

Parte II: Núcleo 2

Capítulo 6

Sistemas operacionais

Este capítulo aborda os objetivos do exame 11 A+ 220-1102 relacionados a sistemas operacionais, com foco nos recursos, ferramentas, versões, ferramentas de linha de comando e configuração e instalação do Microsoft Windows, bem como sistemas operacionais macOS e Linux. Esses objetivos podem abranger 31% das questões do exame:

- **Núcleo 2 (220-1102): Objetivo 1.1:** Identificar os recursos básicos das edições do Microsoft Windows.
- **Núcleo 2 (220-1102): Objetivo 1.2:** Dado um cenário, use a ferramenta de linha de comando apropriada da Microsoft.
- **Núcleo 2 (220-1102): Objetivo 1.3:** Dado um cenário, use recursos e ferramentas do sistema operacional (SO) Microsoft Windows 10.
- **Núcleo 2 (220-1102): Objetivo 1.4:** Dado um cenário, use o utilitário apropriado do Painel de Controle do Microsoft Windows 10.
- **Núcleo 2 (220-1102): Objetivo 1.5:** Dado um cenário, use as configurações apropriadas do Windows.
- **Núcleo 2 (220-1102): Objetivo 1.6:** Dado um cenário, configurar os recursos de rede do Microsoft Windows em um cliente/desktop.
- **Núcleo 2 (220-1102): Objetivo 1.7:** Dado um cenário, aplique os conceitos de instalação e configuração de aplicativos.
- **Núcleo 2 (220-1102): Objetivo 1.8:** Explicar os tipos comuns de SO e suas finalidades.
- **Núcleo 2 (220-1102): Objetivo 1.9:** Dado um cenário, execute instalações e atualizações de SO em um ambiente de SO diversificado.
- **Núcleo 2 (220-1102): Objetivo 1.10:** Identificar recursos e ferramentas comuns do sistema operacional macOS/desktop.

- **Núcleo 2 (220-1102): Objetivo 1.11:** Identificar recursos e ferramentas comuns do SO cliente/desktop Linux.

Muitas versões do Windows foram usadas ao longo dos anos, cada uma trazendo mudanças nos recursos e aparências, mas todas as versões usaram métodos de instalação semelhantes. Para o exame 220-1102 A+, o foco está no Windows 10, com as versões anteriores sendo preteridas para o status legado. O Windows 11 não é especificamente mencionado nos objetivos, embora edições futuras de questões de exames possam se referir a ele. Conforme observado nos objetivos do exame A+:

Versões do Microsoft Windows que não são o fim do Suporte Mainstream (conforme determinado pela Microsoft), até e incluindo o Windows 11, são áreas de conteúdo pretendido da certificação. Assim, os objetivos em que uma versão específica do Microsoft Windows não é indicada no título do objetivo principal podem incluir conteúdo relacionado ao Windows 10 e Windows 11, no que se refere à função do trabalho.

No entanto, uma descrição das principais diferenças entre o Windows 10 e o 11 é garantida e incluída neste capítulo.

Neste capítulo, você é apresentado aos recursos e muitas opções disponíveis para instalar o Windows 10 em sistemas individuais e para implantação em vários computadores. O capítulo também aborda alguns dos recursos e ferramentas importantes do macOS e do Linux.

“Eu já sei disso?” Questionário

O “Eu já sei disso?” questionário permite avaliar se você precisa ler o capítulo inteiro. A [Tabela 6-1](#) lista os principais títulos deste capítulo e a seção “Eu já sei disso?” perguntas do questionário que cobrem o material desses títulos para que você possa avaliar seu conhecimento nessas áreas específicas. As respostas para a pergunta “Eu já sei disso?” questionário aparecem no Apêndice A, “Respostas para a pergunta ‘Eu já sei disso?’ Questionários e perguntas de revisão.

Tabela 6-1 “Eu já sei disso?” Mapeamento de seção para pergunta

Seção de Tópicos Fundamentais	Perguntas
Recursos básicos das edições do Microsoft Windows	1

Seção de Tópicos Fundamentais	Perguntas
Ferramentas de linha de comando da Microsoft	2, 4
Recursos do sistema operacional (SO) do Microsoft Windows 10 e 3	
Ferramentas	
Utilitários do Painel de Controle do Windows 10	5, 6
Configurações do Windows	5
Recursos de rede do Windows em um cliente/área de trabalho	7
Conceitos de instalação e configuração	8
Compreendendo os tipos comuns de sistema operacional	1
Instalações e atualizações do sistema operacional em um sistema operacional diverso	9
Ambiente	
Recursos e ferramentas comuns do sistema operacional macOS/Desktop	9, 10
Recursos e ferramentas comuns do cliente/desktop Linux	9
SO	

CUIDADO

O objetivo da autoavaliação é avaliar seu domínio dos tópicos deste capítulo. Se você não souber a resposta a uma pergunta ou tiver certeza apenas parcial da resposta, marque essa pergunta como errada para fins de autoavaliação. Dar a si mesmo crédito por uma resposta que você adivinhou corretamente distorce os resultados de sua autoavaliação e pode lhe dar uma falsa sensação de segurança.

1. Qual é o caso do FAT32?

- a.** **uma.** Ele usa permissões de arquivo.
- b.** Tem um tamanho máximo de arquivo de 8 GB.
- c.** Arquivos corrompidos podem ser reparados.
- d.** Funciona em computadores macOS.

2. Quais das opções a seguir são ferramentas de linha de comando no Windows 10?

(Escolha todas as que se

aplicam.) **a.** Páginas **b.**

Aplicativo de prompt de comando

c. PowerShell

d. Gerenciador Winscript

3. Qual operação requer a ajuda de um utilitário como o Microsoft

Kit de ferramentas de

implantação? **uma.** instalação de rede

b. instalação de inicialização múltipla

c. instalação autônoma

d. instalação limpa

4. Qual é o nome do modo que você insere ao executar o prompt de comando como

administrador? **uma.** modo supervisor

b. Modo elevado

c. modo de energia

d. Modo de ação

5. Qual das opções a seguir não é uma ferramenta administrativa da Microsoft?

uma. Monitor de desempenho

b. Otimizador de RAM

c. Agendador de tarefas

d. Gerenciamento de impressão

6. Quais dos seguintes são utilitários do Painel de controle? (Escolha tudo isso

aplicar.)

a. Sistema **b.**

Opções da Internet **c.**

Dispositivos e Impressoras

d. Contas de usuário

7. Qual é o nome do processo que envolve tornar uma pasta compartilhada acessível selecionando uma letra de unidade em um computador cliente?

a. Tunelamento

b. Compartilhar

apontando **c.**

Mapeamento **d.** Navegação

8. Quais são as duas tarefas definidas nas configurações de propriedades da placa de rede?

(Escolha duas.) **a.**

Half-duplex ou full duplex **b.** Wake-on-LAN

c. Exceções de firewall

d. acesso VPN

9. Quando um aplicativo não está funcionando e não pode ser fechado corretamente, o que comandos que você pode usar para encerrar o aplicativo no macOS e no Linux? (Escolha um para cada sistema operacional.) **a.** encerrar

b. Forçar Encerramento

c. matar

d. expirar

10. O que é a Máquina do Tempo?

a. Um utilitário de clock que é novo no Windows 10 **b.** Um

utilitário de backup no Linux **c.** Um utilitário de backup macOS **d.**

Um utilitário de backup que é novo no Windows 10

Tópicos Fundamentais

Recursos básicos das edições do Microsoft Windows

220-1102:
Exam

220-1102: Objetivo 1.1: Identificar os recursos básicos das edições do Microsoft Windows.

O Windows 11 foi lançado no segundo semestre de 2021 como uma forma de os usuários do Windows acessarem os serviços e produtos da Microsoft com maior nível de desempenho geral. Embora a experiência do usuário seja visualmente diferente e a experiência da rede seja mais uniforme, a maioria das configurações das funções principais são semelhantes, se não as mesmas. Conhecer o sistema operacional Windows 10 é fundamental para entender os fundamentos do Windows 11.

Edições do Windows 10

O Windows 10 e 11 são o padrão atual para os sistemas operacionais da Microsoft. Quatro versões do Windows 10 são descritas nesta seção:

- **Windows 10 Home:** Esta é a versão de desktop mais básica, com recursos que a maioria dos usuários domésticos precisa. Ele é capaz de ingressar em um pequeno grupo de trabalho doméstico e compartilhar recursos como impressoras, mas não é capaz de ingressar em grandes domínios gerenciados pelo local de trabalho. O Windows 10 Home é mais comumente encontrado pré-instalado por um fabricante de equipamento original (OEM), como Dell ou HP.
- **Windows 10 Pro:** Pro é a versão mais diferente das muitas versões do Windows. O Pro possui todas as funcionalidades do Home, além de recursos adicionais de segurança e gerenciamento encontrados em redes institucionais. Isso inclui Active Directory para gerenciamento de rede, BitLocker e Área de Trabalho Remota. Assim como o Home, o Windows 10 Pro pode ser enviado por OEMs.
- **Windows 10 Pro for Workstations:** as principais diferenças entre o Pro e o Pro for Workstations estão na robustez e no licenciamento. O Pro for Workstations foi projetado para funcionar com computadores de alta potência com chipsets avançados que podem lidar com cargas pesadas de processamento. Em vez de usar uma instalação OEM, o licenciamento deve ser adquirido da Microsoft.
- **Windows 10 Enterprise:** esta versão do Windows 10 possui todos os recursos das outras versões, além de gerenciamento de rede adicionado

e ferramentas de segurança projetadas para profissionais de TI que gerenciam redes de nível empresarial.

A Tabela 6-2 descreve as diferentes versões e a disponibilidade de recursos do exame CompTIA A+ Core 2.



Tabela 6-2 Edições e recursos do Windows 10

Windows 10	Home Pro		Pro para Estações de trabalho	Empreendimento
Edição: ▾				
Recursos ↓				
Acesso de domínio x grupo de trabalho	Grupo de trabalho	Grupo de trabalho ou domínio	Domínio	Domínio
Área de Trabalho	Não	Não	Sim	Sim
Estilos/Controle				
RDP	Somente cliente	Host e cliente	Hospedeiro e cliente	Hospedeiro e cliente
Mínimo RAM 1 GB		2 GB	2 GB	2 GB
BitLocker	Não	Sim	Sim	Sim
gpedit.msc	Não	Sim	Sim	Sim

Diferenças de recursos

Acesso de domínio x grupo de trabalho

A principal diferença entre **acesso de domínio** e computadores de **grupo** de trabalho é como eles são gerenciados. No Windows 10, todos os computadores são padronizados para um grupo de trabalho até ingressarem em um domínio. Os computadores de domínio geralmente são computadores de trabalho gerenciados por um administrador de rede. Os computadores de grupo de trabalho geralmente são computadores domésticos que são pares de outros computadores em uma pequena rede doméstica que pode compartilhar arquivos e impressoras.

Estilos de Área de Trabalho/Interface do Usuário

As versões do Windows 10 vêm com recursos de interface semelhantes, incluindo a opção Visualização de Tarefas (Windows+Tab ou selecionando-a na barra de tarefas). As áreas de trabalho e o papel de parede podem ser aprimorados com o Bing Wallpaper, e os recursos de acesso para deficientes são encontrados em ambos. Quando o computador está sob o controle de um domínio, a experiência pode ser diferente porque um administrador pode usar políticas para limitar áreas de trabalho e outros recursos.

Conexão de Área de Trabalho Remota e Assistência Remota

Para facilitar as conexões com computadores remotos e permitir o controle remoto total, a Microsoft usa o programa Conexão de Área de Trabalho Remota, baseado no [**Protocolo de Área de Trabalho Remota \(RDP\)**](#).

A Área de Trabalho Remota também inclui Assistência Remota, que permite aos usuários convidar um técnico para visualizar sua área de trabalho, na esperança de que o técnico possa corrigir quaisquer problemas encontrados.

Memória de acesso aleatório (RAM)

O Windows 10 requer 1 GB de RAM para uma instalação de 32 bits e 2 GB para uma instalação de 64 bits. Estes são mínimos; dependendo do software instalado e da finalidade do computador, recomenda-se mais RAM.

BitLocker

[**BitLocker**](#) é um utilitário de criptografia de dados que criptografa discos rígidos para maior segurança. Ele criptografa todos os dados, incluindo arquivos pessoais e do sistema. Um programa complementar, o BitLocker To Go, criptografa discos removíveis e unidades USB. O Capítulo 7, “Segurança”, aborda o BitLocker e o BitLocker To Go.

Editor de política de grupo

A Diretiva de Grupo é uma ferramenta para controlar as configurações em um computador autônomo ou em um grupo de computadores em rede. Um administrador de rede pode definir e controlar quase todas as configurações de uma rede usando o Active Directory. A [**Figura 6-1**](#) descreve a saída do comando [**gpedit.msc**](#), mostrando o [**Editor de Diretiva de Grupo**](#) Local em um computador em rede. O Editor de Diretiva de Grupo normalmente não está disponível para o usuário do Windows 10 Home; o comando normalmente retorna uma resposta “gpedit.msc não encontrado”. No entanto, os usuários podem baixar arquivos não oficiais

produtos de fontes não Microsoft e, em seguida, configurar o gerenciamento de configurações.

