente em um modo operacional econômico sempre que não estão em uso. No entanto, para aumentar a economia de energia, experimente alguns dos seguintes métodos usando o comando **hdparm**.

Ele pode ser usado para modificar várias configurações de disco rígido. A opção **-y** alterna instantaneamente o disco rígido para o modo standby. **-Y** coloca-o no modo adormecido. **hdparm -S X** faz o disco rígido ser encerrado após um determinado período de inatividade. Substitua **X** conforme mostrado a seguir: **0** desabilita esse mecanismo, fazendo o disco rígido funcionar continuamente. Valores de **1** a **240** são multiplicados por 5 segundos. Valores de **241** a **251** correspondem de 1 a 11 vezes 30 minutos.

As opções de economia de energia interna do disco rígido podem ser controladas pela opção **-B**. Selecione um valor de **0** a **255** para obter de economia máxima a throughput máximo. O resultado depende do disco rígido usado e é difícil de avaliar. Para tornar um disco rígido mais silencioso, use a opção **-M**. Selecione um valor de **128** a **254** para obter de silencioso a rápido.

Muitas vezes não é fácil colocar o disco rígido em repouso. No Linux, vários processos gravam no disco rígido, ativando-o repetidamente. Portanto, é importante entender como o Linux trata os dados que necessitam ser gravados no disco rígido. Primeiro, todos os dados estão no buffer da memória RAM. Esse buffer é monitorado pelo daemon **pdflush**. Quando os dados atingem uma determinada idade limite ou quando o buffer está cheio até certo grau, o conteúdo do buffer é descarregado para o disco rígido. O tamanho do buffer é dinâmico e depende do tamanho da memória e da carga do sistema. Por padrão, **pdflush** é configurado em intervalos curtos para obter a integridade máxima de dados. Ele verifica o buffer a cada 5 segundos e grava os dados no disco rígido. As seguintes variáveis são interessantes:

`/proc/sys/vm/dirty_writeback_centisecs`

Inclui o atraso até o thread **pdflush** ser acionado (em centésimos de segundo).

/proc/sys/vm/dirty_expire_centisecs

Define o período após o qual uma página modificada deve ser gravada por último. O padrão é 3000, o que equivale a 30 segundos.

/proc/sys/vm/dirty_background_ratio

Porcentagem máxima de páginas modificadas para `pdflush` começar a gravá-las. O padrão é 5 %.

/proc/sys/vm/dirty_ratio

Quando a página modificada exceder essa porcentagem da memória total, os processos serão forçados a gravar buffers modificados durante suas frações de tempo em vez de continuar gravando.



Atenção: Risco à integridade dos dados

As mudanças feitas nas configurações do daemon `pdflush` podem comprometer a integridade dos dados.

Além desses processos, sistemas JFS, como `Btrfs`, `Ext3`, `Ext4`, entre outros, gravam seus metadados independentemente do `pdflush`, que também impede que o disco rígido pare de funcionar. Para evitar isso, foi desenvolvida uma extensão especial de kernel para dispositivos móveis. Para usar a extensão, instale o pacote `laptop-mode-tools` e consulte `/usr/src/linux/Documentation/laptops/laptop-mode.txt` para obter detalhes.

Outro fator importante é o modo como se comportam os programas ativos. Por exemplo, os bons editores gravam regularmente backups ocultos do arquivo modificado no momento para o disco rígido, fazendo com que ele saia do modo de hibernação. Recursos como este podem ser desabilitados às custas da integridade dos dados.

Com relação a isso, o mail daemon postfix usa a variável `POSTFIX_LAPTOP`. Se essa variável for configurada para `sim`, postfix acessa o disco rígido com muito menos frequência.

No SUSE Linux Enterprise Desktop, estas tecnologias são controladas por `laptop-mode-tools`.

36.4 Solução de problemas

Todas as mensagens de erro e os alertas são registrados no diário do sistema, que pode ser consultado com o comando **journalctl** (consulte o [Capítulo 21, **journalctl**: Consultar o diário do systemd](#) para obter mais informações). As seções a seguir abordam os problemas mais comuns.

36.4.1 A frequência da CPU não funciona

Consulte as fontes do kernel para ver se o seu processador é suportado. Você poderá precisar de um módulo de kernel ou de opção especial para ativar o controle de frequência da CPU. Se o pacote kernel-source estiver instalado, essas informações estarão disponíveis em /usr/src/linux/Documentation/cpu-freq/.

37 Memória persistente

Este capítulo contém informações adicionais sobre como usar o SUSE Linux Enterprise com memória principal não volátil, também conhecida como *Memória Persistente*, que consiste em um ou mais NVDIMMs.

37.1 Introdução

Memória persistente é um novo tipo de armazenamento no computador que combina velocidades muito próximas às da RAM dinâmica (DRAM) ao endereçamento byte por byte da RAM, além da permanência das unidades de estado sólido (SSDs, Solid-State Drives).

No momento, a SUSE permite o uso de memória persistente com o SUSE Linux Enterprise Server em máquinas com as arquiteturas AMD64/Intel 64 e POWER.

Como a RAM convencional, a memória persistente é instalada diretamente nos slots de memória da placa-mãe. Dessa forma, ela é fornecida no mesmo fator de formato físico da RAM – como DIMMs. Eles são conhecidos como NVDIMMs: módulos de memória dupla em linha não voláteis.

No entanto, ao contrário da RAM, a memória persistente apresenta vários aspectos similares aos SSDs com base em flash. As duas são baseadas em formatos de circuito de memória de estado sólido, mas, apesar disso, ambas fornecem armazenamento não volátil: O conteúdo é mantido quando o sistema é desligado ou reiniciado. Para ambos os formatos de meio, a gravação de dados é mais lenta do que a leitura, e os dois suportam um número limitado de ciclos de regravagem. Por fim, também como os SSDs, o acesso à memória persistente no nível do setor será possível se isso for mais adequado para um determinado aplicativo.

Modelos diferentes usam formatos distintos de meio de armazenamento eletrônico, como Intel 3D XPoint, ou uma combinação de NAND Flash e DRAM. Há novos formatos de RAM não volátil também em desenvolvimento. Isso significa que fornecedores e modelos diferentes do NVDIMM oferecem características distintas de durabilidade e desempenho.

Como as tecnologias de armazenamento envolvidas estão em um estágio inicial de desenvolvimento, o hardware de fornecedores diferentes pode impor limitações distintas. Dessa forma, as afirmações a seguir são uma generalização.

A memória persistente é até dez vezes mais lenta do que a DRAM, mas cerca de mil vezes mais rápida do que o armazenamento flash. Ela pode ser regravada byte por byte, em vez de usar o processo da memória flash de “apagar e regravar” todo o setor. Por fim, enquanto os ciclos de regravagem são limitados, a maioria dos formatos de memória persistente pode processar milhões de regravagens, em comparação com os milhares de ciclos do armazenamento flash.

Isso apresenta duas consequências importantes:

- Com a tecnologia atual, não é possível executar um sistema apenas com memória persistente e, desse modo, atingir uma memória principal totalmente não volátil. Você deve usar uma mistura de RAM convencional e NVDIMMs. Os aplicativos e o sistema operacional serão executados na RAM convencional, com os NVDIMMs fornecendo o armazenamento suplementar muito rápido.
- As características de desempenho da memória persistente dos diversos fornecedores significam que talvez seja necessário para os programadores prestar atenção nas especificações de hardware dos NVDIMMs em um servidor específico, incluindo quantos NVDIMMs existem e em quais slots de memória eles se encaixam. Isso afetará o uso do hipervisor, a migração de software entre máquinas host diferentes etc.

Esse novo subsistema de armazenamento está definido na versão 6 do padrão ACPI. No entanto, o libnvdimm suporta NVDIMMs anteriores ao padrão, e eles podem ser usados da mesma maneira.

37.2 Termos

Região

Uma *região* é um bloco da memória persistente que pode ser dividido em mais *namespaces*. Não é possível acessar a memória persistente de uma região sem primeiro alocá-la a um namespace.

Namespace

Uma única faixa continuamente endereçada de armazenamento não volátil, comparável a namespaces de SSD do NVM Express ou a LUNs (Logical Units – Unidades Lógicas) de SCSI. Os namespaces aparecem no diretório /dev/cdrom do servidor como dispositivos de blocos separados. Dependendo do método de acesso necessário, os namespaces podem unir o armazenamento de vários NVDIMMs em grandes volumes ou permitir que ele seja particionado em volumes menores.

Modo

Cada namespace também tem um *modo* que define os recursos NVDIMM que estão habilitados para esse namespace. Os namespaces irmão da mesma região pai sempre terão o mesmo tipo, mas poderão ser configurados para ter modos diferentes. Veja a seguir os modos de namespace:

devdax

Modo Dispositivo-DAX. Cria um arquivo de dispositivo de caractere único (/dev/daxX.S). Não requer a criação do sistema de arquivos.

fsdax

Modo Sistema de arquivos-DAX. Padrão, se nenhum outro modo for especificado. Cria um dispositivo de blocos (/dev/pmemX [.Y]) que suporta o DAX para ext4 ou XFS.

sector

Para sistemas de arquivos legados que não efetuam checksum de metadados. Adequado para pequenos volumes de boot. Compatível com outros sistemas operacionais.

raw

Um disco de memória sem rótulo ou metadados. Não suporta a DAX. Compatível com outros sistemas operacionais.



Nota

O modo raw não é suportado pelo SUSE. Não é possível montar sistemas de arquivos em namespaces raw.

Tipo

Cada namespace e região tem um *tipo* que define o modo como a memória persistente associada a esse namespace ou região pode ser acessada. Um namespace sempre tem o mesmo tipo que sua região pai. Há dois tipos diferentes: Memória Persistente, que pode ser configurada de duas formas diferentes, e o Modo de Bloco descontinuado.

Memória persistente (PMEM)

O armazenamento PMEM oferece acesso no nível de bytes, similar ao da RAM. Usando a PMEM, um único namespace pode incluir vários NVDIMMs intercalados, permitindo que todos sejam usados como um único dispositivo.

Há duas maneiras de configurar um namespace PMEM.

PMEM com DAX

Um namespace PMEM configurado para Acesso Direto (DAX) significa que o acesso à memória ignora o cache de página do kernel e vai direto para o meio. O software pode ler ou gravar diretamente cada byte do namespace de maneira separada.

PMEM com tabela de conversão de blocos (BTT, Block Translation Table)

Um namespace PMEM configurado para operar no modo BTT é acessado de setor por setor, como uma unidade de disco convencional, em vez do modelo endereçável por byte mais semelhante ao da RAM. Um mecanismo de tabela de conversão de lotes acessa as unidades do tamanho do setor.

A vantagem da BTT é a proteção de dados. O subsistema de armazenamento garante que cada setor seja completamente gravado no meio subjacente. Se um setor não puder ser completamente gravado (ou seja, se a operação de gravação falhar por algum motivo), todo o setor será revertido ao estado anterior. Portanto, um determinado setor não pode ser parcialmente gravado. Além disso, acesso a namespaces BTT é armazenado em cache pelo kernel. A desvantagem é que não é possível usar o DAX para namespaces BTT.

Modo de bloco (BLK)

O armazenamento do modo de bloco considera cada NVDIMM como um dispositivo separado. Seu uso foi descontinuado e não é mais suportado.

Exceto pelos namespaces `devdax`, todos os outros tipos devem ser formatados com um sistema de arquivos, assim como em uma unidade convencional. O SUSE Linux Enterprise Desktop suporta os sistemas de arquivos `ext2`, `ext4` e `XFS` para essa finalidade.

Acesso direto (DAX)

O DAX permite que a memória persistente seja mapeada diretamente para o espaço de endereço de um processo, por exemplo, usando a chamada do sistema `mmap`.

Endereço físico DIMM (DPA)

Um endereço de memória como uma diferença na memória de um único DIMM; ou seja, começar do zero como o menor byte endereçável nesse DIMM.

Rótulo

Metadados armazenados no NVDIMM, como definições de namespace. É possível acessá-los usando DSMs.

37.3 Casos de uso

37.3.1 PMEM com DAX

É importante observar que esse formato de acesso à memória *não* é transacional. Em caso de queda de energia ou outra falha no sistema, os dados podem não ser totalmente gravados no armazenamento. O armazenamento PMEM será adequado apenas se o aplicativo puder resolver a situação dos dados parcialmente gravados.

37.3.1.1 Aplicativos que se beneficiam de grandes quantidades de armazenamento endereçável por byte

Se o servidor for hospedar um aplicativo que possa usar diretamente grandes quantidades de armazenamento rápido byte por byte, o programador poderá usar a chamada do sistema `mmap` para inserir blocos da memória persistente diretamente no espaço do endereço do aplicativo, sem usar nenhuma RAM do sistema adicional.

37.3.1.2 Evitando o uso do cache de página do kernel

Evite usar o cache de página do kernel se você deseja continuar usando a RAM para o cache de página. Em vez disso, passe-o para os seus aplicativos. Por exemplo, a memória não volátil pode se dedicar a armazenar imagens da VM (Virtual Machine – Máquina Virtual). Como elas não são armazenadas em cache, isso reduz o uso do cache no host, permitindo mais VMs por host.

37.3.2 PMEM com BTT

Isso é útil quando você deseja usar a memória persistente em um conjunto de NVDIMMs como um pool do tipo disco de armazenamento muito rápido. Por exemplo, ao colocar o diário do sistema de arquivos na PMEM com BTT, você aumenta a confiabilidade da recuperação do sistema de arquivos após uma queda de energia ou outra interrupção repentina (consulte a [Seção 37.5.3, “Criando um namespace PMEM com BTT”](#)).

Para aplicativos, esses dispositivos aparecem como SSDs muito rápidas e podem ser usados como qualquer outro dispositivo de armazenamento. Por exemplo, a LVM pode ser colocada em camadas sobre a memória persistente e funcionará normalmente.

A vantagem do BTT é que a atomicidade de gravação do setor é garantida; portanto, até os aplicativos sofisticados que dependem da integridade dos dados continuarão funcionando. O relatório de erros da mídia funciona por meio dos canais de geração de relatórios de erros.

37.4 Ferramentas para gerenciamento de memória persistente

Para gerenciar a memória persistente, é necessário instalar o pacote `ndctl`. Esse procedimento também instala o pacote `libndctl`, que inclui um conjunto de bibliotecas de espaço do usuário para configurar os NVDIMMs.

Essas ferramentas funcionam por meio da biblioteca `libnvdimm`, que suporta três tipos de NVDIMM:

- PMEM
- BLK
- PMEM e BLK simultâneos

O utilitário `ndctl` inclui um conjunto útil de páginas de `manual`, que pode ser acessado com o comando:

```
> ndctl help subcommand
```

Para ver uma lista de subcomandos disponíveis, use:

```
> ndctl --list-cmds
```

Os subcomandos disponíveis incluem:

version

Exibe a versão atual das ferramentas de suporte do NVDIMM.

enable-namespace

Torna o namespace especificado disponível para uso.

disable-namespace

Impede que o namespace especificado seja usado.

create-namespace

Cria um novo namespace com base nos dispositivos de armazenamento especificado.

destroy-namespace

Remove o namespace especificado.

enable-region

Torna a região especificada disponível para uso.

disable-region

Impede que a região especificada seja usada.

zero-labels

Apaga os metadados de um dispositivo.

read-labels

Recupera os metadados do dispositivo especificado.

list

Exibe os dispositivos disponíveis.

help

Exibe as informações sobre como usar a ferramenta.

37.5 Configurando a memória persistente

37.5.1 Vendo o armazenamento NVDIMM disponível

É possível usar o comando `ndctl list` para listar todos os NVDIMMs disponíveis em um sistema.

No exemplo a seguir, o sistema tem três NVDIMMs, que estão em um único conjunto de canal triplo intercalado.

```
# ndctl list --dimms  
  
[  
  {
```

```

    "dev": "nmem2",
    "id": "8089-00-0000-12325476"
  },
  {
    "dev": "nmem1",
    "id": "8089-00-0000-11325476"
  },
  {
    "dev": "nmem0",
    "id": "8089-00-0000-10325476"
  }
]

```

Com um parâmetro diferente, o **ndctl list** também listará as regiões disponíveis.



Nota

As regiões podem não aparecer em ordem numérica.

Apesar de haver apenas três NVDIMMs, eles aparecem como quatro regiões.

```

# ndctl list --regions

[
  {
    "dev": "region1",
    "size": 68182605824,
    "available_size": 68182605824,
    "type": "blk"
  },
  {
    "dev": "region3",
    "size": 202937204736,
    "available_size": 202937204736,
    "type": "pmem",
    "iset_id": 5903239628671731251
  },
  {
    "dev": "region0",
    "size": 68182605824,
    "available_size": 68182605824,
    "type": "blk"
  },
  {
    "dev": "region2",
    "size": 68182605824,

```

```

    "available_size":68182605824,
    "type":"blk"
  }
]

```

O espaço está disponível em dois formatos diferentes: como três regiões separadas de 64 GB do tipo BLK ou como uma região combinada de 189 GB do tipo PMEM, que apresenta todo o espaço nos três NVDIMMs intercalados como um único volume.

Observe que o valor exibido para `available_size` é igual ao de `size`. Isso significa que nada do espaço ainda foi alocado.

37.5.2 Configurando o armazenamento como um único namespace PMEM com DAX

Para o primeiro exemplo, configuraremos nossos três NVDIMMs em um único namespace PMEM com Acesso Direto (DAX).

A primeira etapa é criar um novo namespace.

```

# ndctl create-namespace --type=pmem --mode=fsdax --map=memory
{
  "dev":"namespace3.0",
  "mode":"memory",
  "size":199764213760,
  "uuid":"dc8ebb84-c564-4248-9e8d-e18543c39b69",
  "blockdev":"pmem3"
}

```

Esse procedimento cria um dispositivo de blocos `/dev/pmem3`, que suporta DAX. O `3` no nome do dispositivo é herdado do número da região pai, neste caso, `region3`.

A opção `--map=memory` separa parte do espaço do armazenamento PMEM nos NVDIMMs para que ele possa ser usado para alocar as estruturas de dados internas do kernel denominadas `struct pages`. Dessa forma, o novo namespace PMEM pode ser usado com recursos como `O_DIRECT` I/O e RDMA.

A reserva de parte da memória persistente para estruturas de dados do kernel é o que causa uma redução na capacidade do namespace PMEM em relação à região PMEM pai.

Na sequência, verificamos se o novo dispositivo de blocos está disponível para o sistema operacional:

```

# fdisk -l /dev/pmem3

```

```
Disk /dev/pmem3: 186 GiB, 199764213760 bytes, 390164480 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
```

Antes que possa ser usada, como qualquer outra unidade, ela deverá ser formatado. Neste exemplo, nós a formatamos com XFS:

```
# mkfs.xfs /dev/pmem3
meta-data=/dev/pmem3      isize=256    agcount=4, agsize=12192640 blks
                =          sectsz=4096   attr=2, projid32bit=1
                =          crc=0         finobt=0, sparse=0
data        =             bsize=4096    blocks=48770560, imaxpct=25
                =             sunit=0     swidth=0 blks
naming      =version 2     bsize=4096    ascii-ci=0 ftype=1
log         =internal log  bsize=4096    blocks=23813, version=2
                =             sectsz=4096  sunit=1 blks, lazy-count=1
realtime    =none         extsz=4096    blocks=0, rtextents=0
```

Em seguida, podemos montar a nova unidade em um diretório:

```
# mount -o dax /dev/pmem3 /mnt/pmem3
```

Agora, podemos verificar que temos um dispositivo compatível com DAX:

```
# mount | grep dax
/dev/pmem3 on /mnt/pmem3 type xfs (rw,relatime,attr2,dax,inode64,noquota)
```

O resultado é que agora contamos com um namespace PMEM formatado com o sistema de arquivos XFS e montado com DAX.

Qualquer chamada `mmap()` para arquivos nesse sistema de arquivos retornará endereços virtuais que são mapeados diretamente para a memória persistente em nossos NVDIMMs, ignorando completamente o cache de página.

Qualquer chamada `fsync` ou `msync` nos arquivos nesse sistema de arquivos ainda garantirá que os dados modificados sejam totalmente gravados nos NVDIMMs. Essas chamadas descarregam as linhas de cache do processador associadas a qualquer página que tenha sido modificada no espaço do usuário por meio de mapeamentos `mmap`.

37.5.2.1 Removendo um namespace

Antes de criar qualquer outro tipo de volume que use o mesmo armazenamento, devemos desmontar e, em seguida, remover esse volume PMEM.

Em primeiro lugar, desmonte-o:

```
# umount /mnt/pmem3
```

Em seguida, desabilite o namespace:

```
# ndctl disable-namespace namespace3.0
disabled 1 namespace
```

Por último, apague-o:

```
# ndctl destroy-namespace namespace3.0
destroyed 1 namespace
```

37.5.3 Criando um namespace PMEM com BTT

A BTT oferece atomicidade de gravação de setores, o que faz dela uma boa opção quando você precisa de proteção de dados, por exemplo, para diários do Ext4 e XFS. Em caso de queda de energia, os diários estão protegidos e podem ser recuperados. Os exemplos a seguir mostram como criar um namespace PMEM com BTT no modo de setor e como colocar o diário do sistema de arquivos nesse namespace.

```
# ndctl create-namespace --type=pmem --mode=sector
{
  "dev": "namespace3.0",
  "mode": "sector",
  "uuid": "51ab652d-7f20-44ea-b51d-5670454f8b9b",
  "sector_size": 4096,
  "blockdev": "pmem3s"
}
```

Em seguida, verifique se o novo dispositivo está presente:

```
# fdisk -l /dev/pmem3s
Disk /dev/pmem3s: 188.8 GiB, 202738135040 bytes, 49496615 sectors
Units: sectors of 1 * 4096 = 4096 bytes
Sector size (logical/physical): 4096 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
```

Como o namespace PMEM compatível com DAX que configuramos anteriormente, esse namespace PMEM compatível com BTT consome todo o armazenamento disponível nos NVDIMMs.



Nota

O s à direita no nome do dispositivo (`/dev/pmem3s`) indica o setor e pode ser usado para diferenciar facilmente os namespaces configurados para usar o BTT.

É possível formatar e montar o volume como no exemplo anterior.

O namespace PMEM mostrado aqui não pode usar DAX. Em vez disso, ele usa o BTT para fornecer *atomicidade de gravação do setor*. Em cada gravação de setor efetuada por meio do driver de bloco PMEM, o BTT alocará um novo setor para receber os novos dados. O BTT atualizará atômicamente suas estruturas de mapeamento internas depois que os novos dados forem totalmente gravados para que os dados recém-gravados ainda fiquem disponíveis aos aplicativos. Se acabar a força a qualquer momento durante esse processo, a gravação será completamente perdida, e o aplicativo terá acesso a seus dados antigos, ainda intactos. Isso impede a condição conhecida como "setores interrompidos".

Esse namespace PMEM habilitado para BTT pode ser formatado e usado com um sistema de arquivos assim como qualquer outro dispositivo de blocos padrão. Ele não pode ser usado com DAX. No entanto, os mapeamentos `mmap` para os arquivos nesse dispositivo de blocos usarão o cache de página.

37.5.4 Colocando o diário do sistema de arquivos na PMEM/BTT

Quando você coloca o diário do sistema de arquivos em um dispositivo separado, ele deve usar o mesmo tamanho de bloco que o sistema de arquivos. O tamanho mais provável é 4096, e você pode saber o tamanho do bloco com este comando:

```
# blockdev --getbsz /dev/sda3
```

O exemplo a seguir cria um novo diário do Ext4 em um dispositivo NVDIMM separado, cria o sistema de arquivos em um dispositivo SATA e, em seguida, anexa o novo sistema de arquivos ao diário:

```
# mke2fs -b 4096 -O journal_dev /dev/pmem3s
# mkfs.ext4 -J device=/dev/pmem3s /dev/sda3
```

O exemplo a seguir cria um novo sistema de arquivos XFS em uma unidade SATA e cria o diário em um dispositivo NVDIMM separado:

```
# mkfs.xfs -l logdev=/dev/pmem3s /dev/sda3
```


Consulte `man 8 mkfs.ext4` e `man 8 mkfs.ext4` para obter informações detalhadas sobre as opções.

37.6 Mais informações

Mais informações sobre este tópico estão disponíveis na lista a seguir:

- [Memória persistente Wiki \(https://nvdimm.wiki.kernel.org/\)](https://nvdimm.wiki.kernel.org/) 

Contém instruções sobre como configurar os sistemas NVDIMM, informações sobre testes e links para as especificações relacionadas à habilitação do NVDIMM. Este site é desenvolvido à medida que o suporte a NVDIMM no Linux é desenvolvido.

- [Programação de memória persistente \(http://pmem.io/\)](http://pmem.io/) 

Informações sobre como configurar, usar e programar sistemas com memória não volátil no Linux e em outros sistemas operacionais. Aborda a Biblioteca NVM (NVML, NVM Library), que fornece APIs úteis para programação com memória persistente no espaço do usuário.

- [LIBNVDIMM: Dispositivos não voláteis \(https://www.kernel.org/doc/Documentation/nvdimm/nvdimm.txt\)](https://www.kernel.org/doc/Documentation/nvdimm/nvdimm.txt) 

Destinado a desenvolvedores de kernel, ele faz parte do diretório Documentação na árvore de kernel atual do Linux. Ele explica sobre os diferentes módulos do kernel envolvidos na preparação do NVDIMM, apresenta alguns detalhes técnicos da implementação do kernel e aborda a interface do `sysfs` com o kernel que é usada pela ferramenta `ndctl`.

- [GitHub: pmem/ndctl \(https://github.com/pmem/ndctl\)](https://github.com/pmem/ndctl) 

Biblioteca de utilitários para gerenciar o subsistema `libnvdimm` no kernel do Linux. Inclui também as bibliotecas de espaço do usuário, além de testes de unidade e documentação.

V Serviços

- 38 Gerenciamento de serviços com o YaST **501**
- 39 Sincronização de horário com NTP **503**

38 Gerenciamento de serviços com o YaST

O YaST dispõe de um gerenciador de serviços para controlar o destino padrão do sistema e os serviços, exibir o status do serviço e ler o arquivo de registro. O suporte do YaST à ativação de serviços baseados em soquete do systemd é novo no SUSE Linux Enterprise Desktop 15 SP4 e configura os serviços para serem iniciados sob demanda.

O systemd permite iniciar os serviços sob demanda com a ativação baseada em soquete. Esses serviços têm dois tipos de unidade: serviço e soquete. Por exemplo, o CUPS é controlado por cups.service e cups.socket. O YaST permite selecionar o tipo de inicialização de serviço que você deseja usar.

O *Figura 38.1, “Gerenciador de serviços do YaST”* mostra as opções na caixa suspensa Modo de início: *Na inicialização*, *Sob demanda* e *Manualmente*. Selecione *Sob demanda* para a ativação baseada em soquete. Essa opção abre o soquete da rede de escuta e inicia o serviço mediante solicitação.

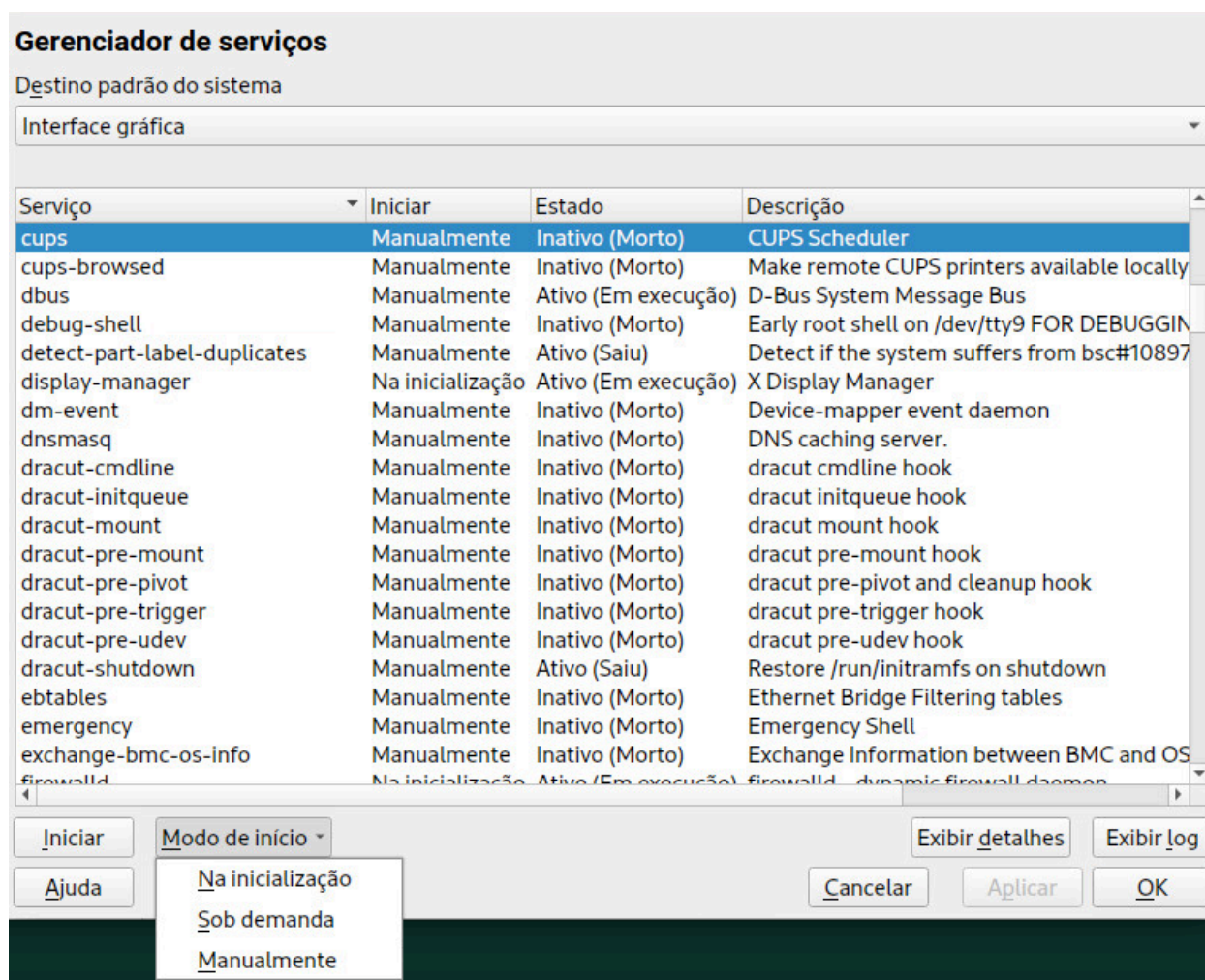


FIGURA 38.1: GERENCIADOR DE SERVIÇOS DO YAST

A opção *Sob demanda* fica visível apenas para serviços que oferecem suporte a ela. No momento, esse subconjunto de serviços é pequeno, como CUPS, dbus, iscsid, iscsiuiio, multipathd, pcsd, rpcbind, TFTP, virtlockd e virtlogd. Consulte [man 5 systemd.socket](#) para obter informações detalhadas sobre o funcionamento da ativação por soquete.

39 Sincronização de horário com NTP

O mecanismo NTP (network time protocol) é um protocolo para sincronizar o horário do sistema na rede. Primeiro, uma máquina pode obter o horário de um servidor, que é uma fonte de horário confiável. Segundo, a máquina pode agir como uma fonte de horário para outros computadores na rede. O objetivo é duplo: manter o tempo absoluto e a sincronização do horário do sistema de todas as máquinas na rede.

Manter um horário exato do sistema é importante em várias situações. Geralmente, o relógio do hardware incorporado não atende aos requisitos dos aplicativos, como bancos de dados ou clusters. A correção manual do horário do sistema levaria a problemas severos pois, por exemplo, um pulso inverso pode causar o mau funcionamento de aplicativos críticos. Em uma rede, geralmente é necessário sincronizar o horário do sistema de todas as máquinas, porém, o ajuste manual do horário não é um bom método. O NTP dispõe de um mecanismo para resolver esses problemas. O serviço NTP ajusta continuamente o horário do sistema com servidores de horário confiáveis na rede. Ele habilita também o gerenciamento de relógios de referência local como relógios controlados pelo rádio.

A partir do SUSE Linux Enterprise Desktop 15, o `chrony` é a implementação padrão do NTP. O `chrony` inclui duas partes: `chronyd` é um daemon que pode ser iniciado no momento da inicialização, e `chronyc` é um programa de interface de linha de comando que monitora o desempenho do `chronyd` e muda vários parâmetros operacionais em tempo de execução.

A partir do SUSE Linux Enterprise Desktop 15.2, o módulo do YaST para configuração do cliente NTP define o `systemd-timer`, em vez do daemon `cron`, para executar o `chrony`, quando ele não está configurado para ser executado como um daemon.



Nota

Para habilitar a sincronização de horário por meio do diretório ativo, siga as instruções no Livro *“Security and Hardening Guide”*, Capítulo 7 *“Active Directory support”*, Seção 7.3.3 *“Joining Active Directory using Windows domain membership”*, *Joining an Active Directory domain using Windows domain membership*.

39.1 Configurando um cliente NTP com YaST

O daemon do NTP (`chronyd`) que acompanha o pacote `chrony` vem predefinido para usar o relógio do hardware do computador local como referência de horário. A precisão de um relógio de hardware depende muito da sua fonte de horário. Por exemplo, um relógio atômico ou um receptor GPS é uma fonte de horário muito precisa, enquanto um chip RTC comum não é uma fonte de horário confiável. O YaST simplifica a configuração de um cliente NTP.

Na janela de configuração do cliente NTP do YaST (*Serviços de Rede > Configuração do NTP*), você pode especificar quando iniciar o daemon do NTP, o tipo de fonte de configuração e adicionar servidores de horário personalizados.

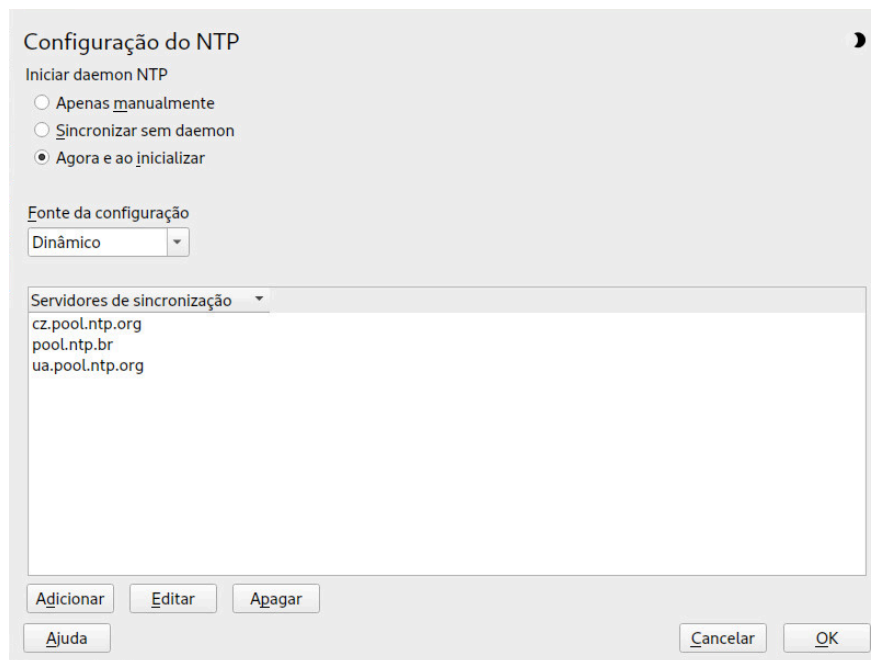


FIGURA 39.1: JANELA DE CONFIGURAÇÃO DO NTP

39.1.1 Início do daemon do NTP

Há três opções que você pode escolher para iniciar o daemon do NTP:

Apenas manualmente

Selecione *Apenas manualmente* para iniciar manualmente o daemon `chrony`.

Sincronizar sem Daemon

Selecione *Sincronizar sem Daemon* para definir o horário do sistema periodicamente sem a execução permanente do chrony. Você pode definir o *Intervalo da Sincronização em Minutos*.

Agora e ao Inicializar

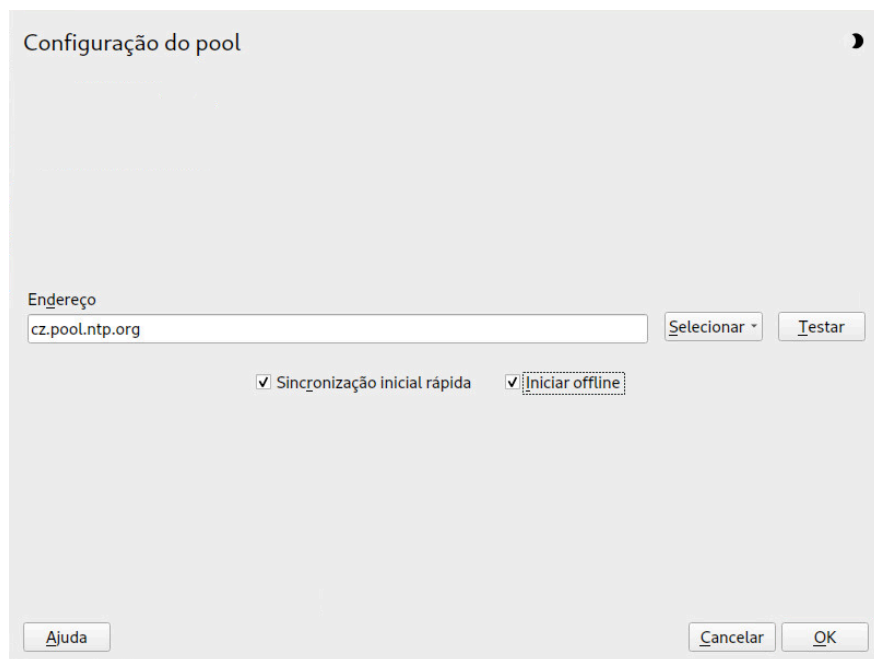
Selecione *Agora e ao inicializar* para iniciar o chronyd automaticamente quando o sistema for inicializado. Essa configuração é recomendada.

39.1.2 Tipo de fonte de configuração

Na caixa suspensa *Fonte de Configuração*, selecione *Dinâmico* ou *Estático*. Defina como *Estático* se o seu servidor usa apenas um conjunto fixo de servidores NTP (públicos). A opção *Dinâmico* é melhor quando sua rede interna oferece servidores NTP via DHCP.

39.1.3 Configurar servidores de horário

Os servidores de horário para consulta do cliente estão listados na parte inferior da janela *Configuração do NTP*. Modifique esta lista conforme necessário com *Adicionar*, *Editar* e *Apagar*. Clique em *Adicionar* para adicionar um novo servidor de horário:



Configuração do pool

Endereço
cz.pool.ntp.org

Selecionar ▼ Testar

☒ Sincronização inicial rápida ☒ Iniciar offline

Ajuda Cancelar OK

FIGURA 39.2: ADICIONANDO UM SERVIDOR DE HORÁRIO

1. No campo *Endereço*, digite o URL do servidor de horário ou do pool de servidores de horário com os quais você deseja sincronizar o horário da máquina. Depois que o URL estiver completo, clique em *Testar* para verificar se ele aponta para uma fonte de horário válida.
2. Ative *Sincronização Inicial Rápida* para acelerar a sincronização de horário por meio do envio de mais solicitações quando o daemon `chronyd` é iniciado.
3. Ative *Iniciar Offline* para acelerar o tempo de inicialização nos sistemas que iniciam o daemon `chronyd` automaticamente e podem não ter uma conexão de Internet no momento da inicialização. Essa opção é útil, por exemplo, para laptops com conexões de rede gerenciadas pelo NetworkManager.
4. Confirme com *OK*.

39.2 Configurando manualmente o NTP na rede

O `chrony` lê sua configuração do arquivo `/etc/chrony.conf`. Para manter o relógio do computador sincronizado, você precisa informar ao `chrony` quais servidores de horário devem ser usados. Você pode usar nomes de servidores ou endereços IP específicos. Por exemplo:

```
server 0.europe.pool.ntp.org
server 1.europe.pool.ntp.org
server 2.europe.pool.ntp.org
```

Você também pode especificar o nome de um *pool*. O nome do pool é resolvido para vários endereços IP:

```
pool pool.ntp.org
```



Dica: Computadores na mesma rede

Para sincronizar o horário em vários computadores na mesma rede, não é recomendável sincronizar todos eles com um servidor externo. Convém especificar um computador como servidor de horário, que é sincronizado com um servidor de horário externo, e o outro computador atua como cliente dele. Adicione uma diretiva `local` ao `/etc/chrony.conf` do servidor para diferenciá-lo de um servidor de horário autorizado:

```
local stratum 10
```


Para iniciar o `chrony`, execute:

```
systemctl start chronyd.service
```

Após a inicialização do `chronyd`, levará algum tempo para estabilizar o horário, e o arquivo drift que corrige o relógio do computador local será criado. Com o arquivo DRIFT, o erro sistemático do relógio do hardware pode ser registrado quando o computador é ligado. A correção é usada imediatamente, resultando em uma estabilidade maior do horário do sistema.