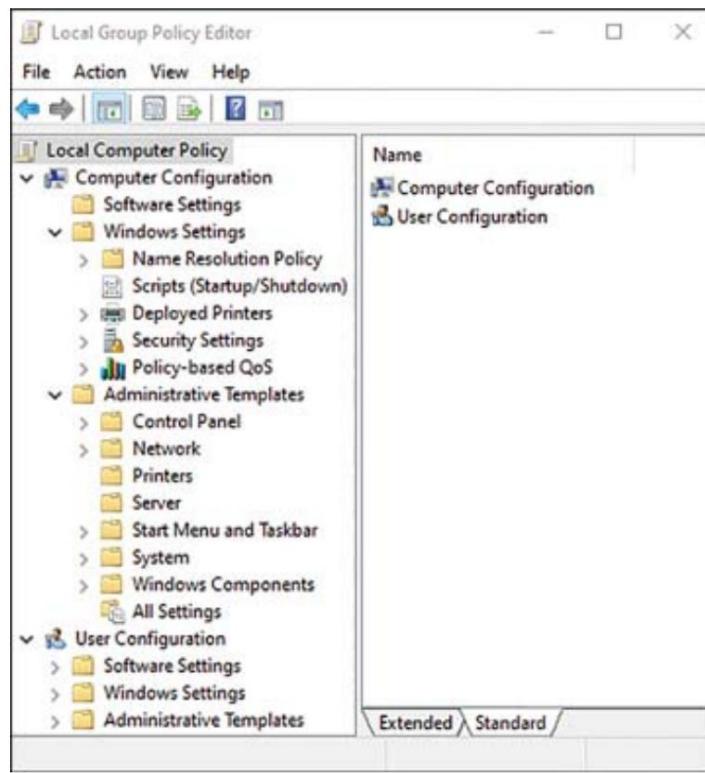


Figura 6-1 Editor de Diretiva de Grupo Local

Caminhos de

atualização As atualizações no local envolvem a atualização das edições do Windows, mantendo os dados, aplicativos e preferências do usuário intactos. A [Tabela 6-3](#) mostra as edições do Windows 10 e os métodos de atualização. A versão mais antiga do sistema operacional Windows 10 permanece em vigor e seu instalador é usado para substituir todos os arquivos do sistema operacional pela nova edição, deixando aplicativos e outras configurações.

Tabela 6-3 Edições do Windows 10 e métodos de atualização compatíveis

Edição do Windows 10:	Comando	produtos	Comprar licença na Microsoft Store
Caminho de atualização para:	ferramentas de linha	Chave	
Home to Pro	não	Sim	Sim

Edição do Windows 10: Caminho de atualização para:	Comando ferramentas de linha	produtos Chave	Comprar licença na Microsoft Store
Pro para Pro para Estações de trabalho	Sim, sem reinicialização	Sim- não reinício	Sim, sem reinicialização
Pro to Enterprise	Sim, sem reinicialização	Sim- não reinício	Não



Ferramentas de linha de comando da Microsoft



220-1102: Objetivo 1.2: Dado um cenário, use a ferramenta de linha de comando apropriada da Microsoft.

O Windows possui várias ferramentas de linha de comando para operação e gerenciamento do sistema. Embora também tenha muitas ferramentas administrativas que oferecem interfaces gráficas para gerenciamento de desempenho e solução de problemas, o domínio desses comandos torna as tarefas comuns muito mais eficientes.

Nos últimos anos, a Microsoft colocou gentilmente o prompt de comando (cmd.exe) no modo de manutenção e o substituiu pelo ambiente de linha de comando mais poderoso do Windows PowerShell. O CMD.exe não desapareceu, mas não é mais o padrão. Todos os comandos nesta seção funcionam da mesma forma em qualquer um dos ambientes; portanto, se você quiser experimentar o prompt do CMD, basta digitar **CMD** na barra de pesquisa e ele aparecerá.

Iniciando uma sessão de prompt de comando com o Windows PowerShell A maioria dos usuários de computador não usa um prompt de linha de comando com frequência. No entanto, os técnicos o utilizam para fazer o seguinte:

- Recupere dados de sistemas que não inicializam normalmente

- Reinstale arquivos de sistema perdidos ou corrompidos
- Imprimir listas de arquivos (o que não pode ser feito no File Explorer ou neste PC)
- Copiar, mover e excluir dados
- Exibir ou definir determinadas configurações do sistema operacional

Você pode iniciar uma sessão de prompt de comando no Windows clicando na opção Windows PowerShell no menu Iniciar; no entanto, outros métodos podem ser mais rápidos. Aqui estão alguns fáceis para começar:

- No Windows 10, pressione Windows+X e clique ou toque em Windows PowerShell para executar no modo padrão. Uma opção para executar como administrador também está disponível.
- Digite **PowerShell** na barra de pesquisa. O aplicativo aparecerá antes que você termine de digitar.
- Segure a tecla Shift enquanto clica com o botão direito do mouse na área de trabalho. A opção PowerShell é exibida.

Comandos disponíveis com privilégios padrão vs.

Privilégios administrativos A maioria

dos comandos na [Tabela 6-4](#) pode ser executada com *privilégios padrão* (por qualquer usuário). No entanto, alguns comandos podem ser executados apenas com *privilégios administrativos* no que é conhecido como *modo elevado* ou *modo administrativo*.

Comandos elevados podem fazer mais alterações operacionais no PC do que comandos básicos.



Tabela 6-4 Comandos do prompt de comando do Windows

Comandos de Navegação

cd (chdir) Altera o diretório de trabalho (pasta).

dir Exibe uma lista do diretório atual e subdiretórios.

Comandos de Navegação

md Cria um diretório na unidade.

(mkdir)

rmdir Remove um diretório vazio.

cd .. Navega para o diretório anterior.

C:\ ou D: Leva você ao prompt de comando da letra da unidade.
ou X:

Ferramentas de linha de comando

ipconfig C:\Users>ipconfig

Exibe informações de configuração de rede TCP/IP para cada adaptador de rede (físico e virtual) no dispositivo.

ping Envia pacotes IP para verificar a conectividade da rede:

C:\Users>ping **cisco.com** (resposta a seguir)

Ping cisco.com [2001:420:1101:1::185] com 32 bytes de dados: Resposta de 2001:420:1101:1::185: time=64ms Resposta de 2001:420:1101:1::185 : time=65ms Resposta de 2001:420:1101:1::185: time=65ms Resposta de 2001:420:1101:1::185: time=69ms

Estatísticas de ping para 2001:420:1101:1::185:

Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),

Tempos de ida e volta aproximados em milissegundos:

Mínimo = 64ms, Máximo = 69ms, Média = 65ms

hostname Retorna o nome do computador do dispositivo local.

C:\Usuários>nome do host

PC de RMcD

Comandos de Navegação

netstat Exibe uma lista de conexões TCP ativas em uma rede local.

C:\Usuários>netstat

Conexões ativas

Protocolo Endereço local Endereço estrangeiro Estado TCP

10.0.0.34:49554 12.64.180.116:https ESTABLISHED (*exemplo de saída; várias linhas omitidas aqui*)

nslookup Reúne as informações do Sistema de Nomes de Domínio (DNS) da rede.

C:\Users>nslookup

Servidor padrão: cdns01.ISPprovider.net Endereço:
2101:568:feed::1

chkdsk* Verifica a unidade especificada em busca de erros e os repara.

C:\Windows>chkdsk (*Nota: Executar como Administrador*)

O tipo do sistema de arquivos é NTFS.

AVISO! Parâmetro /F não especificado.

Executando o CHKDSK no modo somente leitura.

Estágio 1: Examinando a estrutura básica do sistema de arquivos ...

895232 registros de arquivos processados.

Verificação de arquivo concluída.

net user Gerencia contas de usuário (adicionar, remover, alterar).

C:\Usuários> usuário net

Contas de usuário para \\PC-RMcD

administrador Administrador ctctechs

Conta padrão

O comando foi concluído com sucesso.

Comandos de Navegação

uso da net Conecta-se a pastas compartilhadas, semelhante ao mapeamento de uma unidade de rede.

C:\Usuários> **uso** da rede

Novas conexões serão lembradas.

Não há entradas na lista.

tracert Semelhante ao ping, mas retorna informações de caminho para um destino de endereço IP. Semelhante ao comando traceroute no macOS e Linux. Pode ser usado para solucionar problemas de conectividade na Web.

C:\Users>tracert **Cisco.com**

Rastreando a rota para cisco.com [2001:420:1101:1::185]

em um máximo de 30 saltos: 1

5 ms 2601:602:cc01:16e0:623d:26ff:feb9:8830

2 13 ms 12 ms 12 ms 2001:558:4082:c6::1

3 12 ms 13 ms 13 ms 2001:558:a2:601b::1

(20 saltos na saída omitidos)

formato *(Observação: não pratique este comando em um computador operacional!)*

Cria ou recria o sistema de arquivos especificado em armazenamento gravável ou regravável (mídia magnética, flash ou ótica) e substitui o conteúdo e a tabela de arquivos da unidade.

xcopy Copia um ou mais arquivos e pastas para outra pasta ou unidade.

C:\Users>XCOPY **origem [destino] [/A | Para a**

tabela de formatos e funções, digite: C:\Users>help

xcopy

cópia de Copia um ou mais arquivos para outra pasta ou unidade.

Comandos de Navegação

robocopy Cópia de arquivo robusta para Windows. Copia ou move arquivos/pastas; pode ser configurado com várias GUIs opcionais.

Uso :: **ROBOCOPY** origem destino [arquivo [arquivo]...] [opções] origem :: Diretório de origem (unidade:\caminho ou \\servidor\compartilhamento\caminho). destino :: Diretório de destino (unidade:\caminho ou \\servidor\compartilhamento\caminho). arquivo :: Arquivo(s) a copiar (nomes/curingas: o padrão é “*.*”).

Para a tabela de opções, use: C:\Users>help **robocopy**

gpupdate Atualiza a política de grupo em sistemas locais ou do Active Directory.

C:\Users>gpupdate

Atualizando política...

gpresult Exibe o conjunto de políticas resultante para o computador e usuário especificados.

Para o guia de uso, digite: C:\Users>gpresult /?.

shutdown (Nota: Não pratique este comando em um computador operacional!)

Desliga o computador. Para uso, digite: C:\Users>shutdown /?.

sfc* Verifica os arquivos do sistema e substitui os arquivos danificados ou ausentes.

C:\Windows>sfc /scannow (*executar como administrador*)

Iniciando a verificação do sistema. Este processo levará algum tempo.

Iniciando a fase de verificação da verificação do sistema.

Verificação 4% concluída.

[comando] Exibe ajuda para o nome do comando, **[nome]/?** xcopiar /?.

diskpart* (Nota: Não pratique este comando em um computador operacional!)

Cria, remove e gerencia partições de disco.

pathping Semelhante ao **traceroute**, mas fornece informações sobre a rede

latência ao longo do caminho até o destino. **pathping** rastreia e testa conexões de rede para um endereço IP.

C:\Users>pathping cisco.com

Comandos de Navegação

taskkill Interrompe tarefas especificadas em um computador local ou remoto.

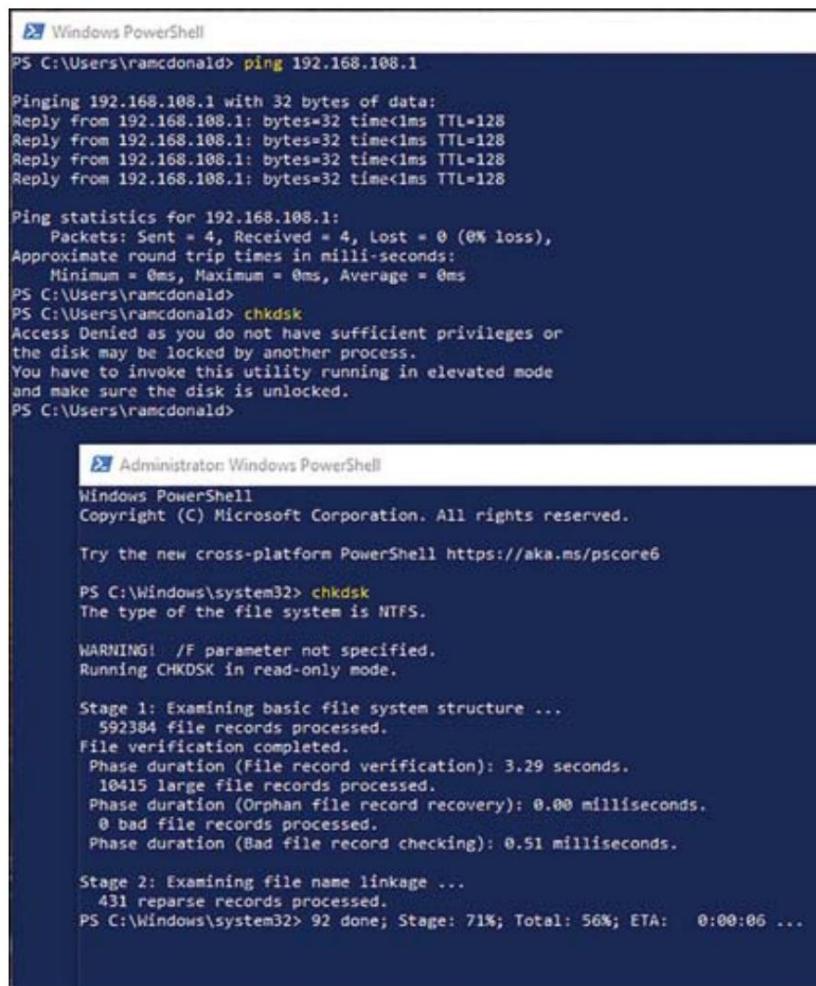
C:\Users>TASKKILL /IM notepad.exe

vencedor Retorna informações de versão do sistema operacional Windows atual.

C:\Usuários>winver

Para executar no modo Administrador, selecione Windows PowerShell (Admin) no menu Windows+X. A janela Prompt de Comando do Administrador é aberta.