Para habilitar o serviço que permite iniciar o `chrony` automaticamente no momento da inicialização, execute:

```
systemctl enable chronyd.service
```

39.3 Configurar o `chronyd` em tempo de execução usando o `chronyc`

Você pode usar o `chronyc` para mudar o comportamento do `chronyd` em tempo de execução. Ele também gera relatórios de status sobre a operação do `chronyd`.

Você pode executar o `chronyc` no modo interativo ou não interativo. Para executar o `chronyc` interativamente, digite `chronyc` na linha de comando. Esse procedimento exibe um prompt e aguarda a entrada do seu comando. Por exemplo, para verificar quantas fontes NTP estão online ou offline, execute:

```
# chronyc
chronyc> activity
200 OK
4 sources online
2 sources offline
1 sources doing burst (return to online)
1 sources doing burst (return to offline)
0 sources with unknown address
```

Para sair do prompt do `chronyc`, digite `quit` ou `exit`.

Se você não precisa usar o prompt interativo, digite o comando diretamente:

```
# chronyc activity
```



Nota: Mudanças temporárias

As mudanças feitas com o **chronyc** não são permanentes. Elas serão perdidas após a próxima reinicialização do **chronyd**. Para mudanças permanentes, modifique o `/etc/chrony.conf`.

Para obter uma lista completa dos comandos do **chronyc**, consulte a página de manual dele (**man 1 chronyc**).

39.4 Sincronização de horário dinâmica em tempo de execução

Embora o **chronyd** seja inicializado normalmente em um sistema que inicializa sem uma conexão de rede, a ferramenta não pode resolver os nomes DNS dos servidores de horário especificados no arquivo de configuração.

O **chronyd** continua tentando resolver os nomes de servidor de horário especificados pelas diretivas do **server**, do **pool** e do **peer** em um intervalo de tempo crescente até obter êxito.

Se o servidor de horário não puder ser acessado quando o **chronyd** for iniciado, você poderá especificar a opção **offline**:

```
server server_address offline
```

O **chronyd** não tentará fazer poll no servidor até ser habilitado usando o seguinte comando:

```
# chronyc online server_address
```

Quando a opção **auto_offline** está definida, o **chronyd** pressupõe que o servidor de horário estava offline quando duas solicitações foram enviadas a ele sem receber uma resposta. Essa opção evita a necessidade de executar o comando “offline” do **chronyc** ao desconectar o link de rede.

39.5 Configurando um relógio de referência local

O pacote de software **chrony** depende de outros programas (como **gpsd**) para acessar os dados de horário por meio do driver SHM ou SOCK. Use a diretiva **refclock** em `/etc/chrony.conf` para especificar um relógio de referência de hardware a ser usado como fonte de horário. Ela

tem dois parâmetros obrigatórios: um nome de driver e um parâmetro específico do driver. Os dois parâmetros são seguidos de zero ou de mais opções do `refclock`. O `chronyd` inclui os seguintes drivers:

- PPS: driver para a API “Pulse-Per-Second” do kernel. Por exemplo:

```
refclock PPS /dev/pps0 lock NMEA refid GPS
```

- SHM: driver de memória compartilhada do NTP. Por exemplo:

```
refclock SHM 0 poll 3 refid GPS1  
refclock SHM 1:perm=0644 refid GPS2
```

- SOCK: driver de soquete de domínio do Unix. Por exemplo:

```
refclock SOCK /var/run/chrony.ttyS0.sock
```

- PHC: driver de relógio do hardware PTP. Por exemplo:

```
refclock PHC /dev/ptp0 poll 0 dpoll -2 offset -37  
refclock PHC /dev/ptp1:nocrossts poll 3 pps
```

Para obter mais informações sobre as opções de drivers individuais, consulte [`man 8 chrony.conf`](#).

39.6 Sincronização do relógio com uma Referência de Horário Externa (ETR, External Time Reference)

O suporte para sincronização do relógio com uma referência de horário externa (ETR) está disponível. A referência de horário externa envia um sinal do oscilador e um sinal de sincronização a cada $2^{**}20$ (2 elevado à potência de 20) microssegundos para manter sincronizados os relógios TOD de todos os servidores conectados.

Para disponibilidade, é possível conectar duas unidades ETR a uma máquina. Se a diferença do relógio for maior do que a tolerância da verificação de sincronização, todas as CPUs terão suas máquinas marcadas indicando que o relógio não está sincronizado. Se isso acontecer, todos os dispositivos DASD de E/S habilitados para XRC serão parados até o relógio ser novamente sincronizado.

O suporte a ETR é ativado por meio de dois atributos sysfs. Execute os seguintes comandos como root:

```
echo 1 > /sys/devices/system/etr/etr0/online  
echo 1 > /sys/devices/system/etr/etr1/online
```

VI Solução de problemas

- 40 Ajuda e documentação **512**
- 41 Reunindo informações do sistema para suporte **518**
- 42 Problemas comuns e suas soluções **550**

40 Ajuda e documentação

O SUSE® Linux Enterprise Desktop vem com várias fontes de informações e documentação, muitas das quais já integradas ao sistema instalado.

Documentação em `/usr/share/doc`

Esse diretório de ajuda tradicional contém vários arquivos de documentação e notas de versão do seu sistema. Também contém informações de pacotes instalados no subdiretório `packages`. Mais informações podem ser encontradas na *Seção 40.1, “Diretório da documentação”*.

Páginas de manual e páginas de informações para comandos do shell

Ao trabalhar com o shell, você não precisa saber de cor as opções de comandos. Tradicionalmente, o shell oferece ajuda integrada por meio das páginas de manual e de informações. Leia mais na *Seção 40.2, “Páginas de manual”* e na *Seção 40.3, “Páginas de informações”*.

Centro de ajuda da área de trabalho

O centro de ajuda da área de trabalho do GNOME (Ajuda) oferece acesso centralizado aos recursos de documentação mais importantes no sistema de forma pesquisável. Esses recursos incluem ajuda online para os aplicativos instalados, páginas de manual, páginas de informações e os manuais do SUSE fornecidos com o produto.

Pacotes de ajuda separados para alguns aplicativos

Quando um novo software é instalado com o YaST, a respectiva documentação, em geral, é instalada automaticamente e aparece no centro de ajuda da área de trabalho. Porém, alguns aplicativos, como o GIMP, podem ter diversos pacotes de ajuda online que podem ser instalados separadamente com o YaST e que não se integram aos centros de ajuda.

40.1 Diretório da documentação

O diretório tradicional para encontrar a documentação do sistema Linux instalado é `/usr/share/doc`. Geralmente, o diretório contém informações sobre os pacotes instalados no sistema, bem como notas de versão, manuais e muito mais.




Nota: O conteúdo depende dos pacotes instalados

No mundo do Linux, muitos manuais e outros tipos de documentação estão disponíveis na forma de pacotes, como um software. As informações encontradas em `/usr/share/docs` também dependem dos pacotes (de documentação) instalados. Se você não encontrar os subdiretórios mencionados aqui, verifique se os respectivos pacotes estão instalados em seu sistema e adicione-os com o YaST, se necessário.

40.1.1 Manuais do SUSE

Fornecemos versões em HTML e PDF de nossos manuais em idiomas diferentes. No subdiretório `manual`, você encontra as versões em HTML de quase todos os manuais do SUSE disponíveis para o seu produto. Para obter uma visão geral de toda a documentação disponível para o seu produto, consulte o prefácio dos manuais.

Se houver mais de um idioma instalado, `/usr/share/doc/manual` poderá conter versões em idiomas diferentes dos manuais. As versões em HTML dos manuais do SUSE também estão disponíveis no centro de ajuda de ambas as áreas de trabalho. Para obter informações sobre onde encontrar as versões em PDF e HTML dos manuais na mídia de instalação, consulte as Notas de Versão do SUSE Linux Enterprise Desktop. Elas estão disponíveis no sistema instalado, no diretório `/usr/share/doc/release-notes/`, ou online, na página da Web específica do produto em <https://www.suse.com/releasenotes//> .

40.1.2 Documentação do pacote

Em `packages`, encontre a documentação incluída nos pacotes de software instalados no sistema. Para qualquer pacote, é criado um subdiretório `/usr/share/doc/packages/NOME_DO_PACOTE`. Ele geralmente contém arquivos README do pacote e às vezes exemplos, arquivos de configuração ou scripts adicionais. A lista a seguir apresenta arquivos típicos encontrados em `/usr/share/doc/packages`. Nenhuma destas entradas é obrigatória, e muitos pacotes podem incluir apenas algumas delas.

AUTHORS

Lista dos principais desenvolvedores.

BUGS

Bugs ou falhas conhecidos. Pode conter também um link para uma página do Bugzilla na Web, onde é possível pesquisar todos os bugs.

CHANGES ,

ChangeLog

Resumo de mudanças de versão para versão. Geralmente interessante para desenvolvedores, pois é bastante detalhado.

COPYING ,

LICENSE

Informações sobre licenciamento.

Perguntas freqüentes

Perguntas e respostas coletadas em listas de endereçamento ou grupos de notícias.

INSTALL

Como instalar esse pacotes no seu sistema. Visto que o pacote já estará instalado no momento em que você ler este arquivo, você poderá ignorar o conteúdo do arquivo com segurança.

README , README.*

Informações gerais sobre o software. Por exemplo, a finalidade e o modo de usá-lo.

TODO

Itens ainda não implementados, mas que provavelmente serão no futuro.

MANIFEST

Lista de arquivos com um breve resumo.

NEWS

Descrição do que há de novo nesta versão.

40.2 Páginas de manual

Páginas de manual são uma parte essencial de qualquer sistema Linux. Elas explicam o uso de um comando e todos os parâmetros e opções disponíveis. As páginas de manual podem ser acessadas com man seguido do nome do comando, por exemplo, man ls.

As páginas de manual são exibidas diretamente no shell. Para navegar nelas, mova-se para cima e para baixo com **Page ↑** e **Page ↓**. Desloque-se entre o início e o fim do documento com **Home** e **End**. Conclua esta exibição pressionando **Q**. Aprenda mais sobre o próprio comando **man** com **man man**. Páginas de manual são classificadas em categorias, como mostrado na *Tabela 40.1, “Páginas de manual – categorias e descrições”* (extraída da página de manual do próprio comando **man**).

TABELA 40.1: PÁGINAS DE MANUAL – CATEGORIAS E DESCRIÇÕES

Número	Descrição
1	Programas executáveis ou comandos de shell
2	Chamadas do sistema (funções fornecidas pelo kernel)
3	Chamadas de biblioteca (funções em bibliotecas de programas)
4	Arquivos especiais (geralmente encontrados em <code>/dev</code>)
5	Convenções e formatos de arquivos (<code>/etc/fstab</code>)
6	Jogos
7	Diversos (incluindo convenções e pacotes de macro); por exemplo, <code>man(7)</code> , <code>groff(7)</code>
8	Comandos de administração de sistema (geralmente, apenas para <code>root</code>)
9	Rotinas de kernel (não padrão)

Cada página de manual consiste em várias partes rotuladas *NAME*, *SYNOPSIS*, *DESCRIPTION*, *SEE ALSO*, *LICENSING* e *AUTHOR*. Pode haver seções adicionais disponíveis, dependendo do tipo de comando.

40.3 Páginas de informações

Páginas de informações são outra fonte importante de informações no sistema. Geralmente, elas são mais detalhadas do que as páginas de manual. Elas abrangem mais do que as opções de linha de comando e, às vezes, incluem tutoriais completos ou documentação de referência. Para ver a página de informações de um determinado comando, digite **info** seguido pelo nome do comando, por exemplo, **info ls**. Você pode procurar uma página de informações com um viewer diretamente no shell e exibir as seções diferentes, denominadas “nós”. Use **Space** para avançar e **<-** para voltar. Em um nó, você também pode procurar com **Page ↑** e **Page ↓**, mas apenas **Space** e **<-** o levarão também para o nó anterior ou subsequente. Pressione **Q** para sair do modo de visualização. Nem todo comando vem com uma página de informações e vice-versa.

40.4 Recursos online

Além das versões online dos manuais do SUSE instaladas em `/usr/share/doc`, você também pode acessar a documentação e os manuais específicos do produto na Web. Para uma visão geral de toda a documentação disponível referente ao SUSE Linux Enterprise Desktop, visite a página de documentação específica do seu produto na Web em <https://documentation.suse.com/>.

Se você estiver pesquisando mais informações relativas ao produto, também poderá consultar os seguintes sites:

Suporte técnico da SUSE

Você encontra o Suporte Técnico do SUSE em <https://www.suse.com/support/>, em caso de dúvidas ou soluções para problemas técnicos.

Comunidade de usuários do SUSE Linux Enterprise Desktop

Comunidade SUSE e Rancher (<https://community.suse.com/>)


Blog da SUSE

O blog da SUSE inclui artigos, dicas, perguntas e respostas: <https://www.suse.com/c/blog/>

Documentação do GNOME

A documentação para usuários, administradores e desenvolvedores do GNOME está disponível em <https://help.gnome.org/>.

Projeto de Documentação do Linux

O TLDP (The Linux Documentation Project — O Projeto de Documentação do Linux) é administrado por uma equipe de voluntários que escrevem a documentação relacionada ao Linux (acesse <https://www.tldp.org> ). É provavelmente o recurso de documentação mais completo do Linux. O conjunto de documentos contém tutoriais para iniciantes, mas é direcionado principalmente a usuários experientes e administradores de sistema profissionais. O TLDP publica HOWTOs (Como Fazer), FAQs e guias (manuais) sob uma licença livre. Partes da documentação do TLDP também estão disponíveis no SUSE Linux Enterprise Desktop.

Você também pode experimentar mecanismos de pesquisa gerais. Por exemplo, use os termos de pesquisa ajuda Linux CD-RW ou problema de conversão de arquivos OpenOffice se tiver problemas com a gravação de CDs ou a conversão de arquivos do LibreOffice.

41 Reunindo informações do sistema para suporte

Para uma rápida visão geral de todas as informações de sistema relevantes de uma máquina, o SUSE Linux Enterprise Desktop oferece o pacote `hostinfo`. Ele também ajuda os administradores do sistema a verificarem se há kernels contaminados (que não são suportados) ou quaisquer pacotes de terceiros instalados na máquina.

Em caso de problemas, é possível criar um relatório detalhado do sistema com a ferramenta de linha de comando `supportconfig` ou o módulo de *Suporte* do YaST. Os dois coletam informações sobre o sistema, como a versão atual do Kernel, o hardware, os pacotes instalados, a configuração da partição, etc. O resultado é um armazenamento de arquivos TAR. Após abrir uma Solicitação de Serviço (SS), você poderá fazer upload do armazenamento TAR para o Suporte Técnico Global. Ele ajuda a localizar o problema que você relatou e a orientá-lo para uma solução.

Você também pode verificar se há problemas conhecidos na saída do `supportconfig` para ajudar a resolvê-los mais rapidamente. Para esta finalidade, o SUSE Linux Enterprise Desktop oferece uma aplicação e uma ferramenta de linha de comando para `Supportconfig Analysis` (SCA).

41.1 Exibindo informações atuais do sistema

Para uma visão geral rápida e fácil de todas as informações do sistema relevantes, use o pacote `hostinfo` ao efetuar login no servidor. Após ser instalado na máquina, o console exibirá as seguintes informações para qualquer usuário `root` que efetuar login nessa máquina:

EXEMPLO 41.1: SAÍDA DE `hostinfo` AO EFETUAR LOGIN COMO `root`

```
Welcome to SUSE Linux Enterprise Server 15 SP2 Snapshot8 (x86_64) - Kernel \r (\l).

Distribution:      SUSE Linux Enterprise Server 15 SP2
Current As Of:    Wed 25 Mar 2020 12:09:20 PM PDT
Hostname:         localhost
Kernel Version:   5.3.18-8-default
Architecture:     x86_64
Installed:        Thu 19 Mar 2020 11:25:13 AM PDT
```

```

Status: Not Tainted
Last Installed Package: Wed 25 Mar 2020 11:42:24 AM PDT
Patches Needed: 0
Security: 0
3rd Party Packages: 219
Network Interfaces
eth0: 192.168.2/24 2002:c0a8:20a::/64
Memory
Total/Free/Avail: 7.4Gi/6.4Gi/6.8Gi (91% Avail)
CPU Load Average: 7 (3%) with 2 CPUs

```

Caso a saída apresente o kernel com status `tainted` (contaminado), consulte a [Seção 41.6, “Suporte aos módulos do kernel”](#) para ver mais detalhes.

41.2 Coletando informações do sistema com o supportconfig

Para criar um arquivo TAR com informações detalhadas do sistema que você pode enviar ao Suporte Técnico Global, use:

- o comando `supportconfig` ou
- o módulo de *Suporte* do YaST.

A ferramenta de linha de comando está incluída no pacote `supportutils`, que é instalado por padrão. O módulo de *Suporte* do YaST também é baseado na ferramenta de linha de comando. Dependendo dos pacotes instalados no sistema, alguns desses pacotes integrarão plug-ins do Supportconfig. Quando o Supportconfig for executado, todos os plug-ins também serão executados e criarão um ou mais arquivos de resultados para o TAR. O benefício desse recurso é que apenas os tópicos que contêm um plug-in específico para eles são marcados. Os plug-ins do Supportconfig são armazenados no diretório `/usr/lib/supportconfig/plugins/`.

41.2.1 Criando um número de solicitação de serviço

É possível gerar armazenamentos do supportconfig a qualquer momento. No entanto, para enviar os dados do Supportconfig ao Suporte Técnico Global, é necessário gerar primeiro um número de solicitação de serviço. Você precisa dele para fazer upload do armazenamento para o suporte.

Para criar uma solicitação de serviço, acesse <https://scc.suse.com/support/requests> e siga as instruções na tela. Anote o número da solicitação de serviço.



Nota: Declaração de privacidade

A SUSE trata os relatórios do sistema como dados confidenciais. Para ver detalhes do nosso compromisso de privacidade, acesse <https://www.suse.com/company/policies/privacy/>.

41.2.2 Destinos de upload

Após criar um número de solicitação de serviço, você poderá fazer upload dos arquivos do Supportconfig para o Suporte Técnico Global, conforme descrito no *Procedimento 41.1, “Enviando informações ao suporte com o YaST”* ou no *Procedimento 41.2, “Enviando informações ao suporte por linha de comando”*. Use um dos seguintes destinos de upload:

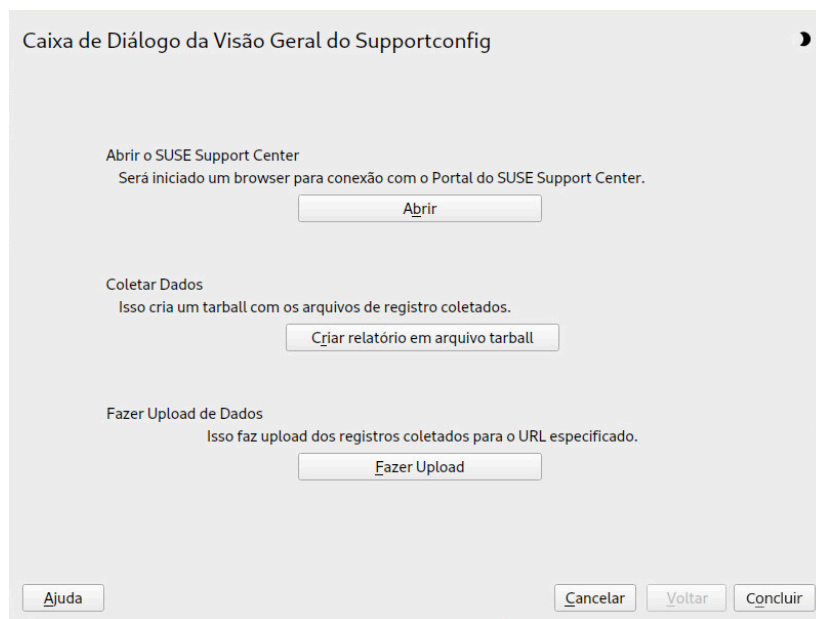
- América do Norte: FTP <ftp://support-ftp.us.suse.com/incoming/>, FTPS <ftps://support-ftp.us.suse.com/incoming/>
- EMEA, Europa, Oriente Médio e África: FTP <ftp://support-ftp.emea.suse.com/incoming>, FTPS <ftps://support-ftp.emea.suse.com/incoming>

Você também pode anexar o armazenamento TAR manualmente à sua solicitação de serviço usando o URL da solicitação de serviço: <https://scc.suse.com/support/requests>.

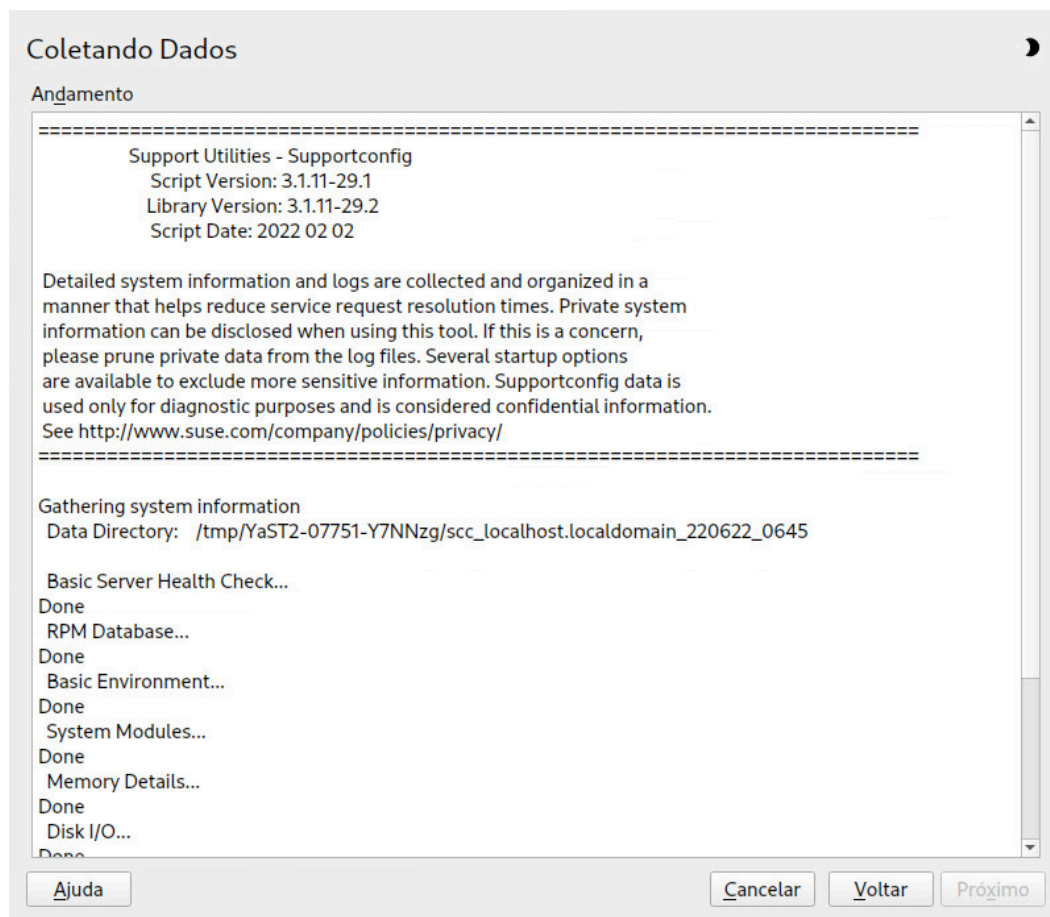
41.2.3 Criando um arquivo supportconfig com o YaST

Para usar o YaST para coletar informações do sistema, faça o seguinte:

1. Inicie o YaST e abra o módulo de *Suporte*.



2. Clique em *Criar relatório em arquivo tarball*.
3. Na janela seguinte, selecione uma das opções do Supportconfig na lista de botões de opção. Por padrão, a opção *Usar Configurações (Técnicas) Personalizadas* está pré-selecionada. Para testar primeiro a função de relatório, use *Reunir apenas uma quantidade mínima de informações*. Para obter mais informações sobre outras opções, consulte a página de manual de **supportconfig**.
Clique em *Avançar*.
4. Digite suas informações de contato. Elas são gravadas no arquivo `basic-environment.txt` e incluídas no arquivo criado.
5. Para enviar o arquivo ao Suporte Técnico Global, insira as *Informações de Upload* necessárias. O YaST propõe um servidor de upload automaticamente. Para modificá-lo, consulte a [Seção 41.2.2, "Destinos de upload"](#) para saber os detalhes dos servidores de upload que estão disponíveis.
Para enviar o arquivo mais tarde, deixe o campo *Informações de Upload* vazio.
6. Clique em *Próximo* para iniciar o processo de coleta de informações.



Quando o processo for concluído, clique em *Próximo*.

7. Para revisar os dados coletados, selecione o arquivo desejado em *Nome do Arquivo* para ver seu conteúdo no YaST. Para remover um arquivo do armazenamento TAR antes de enviá-lo ao suporte, use *Remover dos Dados*. Clique em *Próximo*.
8. Grave o armazenamento TAR. Se você iniciou o módulo do YaST como usuário `root`, o YaST exibe um prompt com a sugestão para gravar o arquivo em `/var/log` (ou em seu diretório pessoal). O formato do nome de arquivo é `scc_HOST_DATE_TIME.tbz`.
9. Para fazer upload do arquivo diretamente para o suporte, verifique se a opção *Fazer upload do tarball de arquivos de registro para URL* está ativada. O *Destino do Upload* mostrado aqui é o mesmo sugerido pelo YaST na [Passo 5](#). Para modificar o destino do upload, verifique os servidores de upload que estão disponíveis na [Seção 41.2.2, "Destinos de upload"](#).
10. Para ignorar o upload, desative a opção *Fazer upload do tarball de arquivos de registro para URL*.

11. Confirme as mudanças para fechar o módulo do YaST.

41.2.4 Criando um arquivo supportconfig da linha de comando

O seguinte procedimento mostra como criar um arquivo do Supportconfig, mas sem o enviar diretamente ao suporte. Para fazer seu upload, é necessário executar o comando com algumas opções, conforme descrito no *Procedimento 41.2, “Enviando informações ao suporte por linha de comando”*.

1. Abra um shell e registre-se como root.
2. Execute o **supportconfig**. Geralmente, basta executar essa ferramenta sem nenhuma outra opção. Algumas opções são muito comuns e aparecem na lista a seguir:

-E E-MAIL ,
-N NOME ,
-O EMPRESA ,
-P TELEFONE

Define os dados de contato: endereço de e-mail (-E), nome da empresa (-O), seu nome (-N) e seu número de telefone (-P).

-i PALAVRAS-CHAVE ,
-F

Limita os recursos que serão verificados. O marcador PALAVRAS-CHAVE é uma lista separada por vírgulas de palavras-chave com distinção entre maiúsculas e minúsculas. Execute o comando **supportconfig -F** para obter uma lista de todas as palavras-chave.

-r NÚMEROSR

Define o número da solicitação de serviço durante o upload do arquivo TAR gerado.

3. Aguarde a ferramenta concluir a operação.
4. O local padrão do arquivo é /var/log, com o formato de nome de arquivo scc_HOST_DATE_TIME.tbz

41.2.5 Compreendendo a saída do **supportconfig**

Se você executar o **supportconfig** pelo YaST ou diretamente, o script lhe apresentará um resumo do que foi feito.

```
Support Utilities - Supportconfig
Script Version: 3.0-98
Script Date: 2017 06 01

[...]
Gathering system information
Data Directory:    /var/log/scc_d251_180201_1525 ❶

Basic Server Health Check...           Done ❷
RPM Database...                         Done ❷
Basic Environment...                   Done ❷
System Modules...                      Done ❷
[...]
File System List...                    Skipped ❸
[...]
Command History...                     Excluded ❹
[...]
Supportconfig Plugins:                 1 ❺
Plugin: pstree...                      Done
[...]
Creating Tar Ball

==[ DONE ]=====
Log file tar ball: /var/log/scc_d251_180201_1525.txz ❻
Log file size:      732K
Log file md5sum:    bf23e0e15e9382c49f92cbce46000d8b
=====
```

- ❶ O diretório de dados temporários para armazenar os resultados. Esse diretório é armazenado como um arquivo tar. Consulte ❹.
- ❷ O recurso foi habilitado (por padrão ou selecionado manualmente) e executado com êxito. O resultado é armazenado em um arquivo (consulte a *Tabela 41.1, “Comparação de recursos e nomes de arquivo no armazenamento TAR”*).
- ❸ O recurso foi ignorado porque alguns arquivos de um ou mais pacotes RPM foram mudados.
- ❹ O recurso foi excluído porque foi desmarcado por meio da opção `-x`.
- ❺ O script encontrou um plug-in e executa o plug-in **pstree**. O plug-in foi encontrado no diretório `/usr/lib/supportconfig/plugins/`. Consulte a página de manual para obter detalhes.

- ⑥ O nome do arquivo tar do armazenamento, por padrão, compactado com xz.

41.2.6 Opções comuns do supportconfig

O utilitário **supportconfig** é geralmente chamado sem nenhuma opção. Exiba uma lista de todas as opções com **supportconfig -h** ou consulte a página de manual. A seguinte lista apresenta uma breve visão geral de alguns casos de uso comuns:

Reduzindo o tamanho das informações coletadas

Usar a opção mínima (**-m**):

```
> sudo supportconfig -m
```

Limitando as informações a determinado tópico

Se você já localizou um problema relacionado apenas à determinada área ou conjunto de recursos, convém limitar as informações coletadas à área específica na próxima execução do **supportconfig**. Por exemplo, se você detectou problemas com a LVM e deseja testar uma mudança recente que você fez na configuração da LVM. Nesse caso, convém coletar as informações mínimas do Supportconfig apenas sobre a LVM:

```
> sudo supportconfig -i LVM
```

É possível separar as palavras-chave adicionais com vírgulas. Por exemplo, um teste de disco adicional:

```
> sudo supportconfig -i LVM,DISK
```

Para ver a lista completa de palavras-chave de recursos que você pode usar para limitar as informações coletadas a determinada área, execute:

```
> sudo supportconfig -F
```

Incluindo informações de contato adicionais na saída:

```
> sudo supportconfig -E tux@example.org -N "Tux Penguin" -O "Penguin Inc." ...
```

(tudo em uma linha)

Coletando os arquivos de registro que já foram girados

```
> sudo supportconfig -l
```

Isso é útil principalmente em ambientes de alto registro ou após uma falha do kernel quando o syslog gira os arquivos de registro após uma reinicialização.

41.2.7 Visão geral do conteúdo do arquivo

O arquivo TAR contém todos os resultados dos recursos. Dependendo do que você selecionou (tudo ou apenas um pequeno conjunto), o TAR pode conter mais ou menos arquivos. É possível limitar o conjunto de recursos por meio da opção `-i` (consulte a [Seção 41.2.6, “Opções comuns do supportconfig”](#)).

Para listar o conteúdo do arquivo, use o seguinte comando `tar`:

```
# tar xf /var/log/scc_earth_180131_1545.tbz
```

Os seguintes nomes de arquivo sempre estão disponíveis no arquivo TAR:

ARQUIVOS MÍNIMOS NO ARMAZENAMENTO

basic-environment.txt

Contém a data em que este script foi executado e informações do sistema, como versão da distribuição, informações do hipervisor, etc.

basic-health-check.txt

Contém algumas verificações básicas de saúde, como tempo de atividade, estatísticas de memória virtual, memória livre e disco rígido, verificações de processos zumbis, etc.

hardware.txt

Contém verificações básicas de hardware, como informações sobre a arquitetura da CPU, lista de todos os hardwares conectados, interrupções, portas de E/S, mensagens de boot do kernel, etc.

messages.txt

Contém mensagens de registro do diário do sistema.

rpm.txt

Contém uma lista de todos os pacotes RPM instalados, o nome, a origem e as versões deles.

summary.xml

Contém algumas informações no formato XML, como distribuição, versão e fragmentos específicos do produto.

supportconfig.txt

Contém informações sobre o próprio script `supportconfig`.

y2log.txt

Contém informações específicas do YaST, como pacotes específicos, arquivos de configuração e arquivos de registro.

A *Tabela 41.1, “Comparação de recursos e nomes de arquivo no armazenamento TAR”* lista todos os recursos disponíveis e seus nomes de arquivo. Outros pacotes de serviço podem estender a lista, assim como os plug-ins.

TABELA 41.1: COMPARAÇÃO DE RECURSOS E NOMES DE ARQUIVO NO ARMAZENAMENTO TAR

Recurso	Nome do arquivo
<u>APPARMOR</u>	<u>security-apparmor.txt</u>
<u>AUDIT</u>	<u>security-audit.txt</u>
<u>AUTOFS</u>	<u>fs-autofs.txt</u>
<u>BOOT</u>	<u>boot.txt</u>
<u>BTRFS</u>	<u>fs-btrfs.txt</u>
<u>DAEMONS</u>	<u>systemd.txt</u>
<u>CIMOM</u>	<u>cimom.txt</u>
<u>CRASH</u>	<u>crash.txt</u>
<u>CRON</u>	<u>cron.txt</u>
<u>DHCP</u>	<u>dhcp.txt</u>
<u>DISK</u>	<u>fs-diskio.txt</u>
<u>DNS</u>	<u>dns.txt</u>
<u>DOCKER</u>	<u>docker.txt</u>
<u>DRBD</u>	<u>drbd.txt</u>
<u>ENV</u>	<u>env.txt</u>
<u>ETC</u>	<u>etc.txt</u>
<u>HA</u>	<u>ha.txt</u>
<u>HAPROXY</u>	<u>haproxy.txt</u>
<u>HISTORY</u>	<u>shell_history.txt</u>
<u>IB</u>	<u>ib.txt</u>

Recurso	Nome do arquivo
<u>IMAN</u>	<u>novell-iman.txt</u>
<u>ISCSI</u>	<u>fs-iscsi.txt</u>
<u>LDAP</u>	<u>ldap.txt</u>
<u>LIVEPATCH</u>	<u>kernel-livepatch.txt</u>
<u>LVM</u>	<u>lvm.txt</u>
<u>MEM</u>	<u>memory.txt</u>
<u>MOD</u>	<u>modules.txt</u>
<u>MPIO</u>	<u>mpio.txt</u>
<u>NET</u>	<u>network-*.txt</u>
<u>NFS</u>	<u>nfs.txt</u>
<u>NTP</u>	<u>ntp.txt</u>
<u>NVME</u>	<u>nvme.txt</u>
<u>OCFS2</u>	<u>ocfs2.txt</u>
<u>OFILES</u>	<u>open-files.txt</u>
<u>PRINT</u>	<u>print.txt</u>
<u>PROC</u>	<u>proc.txt</u>
<u>SAR</u>	<u>sar.txt</u>
<u>SLERT</u>	<u>slert.txt</u>
<u>SLP</u>	<u>slp.txt</u>
<u>SMT</u>	<u>smt.txt</u>
<u>SMART</u>	<u>fs-smartmon.txt</u>
<u>SMB</u>	<u>samba.txt</u>
<u>SRAID</u>	<u>fs-softraid.txt</u>

Recurso	Nome do arquivo
<u>SSH</u>	<u>ssh.txt</u>
<u>SSSD</u>	<u>sssd.txt</u>
<u>SYSCONFIG</u>	<u>sysconfig.txt</u>
<u>SYSFS</u>	<u>sysfs.txt</u>
<u>TRANSACTIONAL</u>	<u>transactional-update.txt</u>
<u>TUNED</u>	<u>tuned.txt</u>
<u>UDEV</u>	<u>udev.txt</u>
<u>UFILES</u>	<u>fs-files-additional.txt</u>
<u>UP</u>	<u>updates.txt</u>
<u>WEB</u>	<u>web.txt</u>
<u>X</u>	<u>x.txt</u>

41.3 Enviando informações ao suporte técnico global

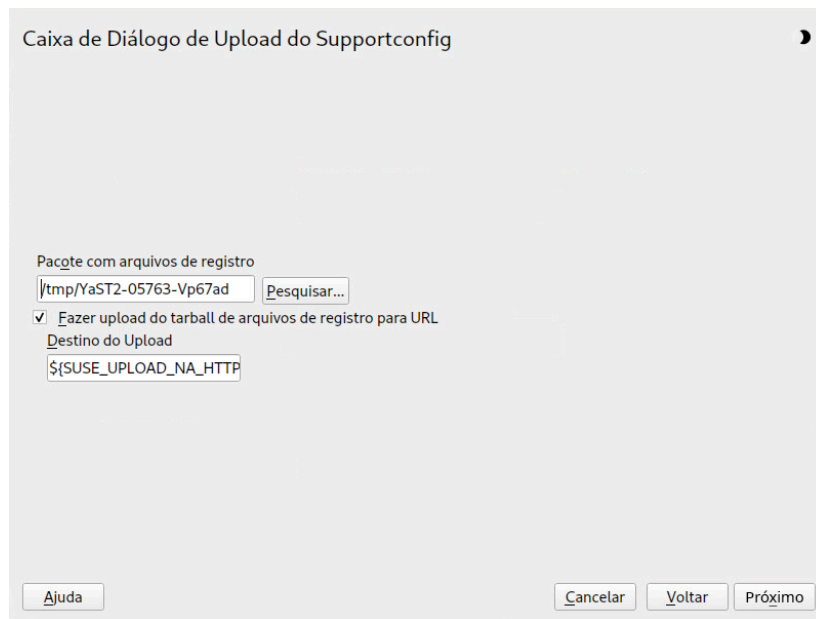
Use o módulo de *Suporte* do YaST ou o utilitário de linha de comando **supportconfig** para submeter as informações do sistema ao Suporte Técnico Global. Se você tiver um problema com o servidor e quiser a ajuda do suporte, precisará abrir primeiro uma solicitação de serviço. Para obter os detalhes, consulte a [Seção 41.2.1, “Criando um número de solicitação de serviço”](#).

Os seguintes exemplos usam 12345678901 como marcador para o número da sua solicitação de serviço. Substitua 12345678901 pelo número da solicitação de serviço que você criou na [Seção 41.2.1, “Criando um número de solicitação de serviço”](#).

PROCEDIMENTO 41.1: ENVIANDO INFORMAÇÕES AO SUPORTE COM O YAST

O seguinte procedimento considera que você já tenha criado um arquivo Supportconfig, mas ainda não tenha feito upload dele. Verifique se você incluiu suas informações de contato no armazenamento, conforme descrito na [Seção 41.2.3, “Criando um arquivo supportconfig com o YaST”, Passo 4](#). Para ver instruções de como gerar e enviar de uma só vez um arquivo Supportconfig, consulte a [Seção 41.2.3, “Criando um arquivo supportconfig com o YaST”](#).

1. Inicie o YaST e abra o módulo de *Suporte*.
2. Clique em *Fazer Upload*.
3. Em *Pacote com arquivos de registro*, especifique o caminho para o arquivo Supportconfig existente ou use a opção *Procurar*.
4. O YaST propõe um servidor de upload automaticamente. Para modificá-lo, consulte a [Seção 41.2.2, “Destinos de upload”](#) para saber os detalhes de quais servidores de upload estão disponíveis.



Continue com *Próximo*.

5. Clique em *Concluir*.

PROCEDIMENTO 41.2: ENVIANDO INFORMAÇÕES AO SUPORTE POR LINHA DE COMANDO

O seguinte procedimento considera que você já tenha criado um arquivo Supportconfig, mas ainda não tenha feito upload dele. Para ver instruções de como gerar e enviar de uma só vez um arquivo Supportconfig, consulte a [Seção 41.2.3, “Criando um arquivo supportconfig com o YaST”](#).

1. Servidores com conectividade à Internet:
 - a. Para usar o destino de upload padrão, execute:

```
> sudo supportconfig -ur 12345678901
```


- b. Para o destino de upload seguro, use o seguinte:

```
> sudo supportconfig -ar 12345678901
```

2. Servidores *sem* conectividade à Internet

- a. Execute o seguinte:

```
> sudo supportconfig -r 12345678901
```

- b. Faça upload manualmente do arquivo `/var/log/scc_SR12345678901*tbz` para um dos nossos servidores FTP. O servidor que deverá ser usado depende da sua localização global. Para uma visão geral, consulte a [Seção 41.2.2, “Destinos de upload”](#).

3. Depois que o armazenamento TAR estiver no diretório de entrada do nosso servidor FTP, ele será automaticamente anexado à sua solicitação de serviço.

41.4 Analisando as informações do sistema

É possível analisar os relatórios do sistema criados com o **supportconfig** para ver se há problemas conhecidos e agilizar sua solução. Para esta finalidade, o SUSE Linux Enterprise Desktop oferece uma aplicação e uma ferramenta de linha de comando para **Supportconfig Analysis** (SCA). A aplicação SCA é uma ferramenta não interativa executada no servidor. A ferramenta SCA (**scatool** incluída no pacote `sca-server-report`) é executada no lado do cliente por linha de comando. As duas ferramentas analisam os arquivos Supportconfig dos servidores afetados. A análise inicial do servidor ocorre na aplicação SCA ou na estação de trabalho em que a **scatool** é executada. Nenhum ciclo de análise é realizado no servidor de produção.