A Figura 6-2 mostra um exemplo de ambos.



```
PS C:\Users\ramcdonald> ping 192.168.108.1

Pinging 192.168.108.1 with 32 bytes of data:
Reply from 192.168.108.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.108.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\ramcdonald>
PS C:\Users\ramcdonald> chkdsk
Access Denied as you do not have sufficient privileges or
the disk may be locked by another process.
You have to invoke this utility running in elevated mode
and make sure the disk is unlocked.
PS C:\Users\ramcdonald>

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> chkdsk
The type of the file system is NTFS.

WARNING! /F parameter not specified.
Running CHKDSTK in read-only mode.

Stage 1: Examining basic file system structure ...
      592384 file records processed.
File verification completed.
Phase duration (File record verification): 3.29 seconds.
  10415 large file records processed.
Phase duration (Orphan file record recovery): 0.00 milliseconds.
  0 bad file records processed.
Phase duration (Bad file record checking): 0.51 milliseconds.

Stage 2: Examining file name linkage ...
      431 reparse records processed.
PS C:\Windows\system32> 92 done; Stage: 71%; Total: 56%; ETA:  0:00:06 ...
```

Figura 6-2 Windows PowerShell em Normal (Superior) e Administrador

Modo (inferior)—Observe que o comando **ping** foi bem-sucedido em Modo normal, mas o comando **chkdsk** é executado apenas no administrador Modo

Comandos de linha de comando do Windows

A Tabela 6-4 lista os comandos básicos e seus usos. Os comandos estão listados aqui em letras maiúsculas, mas o Windows permite que você os insira em letras minúsculas, maiúsculas ou mistas. Abra um prompt de comando e experimente esses comandos em preparação para o exame. Mais detalhes do comando são fornecidos após a tabela.

O primeiro conjunto de comandos refere-se aos comandos de navegação que levam o usuário a diferentes diretórios no drive. Eles são seguidos pelas ferramentas de linha de comando que fornecem informações ou executam tarefas para o usuário. Os comandos listados com um asterisco (*) devem ser executados no modo Administrador. Experimente estes comandos em seu PC para se familiarizar com as informações de entrada e saída.

formato



No Windows, o comando **format** é usado principalmente para criar ou recriar o sistema de arquivos especificado em armazenamento gravável ou regravável (mídia magnética, flash ou óptica). No processo, o conteúdo da unidade é substituído.

formato parece “destruir” o conteúdo anterior do armazenamento magnético (como um disco rígido), mas se o **formato** for usado em um disco rígido por engano, programas de recuperação de dados de terceiros podem ser usados para recuperar dados da unidade. Isso é possível porque a maior parte da superfície do disco não é alterada pelo **formato** quando uma opção de formatação rápida é selecionada.

O Windows substitui toda a superfície de um disco com zeros se a opção Formatação rápida não estiver selecionada. Se a opção Formatação rápida ou Formatação segura for usada, o conteúdo do disco será marcado para exclusão, mas poderá ser recuperado com um software de recuperação de dados de terceiros.

Observação

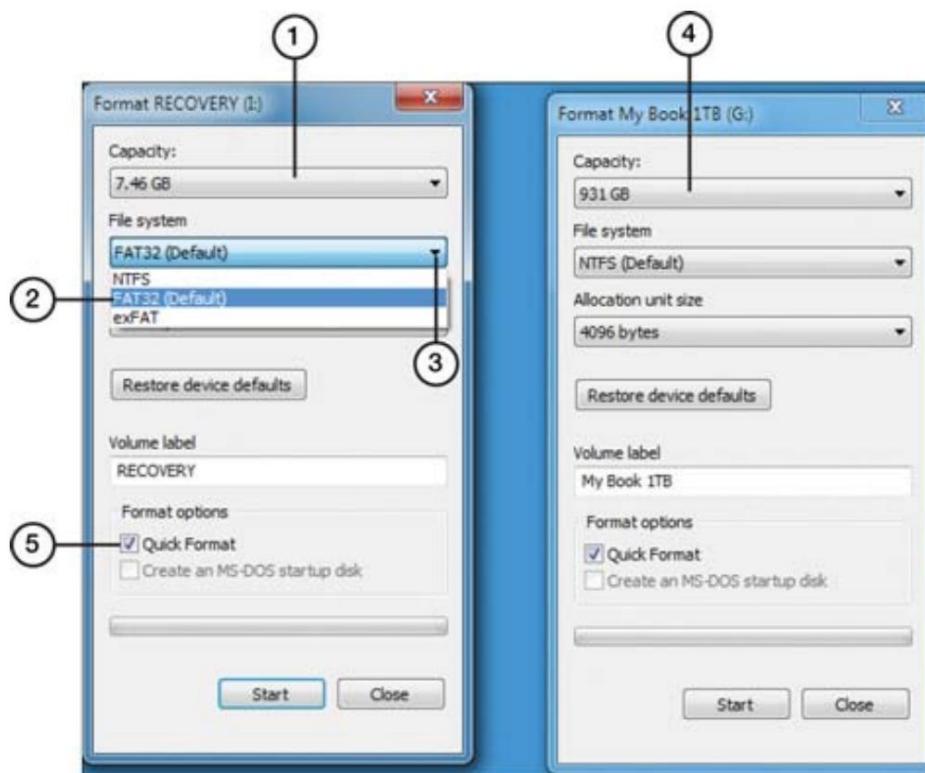
O processo de formatação do disco rígido que o comando **format** executa (que cria o sistema de arquivos) às vezes é chamado de formato padrão, para diferenciá-lo do formato de baixo nível que os fabricantes de discos rígidos usam para configurar estruturas magnéticas no disco rígido .

Usando o formato com Flash USB e Unidades de Mídia Removíveis

Embora as unidades de memória flash USB e as unidades de mídia removível sejam pré-formatadas na fábrica, a **formatação** ainda é útil para apagar rapidamente o conteúdo de um disco, especialmente se ele contiver muitos arquivos ou pastas. Ele também coloca novas marcações de setor no disco.

Formatando unidades com o explorador de arquivos

Use o Windows File Explorer/Este PC para formatar todos os tipos de unidades. Clique com o botão direito do mouse na unidade que deseja formatar e selecione Formatar. As opções de formato para Windows são exibidas (consulte a [Figura 6-3](#)). A ferramenta Formatar também está disponível no Gerenciamento de disco; para a maioria dos usuários, este é o método preferido de formatação de discos.



1. Flash drive capacity
2. FAT32 is default file system
3. Click or tap to see other file system options (NTFS, exFAT)
4. Hard disk capacity
5. Click or tap to clear checkbox for full format

Figura 6-3 O menu Formatar para uma unidade flash (à esquerda) e para um disco rígido Disco (Direito)

Usando o formato do prompt de comando

O comando **format** substitui o conteúdo atual da unidade de destino, a menos que a opção /**Q** (formatação rápida) seja usada. Quando /**Q** é usado, apenas a tabela de alocação de arquivos e a pasta raiz são substituídas. Para recuperar dados de uma unidade formatada, você deve usar um software de recuperação de dados de terceiros.

O comando **format** inclui uma variedade de opções para uso com discos rígidos, mídia removível e unidades ópticas e unidades de memória flash USB. Seguem os exemplos mais úteis:

formato F: /FS: exFAT formata a unidade F: usando o sistema de arquivos exFAT.

format F: /Q executa uma formatação rápida na unidade F:.

Para ver as opções adicionais de **formato**, use **format /?**.

Observe que os sistemas de arquivos FAT e FAT32 impõem as seguintes restrições ao número de clusters em um volume:

FAT: número de clusters ≥ 65.526

FAT32: 65.526 < Número de clusters < 4.177.918

format interrompe imediatamente o processamento se decidir que os requisitos anteriores não podem ser atendidos usando o tamanho de cluster especificado. A compactação NTFS não tem suporte para tamanhos de unidade de alocação acima de 4.096.



cópia de

O comando **copy** copia arquivos de uma unidade e pasta para outra pasta e unidade. A pasta especificada por **copy** já deve existir na unidade de destino. A **cópia** não funciona com arquivos que possuem o sistema ou atributos de arquivo oculto; para copiar esses arquivos, use **xcopy** ou **robocopy**.

A sintaxe para **copiar** no Windows é a seguinte:

**copiar [/D] [/V] [/N] [/Y | /-Y] [/Z] [/L] [/A | /B] *fonte* [/A | /B]
[+ *fonte* [/A | /B] [+ ...]] [*destino* [/A | /B]]**

Seguem alguns exemplos:

copy*.* F: copia todos os arquivos na pasta atual para a pasta atual no F: conduzir.

copy*.TXT C:\Users\Username copia todos os arquivos .txt na pasta atual para a pasta *Username* na unidade C:.

copyC:\WINDOWS\TEMP*.BAK copia todos os arquivos *.bak na pasta \Windows\Temp na unidade C: para a pasta atual. **copyC:**

\WINDOWS*.BMP D: copia todos os arquivos .bmp na pasta \Windows na unidade C: para a pasta atual na unidade D:.

Para ver uma lista de todas as opções de **cópia**, use **copy/?**.



xcopy

Na maioria dos casos, o comando **xcopy** pode ser usado no lugar de **copy**. Tem as seguintes vantagens:

- **Fornece operação mais rápida em um grupo de arquivos:** **xcopy** lê os arquivos especificados na RAM convencional antes de copiá-los para o destino.
- **Cria pastas conforme necessário:** se você especificar o nome da pasta de destino na linha de comando **xcopy**, a pasta de destino será criada, se necessário.
- **Opera como um utilitário de backup:** o **xcopy** pode ser usado para alterar o bit de arquivamento em arquivos de ativado para desativado, para permitir que seja usado no lugar de programas de backup comerciais.
- **Copia arquivos alterados ou criados em ou após uma data especificada:** Isso é útil ao usar o **xcopy** como um substituto para programas de backup comerciais.

O **xcopy** pode ser usado para “clonar” o conteúdo de uma unidade inteira para outra unidade. Por exemplo, o comando a seguir copia todo o conteúdo da unidade D: para a unidade H::

xcopyD:\ H:\ /H /S /E /K /C /R

Este comando copia todos os arquivos da pasta raiz (diretório raiz) e subpastas na unidade D: para a pasta raiz e subpasta na unidade H:, incluindo sistema e arquivos ocultos, pastas e subpastas vazias e atributos de arquivo.

Esse processo continua mesmo se forem detectados erros e substitui os arquivos somente leitura.

Para ver uma lista de todas as opções de **xcopy**, use **xcopy/?**, conforme mostrado anteriormente na [Tabela 6-4](#).



robocopy

robocopy é um utilitário robusto de cópia de arquivos do Windows que pode ser usado no lugar do **xcopy**. O **robocopy** oferece várias vantagens sobre o **xcopy**, incluindo a capacidade de tolerar pausas nas conexões de rede, espelhar o conteúdo das pastas de origem e destino removendo arquivos e também copiando arquivos, para executar cópias multithread para cópias mais rápidas em PCs multicore, para log copy processos e para listar ou copiar arquivos que correspondam aos critérios especificados (incluindo o tamanho mínimo do arquivo).

A sintaxe para **robocopy** para Windows está disponível em <https://technet.microsoft.com/en-us/library/cc733145.aspx>. Vejamos dois exemplos do que você pode fazer com **robocopy**.

Para copiar arquivos na *pasta de origem* com pelo menos 16 MB (16.777.216 bytes) de tamanho para uma *pasta de destino*, use

robocopy C:\SOURCEFOLDER D:\TARGETFOLDER /MIN:16777216

Adicione a opção **/L** ao final deste comando para listar os arquivos a serem copiados.

Para espelhar uma pasta local em uma pasta de rede com ajustes para uma operação mais confiável e omitir arquivos ocultos (/XA:H), use:

```
robocopy\\SOURCESERVER\\SHARE  
\\SERVIDOR DE DESTINO\\COMPARTILHAR /MIR /FFT /Z /XA:H /W:5
```

/FFT usa a regra de 2 segundos para comparar arquivos, o que pode impedir a recopia de arquivos que não foram alterados, mas que possuem um carimbo de data/hora que está um segundo ou dois diferente da versão do destino. /W:5 altera o tempo de espera entre novas tentativas do padrão de 30 segundos para 5 segundos.

Esses exemplos foram adaptados da excelente postagem do TechNet Wiki “Robocopy and a Few Examples,” disponível em https://social.technet.microsoft.com/wiki/contents/articles/1073.robocopy_and-a-few-examples.aspx.

Como você pode ver nesses exemplos, o **robocopy** usa uma sintaxe muito diferente do **xcopy**. Se você usou o **robocopy** no Windows XP ou versões anteriores, lembre-se de que o **robocopy** teve alterações de sintaxe em suas diferentes versões. Por esses motivos, talvez você prefira executá-lo por meio de uma GUI, como a GUI **robocopy** disponível em [https://docs.microsoft.com/en-us/previousversions/technet-magazine/cc160891\(v=msdn.10\)](https://docs.microsoft.com/en-us/previousversions/technet-magazine/cc160891(v=msdn.10)) ou GUIs de terceiros disponíveis online.



diskpart

diskpart é um programa de gerenciamento de disco incluído no Windows. Ele pode ser usado para executar comandos de particionamento e gerenciamento de disco que não estão incluídos no módulo Gerenciamento de disco do Gerenciamento do computador.

Quando você executa o diskpart, uma nova janela é aberta com um prompt `diskpart>`. Somente comandos diskpart podem ser inseridos nesta janela. Para obter uma lista completa dos comandos diskpart, use `diskpart/?`.

A Figura 6-4 demonstra dois comandos do **diskpart** : `select disk X` e `detail disk`. Neste exemplo, diskpart mostra que a unidade de disco selecionada é a unidade de inicialização, contém o arquivo de paginação e é usada para armazenar informações de despejo de memória.

```
C:\Windows\system32\diskpart.exe
DISKPART> select disk 1
Disk 1 is now the selected disk.
DISKPART> detail disk
ST3500320AS ATA Device
Disk ID: 8230499F
Type : ATA
Status : Online
Path : 0
Target : 0
LBA ID : 0
Location Path : PCIROOT(0)>PCI(1200)>ATA(C00T00100)
Current Read-only State : No
Read-only : No
Boot Disk : Yes
Pagefile Disk : Yes
Hibernation File Disk : No
Crashdump Disk : Yes
Clustered Disk : No
Volume ### Ltr Label Fs Type Size Status Info
Volume 4            System Rese NTFS Partition 100 MB Healthy System Boot
Volume 5            C      NTFS Partition 465 GB Healthy
DISKPART>
```

Figura 6-4 Usando **diskpart** para determinar detalhes sobre o selecionado Disco



sfc

Verificador de arquivos do sistema (**sfc**) é um utilitário do Windows que verifica arquivos de sistema protegidos (como arquivos .dll, .sys, .ocx e .exe, bem como alguns arquivos de fonte usados pela área de trabalho do Windows) e substitui versões incorretas ou ausentes arquivos com os arquivos corretos.

Use o **sfc** para corrigir problemas com programas integrados do Windows causados pela instalação de arquivos obsoletos do sistema Windows, erro do usuário, exclusão deliberada, infecções por vírus ou cavalos de Tróia e problemas semelhantes.

Para executar o **sfc**, abra o prompt de comando no modo elevado (ou seja, execute como administrador) e digite **sfc** com a opção apropriada. Uma opção típica é **sfc/scannow**, que verifica imediatamente todos os arquivos protegidos (consulte a [Figura 6-5](#)).

```
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>sfc /scannow
Beginning system scan. This process will take some time.
Beginning verification phase of system scan.
Verification 100% complete.

Windows Resource Protection found corrupt files and successfully repaired them. Details are included in the CBS.Log windir\Logs\CMS\CMS.log. For example C:\Windows\Logs\CMS\CMS.log
C:\Windows\system32>
```

Figura 6-5 sfc /scannow informa que arquivos corrompidos foram reparados

Outra opção é **sfc /scanonce**, que verifica todos os arquivos protegidos na próxima inicialização. Se o SFC descobrir que alguns arquivos estão faltando e os arquivos de substituição não estiverem disponíveis em seu sistema, você será solicitado a reinserir o disco de distribuição do Windows para que os arquivos possam ser copiados para o cache DLL. Outras opções incluem **/scanboot**, que verifica todos os arquivos protegidos sempre que o sistema é iniciado; **/revert**, que retorna a configuração de digitalização para o padrão; e **/purgecache** e **/cachesize=x**, que permitem ao usuário excluir o cache do arquivo e modificar seu tamanho.

Se forem detectados erros, eles serão registrados no arquivo CBS.log, localizado em %WinDir%\Logs\CMS\.

Para ler o conteúdo do CBS.log, você pode usar o comando **findstr**, que envia os detalhes para um arquivo separado chamado sfcdetails.txt.

Para obter mais informações sobre como usar **sfc** e **findstr** e para saber como substituir arquivos de sistema corrompidos manualmente se o **sfc** não puder fazer isso, consulte <https://support.microsoft.com/en-us/kb/929833>.



chkdsk

chkdsk é uma ferramenta de linha de comando para verificar erros nas unidades de disco e, opcionalmente, reparar esses erros. Ele deve ser executado no modo elevado/administrador. Observe que alguns comandos diferem, dependendo do sistema de arquivos (FAT/FAT32 ou NTFS) da unidade de destino. A sintaxe do comando **chkdsk** é a seguinte:

```
chkdsk [volume][[caminho]nome do arquivo]] [/F] [/V] [/R] [/X] [/I] [/C] [/L[:tamanho]] [/B]
```

Considere estes exemplos:

chkdsk/F verifica e corrige erros na unidade atual.

chkdskF: /F verifica e corrige erros na unidade F:.

Se **chkdsk/F** for executado na unidade do sistema, a seguinte mensagem será exibida:

[Clique aqui para ver a imagem do código](#)

O tipo do sistema de arquivos é NTFS.

Não é possível bloquear a unidade atual.

Chkdsk não pode ser executado porque o volume está sendo usado por outro processo. Gostaria de agendar este volume para ser verificado na próxima vez que o sistema for reiniciado? (S/N)

Se você responder Y, o chkdsk será executado antes que a área de trabalho do Windows apareça e exiba uma mensagem na área de notificação sobre a condição da unidade. Se o **chkdsk/F** for executado em uma unidade que não seja do sistema, ele será executado imediatamente.

Para obter uma lista completa das opções do chkdsk, use **chkdsk/?**.



gpupdate

gpupdate é usado para atualizar a Diretiva de Grupo em um computador local ou remoto.

Sua sintaxe segue:

```
gpupdate [/Destino:{Computador | Usuário}] [/Force] [/Espera:<valor>]  
[/Logoff] [/Boot] [/Sync]
```

Por exemplo, você pode usar este comando para atualizar a Diretiva de Grupo em um computador especificado chamado **AccountingPC** e, em seguida, reiniciar esse computador após a conclusão do processamento:

```
gpupdate/target:accountingpc /boot
```

Para obter uma lista completa de opções para o comando **gpupdate**, use **gpupdate/?**.

gpresult

Use **gpresult** para exibir a política atual para um usuário e computador especificados.

Sua sintaxe segue:

```
gpresult [/S sistema [/U nome de usuário [/P [senha]]]] [/SCOPE escopo]  
[/USER nome de usuário -alvo] [/R | /V | /Z] [(/X | /H) <nome do arquivo> [/F]]
```

Para obter uma lista completa de opções para o comando **gpresult**, use **gpresult/?**.

Considere estes exemplos:

gpresult/R exibe dados resumidos. **gpresult/**

H GPReport.xhtml salva um relatório como GPReport.xhtml. **gpresult/USER**

targetusername /V fornece informações detalhadas para o nome de usuário especificado.

caminho

pathping é um comando do PowerShell para coletar informações sobre rotas e latência (ou atraso) nas comunicações em uma rede ou na Internet. O comando **ping** simplesmente testa a disponibilidade de um endereço, enquanto o **pathping** coleta estatísticas sobre a jornada dos pacotes IP.

Sistema Operacional Microsoft Windows 10 (SO) Recursos e ferramentas



220-1102: Objetivo 1.3: Dado um cenário, use recursos e ferramentas do sistema operacional (SO) Microsoft Windows 10.

Muitas ferramentas administrativas do Windows fornecem interfaces gráficas para gerenciamento de desempenho e solução de problemas. Dominar essas ferramentas torna as tarefas comuns muito mais eficientes.

Gerenciador de

Tarefas O utilitário **Gerenciador** de Tarefas fornece uma visão útil em tempo real do funcionamento interno do Windows e dos programas em execução. O Gerenciador de Tarefas é exibido de várias maneiras:

- Clique com o botão direito do mouse na barra de tarefas e selecione Gerenciador de Tarefas.
- Pressione Ctrl+Shift+Esc.
- Digite **Gerenciador de Tarefas** na caixa de pesquisa.

- Pressione Ctrl+Alt+Del e selecione Gerenciador de Tarefas na caixa de diálogo Segurança do Windows.

Qualquer uma das abordagens anteriores abre o Gerenciador de Tarefas, mostrado na [Figura 6-6](#).

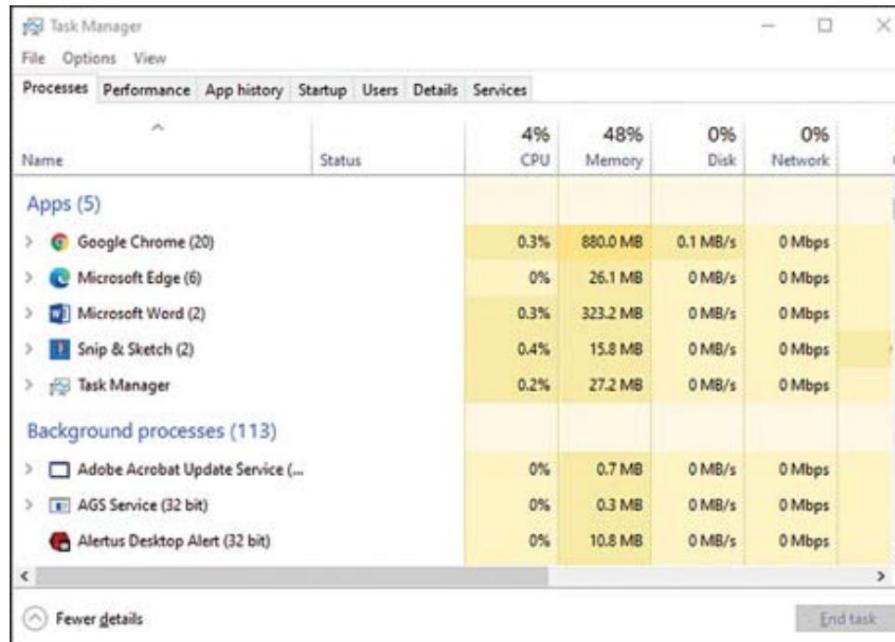


Figura 6-6 A guia Processo do Gerenciador de Tarefas do Windows no Windows 10

O Gerenciador de Tarefas do Windows 10 inclui as seguintes guias:

- **Processos:** exibe aplicativos e processos em segundo plano na memória
- **Desempenho:** Exibe CPU, memória, unidades de disco, Bluetooth, Estatísticas de Ethernet e Wi-Fi
- **Histórico do aplicativo:** exibe o uso de recursos do aplicativo na sessão atual do sistema
- **Inicialização:** exibe programas de inicialização e seu impacto no desempenho do sistema
- **Usuários:** lista os usuários atuais
- **Detalhes:** Exibe PID, status, nome de usuário, CPU e uso de memória por aplicativo ou serviço
- **Serviços:** lista os serviços e seus status

Um dos usos mais comuns do Gerenciador de Tarefas é finalizar programas (processos) que estão com defeito. Para encerrar um programa, clique na guia Processos, clique com o botão direito do mouse no processo do programa não responsivo e selecione Finalizar tarefa. Também é possível clicar com o botão direito do mouse em um processo e escolher detalhes adicionais sobre o status.

Snap-in do Microsoft Management Console (MMC) Em vez de procurar diferentes utilitários em diferentes lugares no Windows, é mais simples usar a janela do console de gerenciamento do computador. Possui a maioria das ferramentas necessárias em um sistema de janelas organizado. A forma como você abre o Gerenciamento do Computador depende da versão do Windows.

O Gerenciamento do Computador é um exemplo do **Console de Gerenciamento Microsoft (MMC)**, que é um console em branco que usa várias janelas de console de snap-in. O MMC salva os consoles que você encaixa e lembra o último local em que você trabalhou, o que o torna uma ferramenta valiosa e que economiza tempo.

Para abrir o MMC, digite **MMC** na caixa Executar. Um novo MMC em branco aparece. Para adicionar as janelas do console, vá para **Arquivo > Adicionar/Remover Snap-in** (ou pressione Ctrl+M). A partir daí, clique no botão Adicionar para selecionar o console desejado, como Gerenciamento do computador, Logs e alertas de desempenho ou Controles ActiveX.

Quando terminar de usá-lo, salve o MMC e considere adicioná-lo como um atalho na área de trabalho ou na área de Início rápido e talvez adicionar um atalho de teclado para abri-lo. O MMC lembra todas as janelas do console adicionadas e inicia você no local usado quando o programa foi fechado.

O MMC versão 3.0 é usado com o Windows 10.

Visualizador de eventos

O **Visualizador de eventos (eventvwr.msc)** permite que um administrador rastreie e registre logins de eventos, ações de segurança, travamentos e outros eventos ocorridos no computador. A **Figura 6-7** mostra um exemplo dos eventos rastreados no Visualizador de Eventos para Windows 10.

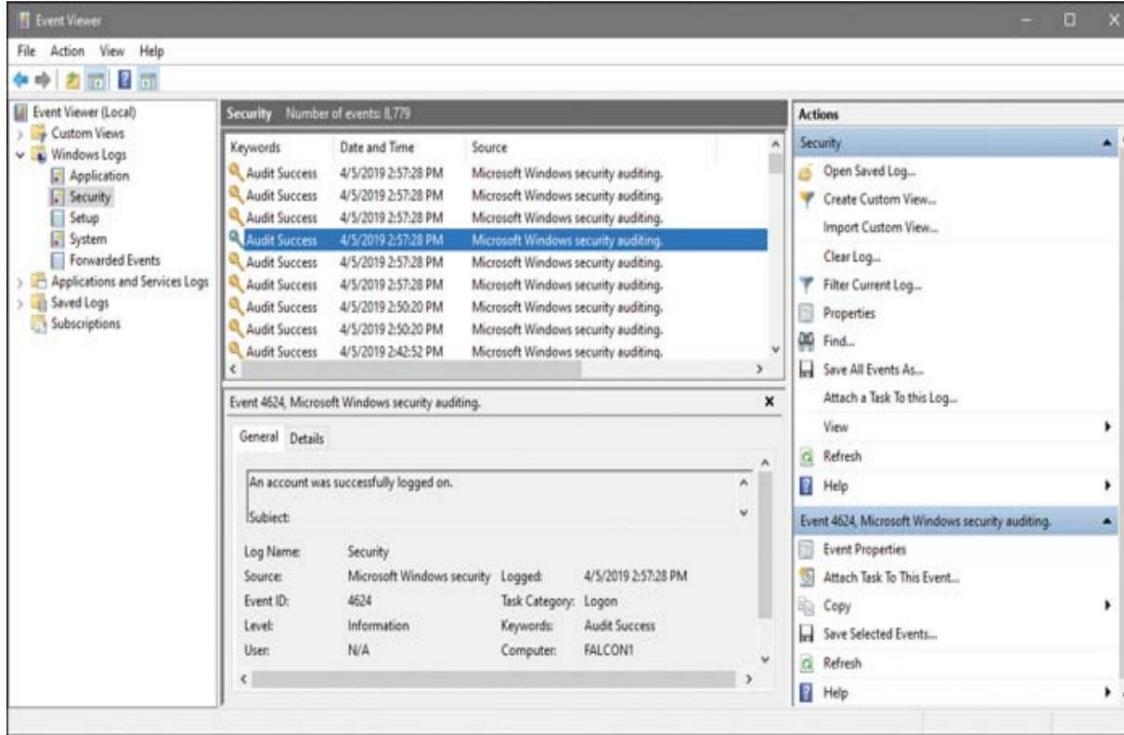


Figura 6-7 Visualizador de eventos

Gerenciamento de Disco

O snap-in **Gerenciamento de disco (diskmgmt.msc)** do MMC é um aplicativo baseado em GUI para análise e configuração de discos rígidos. Tente algumas das configurações listadas nas seções a seguir em um computador de teste com uma ou duas unidades de espaço não particionado. O Gerenciamento de disco também pode ser acessado clicando com o botão direito do mouse no ícone do Windows (iniciar) e selecionando Gerenciamento de disco no menu exibido.