Tanto a aplicação quanto a ferramenta de linha de comando precisam de padrões específicos do produto, que as permitem analisar a saída do Supportconfig dos produtos associados. Cada padrão é um script que analisa e avalia um arquivo Supportconfig referente a um problema conhecido. Os padrões estão disponíveis como pacotes RPM.

É possível também desenvolver seus próprios padrões, conforme descrito resumidamente na [Seção 41.4.3, “Desenvolvendo padrões de análise personalizados”](#).

41.4.1 Ferramenta de linha de comando SCA

A ferramenta de linha de comando SCA permite analisar uma máquina local usando o **supportconfig** e os padrões de análise referentes ao produto específico que está instalado na máquina local. A ferramenta cria um relatório HTML que mostra os resultados da análise. Para obter um exemplo, consulte a *Figura 41.1, “Relatório HTML gerado pela ferramenta SCA”*.

Supportconfig Analysis Report

Server Information

Analysis Date:
Archive File:

/4/25/2014 11:22
/var/log/nts_barett-2_140425_1119.html

Server Name: barett-2
Distribution: SUSE Linux Enterprise Server 12 (x86_64)
Hypervisor: KVM (QEMU Virtual CPU)
Kernel Version: 3.12.14-1-default

Hardware: Bochs
Service Pack: 0
Identity: Virtual Machine (QEMU Virtual CPU)
Supportconfig Version: 3.0-18

Conditions Evaluated as Critical

Category	Message	Solutions
Basic Health	2 Basic Health Message(s)	
Basic Health SLE Kernel	Kernel Status -- Tainted: F O	TID
Basic Health SLE System	Last system down was not clean on Mon Mar 24 17:37:04 2014 and 1 additional failure(s)	TID TID1
SLE	2 SLE Message(s)	

Conditions Evaluated as Warning

Category	Message	Solutions
SLE	1 SLE Message(s)	

Conditions Evaluated as Recommended

Category	Message	Solutions
SLE	1 SLE Message(s)	

Conditions Evaluated as Success

Category	Message	Solutions
Security	1 Security Message(s)	
Security SLE AppArmor	There are no AppArmor reject messages	TID Doc
Basic Health	8 Basic Health Message(s)	
Basic Health SLE Kernel	Context switches per second observed: 79	TID
Basic Health SLE Kernel	Interrupts per second observed: 51	TID
Basic Health SLE CPU	Utilization: 1.00%, Idle: 99.00%	TID
Basic Health SLE Disk	Mount on / has highest used space: 22%	TID TID2
Basic Health SLE Kernel	2% CPU load within limits, CPUs: 1, Load Average: 0.02	TID Web Wikipedia
Basic Health SLE Memory	Memory used 29% - Swapping: No	TID
Basic Health SLE Processes	0 Uninterruptible processes observed	TID
Basic Health SLE Processes	0 Zombie processes observed	TID

FIGURA 41.1: RELATÓRIO HTML GERADO PELA FERRAMENTA SCA

O comando **scatool** está incluído no pacote **sca-server-report**. Ele não é instalado por padrão. Você também precisa do pacote **sca-patterns-base** e de qualquer um dos pacotes **sca-patterns-*** específicos do produto correspondentes ao produto instalado na máquina em que deseja executar o comando **scatool**.

Execute o comando **scatool** como usuário **root** ou com **sudo**. Ao chamar a ferramenta SCA, é possível analisar um arquivo TAR **supportconfig** existente ou deixar que ela gere e analise um novo arquivo de uma vez. A ferramenta também oferece um console interativo com complementação de guia. É possível executar o **supportconfig** em uma máquina externa e executar as análises subsequentes na máquina local.

Veja a seguir alguns exemplos de comandos:

`sudo scatool -s`

Chama o **`supportconfig`** e gera um novo arquivo Supportconfig na máquina local. Analisa o armazenamento para ver se há problemas conhecidos aplicando os padrões de análise da SCA correspondentes ao produto instalado. Exibe o caminho para o relatório HTML que é gerado com base nos resultados da análise. Normalmente, ele é gravado no mesmo diretório do arquivo Supportconfig.

`sudo scatool -s -o /opt/sca/reports/`

Igual ao **`sudo scatool -s`**, só que o relatório HTML é gravado no caminho especificado com **`-o`**.

`sudo scatool -a CAMINHO_PARA_TARBALL_OU_DIR`

Analisa o arquivo de armazenamento Supportconfig especificado (ou o diretório indicado no qual o arquivo Supportconfig foi extraído). O relatório HTML gerado é gravado no mesmo local do arquivo ou diretório do Supportconfig.

`sudo scatool -a SERVIDOR_SLES.EMPRESA.COM`

Estabelece uma conexão SSH com um servidor externo **`SERVIDOR_SLES.EMPRESA.COM`** e executa o **`supportconfig`** no servidor. Em seguida, o arquivo Supportconfig é copiado novamente na máquina local e analisado nela. O relatório HTML gerado é gravado no diretório padrão **`/var/log`**. (Apenas o arquivo Supportconfig é criado em **`SERVIDOR_SLES.EMPRESA.COM`**).

`sudo scatool -c`

Inicia o console interativo da **`scatool`**. Pressione **`-|`** duas vezes para ver os comandos disponíveis.

Para mais opções e informações, execute **`sudo scatool -h`** ou consulte a página de manual de **`scatool`**.

41.4.2 Aplicação SCA

Se você usar a aplicação SCA para analisar arquivos Supportconfig, configure um servidor dedicado (ou máquina virtual) como servidor da aplicação SCA. Depois disso, o servidor da aplicação SCA poderá ser usado para analisar arquivos Supportconfig em todas as máquinas da sua empresa que tenham o SUSE Linux Enterprise Server ou o SUSE Linux Enterprise Desktop.

Basta fazer upload dos arquivos Supportconfig para o servidor da aplicação para análise. Não é necessária nenhuma interação. Em um banco de dados MariaDB, a aplicação SCA monitora todos os arquivos Supportconfig que foram analisados. É possível ler os relatórios da SCA diretamente da interface da Web da aplicação. Se você preferir, a aplicação poderá enviar o relatório HTML por e-mail para qualquer usuário administrativo. Para obter os detalhes, consulte a [Seção 41.4.2.5.4, “Enviando relatórios da SCA por e-mail”](#).

41.4.2.1 Inicialização Rápida da instalação

Para instalar e configurar rapidamente a aplicação SCA por linha de comando, siga as instruções neste documento. O procedimento é voltado para especialistas e está centrado na instalação limpa e nos comandos de configuração. Para obter mais informações, consulte a descrição mais detalhada da [Seção 41.4.2.2, “Pré-requisitos”](#) até a [Seção 41.4.2.3, “Instalação e configuração básica”](#).

PRÉ-REQUISITOS

- Padrão da Web e LAMP
- Módulo da Web e de Criação de Scripts (você deve registrar a máquina para selecionar esse módulo).



Nota: Privilégios de root necessários

Todos os comandos do procedimento a seguir devem ser executados como root.

PROCEDIMENTO 41.3: INSTALAÇÃO USANDO FTP ANÔNIMO PARA UPLOAD

Depois que a aplicação estiver funcionando, não será necessária mais nenhuma interação manual. Portanto, esta forma de configurar a aplicação é ideal ao usar tarefas cron para criar e fazer upload de arquivos Supportconfig.

1. Na máquina em que a aplicação será instalada, efetue login em um console e execute os seguintes comandos (certifique-se de aceitar os pacotes recomendados):

```
> sudo zypper install sca-appliance-* sca-patterns-* \
vsftpd yast2 yast2-ftp-server
> sudo systemctl enable apache2
> sudo systemctl start apache2
> sudo systemctl enable vsftpd
> sudo systemctl start vsftpd
> sudo yast ftp-server
```

2. No Servidor FTP do YaST, selecione *Autenticação > Habilitar Upload > Anônimo Pode Fazer Upload > Concluir > Sim* para Criar `/srv/ftp/upload`.
3. Execute os seguintes comandos:

```
> sudo systemctl enable mysql
> sudo systemctl start mysql
> sudo mysql_secure_installation
> sudo setup-sca -f
```

A `mysql_secure_installation` cria uma senha de `root` do MariaDB.

PROCEDIMENTO 41.4: INSTALAÇÃO USANDO SCP/TMP PARA UPLOAD

Esta forma de configurar a aplicação requer interação manual para digitar a senha SSH.

1. Na máquina de instalação da aplicação, efetue login no console.
2. Execute os seguintes comandos:

```
> sudo zypper install sca-appliance-* sca-patterns-*
> sudo systemctl enable apache2
> sudo systemctl start apache2
> sudo systemctl enable mysql
> sudo systemctl start mysql
> sudo mysql_secure_installation
> sudo setup-sca
```

41.4.2.2 Pré-requisitos

Para executar um servidor da aplicação SCA, são necessários os seguintes pré-requisitos:

- Todos os pacotes `sca-appliance-*`.
- O pacote `sca-patterns-base`. Além disso, qualquer um dos `sca-patterns-*` específicos do produto, de acordo com o tipo de arquivo Supportconfig que você deseja analisar com a aplicação.
- Apache
- PHP
- MariaDB
- Servidor FTP anônimo (opcional)

41.4.2.3 Instalação e configuração básica

Conforme listado na [Seção 41.4.2.2, “Pré-requisitos”](#), a aplicação SCA possui várias dependências em outros pacotes. Portanto, você precisa fazer algumas preparações antes de instalar e configurar o servidor da aplicação SCA:

1. No Apache e no MariaDB, instale os padrões de instalação da [Web](#) e [LAMP](#).
2. Configure o Apache, o MariaDB e, opcionalmente, um servidor FTP anônimo.
3. Configure o Apache e o MariaDB para iniciarem no momento da inicialização:

```
> sudo systemctl enable apache2 mysql
```

4. Inicie os dois serviços:

```
> sudo systemctl start apache2 mysql
```

Agora você pode instalar a aplicação SCA e configurá-la conforme descrito no [Procedimento 41.5, “Instalando e configurando a aplicação SCA”](#).

PROCEDIMENTO 41.5: INSTALANDO E CONFIGURANDO A APLICAÇÃO SCA

Após instalar os pacotes, use o script **setup-sca** para a configuração básica do banco de dados de administração e relatório MariaDB, que é usado pela aplicação SCA.

Ele pode ser usado para configurar as seguintes opções disponíveis para fazer upload dos arquivos Supportconfig de suas máquinas para a aplicação SCA:

- [scp](#)
- servidor FTP anônimo

1. Instale a aplicação e a biblioteca de padrões com base na SCA:

```
> sudo zypper install sca-appliance-* sca-patterns-base
```

2. Instale também os pacotes de padrões de acordo com os tipos de arquivos Supportconfig que você deseja analisar. Por exemplo, se você tem servidores SUSE Linux Enterprise Server 12 e SUSE Linux Enterprise Server 15 em seu ambiente, instale os dois pacotes [sca-patterns-sle12](#) e [sca-patterns-sle15](#).

Para instalar todos os padrões disponíveis:

```
> sudo zypper install sca-patterns-*
```

3. Para a configuração básica da aplicação SCA, use o script **setup-sca**. O modo como ele é chamado depende de como você deseja fazer upload dos arquivos Supportconfig para o servidor da aplicação SCA:

- Se você configurou um servidor FTP anônimo que usa o diretório `/srv/ftp/upload`, execute o script de configuração com a opção `-f`. Siga as instruções na tela:

```
> sudo setup-sca -f
```



Nota: Servidor FTP que usa outro diretório

Se o seu servidor FTP usa um diretório diferente do `/srv/ftp/upload`, ajuste os seguintes arquivos de configuração para apontarem para o diretório correto: `/etc/sca/sdagent.conf` e `/etc/sca/sdbroker.conf`.

- Para fazer upload dos arquivos Supportconfig para o diretório `/tmp` do servidor da aplicação SCA usando o comando **scp**, chame o script de configuração sem nenhum parâmetro. Siga as instruções na tela:

```
> sudo setup-sca
```

O script de configuração executa algumas verificações referentes a seus requisitos e configura os componentes necessários. Ele pede duas senhas: a senha de `root` MySQL do MariaDB que você configurou e uma senha de usuário da Web usada para efetuar login na interface da Web da aplicação SCA.

4. Digite a senha de `root` existente do MariaDB. Isso permite que a aplicação SCA se conecte com o MariaDB.
5. Defina uma senha para o usuário da Web. Ela será gravada em `/srv/www/htdocs/sca/web-config.php` e definida como a senha do usuário `scdiag`. Tanto o nome de usuário quanto a senha podem ser mudados a qualquer momento. Consulte a [Seção 41.4.2.5.1, "Senha da interface da Web"](#).

Após a instalação e configuração bem-sucedidas, a aplicação SCA estará pronta para uso. Consulte a [Seção 41.4.2.4, "Usando a aplicação SCA"](#). No entanto, você deve modificar algumas opções, como mudar a senha da interface da Web, mudar a fonte das atualizações dos padrões da SCA, habilitar o modo de arquivamento ou configurar notificações por e-mail. Para ver os detalhes sobre isso, consulte a [Seção 41.4.2.5, "Personalizando a aplicação SCA"](#).



Atenção: Proteção de dados;

Como os relatórios no servidor da aplicação SCA incluem informações relacionadas à segurança, proteja os dados no servidor da aplicação SCA contra acesso não autorizado.

41.4.2.4 Usando a aplicação SCA

É possível fazer upload dos arquivos Supportconfig existentes para a aplicação SCA manualmente ou criar novos arquivos Supportconfig e fazer upload deles para a aplicação SCA em uma etapa. O upload pode ser feito por FTP ou SCP. Nos dois, é necessário saber o URL para acessar a aplicação SCA. Para upload por FTP, um servidor FTP precisa ser configurado para a aplicação SCA. Consulte o [Procedimento 41.5, “Instalando e configurando a aplicação SCA”](#).

41.4.2.4.1 Fazendo upload de arquivos supportconfig para a aplicação SCA

- Para criar um arquivo Supportconfig e fazer upload dele por FTP (anônimo):

```
> sudo supportconfig -U "ftp://SCA-APPLIANCE.COMPANY.COM/upload"
```

- Para criar um arquivo Supportconfig e fazer upload dele por SCP:

```
> sudo supportconfig -U "scp://SCA-APPLIANCE.COMPANY.COM/tmp"
```

Você deverá informar a senha de usuário root do servidor que executa a aplicação SCA.

- Para fazer upload de um ou vários arquivos manualmente, copie os arquivos de armazenamento existentes (que costumam estar em /var/log/scc_*.tbz) para a aplicação SCA. Como destino, use o diretório /tmp do servidor da aplicação ou o diretório /srv/ftp/upload (se FTP estiver configurado para o servidor da aplicação SCA).

41.4.2.4.2 Vendo relatórios da SCA

É possível ver os relatórios da SCA de qualquer máquina que tenha um browser instalado e acesso à página de índice de relatórios da aplicação SCA.

1. Inicie o browser da Web e verifique se o JavaScript e os cookies estão habilitados.
2. Como URL, insira a página de índice de relatórios da aplicação SCA.

<https://sca-appliance.company.com/sca>

Se estiver em dúvida, pergunte ao administrador do sistema.

3. Você deverá informar o nome de usuário e a senha para efetuar login.

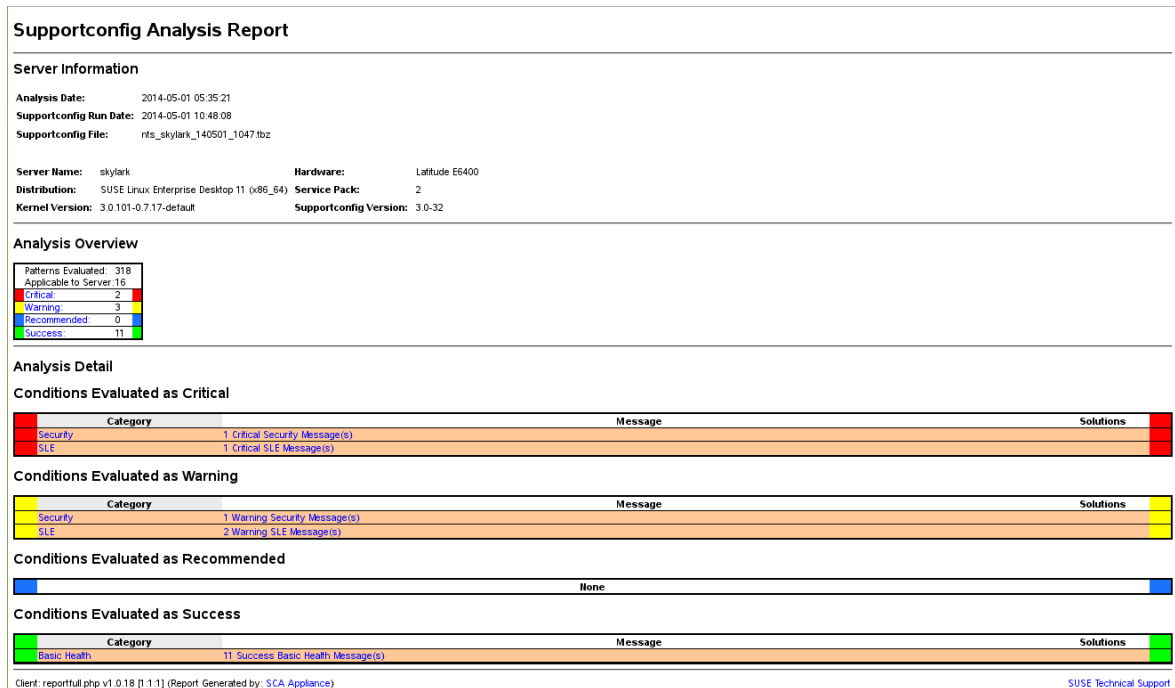


FIGURA 41.2: RELATÓRIO HTML GERADO PELA APLICAÇÃO SCA

4. Após o login, clique na data do relatório que deseja ler.
5. Clique primeiro na categoria *Basic Health* (Saúde Básica) para expandi-la.
6. Na coluna *Message* (Mensagem), clique em uma entrada. O artigo correspondente é aberto na Base de Dados de Conhecimento SUSE. Leia a solução proposta e siga as instruções.
7. Se a coluna *Solutions* (Soluções) do *Relatório da Supportconfig Analysis* mostrar qualquer outra entrada, clique nela. Leia a solução proposta e siga as instruções.
8. Consulte a Base de Dados de Conhecimento SUSE (<https://www.suse.com/support/kb/>) para ver resultados diretamente relacionados ao problema identificado pela SCA. Resolva o problema.
9. Procure resultados que possam ser usados proativamente para evitar futuros problemas.

41.4.2.5 Personalizando a aplicação SCA

As seguintes seções mostram como mudar a senha da interface da Web, como mudar a fonte das atualizações dos padrões da SCA, como habilitar o modo de arquivamento e como configurar notificações por e-mail.

41.4.2.5.1 Senha da interface da Web

A interface da Web da aplicação SCA requer nome de usuário e senha para login. O nome de usuário padrão é `scdiag` e a senha padrão é `linux` (caso não tenham sido especificados de outra forma. Consulte o [Procedimento 41.5, “Instalando e configurando a aplicação SCA”](#)). Mude a senha padrão para uma senha segura na primeira oportunidade. É possível também modificar o nome de usuário.

PROCEDIMENTO 41.6: MUDANDO NOME DE USUÁRIO OU SENHA DA INTERFACE DA WEB

1. Efetue login como usuário `root` no console do sistema do servidor da aplicação SCA.
2. Abra o `/srv/www/htdocs/sca/web-config.php` em um editor.
3. Mude os valores de `$username` e `$password` conforme desejado.
4. Grave o arquivo e saia.

41.4.2.5.2 Atualizações dos padrões da SCA

Por padrão, todos os pacotes `sca-patterns-*` são atualizados regularmente por um cron `root` que executa o script `sdagent-patterns` durante a noite, que, por sua vez, executa `zypper update sca-patterns-*`. Uma atualização regular de sistema atualiza todos os pacotes de padrões e da aplicação SCA. Para atualizar a aplicação SCA e os padrões manualmente, execute:

```
> sudo zypper update sca-*
```

Por padrão, as atualizações são instaladas do repositório de atualização do SUSE Linux Enterprise 15 SP4. Você poderá mudar a fonte das atualizações para um servidor RMT, se desejado. Quando `sdagent-patterns` executa `zypper update sca-patterns-*`, ele acessa as atualizações do canal de atualização configurado no momento. Se esse canal estiver em um servidor RMT, os pacotes serão acessados de lá.