CUIDADO

Algumas operações apagam todo o conteúdo da unidade. Certifique-se de fazer backup de todos os dados que deseja manter antes de tentar qualquer uma dessas tarefas.

Estado da unidade

O Gerenciamento de disco exibe o status das unidades conectadas com Status da unidade.

A Figura 6-8 exibe os discos e seus status na parte superior da janela. Por exemplo, a partição C: está íntegra. Esta janela também mostra a porcentagem do disco usado e outras informações, como se o disco está sendo formatado, se é básico ou dinâmico e se falhou.

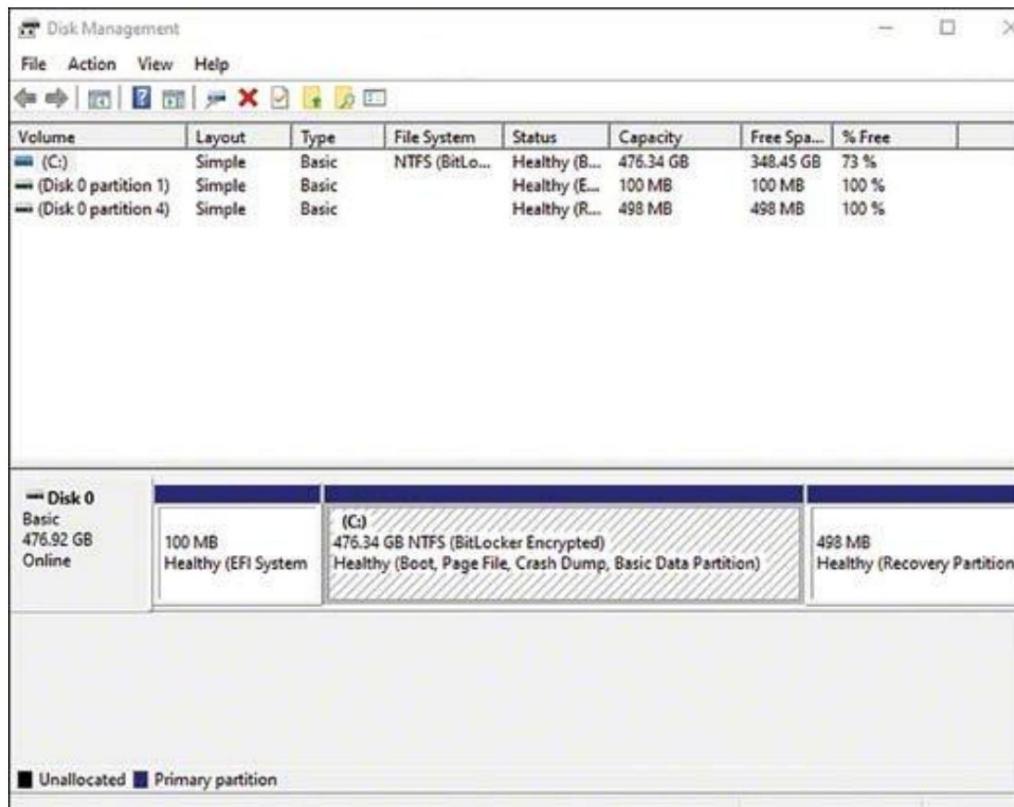


Figura 6-8 Usando o Gerenciamento de Disco

Em alguns casos, você pode ver um status de “estrangeiro”. Isso significa que um disco dinâmico foi movido de outro computador (com outro sistema operacional Windows) para o computador local e não pode ser acessado corretamente.

Para corrigir isso e habilitar o acesso ao disco, adicione o disco à configuração do sistema do seu computador.

Para adicionar um disco à configuração do sistema do computador, clique com o botão direito do mouse no disco e clique em Importar discos externos. Quaisquer volumes existentes no disco externo tornam-se visíveis e acessíveis quando você importa o disco.

Agendador de tarefas

O Windows usa **o Agendador de Tarefas (taskschd.msc)** para executar uma tarefa em um agendamento especificado.

Para criar uma tarefa básica no Windows, siga este procedimento:

Etapa 1. Digite **Agendador de Tarefas** (ou **taskschd.msc**) na barra de pesquisa ou Executar caixa.

Etapa 2. Clique em **Criar tarefa básica** no menu Ações.

Etapa 3. Digite um nome e uma descrição para a tarefa e clique em **Avançar**.

Etapa 4. Selecione um intervalo (por exemplo, Diário, Semanal, Mensal, Apenas uma vez, Quando meu computador iniciar, Quando eu fizer logon ou Quando um evento específico for registrado) e clique em **Avançar**.

Etapa 5. Especifique quando iniciar a tarefa e a recorrência e se deseja sincronizar entre fusos horários; em seguida, clique em **Avançar**.

Etapa 6. Especifique para iniciar um programa (ou enviar um e-mail ou exibir uma mensagem) e clique em **Avançar**.

Etapa 7. Selecione um programa ou script para executar, adicione opções (argumentos) e especifique onde iniciar o programa ou script. Clique em **Avançar**.

Etapa 8. Revise as configurações da tarefa (consulte a [Figura 6-9](#)) e clique em **Concluir**.

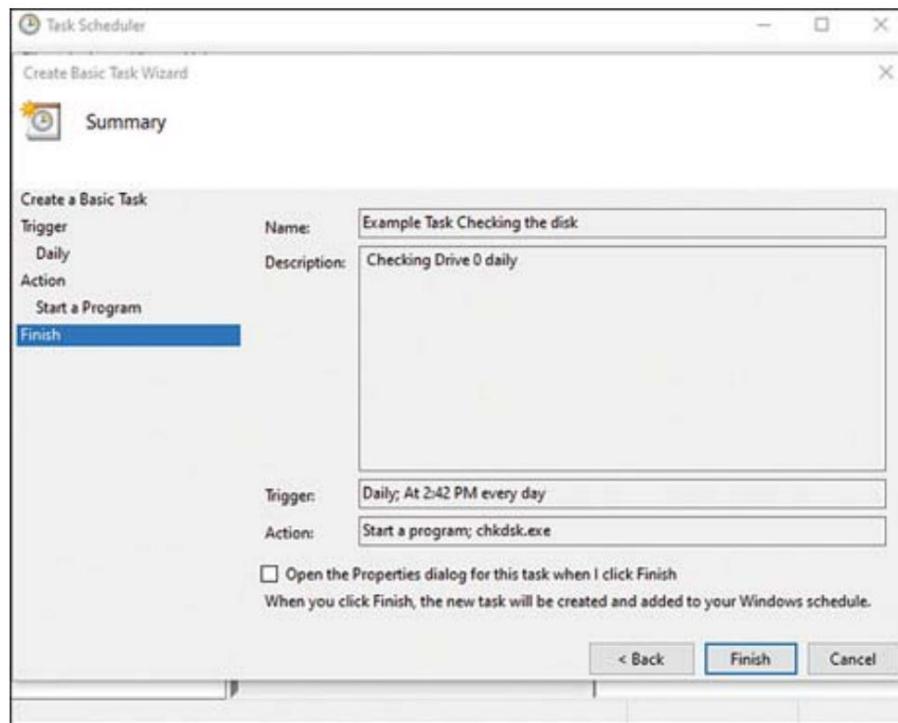


Figura 6-9 Revisando uma tarefa de verificação de disco criada com a tarefa Agendador

A tarefa é salva na biblioteca do Agendador de Tarefas (consulte a [Figura 6-10](#)). As tarefas podem ser editadas ou excluídas nesta pasta conforme necessário.

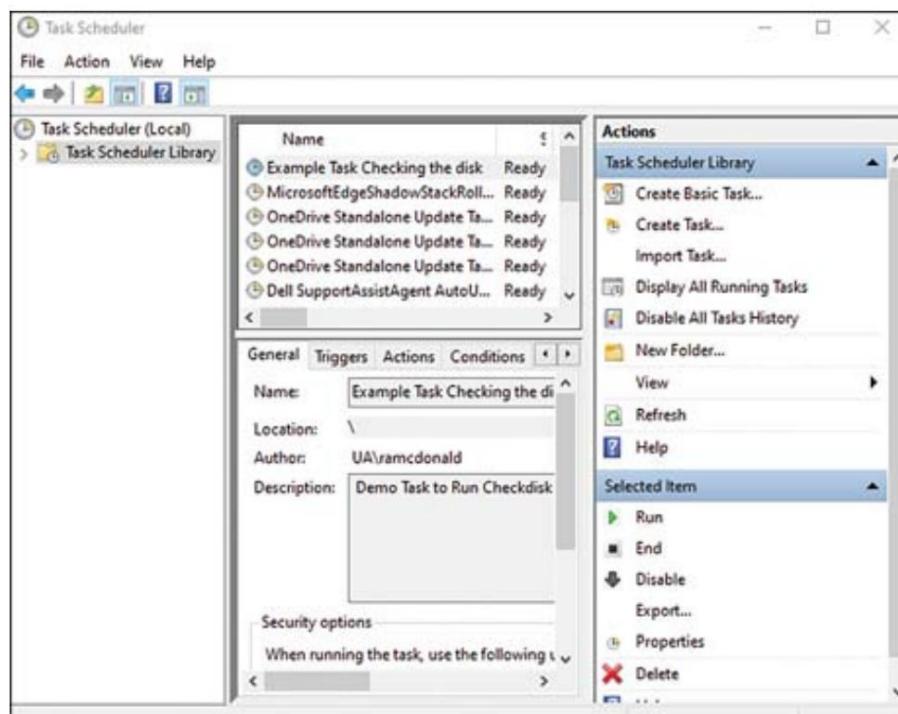


Figura 6-10 A Biblioteca do Agendador de Tarefas Depois que uma Nova Tarefa é Adicionada (a Nova Tarefa é Listada Primeiro, Neste Exemplo)

Gerenciador de Dispositivos



O Gerenciador de dispositivos do Windows ([devmgmt.msc](#)) é usado para exibir categorias de dispositivos instalados e dispositivos específicos instalados, bem como para solucionar problemas com dispositivos.

Para iniciar o Gerenciador de dispositivos no Windows 10, siga estas etapas:

Etapa 1. Na barra de pesquisa, digite **Gerenciador de dispositivos** ou digite **devmgmt.msc** na caixa Executar.

Etapa 2. Abra o Gerenciador de dispositivos.

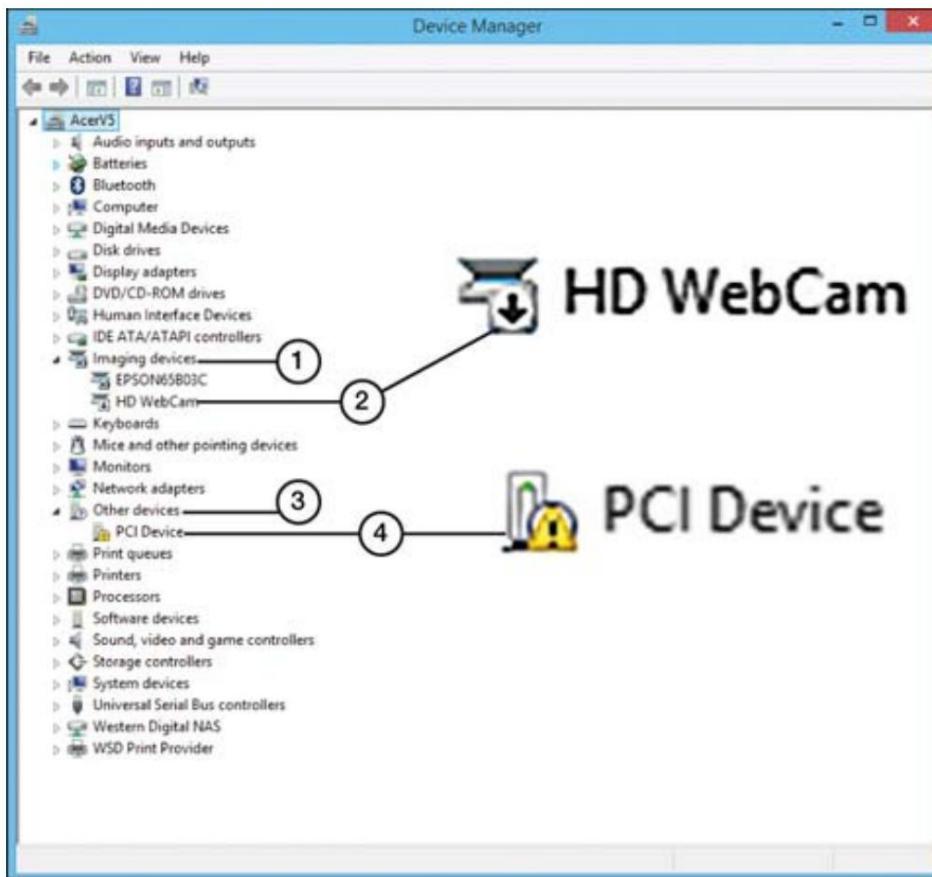
Etapa 3. Clique ou toque no link **Gerenciador de dispositivos**.

Alternativamente:

Etapa 1. Pressione Windows+X.

Etapa 2. Selecione **Gerenciador de dispositivos**.