PROCEDIMENTO 41.7: DESABILITANDO ATUALIZAÇÕES AUTOMÁTICAS DOS PADRÕES DA SCA

1. Efetue login como usuário `root` no console do sistema do servidor da aplicação SCA.
2. Abra o `/etc/sca/sdagent-patterns.conf` em um editor.

3. Mudar a entrada

```
UPDATE_FROM_PATTERN_REPO=1
```

para

```
UPDATE_FROM_PATTERN_REPO=0
```

4. Grave o arquivo e saia. Não é necessário reiniciar a máquina para aplicar a mudança.

41.4.2.5.3 Modo de arquivamento

Todos os arquivos Supportconfig serão apagados da aplicação SCA depois de serem analisados e de seus resultados serem armazenados no banco de dados MariaDB. Para fins de solução de problemas, no entanto, convém manter cópias dos arquivos Supportconfig de uma máquina. Por padrão, o modo de arquivamento está desabilitado.

PROCEDIMENTO 41.8: HABILITANDO O MODO DE ARQUIVAMENTO NA APLICAÇÃO SCA

1. Efetue login como usuário `root` no console do sistema do servidor da aplicação SCA.
2. Abra o `/etc/sca/sdagent.conf` em um editor.

3. Mudar a entrada

```
ARCHIVE_MODE=0
```

para

```
ARCHIVE_MODE=1
```

4. Grave o arquivo e saia. Não é necessário reiniciar a máquina para aplicar a mudança.

Após habilitar o modo de arquivamento, a aplicação SCA gravará os arquivos Supportconfig no diretório `/var/log/archives/saved`, em vez de apagá-los.

41.4.2.5.4 Enviando relatórios da SCA por e-mail

A aplicação SCA pode enviar um arquivo HTML de relatório por e-mail referente a cada Supportconfig analisado. Por padrão, este recurso está desabilitado. Ao habilitá-lo, você pode definir uma lista de endereços de e-mail para os quais os relatórios devem ser enviados. Defina um nível de mensagens de status que acione o envio de relatórios (`STATUS_NOTIFY_LEVEL`).

VALORES POSSÍVEIS PARA `STATUS_NOTIFY_LEVEL`

`$STATUS_OFF`

Desativar o envio de relatórios HTML.

`$STATUS_CRITICAL`

Enviar apenas relatórios da SCA que incluam CRITICAL (Crítico).

`$STATUS_WARNING`

Enviar apenas relatórios da SCA que incluam WARNING (Aviso) ou CRITICAL.

`$STATUS_RECOMMEND`

Enviar apenas relatórios da SCA que incluam RECOMMEND (Recomendado), WARNING ou CRITICAL.

`$STATUS_SUCCESS`

Enviar relatórios da SCA que incluam SUCCESS (Êxito), RECOMMEND, WARNING ou CRITICAL.

PROCEDIMENTO 41.9: CONFIGURANDO NOTIFICAÇÕES POR E-MAIL PARA RELATÓRIOS DA SCA

1. Efetue login como usuário `root` no console do sistema do servidor da aplicação SCA.
2. Abra o `/etc/sca/sdagent.conf` em um editor.
3. Pesquise a entrada `STATUS_NOTIFY_LEVEL`. Por padrão, ela está definida como `$STATUS_OFF` (notificações por e-mail desabilitadas).
4. Para habilitar as notificações por e-mail, mude `$STATUS_OFF` para o nível de mensagens de status para o qual deseja gerar relatórios por e-mail, por exemplo:

```
STATUS_NOTIFY_LEVEL=$STATUS_SUCCESS
```

Para obter os detalhes, consulte a [Valores possíveis para STATUS_NOTIFY_LEVEL](#).

5. Para definir a lista de destinatários que devem receber os relatórios:
 - a. Pesquise a entrada `EMAIL_REPORT='root'`.

- b. Substitua `root` pela lista de endereços de e-mail aos quais enviar os relatórios da SCA. Os endereços de e-mail devem ser separados por espaços. Por exemplo:

```
EMAIL_REPORT='tux@my.company.com wilber@your.company.com'
```

6. Grave o arquivo e saia. Não é necessário reiniciar a máquina para aplicar as mudanças. Todos os relatórios futuros da SCA serão enviados por e-mail aos endereços especificados.

41.4.2.6 Fazendo backup e restaurando o banco de dados

Para fazer backup e restaurar o banco de dados MariaDB que armazena os relatórios da SCA, use o comando `scadb`, conforme descrito a seguir. O `scadb` está incluído no pacote `sca-appliance-broker`.

PROCEDIMENTO 41.10: FAZENDO BACKUP DO BANCO DE DADOS

1. Efetue login como usuário `root` no console do sistema do servidor que executa a aplicação SCA.
2. Coloque a aplicação no modo de manutenção executando:

```
# scadb maint
```

3. Inicie o backup com:

```
# scadb backup
```

Os dados são gravados em um armazenamento TAR: `sca-backup-*.sql.gz`.

4. Se você usa o banco de dados de criação de padrões para desenvolver seus próprios padrões (consulte a [Seção 41.4.3, "Desenvolvendo padrões de análise personalizados"](#)), faça backup também destes dados:

```
# sdpdb backup
```

Os dados são gravados em um armazenamento TAR: `sdp-backup-*.sql.gz`.

5. Copie os seguintes dados para outra máquina ou para um meio de armazenamento externo:

- sca-backup-*.sql.gz
- sdp-backup-*.sql.gz
- /usr/lib/sca/patterns/local (necessário apenas se você criar padrões personalizados)

6. Ative novamente a aplicação SCA com:

```
# scadb reset agents
```

PROCEDIMENTO 41.11: RESTAURANDO O BANCO DE DADOS

Para restaurar o banco de dados do backup, faça o seguinte:

1. Efetue login como usuário root no console do sistema do servidor que executa a aplicação SCA.
2. Copie os armazenamentos TAR sca-backup-*.sql.gz e sdp-backup-*.sql.gz mais recentes para o servidor da aplicação SCA.
3. Para descompactar os arquivos, execute:

```
# gzip -d *-backup-*.sql.gz
```

4. Para importar os dados para o banco de dados, execute:

```
# scadb import sca-backup-*.sql
```

5. Se você usa o banco de dados de criação de padrões para criar seus próprios padrões, importe também os seguintes dados com:

```
# sdpdb import sdp-backup-*.sql
```

6. Se você usa padrões personalizados, restaure também /usr/lib/sca/patterns/local dos dados do backup.

7. Ative novamente a aplicação SCA com:

```
# scadb reset agents
```

8. Atualize os módulos de padrão no banco de dados com:

```
# sdagent-patterns -u
```

41.4.3 Desenvolvendo padrões de análise personalizados

A aplicação SCA vem com um ambiente completo de desenvolvimento de padrões (o Banco de Dados de Padrões da SCA), que permite desenvolver padrões personalizados. Os padrões podem ser desenvolvidos em qualquer linguagem de programação. Para disponibilizá-los para o processo de análise do Supportconfig, eles devem ser gravados em `/usr/lib/sca/patterns/local` e ser executáveis. Tanto a aplicação quanto a ferramenta SCA executam os padrões personalizados nos novos arquivos Supportconfig como parte do relatório de análise. Para obter instruções detalhadas sobre como criar (e testar) seus próprios padrões, visite <https://www.suse.com/c/blog/sca-pattern-development/>.

41.5 Coletando informações durante a instalação

Durante a instalação, o `supportconfig` não está disponível. No entanto, você pode coletar arquivos de registro do YaST usando `save_y2logs`. Esse comando criará um arquivo `.tar.xz` no diretório `/tmp`.

Se aparecerem problemas muito no começo da instalação, talvez seja possível coletar informações do arquivo de registro criado por `linuxrc`. `linuxrc` é um comando pequeno que é executado antes de o YaST ser iniciado. Esse arquivo de registro está disponível em `/var/log/linuxrc.log`.



Importante: Arquivos de registro de instalação não disponíveis no sistema instalado

Os arquivos de registro disponíveis durante a instalação não estão mais disponíveis no sistema instalado. Grave apropriadamente os arquivos de registro de instalação enquanto o instalador ainda está em execução.

41.6 Suporte aos módulos do kernel

Um requisito importante para todo sistema operacional empresarial é o nível de suporte que você recebe do ambiente. Os módulos do Kernel são o conector mais relevante entre o hardware (“controladoras”) e o sistema operacional. Cada módulo do kernel no SUSE Linux Enterprise possui um flag supported (suportado) que pode ter três valores:

- “yes”, portanto, supported
- “external” (externo), portanto, supported
- “” (vazio, não definido), portanto unsupported (não suportado)

As seguintes regras são válidas:

- Por padrão, todos os módulos de um kernel autorrecompilado são marcados como não suportados.
- Os módulos do Kernel suportados pelos parceiros do SUSE e distribuídos pelo SUSE SolidDriver Program são marcados como “externos”.
- Se o flag supported não estiver definido, o carregamento do módulo contaminará o kernel. Kernels contaminados não são suportados. Os módulos do Kernel não suportados estão incluídos em um pacote RPM adicional (kernel-FLAVOR-extra). Esse pacote apenas está disponível para o SUSE Linux Enterprise Desktop e a SUSE Linux Enterprise Workstation Extension. Por padrão, esses kernels não são carregados (TIPO = default | xen | ...). Esses módulos não suportados também não estão disponíveis no instalador, e o pacote kernel-FLAVOR-extra não faz parte da mídia do SUSE Linux Enterprise.
- Os módulos do kernel não incluídos em uma licença compatível com a licença do kernel do Linux também contaminarão o kernel. Para obter detalhes, consulte /usr/src/linux/Documentation/sysctl/kernel.txt e o estado de /proc/sys/kernel/tainted.

41.6.1 Informações técnicas

- **Kernel do Linux:** O valor d `/proc/sys/kernel/unsupported` usa o padrão `2` no SUSE Linux Enterprise 15 SP4 (`do not warn in syslog when loading unsupported modules`). Esse padrão é usado no instalador e no sistema instalado. Consulte `/usr/src/linux/Documentation/sysctl/kernel.txt` para obter mais informações.
- **modprobe:** O utilitário `modprobe` de verificação de dependências de módulos e carregamento dos módulos apropriados confirma se o valor do flag é `supported` (suportado). Se o valor for “sim” ou “externo”, o módulo será carregado, do contrário, não. Para obter informações sobre como anular este comportamento, consulte a [Seção 41.6.2, “Trabalhando com módulos não suportados”](#).



Nota: Suporte

Em geral, o SUSE não suporta a remoção de módulos de armazenamento por `modprobe -r`.

41.6.2 Trabalhando com módulos não suportados

Embora a capacidade de suporte geral seja importante, algumas situações podem exigir o carregamento de um módulo não suportado. Por exemplo, para fins de teste ou depuração, ou se o seu fornecedor de hardware disponibilizar um hotfix.

- Para anular o padrão, copie `/lib/modprobe.d/10-unsupported-modules.conf` para `/etc/modprobe.d/10-unsupported-modules.conf` e mude o valor da variável `allow_unsupported_modules` de `0` para `1`. Não edite o `/lib/modprobe.d/10-unsupported-modules.conf` diretamente. As mudanças serão sobregravadas sempre que o pacote `suse-module-tools` for atualizado.
Se for necessário um módulo não suportado no `initrd`, lembre-se de executar `dracut -f` para atualizar o `initrd`.

Para apenas tentar carregar um módulo uma vez, é possível usar a opção `--allow-unsupported-modules` com `modprobe`. Para obter mais informações, consulte os comentários em `/lib/modprobe.d/10-unsupported-modules.conf` e a página de manual do `modprobe`.

- Durante a instalação, módulos não suportados podem ser adicionados por meio de discos de atualização de driver, e eles serão carregados. Para impor o carregamento de módulos não suportados durante a inicialização e posteriormente, use a opção de linha de comando do kernel `oem-modules`. Durante a instalação e inicialização do pacote `suse-module-tools`, o flag do kernel `TAINT_NO_SUPPORT` (`/proc/sys/kernel/tainted`) será avaliado. Se o kernel já foi contaminado, `allow_unsupported_modules` será habilitado. Isso impede que módulos não suportados acessem o sistema que está sendo instalado. Se não houver nenhum módulo não suportado durante a instalação e não for usada a outra opção de linha de comando especial do kernel (`oem-modules=1`), o padrão ainda será de não permitir módulos não suportados.

Lembre-se de que carregar e executar módulos não suportados tornam o kernel e todo o sistema não suportados pelo SUSE.

41.7 Mais informações

- `man supportconfig`: A página de manual de `supportconfig`.
- `man supportconfig.conf`: A página de manual do arquivo de configuração `Supportconfig`.
- `man scatool`: A página de manual de `scatool`.
- `man scadb`: A página de manual de `scadb`.
- `man setup-sca`: A página de manual de `setup-sca`.
- <https://mariadb.com/kb/en/>: A documentação do MariaDB.
- <https://www.suse.com/c/blog/sca-pattern-development/>: Instruções sobre como criar (e testar) seus próprios padrões da SCA.
- <https://www.suse.com/c/blog/basic-server-health-check-supportconfig/>: Uma verificação da saúde básica do servidor com o `supportconfig`.

- <https://community.microfocus.com/t5/GroupWise-Tips-Information/Create-Your-Own-Supportconfig-Plugin/ta-p/1783289> ➦: Criar seu próprio plug-in Supportconfig.
- <https://www.suse.com/c/blog/creating-a-central-supportconfig-repository/> ➦: Criar um repositório central do Supportconfig.

42 Problemas comuns e suas soluções

Este capítulo descreve uma gama de problemas em potencial e suas soluções. Mesmo se a sua situação não esteja listada aqui com precisão, poderá haver alguma semelhante que ofereça dicas para a solução do seu problema.

42.1 Localizando e reunindo informações

O Linux reporta os dados de forma bastante detalhada. Há vários lugares para você pesquisar caso tenha problemas com seu sistema, sendo que a maioria é padrão para sistemas Linux em geral, e alguns relevantes aos sistemas SUSE Linux Enterprise Desktop. É possível ver a maioria dos arquivos de registro com o YaST (*Diversos > Registro de Inicialização*).

O YaST permite coletar todas as informações de sistema necessárias à equipe de suporte. Use *Outros > Suporte* e selecione a categoria do problema. Quando todas as informações forem reunidas, anexe-as à sua solicitação de suporte.

Veja a seguir uma lista dos arquivos de registro verificados com mais frequência com a descrição de seus objetivos principais. Os caminhos contendo `~` referem-se ao diretório pessoal do usuário atual.

TABELA 42.1: ARQUIVOS DE REGISTRO

Arquivo de registro	Descrição
<u><code>~/.xsession-errors</code></u>	Mensagens de aplicativos de área de trabalho atualmente em execução.
<u><code>/var/log/apparmor/</code></u>	Arquivos de registro do AppArmor, consulte a <i>Livro "Security and Hardening Guide"</i> para obter informações detalhadas.
<u><code>/var/log/audit/audit.log</code></u>	Arquivo de registro do Audit para monitorar qualquer acesso a arquivos, diretórios ou recursos do seu sistema, bem como rastrear as chamadas do sistema. Consulte o <i>Livro "Security and Hardening Guide"</i> para obter as informações detalhadas.

Arquivo de registro	Descrição
<u>/var/log/mail.*</u>	Mensagens do sistema de correio.
<u>/var/log/NetworkManager</u>	Arquivo de registro do NetworkManager para coleta de problemas de conectividade da rede
<u>/var/log/samba/</u>	Diretório contendo mensagens do registro de cliente e servidor do Samba.
<u>/var/log/warn</u>	Todas as mensagens do kernel e do daemon do registro do sistema com o nível “warning” ou superior.
<u>/var/log/wtmp</u>	Arquivo binário contendo registros de login de usuário para a sessão da máquina atual. Exiba-o com <u>last</u> .
<u>/var/log/Xorg.*.log</u>	Vários arquivos de registro de inicialização e tempo de execução do X Window System. São úteis para depurar inicializações malsucedidas do X.
<u>/var/log/YaST2/</u>	Diretório contendo ações do YaST e seus resultados.
<u>/var/log/zypper.log</u>	Arquivo de registro do Zypper.

Além dos arquivos de registro, a sua máquina também lhe fornece informações sobre o sistema em execução. Consulte a [Tabela 42.2: Informações do sistema com o sistema de arquivos /proc](#)

TABELA 42.2: INFORMAÇÕES DO SISTEMA COM O SISTEMA DE ARQUIVOS /proc

Arquivo	Descrição
<u>/proc/cpuinfo</u>	Contém informações do processador, incluindo o seu tipo, marca, modelo e desempenho.

Arquivo	Descrição
<u>/proc/dma</u>	Mostra quais canais DMA estão sendo usados no momento.
<u>/proc/interrupts</u>	Mostra quais interrupções estão em uso e quantas de cada foram usadas.
<u>/proc/iomem</u>	Exibe o status da memória de E/S (entrada/saída).
<u>/proc/ioports</u>	Mostra quais portas de E/S estão em uso no momento.
<u>/proc/meminfo</u>	Exibe o status da memória.
<u>/proc/modules</u>	Exibe os módulos individuais.
<u>/proc/mounts</u>	Exibe os dispositivos montados no momento.
<u>/proc/partitions</u>	Mostra o particionamento de todos os discos rígidos.
<u>/proc/version</u>	Exibe a versão atual do Linux.

Além do sistema de arquivos /proc, o kernel do Linux exporta informações com o módulo sysfs, um sistema de arquivos na memória. Esse módulo representa objetos Kernel, seus atributos e relacionamentos. Para obter mais informações sobre o sysfs, consulte o contexto de udev no [Capítulo 29, Gerenciamento dinâmico de dispositivos do kernel com udev](#). A [Tabela 42.3](#) contém uma visão geral dos diretórios mais comuns em /sys.

TABELA 42.3: INFORMAÇÕES DO SISTEMA COM O SISTEMA DE ARQUIVOS /sys

Arquivo	Descrição
<u>/sys/block</u>	Contém subdiretórios para cada dispositivo de bloco descoberto no sistema. Geralmente, esses dispositivos são de tipo de disco.
<u>/sys/bus</u>	Contém subdiretórios para cada tipo de barramento físico.

Arquivo	Descrição
<u>/sys/class</u>	Contém subdiretórios agrupados como tipos funcionais de dispositivos (como gráficos, de rede, de impressora etc)
<u>/sys/device</u>	Contém a hierarquia global de dispositivos.

O Linux vem com várias ferramentas para monitoramento e análise do sistema. Consulte o *Livro "System Analysis and Tuning Guide", Capítulo 2 "System monitoring utilities"* para obter uma seleção das mais importantes usadas em diagnósticos de sistema.

Cada um dos seguintes cenários começa com um cabeçalho que descreve o problema, seguido de um ou dois parágrafos apresentando sugestões para solução, referências disponíveis para consultar soluções mais detalhadas e referências cruzadas para outros cenários relacionados.

42.2 Problemas de boot

Problemas de boot são situações em que o sistema não é inicializado apropriadamente (não é inicializado no destino e na tela de login esperados).

42.2.1 Falha ao carregar o carregador de boot GRUB 2

Se o hardware estiver funcionando de forma adequada, é possível que o carregador de boot esteja corrompido e que o Linux não possa ser iniciado na máquina. Neste caso, é necessário consertar o carregador de boot. Para isso, é necessário iniciar o Sistema de Recuperação conforme descrito na *Seção 42.5.2, "Usando o sistema de recuperação"* e seguir as instruções na *Seção 42.5.2.4, "Modificando e reinstalando o carregador de boot"*.

Você também pode usar o Sistema de Recuperação para corrigir o carregador de boot da maneira a seguir. Inicialize a máquina da mídia de instalação. Na tela de boot, escolha *Mais > Inicializar Sistema Linux*. Selecione o disco que contém o sistema instalado e o kernel com as opções de kernel padrão.

Quando o sistema for inicializado, inicie o YaST e alterne para *Sistema > Carregador de boot*. Verifique se a opção *Gravar Código de Boot genérico no MBR* está habilitada e clique em *OK*. Esse procedimento corrige o carregador de boot corrompido sobregravando-o ou instala-o, se estiver ausente.

Outros motivos para a máquina não inicializar podem estar relacionadas ao BIOS:

Configurações do BIOS

Verifique o BIOS para obter referências sobre o disco rígido. O GRUB 2 pode não ser iniciado simplesmente porque o próprio disco rígido não foi encontrado com as configurações atuais do BIOS.

Ordem de boot do BIOS

Verifique se a ordem de inicialização do sistema inclui o disco rígido. Se a opção do disco rígido não tiver sido habilitada, o sistema talvez seja instalado de forma adequada, mas não seja inicializado quando o acesso ao disco rígido for necessário.