Para visualizar os dispositivos em uma categoria específica, clique no sinal de mais (+) ao lado do nome da categoria, conforme mostrado na [Figura 6-11](#). Se uma determinada categoria contiver um dispositivo com problemas, a categoria será aberta automaticamente quando você iniciar o Gerenciador de dispositivos.



1. Imaging devices category has a device with a problem
2. The HD webcam has been disabled
3. Other devices category is used for unidentified devices
4. An unidentified device

Figura 6-11 Gerenciador de dispositivos com categorias selecionadas expandidas

Observação

Diferentes sistemas têm diferentes categorias listadas no Gerenciador de dispositivos porque o Gerenciador de dispositivos lista apenas categorias para hardware instalado. Por exemplo, o sistema mostrado na [Figura 6-11](#) é um laptop, portanto, possui uma categoria de baterias.

Se um computador tiver dispositivos com defeito de forma que o Gerenciador de dispositivos possa detectar ou se tiver dispositivos desativados, eles serão exibidos assim que você abrir o Gerenciador de dispositivos. Por exemplo, na [Figura 6-11](#), a categoria Imaging Devices lista um dispositivo desativado, indicado por uma seta para baixo

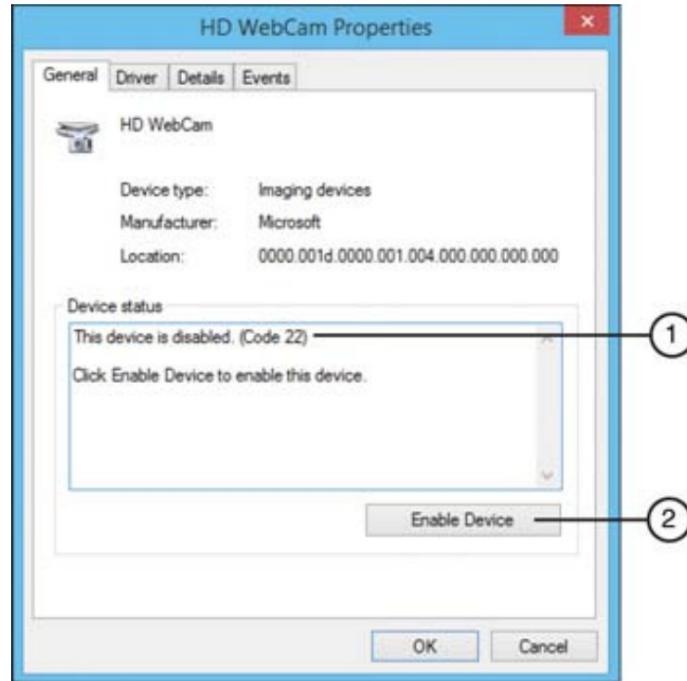
ícone. A categoria Outros dispositivos lista um dispositivo que não pode ser executado, indicado por um ponto de exclamação (!) em um triângulo amarelo.

Se um dispositivo com defeito ou desativado for uma porta de E/S, como uma porta serial, paralela ou USB, qualquer dispositivo conectado a essa porta não funcionará até que esteja funcionando corretamente.

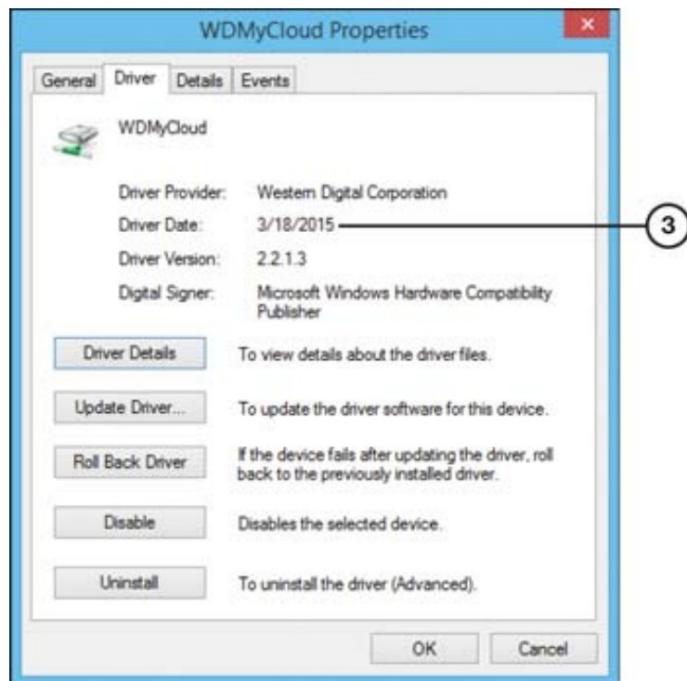
Para ver mais informações sobre um dispositivo específico, clique duas vezes no dispositivo para abrir sua folha de propriedades. As folhas de propriedades do dispositivo têm uma guia Geral e algumas combinações de outras guias, incluindo as seguintes:

- **Geral:** exibe o tipo de dispositivo, fabricante, localização, status, um botão de solução de problemas e uso. Aplica-se a todos os dispositivos.
- **Propriedades:** Exibe as configurações específicas do dispositivo. Aplica-se a dispositivos multimídia.
- **Driver:** exibe detalhes do driver e informações sobre a versão. Aplica-se a todos os dispositivos.
- **Detalhes:** Exibe detalhes técnicos sobre o dispositivo. Aplica-se a todos os dispositivos.
- **Políticas:** otimiza unidades externas para remoção ou desempenho rápido.
Aplica-se a unidades USB, FireWire (IEEE 1394) e eSATA.
- **Recursos:** Exibe recursos de hardware como IRQ, DMA, memória e endereço de porta de E/S. Aplica-se a dispositivos de E/S.
- **Volumes:** exibe informações sobre a unidade, como status, tipo e capacidade.
Clique em Preencher para recuperar informações. Aplica-se a unidades de disco rígido.
- **Potência:** Exibe a potência disponível por porta. Aplica-se a hubs raiz USB e hubs genéricos.
- **Gerenciamento de energia:** especifica as configurações de gerenciamento de energia específicas do dispositivo. Aplica-se a dispositivos USB, rede, teclado e mouse.

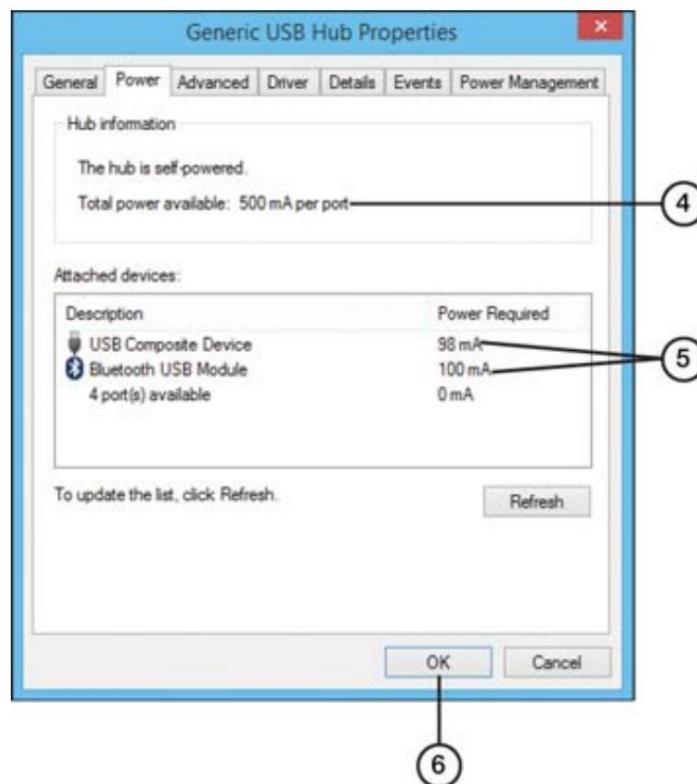
A Figura 6-12 ilustra algumas dessas guias.



1. Device status—disabled device (Code 22)
2. Troubleshoot button—click or tap to enable device



3. Driver overview



4. Available power per USB port on this hub
5. Power required for connected devices
6. Click or tap to close properties sheet

Figura 6-12 Guias selecionadas do Gerenciador de dispositivos: a guia Geral para um Dispositivo desativado (A), a guia Driver para um dispositivo de armazenamento de rede (B) e a guia Energia para um hub USB (C)

Para solucionar problemas com um dispositivo no Gerenciador de dispositivos, abra sua folha de propriedades clicando duas vezes no dispositivo. Use a guia Geral (mostrada na [Figura 6-12](#)) para exibir o status do dispositivo e solucionar problemas do dispositivo desativado ou com defeito.

Quando você tem um dispositivo com defeito, como o mostrado à esquerda na [Figura 6-12](#), você tem várias opções para resolver o problema:

- Procure o código do Gerenciador de dispositivos para determinar o problema e sua solução. (Consulte a [Tabela 6-5](#) para alguns exemplos de códigos e soluções do gerenciador de dispositivos.)
- Clique no botão de solução de problemas (se houver) exibido na guia Propriedades gerais do dispositivo; o nome e o uso do botão dependem do problema.

A Tabela 6-5 lista alguns exemplos, seus significados e o botão de solução (se houver).

- Altere recursos manualmente (principalmente em sistemas mais antigos que não usam gerenciamento de energia ACPI). Se a natureza do problema for um conflito de recursos, você pode clicar na guia Recursos, alterar as configurações e tentar eliminar o conflito.
- Atualize os drivers manualmente. Se o problema for um problema de driver, mas um botão Atualizar driver não estiver disponível, abra a guia Driver e instale um novo driver para o dispositivo.

Tabela 6-5 Exemplos de alguns códigos e soluções do gerenciador de dispositivos

Código Número	Problema	Solução recomendada
1	Este dispositivo não está configurado corretamente.	Atualize o driver.
3	O driver deste dispositivo pode estar corrompido ou seu sistema pode estar com pouca memória ou outros recursos.	Feche alguns aplicativos abertos. Desinstale e reinstale o driver.
		Instale RAM adicional.
10	O dispositivo não pode iniciar.	Atualize o driver. Consulte o artigo de Ajuda e Suporte da Microsoft 943104 para obter mais informações.
12	Este dispositivo não pode encontrar o suficiente Você pode usar os recursos gratuitos que ele pode usar. Se a assistente de solução de problemas desejar usar este dispositivo, o Gerenciador de dispositivos preparará disponibilidade para os dispositivos conflitantes neste sistema. é dispositivo, desative o dispositivo.	
		Desative o dispositivo.
22	O dispositivo está desativado.	Habilite o dispositivo.

Você também pode usar o Gerenciador de dispositivos para desativar um dispositivo que esteja em conflito com outro dispositivo. Para desativar um dispositivo, siga estas etapas:

Etapa 1. Clique no sinal de adição (+) ao lado da categoria do dispositivo que contém o dispositivo.

Etapa 2. Clique duas vezes no dispositivo, clique na guia **Driver** e selecione **Desativar**.

Dependendo do dispositivo, pode ser necessário removê-lo fisicamente do sistema para resolver um conflito. Para usar o Gerenciador de dispositivos para remover um dispositivo, siga estas etapas:

Etapa 1. Clique no sinal de adição (+) ao lado da categoria do dispositivo que contém o dispositivo.

Etapa 2. Clique duas vezes no dispositivo e selecione **Desinstalar**.

Etapa 3. Desligue o sistema e remova o dispositivo físico.

Ou:

Etapa 1. Clique duas vezes no dispositivo e selecione **Propriedades**.

Etapa 2. Clique na guia **Driver** e clique no botão **Desinstalar**.

Etapa 3. Desligue o sistema e remova o dispositivo físico.

Se um dispositivo não funcionar corretamente após uma atualização de driver, reverta o driver. Clique no botão Reverter driver na guia Driver para retornar à versão anterior do driver.

Gerenciador de certificados

Gerenciador [**de certificados \(certmgr.msc\)**](#) permite importar, exportar, modificar ou excluir certificados raiz. Esses certificados digitais são como o Windows gerencia a autenticação ao enviar e receber informações. Isso inclui autenticação de usuário pessoal, bem como certificados confiáveis para uma empresa.

As informações para cada certificado emitido incluem o seguinte:

- Concedida a

- Emitida pela
- Data de validade
- Finalidade pretendida (por exemplo, autenticação de servidor)
- Nome amigável
- Status

Você pode visualizar seus certificados de segurança acessando a ferramenta e digitando **Certificado** (ou **certmgr.msc**) na barra de pesquisa. A [Figura 6-13](#) mostra um exemplo dos diferentes tipos de títulos.

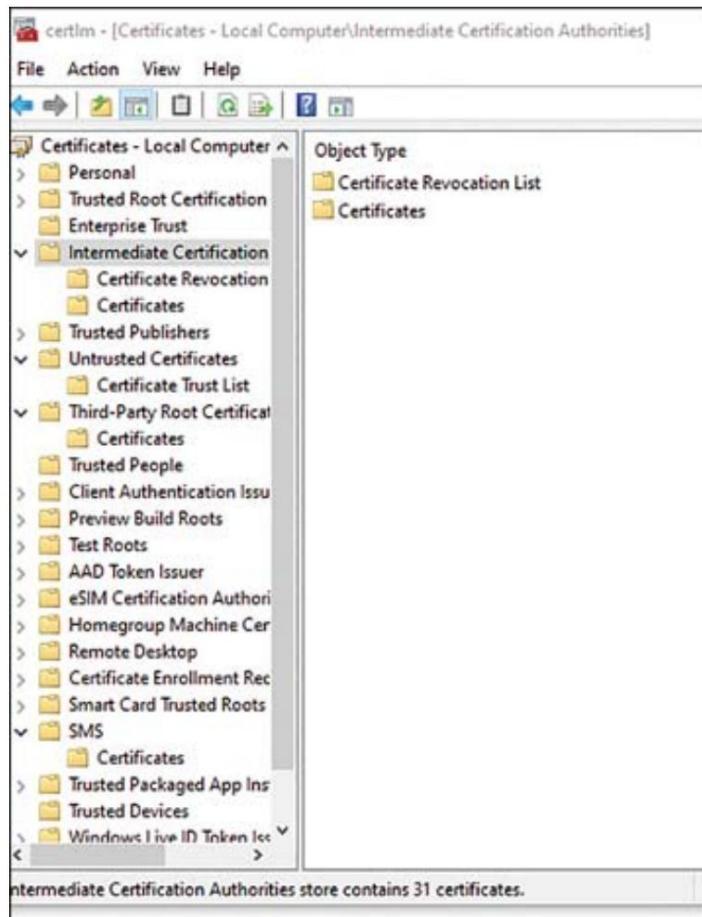


Figura 6-13 Gerenciador de certificados

Usuários e grupos locais

[**Usuários e grupos locais \(lusrmgr.msc\)**](#) é um console snap-in para gerenciar usuários e grupos locais. As configurações locais de usuário ou grupo habilitam o

administrador para atribuir permissões que regulam o acesso e as atividades na máquina local.