42.2.2 Não é exibido nenhum prompt nem tela de login

Isso costuma ocorrer após uma falha de atualização do kernel e é conhecido como *pânico do kernel* devido ao tipo de erro do console do sistema que às vezes se verifica no estágio final do processo. Se a máquina realmente tiver sido reinicializada após uma atualização de software, o objetivo imediato é reinicializá-la usando a versão antiga e segura do kernel do Linux e os arquivos associados. Isso pode ser feito na tela do carregador de boot GRUB 2 durante o processo de boot da seguinte forma:

1. Reinicialize o computador usando o botão de reinicialização ou desligue-o e ligue-o novamente.
2. Quando a tela de boot do GRUB 2 for exibida, selecione a entrada *Opções Avançadas* e escolha o kernel anterior no menu. A máquina será inicializada com a versão anterior do kernel e seus arquivos associados.
3. Após a conclusão do processo de boot, remova o kernel recém-instalado e, se necessário, defina a entrada de boot padrão como o kernel antigo usando o módulo *Carregador de Boot* do YaST. Para obter mais informações, consulte [Seção 18.3, “Configurando o carregador de boot com o YaST”](#). No entanto, isso talvez não seja necessário porque as ferramentas automatizadas de atualização normalmente o modificam durante o processo de rollback.
4. Reinicialize.

Se isso não resolver o problema, inicie o computador usando a mídia de instalação. Após a inicialização da máquina, prossiga com o [Passo 3](#).

42.2.3 Não há login gráfico

Se a máquina ligar, mas não for inicializada no gerenciador de login gráfico, evite problemas com a opção de destino do systemd padrão ou com a configuração do X Window System. Para verificar o destino padrão atual do systemd, execute o comando **`sudo systemctl get-default`**. Se o valor retornado *não* for `graphical.target`, execute o comando **`sudo systemctl isolate graphical.target`**. Se a tela gráfica de login for iniciada, efetue login e inicie o *YaST* > *Sistema* > *Services Manager* (Gerenciador de Serviços) e defina o *Default System Target* (Destino do Sistema Padrão) como *Graphical Interface* (Interface Gráfica). De agora em diante, o sistema deverá ser inicializado na tela gráfica de login.

Se a tela gráfica de login não for iniciada mesmo depois de ter sido inicializada ou alternada para o destino gráfico, a área de trabalho ou o software do X Window provavelmente foi mal configurado ou estava corrompido. Examine os arquivos de registro em `/var/log/Xorg.*.log` para ver as mensagens detalhadas do servidor X enquanto ele tentava iniciar. Se a área de trabalho falhar durante a inicialização, talvez ela registre mensagens de erro no diário do sistema que possam ser consultadas com o comando **`journalctl`** (consulte o [Capítulo 21, `journalctl`: Consultar o diário do systemd](#) para obter mais informações). Se essas mensagens de erro sugerirem um problema de configuração no servidor X, tente corrigi-lo. Se o sistema gráfico ainda não aparecer, reinstale a área de trabalho gráfica.

42.2.4 Não é possível montar a partição Btrfs raiz

Se uma partição `btrfs` raiz for corrompida, tente as seguintes opções:

- Monte a partição com a opção `-o recovery`.
- Se isso não funcionar, execute **`btrfs-zero-log`** na partição raiz.

42.2.5 Forçar verificação de partições raiz

Se a partição raiz for corrompida, use o parâmetro `forcefsck` no prompt de boot. Esse procedimento passa a opção `-f` (forçar) para o comando **`fsck`**.

42.2.6 Desabilitar a troca (swap) para habilitar a inicialização

Quando um dispositivo de troca não está disponível e o sistema não consegue habilitá-lo durante a inicialização, pode haver falha na inicialização. Tente desabilitar todos os dispositivos de troca anexando as seguintes opções à linha de comando do kernel:

```
systemd.device_wants_unit=off systemd.mask=swap.target
```

Você também pode tentar desabilitar dispositivos de troca específicos:

```
systemd.mask=dev-sda1.swap
```

42.2.7 O GRUB 2 falha durante a reinicialização em um sistema de boot duplo

Se o GRUB 2 falhar durante a reinicialização, desabilite a configuração Fast Boot no BIOS.

42.3 Problemas de login

Há problemas de login quando sua máquina é inicializada na tela de boas-vindas ou no prompt de login esperados, mas se recusa a aceitar o nome de usuário e a senha ou os aceita mas não se comporta apropriadamente (não inicia a área de trabalho gráfica, produz erros, passa para uma linha de comando, etc).

42.3.1 Falha nas combinações de nome de usuário e senha válidas

Isso geralmente ocorre quando o sistema está configurado para usar autenticação de rede ou serviços de diretório e, por algum motivo, não pode recuperar os resultados de seus servidores configurados. O usuário `root`, como o único usuário local, é o único que ainda pode efetuar login nessas máquinas. Veja a seguir alguns motivos comuns para uma máquina parecer funcional, mas não conseguir processar logins corretamente:

- A rede não está funcionando. Para obter mais instruções sobre isso, consulte a [Seção 42.4, “Problemas de rede”](#).
- O DNS não está funcionando no momento (o que impede o GNOME de trabalhar e o sistema de efetuar solicitações válidas a servidores seguros). Uma indicação de que esse é o caso é que a máquina leva muito tempo para responder a qualquer ação. Há mais informações a respeito desse tópico na [Seção 42.4, “Problemas de rede”](#).
- Se o sistema estiver configurado para usar Kerberos, o horário local do sistema poderá ter ultrapassado a variação aceita com o horário do servidor Kerberos (geralmente 300 segundos). Se o NTP (protocolo de horário de rede) não estiver funcionando de forma adequada ou os servidores NTP locais não estiverem funcionando, a autenticação do Kerberos não funcionará pois depende da sincronização comum do relógio na rede.
- A configuração de autenticação do sistema está definida incorretamente. Verifique se há erros de digitação ou ordem incorreta de diretivas nos arquivos de configuração PAM envolvidos. Para obter informações adicionais sobre o PAM e a sintaxe dos arquivos de configuração envolvidos, consulte o *Livro “Security and Hardening Guide”, Capítulo 2 “Authentication with PAM”*.
- A partição pessoal está criptografada. Há mais informações a respeito desse tópico na [Seção 42.3.3, “Falha de login na partição pessoal criptografada”](#).

Em todos os casos que não envolvem problemas de rede externos, a solução é reinicializar o sistema em um modo de usuário único e reparar a configuração antes de inicializar novamente no modo de operação e tentar efetuar login novamente. Para inicializar no modo de usuário único:

1. Reinicialize o sistema. A tela de boot é exibida e apresenta um prompt.
2. Pressione **Esc** para sair da splash screen e entrar no menu baseado em texto do GRUB 2.
3. Pressione **B** para entrar no editor do GRUB 2.

4. Adicione o seguinte parâmetro à linha com os parâmetros do kernel:

```
systemd.unit=rescue.target
```

5. Pressione **F10**.
6. Digite o nome de usuário e a senha de root.
7. Faça as mudanças necessárias.
8. Inicialize no modo completo multiusuário e de rede inserindo **systemctl isolate graphical.target** na linha de comando.

42.3.2 Nome de usuário e senha válidos que não são aceitos

Esse é o um dos problemas mais comuns que os usuários podem encontrar, pois há vários motivos pelos quais isso pode ocorrer. Dependendo de você usar gerenciamento e autenticação de usuário local ou autenticação em rede, as falhas de login ocorrem por motivos diferentes.

O gerenciamento de usuário local pode falhar pelos seguintes motivos:

- O usuário pode ter digitado a senha errada.
- O diretório pessoal do usuário que contém arquivos de configuração da área de trabalho está corrompido ou protegido contra gravação.
- Talvez haja problemas com o sistema X Window ao autenticar esse usuário específico, especialmente se o diretório pessoal do usuário tiver sido usado com outra distribuição do Linux antes da instalação da atual.

Para encontrar o motivo de uma falha de login local, proceda da seguinte maneira:

1. Verifique se o usuário memorizou a senha corretamente antes de começar a depurar todo o mecanismo de autenticação. Se o usuário não se lembrar da senha correta, use o módulo Gerenciamento de Usuário do YaST para mudar a senha dele. Fique atento à tecla **Caps Lock** e libere-a, se necessário.
2. Efetue login como root e consulte o diário do sistema com o comando **journalctl -e** para verificar se há mensagens de erro do processo de login e do PAM.

3. Tente efetuar login de um console (usando **Ctrl – Alt – F1**). Se esse procedimento for bem-sucedido, não será responsabilidade do PAM, pois é possível autenticar o usuário nessa máquina. Tente localizar quaisquer problemas com o X Window System ou com a área de trabalho do GNOME. Para obter mais informações, consulte a [Seção 42.3.4, “A área de trabalho do GNOME tem problemas”](#).
4. Se o diretório pessoal do usuário foi usado com outra distribuição Linux, remova o arquivo `Xauthority` no diretório do usuário. Use um login de console por meio de **Ctrl – Alt – F1** e execute `rm .Xauthority` como esse usuário. Isso deve eliminar problemas de autenticação X para o usuário. Tente o login gráfico novamente.
5. Se não for possível iniciar a área de trabalho devido a arquivos de configuração corrompidos, continue na [Seção 42.3.4, “A área de trabalho do GNOME tem problemas”](#).

Veja a seguir a lista dos motivos comuns de possível falha na autenticação de rede de um usuário específico em determinada máquina:

- O usuário pode ter digitado a senha errada.
- O nome de usuário existe nos arquivos de autenticação locais da máquina e também são fornecidos por um sistema de autenticação de rede, gerando conflitos.
- O diretório pessoal existe mas está corrompido ou não disponível. Talvez ele esteja protegido contra gravação ou está em um servidor inacessível no momento.
- O usuário não tem permissão para efetuar login neste host específico no sistema de autenticação.
- A máquina mudou os nomes de host, por algum motivo, e o usuário não tem permissão para efetuar login nesse host.
- A máquina não pode acessar o servidor de diretório ou o servidor de autenticação que contém as informações do usuário.
- Talvez haja problemas com o sistema X Window ao autenticar esse usuário específico, especialmente se o diretório pessoal do usuário tiver sido usado com outra distribuição do Linux antes da instalação da atual.

Para localizar a causa das falhas de login com a autenticação de rede, proceda da seguinte maneira:

1. Verifique se o usuário memorizou a senha corretamente antes de começar a depurar todo o mecanismo de autenticação.

2. Determine o servidor de diretórios usado pela máquina para autenticação e verifique se ele está funcionando e se comunicando corretamente com as outras máquinas.
3. Determine se o nome e a senha do usuário funcionam em outras máquinas para verificar se os dados de autenticação existem e são distribuídos apropriadamente.
4. Verifique se outro usuário pode efetuar login na máquina com comportamento incorreto. Se outro usuário ou o usuário `root` puder efetuar login sem dificuldade, efetue login e examine o diário do sistema com o comando `journalctl -e > arquivo`. Localize as marcações de horário que correspondem às tentativas de login e determine se o PAM produziu alguma mensagem de erro.
5. Tente efetuar login de um console (usando `Ctrl - Alt - F1`). Se der certo, o problema não é do PAM ou do servidor de diretórios no qual o diretório pessoal do usuário está hospedado, pois é possível autenticar o usuário nessa máquina. Tente localizar quaisquer problemas com o X Window System ou com a área de trabalho do GNOME. Para obter mais informações, consulte a *Seção 42.3.4, “A área de trabalho do GNOME tem problemas”*.
6. Se o diretório pessoal do usuário foi usado com outra distribuição Linux, remova o arquivo `Xauthority` no diretório do usuário. Use um login de console por meio de `Ctrl - Alt - F1` e execute `rm .Xauthority` como esse usuário. Isso deve eliminar problemas de autenticação X para o usuário. Tente o login gráfico novamente.
7. Se não for possível iniciar a área de trabalho devido a arquivos de configuração corrompidos, continue na *Seção 42.3.4, “A área de trabalho do GNOME tem problemas”*.

42.3.3 Falha de login na partição pessoal criptografada

Recomenda-se o uso de uma partição pessoal criptografada para laptops. Se você não puder efetuar login no seu laptop, o motivo geralmente é simples: a sua partição pode não estar desbloqueada.

Durante a inicialização, é necessário digitar a frase secreta para desbloquear a partição criptografada. Se você não a digitar, o processo de boot continuará, deixando a partição bloqueada.

Para desbloquear a partição criptografada, faça o seguinte:

1. Passe para o console de texto com `Ctrl - Alt - F1` .
2. Torne-se `root` .

3. Reinicie o processo de desbloqueio novamente com:

```
# systemctl restart home.mount
```

4. Digite sua frase secreta para desbloquear a partição criptografada.
5. Saia do console de texto e volte para a tela de login com **Alt** – **F7** .
6. Efetue login como de costume.

42.3.4 A área de trabalho do GNOME tem problemas

Se você tiver problemas com a área de trabalho do GNOME, há várias maneiras de solucioná-los no ambiente gráfico da área de trabalho. O procedimento recomendado descrito abaixo oferece a opção mais segura para corrigir uma área de trabalho do GNOME com problema.

PROCEDIMENTO 42.1: SOLUCIONANDO PROBLEMAS DO GNOME

1. Inicie o YaST e alterne para *Segurança e usuários*.
2. Abra a caixa de diálogo *Gerenciamento de usuários e grupos* e clique em *Adicionar*.
3. Preencha os campos obrigatórios e clique em *OK* para criar um usuário.
4. Efetue logout e login como o novo usuário. Isso gera um novo ambiente do GNOME.
5. Copie os subdiretórios individuais dos diretórios `~/.local/` e `~/.config/` da conta do usuário antiga para os respectivos diretórios da nova conta do usuário.
Efetue logout e login novamente como o novo usuário após cada operação de cópia para verificar se o GNOME ainda funciona corretamente.
6. Repita a etapa anterior até encontrar o arquivo de configuração que provoca o erro no GNOME.
7. Efetue login como o usuário antigo e mova o arquivo de configuração inválido para um local diferente. Efetue logout e login novamente como o usuário antigo.
8. Apague o usuário criado anteriormente.

42.4 Problemas de rede

Quaisquer problemas do seu sistema podem estar relacionados à rede, mesmo que inicialmente não transmitam essa impressão. Por exemplo, o motivo para um sistema não permitir o login de usuários pode ser algum tipo de problema de rede. Esta seção apresenta uma lista de verificação simples que você pode aplicar para identificar a causa de qualquer problema de rede encontrado.

PROCEDIMENTO 42.2: COMO IDENTIFICAR PROBLEMAS DE REDE

Ao verificar a conexão de rede da sua máquina, proceda da seguinte maneira:

1. Se você usa uma conexão Ethernet, verifique o hardware primeiro. Verifique se o cabo de rede está acoplado corretamente no computador e no roteador (ou hub etc). As luzes de controle próximas ao seu conector Ethernet normalmente estão ativas.
Se a conexão falhar, verifique se o cabo de rede funciona com outra máquina. Se funcionar, a placa de rede será a causa da falha. Se houver hubs ou switches incluídos na configuração da sua rede, eles também podem estar com defeito.
2. Se estiver usando uma conexão sem fio, verifique se o link sem fio pode ser estabelecido por outras máquinas. Do contrário, contate o administrador da rede wireless.
3. Após verificar sua conectividade de rede básica, tente descobrir qual serviço não está respondendo. Reúna as informações de endereço de todos os servidores de rede necessários na configuração. Procure-os no módulo YaST apropriado ou consulte o administrador de sistema. A lista a seguir mostra alguns servidores de rede típicos envolvidos em uma configuração juntamente com os sintomas de uma interrupção.

DNS (serviço de nomes)

Um serviço de nomes inoperante ou defeituoso afeta a funcionalidade da rede de várias maneiras. Se a máquina local depender de quaisquer servidores de rede para autenticação e esses servidores não forem encontrados devido a problemas de resolução de nome, os usuários não poderão nem efetuar login. As máquinas na rede gerenciadas por um servidor de nomes com defeito não podem “ver” umas às outras nem se comunicar.

NTP (serviço de horário)

Um serviço NTP defeituoso ou totalmente inoperante pode afetar a funcionalidade do servidor X e a autenticação Kerberos.

NFS (serviço de arquivos)

Se qualquer aplicativo precisar de dados armazenados em um diretório NFS montado, ele não poderá ser iniciado nem funcionar apropriadamente se esse serviço estiver inoperante ou mal configurado. No pior cenário possível, a configuração da área de trabalho pessoal de um usuário não será exibida se o seu diretório pessoal que contém o subdiretório `.gconf` não for encontrado por causa de um servidor NFS defeituoso.

Samba (serviço de arquivos)

Se qualquer aplicativo precisar de dados armazenados em um diretório em um servidor Samba defeituoso, ele não poderá ser iniciado nem funcionar apropriadamente.

NIS (gerenciamento de usuários)

Se o sistema SUSE Linux Enterprise Desktop usar um servidor NIS defeituoso para fornecer os dados dos usuários, os usuários não poderão efetuar login na máquina.

LDAP (gerenciamento de usuários)

Se o sistema SUSE Linux Enterprise Desktop usar um servidor LDAP defeituoso para fornecer os dados dos usuários, os usuários não poderão efetuar login na máquina.

Kerberos (autenticação)

A autenticação não funcionará e o login em qualquer máquina falhará.

CUPS (impressão de rede)

Os usuários não conseguem imprimir.

4. Verifique se os servidores de rede estão em execução e se a configuração de rede permite estabelecer uma conexão:



Importante: Limitações

O procedimento de depuração descrito abaixo aplica-se somente a uma configuração simples de servidor/cliente de rede que não envolva roteamento interno. Supõe-se que o servidor e o cliente integrem a mesma sub-rede sem necessidade de roteamento adicional.

- a. Use **ping** ENDEREÇO_IP/NOMEDEHOST (substitua pelo nome de host ou endereço IP do servidor) para verificar se cada um deles está ativo e respondendo à rede. Se esse comando for bem-sucedido, ele informará que o host que você estava procurando está em execução e o serviço de nomes da rede está configurado corretamente. Se o ping falhar com destination host unreachable, o seu sistema ou o servidor desejado não está configurado de forma adequada ou está inoperante. Verifique se o seu sistema está acessível executando **ping** endereço IP ou SEU_NOMEDEHOST de outra máquina. Se você conseguir acessar a sua máquina de outra máquina, significa que o servidor não está em execução ou não foi configurado corretamente. Se o ping falhar com unknown host (host desconhecido), o serviço de nomes não foi configurado corretamente ou o nome de host usado estava incorreto. Para obter mais verificações sobre esse assunto, consulte a [Passo 4.b](#). Se o ping ainda falhar, significará que a placa de rede não está configurada de forma correta ou o hardware de rede está defeituoso.
- b. Use **host** NOMEDEHOST para verificar se o nome de host do servidor ao qual você está tentando se conectar foi apropriadamente convertido em um endereço IP e vice-versa. Se esse comando retornar o endereço IP do host, significará que o serviço de nomes está funcionando. Se houver falha nesse comando **host**, verifique todos os arquivos de configuração de rede relacionados à resolução de nomes e de endereços no seu host:

/var/run/netconfig/resolv.conf

Este arquivo é usado para controlar o domínio e o servidor de nomes que você está usando no momento. Ele é um link simbólico para /run/netconfig/resolv.conf e costuma ser ajustado automaticamente pelo YaST ou DHCP. Verifique se esse arquivo tem a estrutura a seguir e se todos os endereços de rede e nomes de domínio estão corretos:

```
search FULLY_QUALIFIED_DOMAIN_NAME
nameserver IPADDRESS_OF_NAMESERVER
```

Este arquivo pode conter mais de um endereço de servidor de nomes, mas pelo menos um deles deve estar correto para fornecer a resolução de nomes para o seu host. Se necessário, ajuste o arquivo usando o módulo Configurações de Rede do YaST (guia Nome de host/DNS).

Se sua conexão de rede é executada por DHCP, habilite o DHCP para mudar o nome de host e as informações de serviço de nomes selecionando *Definir nome de host via DHCP* (pode ser definido globalmente para qualquer interface ou por interface) e *Atualizar Servidores de Nomes e Lista de Pesquisa via DHCP* no módulo Configurações de Rede do YaST (guia Nome de host/DNS).

/etc/nsswitch.conf

Este arquivo informa ao Linux onde procurar informações de serviço de nomes. Ele deve ter a seguinte aparência:

```
...
hosts: files dns
networks: files dns
...
```

A entrada dns é essencial. Ela informa ao Linux para usar um servidor de nomes externo. Normalmente, essas entradas são gerenciadas automaticamente pelo YaST, mas convém verificar.

Se todas as entradas relevantes no host estiverem corretas, deixe o seu administrador de sistema verificar a configuração do servidor DNS para obter as informações de zona corretas. Se você verificou se a configuração DNS do seu host e o servidor DNS estão corretos, continue verificando a configuração da rede e do dispositivo de rede.

- c. Se o sistema não puder estabelecer uma conexão a um servidor de redes e você excluiu problemas de serviço de nomes da lista de possíveis responsáveis, verifique a configuração da placa de rede.

Use o comando **ip addr show DISPOSITIVO_DE_REDE** para verificar se esse dispositivo foi configurado apropriadamente. Verifique se o endereço inet com a máscara de rede (/MÁSCARA) está corretamente configurado. Um erro no endereço IP ou um bit ausente na máscara de rede inutilizam a configuração de rede. Se necessário, execute essa verificação no servidor também.

- d. Se o hardware de rede e o serviço de nomes estiverem configurados apropriadamente e em execução, mas algumas conexões de rede externas ainda tiverem longos tempos de espera ou falharem totalmente, use **traceroute NOME_DE_DOMÍNIO_COMPLETO_E_QUALIFICADO** (executado como root) para controlar a rota de rede tomada pelas solicitações. Esse comando lista qualquer gateway (hop) que uma solicitação da sua máquina transmitir no caminho ao seu

destino. Ele lista o tempo de resposta de cada salto e se esse salto é acessível. Use uma combinação de traceroute e ping para identificar o responsável e informar aos administradores.

Após identificar a causa do problema de rede, você mesmo poderá resolvê-lo (se o problema estiver na sua máquina) ou informar os administradores do sistema da rede sobre suas descobertas para que eles possam reconfigurar os serviços ou reparar os sistemas necessários.

42.4.1 Problemas no NetworkManager

Se você tiver problema com a conectividade da rede, restrinja-a conforme descrito no *Procedimento 42.2, “Como identificar problemas de rede”*. Se tudo indicar que a culpa é do NetworkManager, faça o seguinte para obter os registros com dicas sobre o motivo da falha do NetworkManager:

1. Abra um shell e efetue login como `root`.

2. Reinicie o NetworkManager:

```
> sudo systemctl restart NetworkManager
```

3. Abra uma página da Web, por exemplo <http://www.opensuse.org>, como usuário normal para ver se você consegue se conectar.

4. Colete as informações sobre o estado do NetworkManager em `/var/log/NetworkManager`.

Para obter maiores informações sobre o NetworkManager, consulte o *Capítulo 31, Usando o NetworkManager*.

42.5 Problemas de dados

Problemas de dados ocorrem quando a máquina pode ou não inicializar corretamente, mas em ambos os casos, está claro que há dados corrompidos no sistema e que o sistema precisa ser recuperado. Essas situações exigem um backup dos seus dados críticos, permitindo que você recupere o estado anterior à falha do sistema.

42.5.1 Gerenciando imagens de partição

Às vezes é necessário fazer um backup de uma partição inteira ou até do disco rígido. O Linux possui a ferramenta **dd**, capaz de criar uma cópia exata do seu disco. Combinada ao **gzip**, faz você economizar espaço.

PROCEDIMENTO 42.3: FAZENDO BACKUP E RESTAURANDO DISCOS RÍGIDOS

1. Inicie um Shell como usuário root.
2. Selecione o seu dispositivo de origem. Normalmente, ele assemelha-se a /dev/sda (com a etiqueta SOURCE).
3. Indique onde deseja armazenar sua imagem (com a etiqueta CAMINHO_BACKUP). Esse local deverá ser diferente do dispositivo de origem. Em outras palavras: se você fizer backup de /dev/sda, seu arquivo de imagem poderá não ser armazenado em /dev/sda.
4. Execute os comandos para criar um arquivo de imagem compactado:

```
# dd if=/dev/SOURCE | gzip > /BACKUP_PATH/image.gz
```

5. Recupere o disco rígido usando os seguintes comandos:

```
# gzip -dc /BACKUP_PATH/image.gz | dd of=/dev/SOURCE
```

Se você precisa fazer backup apenas de uma partição, substitua o marcador ORIGEM pela sua partição. Nesse caso, o seu arquivo de imagem pode usar o mesmo disco rígido, só que em outra partição.

42.5.2 Usando o sistema de recuperação

Há vários motivos para um sistema não ser inicializado ou executado apropriadamente. Um sistema de arquivos corrompido após uma falha do sistema, arquivos de configuração corrompidos ou uma configuração de carregador de boot corrompida são os mais comuns.

Para ajudá-lo a resolver esse tipo de situação, o SUSE Linux Enterprise Desktop oferece um sistema de recuperação que você pode inicializar. que consiste em um pequeno sistema Linux que pode ser carregado em um disco de RAM e montado como um sistema de arquivos raiz, permitindo acesso externo às partições Linux. Com o sistema de recuperação, você pode recuperar ou modificar qualquer aspecto importante do sistema.

- Manipule qualquer tipo de arquivo de configuração.
- Verifique se há defeitos no sistema de arquivos e inicie processos de reparo automáticos.
- Acesse o sistema instalado em um ambiente de “mudança de raiz”.
- Verifique, modifique e reinstale a configuração do carregador de boot.
- Recuperar-se de um driver de dispositivo instalado incorretamente ou um kernel inutilizável.
- Redimensione as partições usando o comando parted. Encontre mais informações sobre esta ferramenta no site GNU Parted na Web <http://www.gnu.org/software/parted/parted.html>.

É possível carregar o sistema de recuperação a partir de várias origens e locais. A opção mais simples é inicializar o sistema de recuperação a partir do meio original de instalação.

1. Insira o meio de instalação na unidade de DVD.
2. Reinicialize o sistema.
3. Na tela de boot, pressione **F4** e escolha *DVD-ROM*. Em seguida, escolha *Sistema de Recuperação* no menu principal.
4. Digite root no prompt Rescue: . Não é necessário inserir uma senha.

Se a sua configuração de hardware não inclui uma unidade de DVD, você poderá inicializar o sistema de recuperação a partir de uma fonte na rede. O seguinte exemplo aplica-se a um cenário de boot remoto. Se você estiver usando outro meio de boot, como um DVD, modifique o arquivo info adequadamente e inicialize como em uma instalação normal.

1. Insira a configuração do seu boot PXE e adicione as linhas install=PROTOCOLO://FONTE_INST e rescue=1 . Se precisar iniciar o sistema de recuperação, prefira repair=1 . Como em uma instalação normal, PROTOCOL significa qualquer um dos protocolos de rede suportados (NFS, HTTP, FTP etc.) e INSTSOURCE é o caminho da origem de instalação da rede.
2. Inicialize o sistema usando “Wake on LAN”, conforme descrito na *Livro “Deployment Guide”, Capítulo 13 “Preparing network boot environment”, Seção 13.5 “Using wake-on-LAN for remote wakeups”*.

3. Digite `root` no prompt `Rescue:`. Não é necessário inserir uma senha.

Ao acessar o sistema de recuperação, você pode usar os consoles virtuais acessando-os por meio das teclas `Alt – F1` a `Alt – F6`.

Um shell e outros utilitários eficientes, como o programa de montagem, estão disponíveis no diretório `/bin`. O diretório `/sbin` contém utilitários de arquivo e rede importantes para análise e conserto do sistema de arquivos. Esse diretório também inclui os binários mais importantes para a manutenção do sistema, por exemplo, `fdisk`, `mkfs`, `mkswap`, `mount`, `shutdown`; e `ip` e `ss` para a manutenção da rede. O diretório `/usr/bin` contém o vi editor, find, less e SSH.

Para ver as mensagens do sistema, use o comando `dmesg` ou exiba o registro do sistema com `journalctl`.

42.5.2.1 Verificando e manipulando arquivos de configuração

Como exemplo de uma configuração que possa ser corrigida por meio do sistema de recuperação, suponha que você tenha um arquivo de configuração defeituoso que impeça a inicialização adequada do sistema. Você pode corrigir isso usando o sistema de recuperação.

Para manipular um arquivo de configuração, faça o seguinte:

1. Inicie o sistema de recuperação usando um dos métodos descritos acima.
2. Para montar uma sistema de arquivos raiz localizado em `/dev/sda6` para o sistema de recuperação, use o seguinte comando:

```
> sudo mount /dev/sda6 /mnt
```

Agora, todos os diretórios do sistema estão localizados em `/mnt`

3. Mude o diretório para o sistema de arquivos raiz montado:

```
> sudo cd /mnt
```

4. Abra o arquivo de configuração problemático no editor vi. Ajuste e grave a configuração.
5. Desmonte o sistema de arquivos raiz no sistema de recuperação:

```
> sudo umount /mnt
```

6. Reinicialize a máquina.

42.5.2.2 Reparando e verificando sistemas de arquivos

Geralmente, não é possível reparar sistemas de arquivos em um sistema em execução. Se você tiver sérios problemas, talvez não consiga montar seu sistema de arquivos raiz e a inicialização do sistema poderá ser encerrada com “kernel panic”. Nesse caso, a única maneira será reparar o sistema externamente. O sistema inclui os utilitários para verificar e consertar os sistemas de arquivos `btrfs`, `ext2`, `ext3`, `ext4`, `xfs`, `dosfs` e `vfat`. Procure pelo comando `fsck.SISTEMADEARQUIVOS`. Por exemplo, se você precisar de uma verificação do sistema de arquivos `btrfs`, use `fsck.btrfs`.

42.5.2.3 Acessando o sistema instalado

Se você precisa acessar o sistema instalado do sistema de recuperação, faça isso em um ambiente *raiz de mudança*. Por exemplo, para modificar a configuração do carregador de boot ou executar um utilitário de configuração de hardware.

Para configurar um ambiente de mudança de raiz com base no sistema instalado, faça o seguinte:

1. Dica: Importar grupos de volume LVM

Se você usa uma configuração LVM (consulte o *Livro “Deployment Guide”, Capítulo 6 “Expert Partitioner”, Seção 6.2 “LVM configuration”* para obter mais detalhes gerais), importe todos os grupos de volume existentes para poder localizar e montar o(s) dispositivo(s):

```
rootvgimport -a
```

Execute `lsblk` para verificar qual nó corresponde à partição raiz. No exemplo, o nó é `/dev/sda2`:

```
> lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINT
sda          8:0    0 149,1G  0 disk
├─sda1       8:1    0    2G  0 part  [SWAP]
├─sda2       8:2    0   20G  0 part  /
└─sda3       8:3    0  127G  0 part
   └─cr_home 254:0    0  127G  0 crypt /home
```


2. Monte a partição raiz pelo sistema instalado:

```
> sudo mount /dev/sda2 /mnt
```

3. Monte as partições /proc, /dev e /sys:

```
> sudo mount -t proc none /mnt/proc  
> sudo mount --rbind /dev /mnt/dev  
> sudo mount --rbind /sys /mnt/sys
```

4. Agora, você pode “mudar a raiz” para o novo ambiente, mantendo o shell bash:

```
> chroot /mnt /bin/bash
```

5. Por fim, monte as partições restantes no sistema instalado:

```
> mount -a
```

6. Agora, você tem acesso ao sistema instalado. Antes de reinicializar o sistema, desmonte as partições com umount -a e saia do ambiente de “mudança de raiz” com exit.



Atenção: Limitações

Embora você tenha acesso total aos arquivos e aplicativos do sistema instalado, há algumas limitações. O kernel em execução é o que foi inicializado com o sistema de recuperação, e não com o ambiente de mudança de raiz. Ele suporta apenas o hardware essencial, e não é possível adicionar módulos do kernel do sistema instalado, a menos que as versões do kernel sejam idênticas. Verifique sempre a versão do kernel em execução (recuperação) com uname -r e, em seguida, descubra se existe um subdiretório correspondente no diretório /lib/modules no ambiente raiz de mudança. Em caso positivo, você poderá usar os módulos instalados, do contrário, precisará fornecer as versões corretas em outra mídia, como um disco flash. Na maioria das vezes, a versão do kernel de recuperação é diferente da que está instalada, portanto, não é possível simplesmente acessar a placa de som, por exemplo. Também não será possível iniciar uma interface gráfica de usuário.

Observe também que você sai do ambiente de “mudança de raiz” ao percorrer o console com as teclas **Alt + F1** a **Alt + F6**.

42.5.2.4 Modificando e reinstalando o carregador de boot

Às vezes, não é possível reinicializar um sistema porque a configuração do carregador de boot está corrompida. As rotinas de inicialização não podem, por exemplo, converter unidades físicas em locais reais no sistema de arquivos Linux sem um carregador de boot ativo.

Para verificar a configuração do carregador de boot e reinstalá-lo, faça o seguinte:

1. Execute as etapas necessárias para acessar o sistema instalado como descrito em [Seção 42.5.2.3, “Acessando o sistema instalado”](#).
2. Verifique se o carregador de boot GRUB 2 está instalado no sistema. Se não estiver, instale o pacote `grub2` e execute

```
> sudo grub2-install /dev/sda
```

3. Verifique se os arquivos a seguir estão configurados corretamente de acordo com os princípios de configuração do GRUB 2, descritos no [Capítulo 18, Carregador de boot GRUB 2](#), e aplique as correções, se necessário.

- `/etc/default/grub`
- `/boot/grub2/device.map` (arquivo opcional, presente apenas se criado manualmente)
- `/boot/grub2/grub.cfg` (arquivo gerado, não o edite)
- `/etc/sysconfig/bootloader`

4. Reinstale o carregador de boot usando a seguinte sequência de comandos:

```
> sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

5. Desmonte as partições, efetue logout do ambiente de “mudança de root” e reinicialize o sistema:

```
> umount -a  
exit  
reboot
```

42.5.2.5 Corrigindo a instalação do kernel

Uma atualização do kernel pode introduzir um novo bug capaz de afetar a operação do sistema. Por exemplo, um driver de parte do hardware no sistema pode estar com falha, o que o impede de acessá-lo e usá-lo. Nesse caso, reverta para o último kernel em funcionamento (se disponível no sistema) ou instale o kernel original pela mídia de instalação.



Dica: Como manter os últimos kernels após a atualização

Para evitar falhas na inicialização após uma atualização do kernel com defeito, use o recurso multiversão do kernel e indique ao `libzypp` quais kernels deseja manter após a atualização.

Por exemplo, para sempre manter os dois últimos kernels e o kernel atual em execução, adicione

```
multiversion.kernels = latest,latest-1,running
```

ao arquivo `/etc/zypp/zypp.conf`. Consulte a [Capítulo 27, Instalando várias versões do kernel](#) para obter mais informações.

Um caso semelhante é quando você precisa reinstalar ou atualizar um driver com defeito em um dispositivo não suportado pelo SUSE Linux Enterprise Desktop. Por exemplo, quando o fornecedor do hardware utiliza determinado dispositivo, como um controlador RAID de hardware, que precisa de um driver binário para ser reconhecido pelo sistema operacional. Normalmente, o fornecedor lança um DUD (Driver Update Disk — Disco de Atualização do Driver) com a versão corrigida ou atualizada do driver necessário.

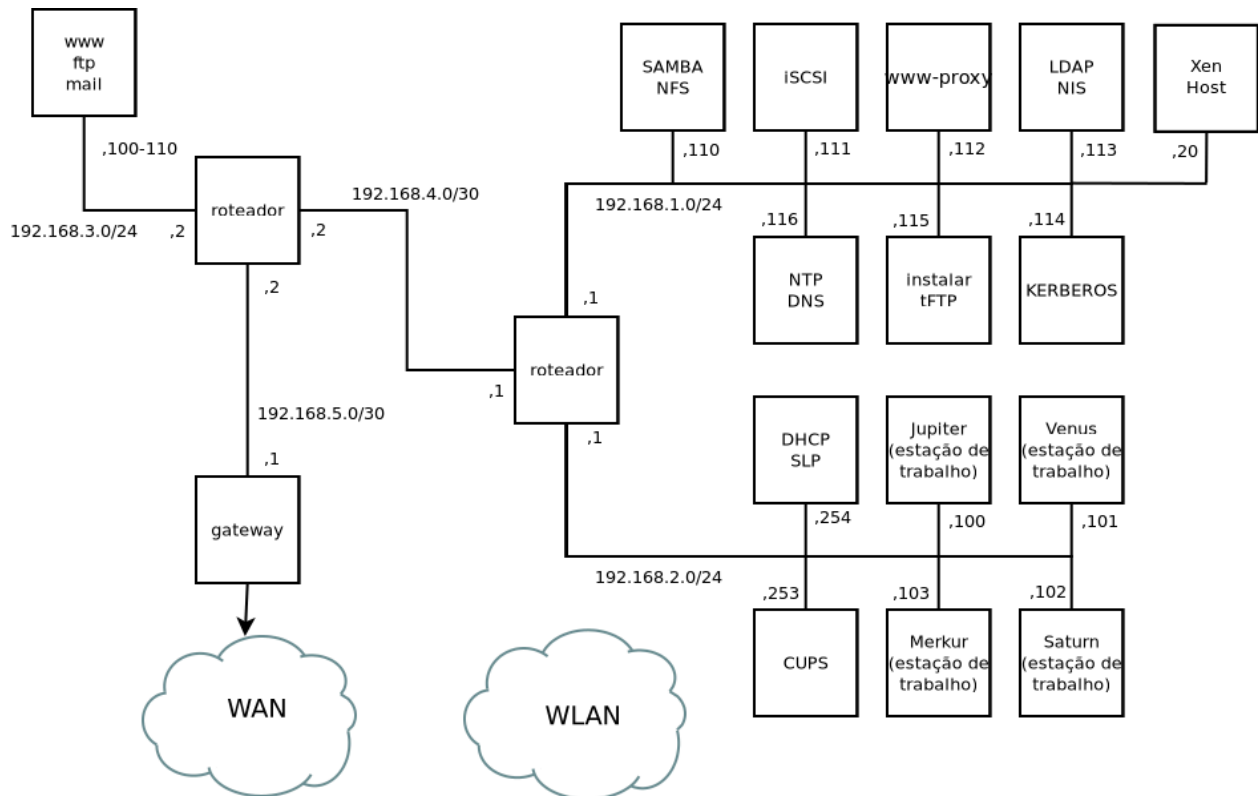
Nos dois casos, você precisa acessar o sistema instalado no modo de recuperação e corrigir o problema relacionado ao kernel; do contrário, o sistema poderá não ser inicializado corretamente:

1. Inicialize da mídia de instalação do SUSE Linux Enterprise Desktop.
2. Se você estiver recuperando após uma atualização do kernel com defeito, ignore esta etapa. Se precisar usar um disco de atualização de driver (DUD), pressione **F6** para carregar a atualização de driver depois que o menu de boot aparecer e, em seguida, escolha o caminho ou URL para a atualização de driver e confirme clicando em *Sim*.
3. Escolha *Sistema de Recuperação* no menu de boot e pressione **Enter**. Se você usar o DUD, será solicitado a especificar o local em que a atualização de driver está armazenada.

4. Digite `root` no prompt `Rescue:` . Não é necessário inserir uma senha.
5. Monte manualmente o sistema de destino e “mude a raiz” para o novo ambiente. Para obter mais informações, consulte a [Seção 42.5.2.3, “Acessando o sistema instalado”](#).
6. Se você usar o DUD, instale/reinstale/atualize o pacote de driver do dispositivo com defeito. Sempre verifique se a versão do kernel instalada corresponde exatamente à versão do driver que está instalando.
Se você estiver corrigindo uma instalação de atualização do kernel com defeito, poderá instalar o kernel original da mídia de instalação com o procedimento a seguir.
 - a. Identifique o seu dispositivo de DVD com `hwinfo --cdrom` e monte-o com `mount /dev/sr0 /mnt`.
 - b. Navegue até o diretório em que os arquivos do kernel estão armazenados no DVD, por exemplo, `cd /mnt/suse/x86_64/`.
 - c. Instale os pacotes necessários `kernel-*`, `kernel-*-base` e `kernel-*-extra` de acordo com o seu tipo, usando o comando `rpm -i`.
7. Atualize os arquivos de configuração e reinicialize o carregador de boot, se necessário. Para obter mais informações, consulte a [Seção 42.5.2.4, “Modificando e reinstalando o carregador de boot”](#).
8. Remova a mídia inicializável da unidade do sistema e reinicialize-o.

A Rede de exemplo

Este exemplo de rede é usado em todos os capítulos relacionados à rede na documentação do SUSE® Linux Enterprise Desktop.



B GNU licenses

This appendix contains the GNU Free Documentation License version 1.2.

GNU Free Documentation License

Copyright (C) 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non-commercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or

XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or non-commercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <https://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU
Free Documentation License".
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.