Você pode acessar usuários e grupos locais de várias maneiras. Tente estes em uma máquina local:

- Pressione Windows+R para acessar o aplicativo Executar; em seguida, digite **lusrmgr.msc**.
- Abra o aplicativo de gerenciamento do computador e selecione Usuários e grupos.

Esta ferramenta permite ver todas as contas, visíveis e ocultas, no computador, bem como criar e gerir novos utilizadores e grupos. Por padrão, o Windows usa algumas contas internas, como Administrador, DefaultAccount e Guest. O antivírus do Windows Defender usa a conta WDAGUtility.

Monitor de desempenho

O Windows **Performance Monitor (perfmon.msc)** pode ser usado para monitoramento de desempenho em tempo real ou para registrar o desempenho ao longo do tempo.

Para acessar o Monitor de desempenho, abra o prompt Executar e procure Monitor de desempenho (ou apenas digite **perfmon**) na caixa de pesquisa e clique no nó Monitor de desempenho.

Muitos tipos diferentes de fatores de desempenho podem ser medidos. Você pode medir objetos, incluindo dispositivos físicos, como processador e memória, e software, como protocolos e serviços. Esses objetos são medidos com contadores. Por exemplo, um contador comum para o processador é % Processor Time.

Para ver se RAM adicional é necessária em um sistema, por exemplo, selecione o objeto denominado Arquivo de Paginação; em seguida, selecione os contadores % Usage e Pages/Seg, conforme descrito nas etapas a seguir:

Etapa 1. Clique no sinal + ou clique com o botão direito do mouse na tabela abaixo do gráfico e selecione **Adicionar contadores**.

Etapa 2. Selecione **Arquivo de paginação** como o objeto de desempenho e escolha **% Uso**.

Etapa 3. Clique em **Adicionar**.

Etapa 4. Selecione **Memória** como o objeto de desempenho e, em seguida, escolha **Páginas/seg** no menu suspenso.

Etapa 5. Clique em **Adicionar**.

Etapa 6. Clique em **OK** e execute os aplicativos normais para este computador.

Se o Monitor de desempenho indicar que o contador de % de uso do arquivo de paginação está consistentemente perto de 100 por cento ou o contador de páginas de memória/segundo está consistentemente maior que 5, adicione RAM para melhorar o desempenho.

Ferramentas Adicionais

Um técnico precisa saber informações sobre uma máquina e, em seguida, executar tarefas rotineiras, como manutenção de disco e outros ajustes. As ferramentas a seguir podem fornecer rapidamente informações e opções de manutenção. Basta digitar o nome da ferramenta na barra de pesquisa do Windows para obter acesso rápido aos aplicativos.

Informações do sistema (msinfo32)

A ferramenta **System Information (msinfo32.exe)** exibe uma grande quantidade de informações sobre o hardware do computador e a instalação do Windows em um sistema. Para acessar a ferramenta, digite **msinfo32** na barra de pesquisa ou execute **msinfo.exe**.

O Resumo do sistema (consulte a [Figura 6-14](#)) fornece informações básicas sobre a instalação do Windows e a configuração do hardware. Basta clicar em um subnó (painel esquerdo) para obter informações mais detalhadas sobre hardware do sistema, componentes ou ambiente de software. Para ir mais fundo, abra os nós no painel esquerdo. A [Figura 6-15](#) mostra os módulos de programa carregados listados.



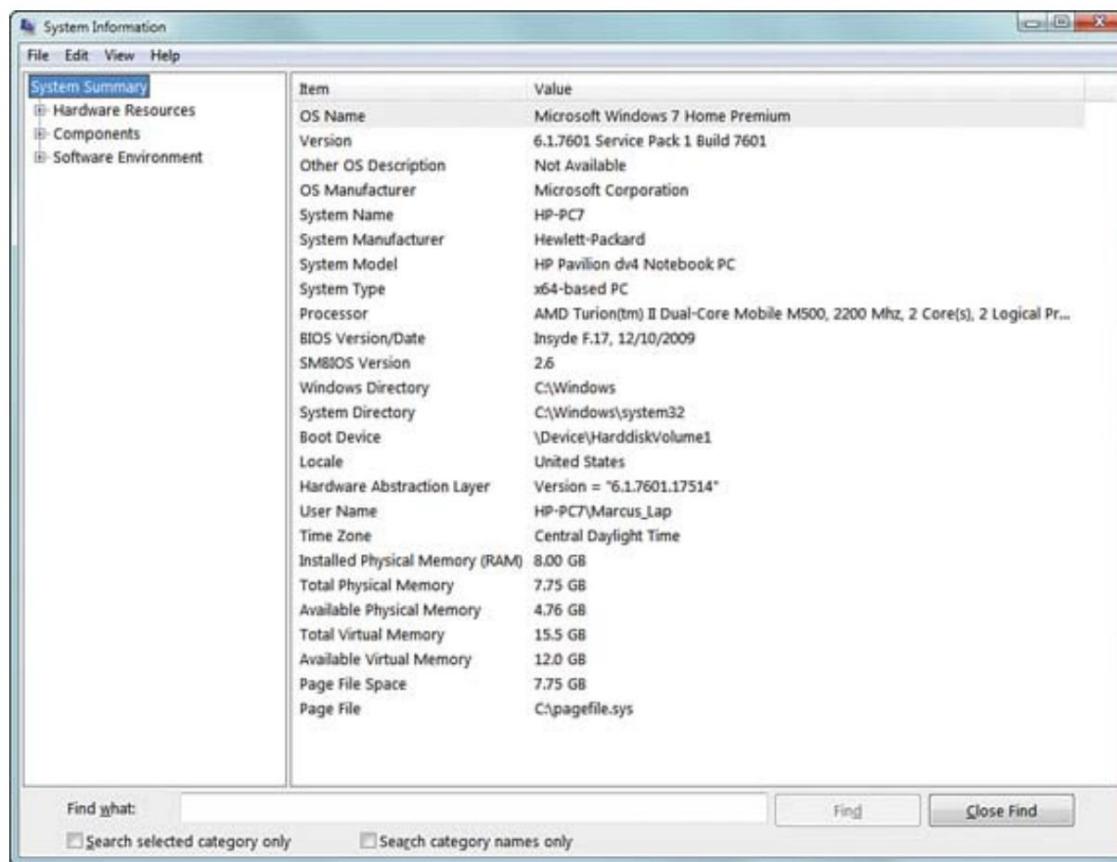


Figura 6-14 Resumo do sistema msinfo32

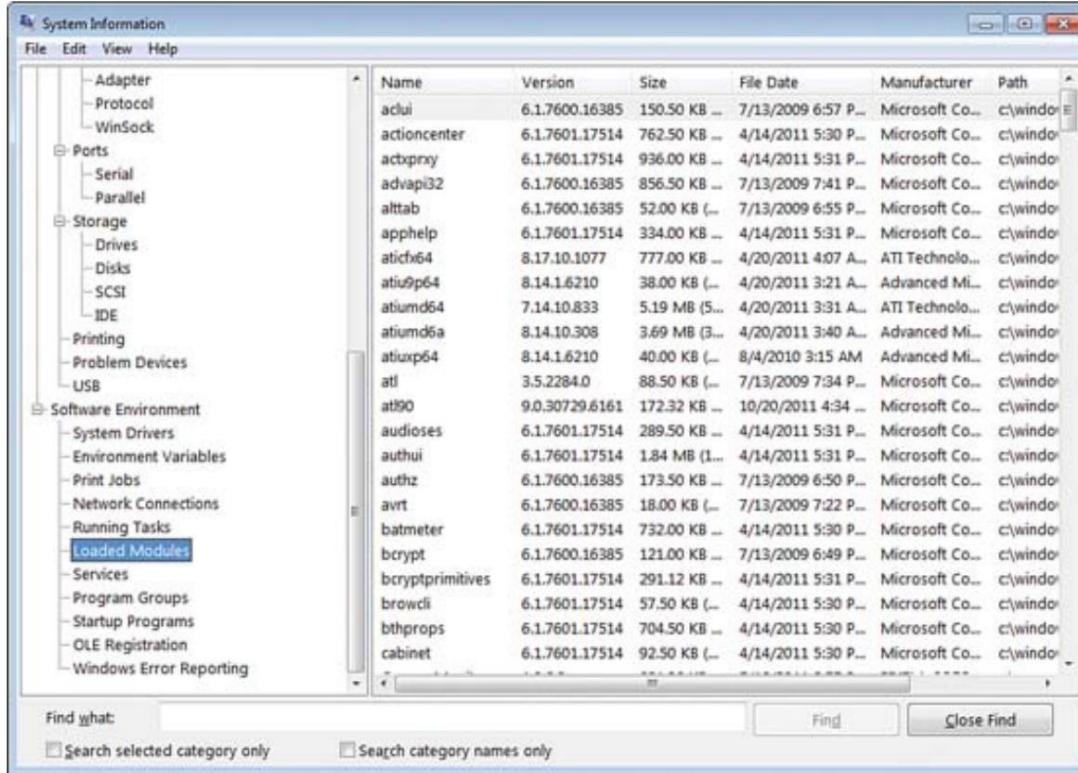


Figura 6-15 Exibição dos módulos do programa carregado msinfo32 (painele direito)

Use a janela Localizar para localizar informações específicas. Use o menu Arquivo para salvar um relatório ou exportá-lo como um arquivo de texto.

Monitor de recursos

O [**Monitor de recursos \(resmon.exe\)**](#) é semelhante ao Monitor de desempenho, mencionado anteriormente nesta seção. Ambos rastreiam o desempenho da CPU, memória e assim por diante. Para a maioria dos usuários, o Monitor de desempenho é suficiente para encontrar a maioria dos problemas e desabilitar processos, mas às vezes é necessária uma compreensão mais profunda dos recursos: é aí que entra o Monitor de recursos. O Monitor de recursos permite um rastreamento mais detalhado dos recursos. As figuras a seguir mostram os detalhes mais detalhados oferecidos no Monitor de recursos. A [Figura 6-16](#) descreve a visão geral fornecida quando o monitor é aberto; A [Figura 6-17](#) detalha as informações da rede, com informações adicionais sobre atividade, conexões e portas. Os gráficos à direita fornecem um contexto visual para os dados à esquerda.

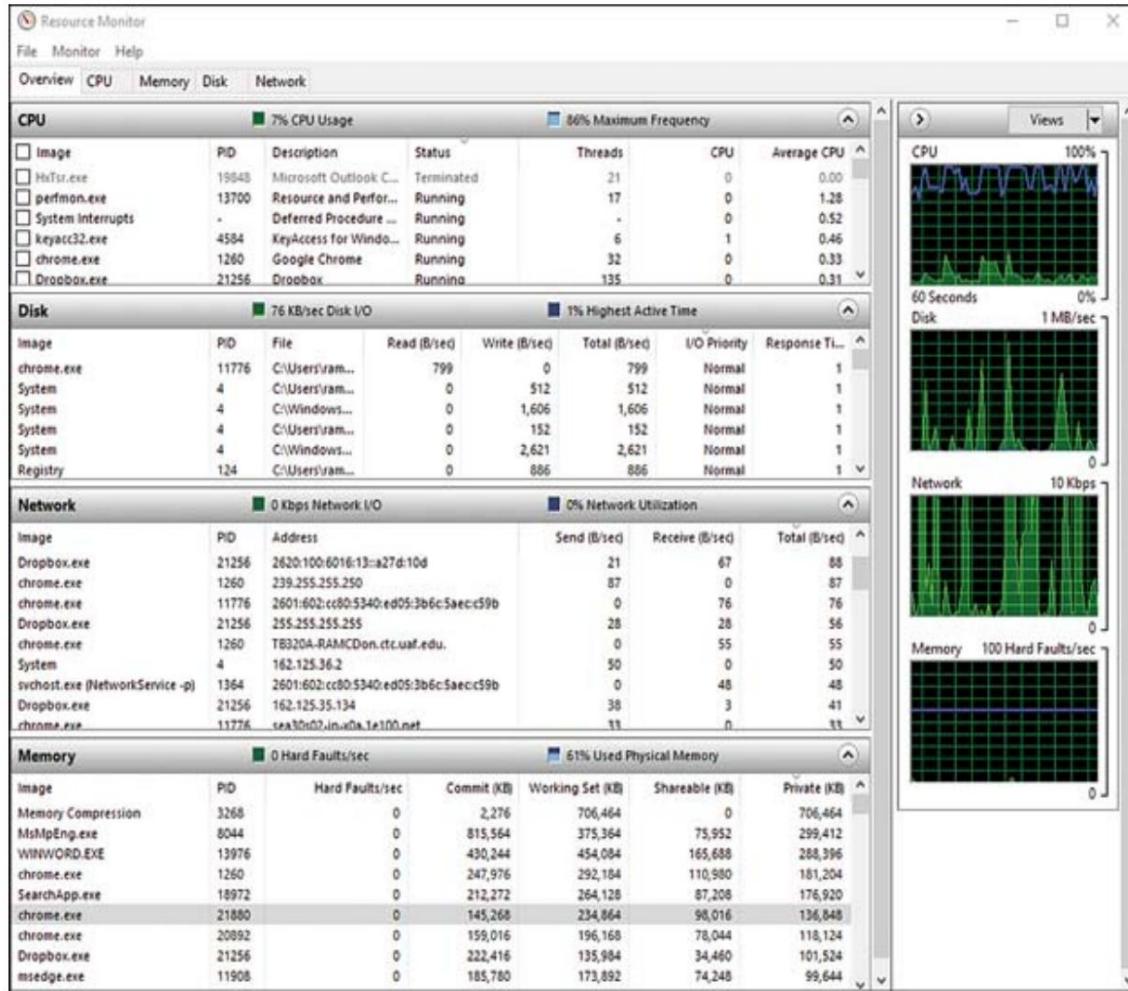


Figura 6-16 Janela do monitor de recursos (resmon.exe)

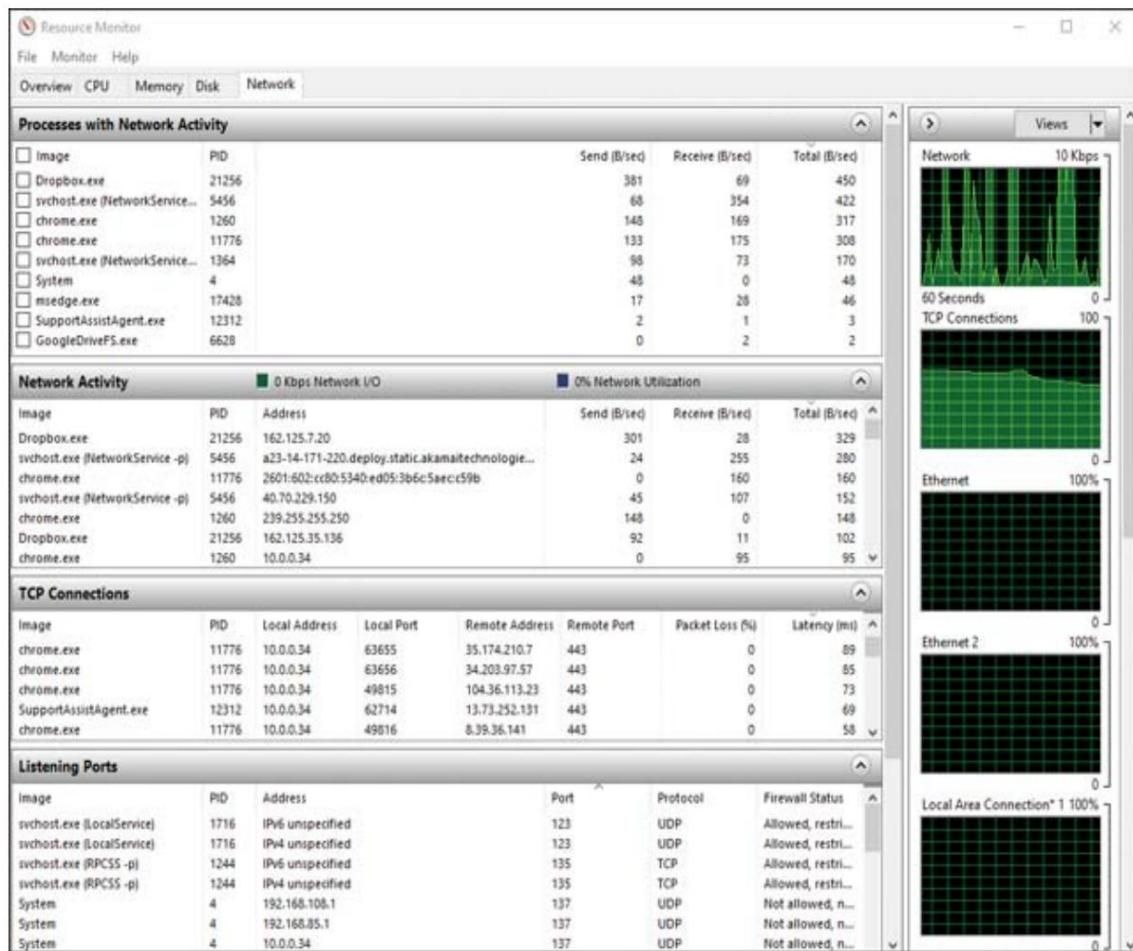


Figura 6-17 Monitor de recursos com a guia Rede selecionada

Key Topic

Utilitário de configuração do sistema

Use o utilitário de configuração do [sistema \(msconfig.exe\)](#) para configurar como o Windows é iniciado, para escolher programas e serviços de inicialização e para alterar o procedimento de inicialização.

O utilitário Microsoft System Configuration (msconfig.exe) permite a desativação seletiva de programas e serviços executados na inicialização. Se um computador estiver instável, funcionar mais lentamente do que o normal ou tiver problemas para inicializar ou desligar, o uso do msconfig pode ajudá-lo a determinar se um programa ou serviço em execução quando o sistema é iniciado está com defeito.

Para iniciar msconfig.exe, pressione Windows+R, digite **msconfig** e pressione Enter.

O msconfig possui uma interface multitabbed usada para controlar as opções de inicialização. A guia Geral (consulte a [Figura 6-18](#)) oferece Inicialização Normal, Diagnóstico (inicialização limpa) ou Seletiva. (Você escolhe quais itens e serviços carregar.) Use a guia Boot para especificar como inicializar um sistema Windows.

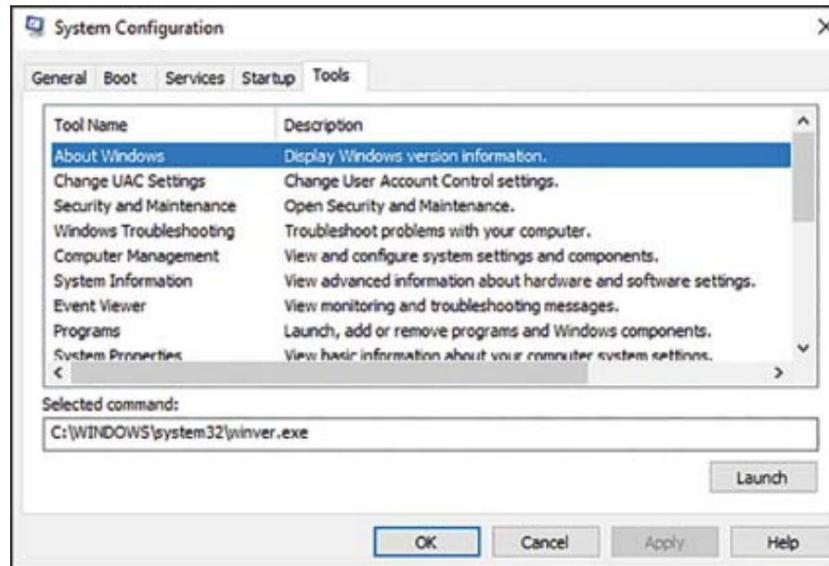


Figura 6-18 Guia de ferramentas do Utilitário de configuração do sistema (msconfig) em Windows 10

Use a guia Serviços para desativar ou reativar os serviços do sistema. Use a guia Ferramentas para iniciar a Restauração do sistema, Gerenciamento do computador e outras tarefas de gerenciamento. Ao tentar isso, observe que a guia Inicialização, antes usada para gerenciar programas de inicialização, agora está vinculada ao Gerenciador de Tarefas para essas alterações.

A [Figura 6-18](#) mostra a guia Ferramentas da caixa de diálogo Configuração do sistema no Windows 10. Observe que muitas das ferramentas listadas nesta seção podem ser acessadas a partir deste utilitário.

GORJETA

Quando você seleciona uma ferramenta na guia Ferramentas, o msconfig exibe a linha de comando necessária para executá-la. Adicione as opções desejadas antes de iniciar a ferramenta.

Limpeza de disco

A **Limpeza de Disco (cleanmgr.exe)** é um utilitário para otimizar unidades, removendo arquivos desnecessários e liberando espaço para um melhor desempenho do disco. A execução de **cleanmgr.exe** abre uma janela para escolher um disco para limpar. Quando um disco é selecionado, outra janela é aberta e apresenta caixas de seleção para selecionar os tipos de arquivo que podem ser removidos. Esses arquivos incluem arquivos temporários da Internet, a Lixeira e outros arquivos temporários. Se ainda for necessário mais espaço, selecione Limpar arquivos do sistema na Limpeza de disco e escolha os tipos de arquivo que você não precisa mais.

O Storage Sense é uma ferramenta conveniente no Windows 10 e 11 que facilita a manutenção automática do uso do armazenamento em um PC. Acesse o Storage Sense abrindo **Configurações > Sistema > Armazenamento**. A partir daqui, você pode habilitar ou desabilitar o Storage Sense. Se estiver ativado, outras configurações determinam como lidar com arquivos temporários e preferências para executar o utilitário.

Desfragmentar/otimizar unidades de disco A

desfragmentação de uma unidade de disco rígido pode ajudar a melhorar o desempenho do sistema, especialmente se a unidade for trocada com frequência. Com uso intenso, os dados em um disco podem se espalhar pela unidade, o que retarda o acesso. A desfragmentação é o processo de reorganização dos dados em blocos contíguos. A desfragmentação do armazenamento SSD não é tão necessária quanto nos HDDs, mas o Windows ainda pode desfragmentar SSDs em um agendamento com o aplicativo Optimize Drives (dfregui.exe) no Windows 10. A desfragmentação é definida por padrão e também pode ser agendada. A [Figura 6-19](#) mostra o aplicativo Optimize Drives no Windows 10.

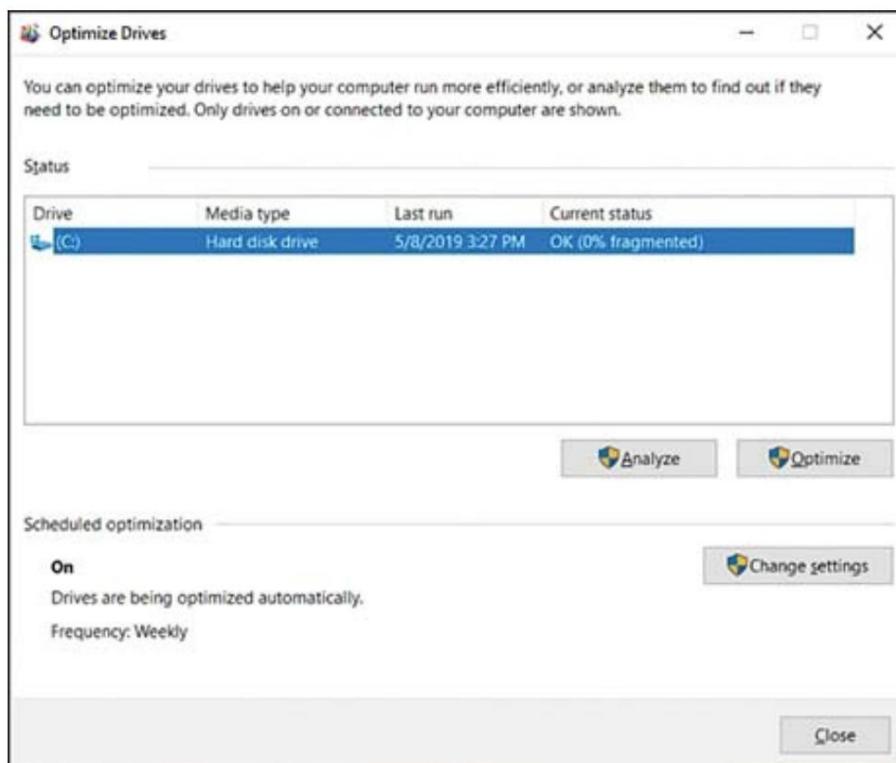


Figura 6-19 O aplicativo Optimize Drives no Windows 10

Editor do Registro



O Registro do Windows é um banco de dados hierárquico que contém todas as configurações e configurações usadas pelo Windows. O Editor do Registro é o aplicativo que você usa para exibir ou editar definições e configurações. Usuários avançados podem modificar e criar configurações no banco de dados do Registro.

Na maioria das circunstâncias normais, o Registro não precisa ser editado ou mesmo visualizado. No entanto, a edição do Registro pode ser necessária nas seguintes circunstâncias:

- Para visualizar uma configuração do sistema que não pode ser visualizada por outras interfaces.
- Para adicionar, modificar (alterando valores ou dados) ou remover uma chave do Registro que não pode ser alterada nos menus normais do Windows ou nas configurações do aplicativo. Isso pode ser necessário, por exemplo, para remover vestígios de um

programa ou dispositivo de hardware que não foi desinstalado corretamente ou para permitir a instalação de um novo dispositivo ou programa.

- Para fazer backup do Registro em um arquivo.

Para acessar o **[Editor do Registro \(regedit.exe\)](#)**, pressione Windows+R, digite o comando **regedit** e pressione Enter; ou use a barra de pesquisa e digite **regedit**.

As alterações feitas usando o regedit são salvas automaticamente ao sair. No entanto, pode ser necessário fazer logoff e logon novamente ou reiniciar o sistema para que as alterações entrem em vigor.

CUIDADO

O Registro nunca deve ser editado, a menos que uma cópia de backup tenha sido feita primeiro.

Nenhuma opção Desfazer existe para edições individuais e não há como descartar todas as alterações ao sair do regedit.

Editar o Registro do Windows pode ser difícil porque as chaves do Registro podem ser expressas em decimal, hexadecimal ou texto. Ao editar o Registro, certifique-se de seguir cuidadosamente as instruções do fornecedor.

A [Figura 6-20](#) mostra o Registro com uma modificação sendo feita na chave do Registro MenuShowDelay, que não pode ser acessada nos menus de exibição normais do Windows.

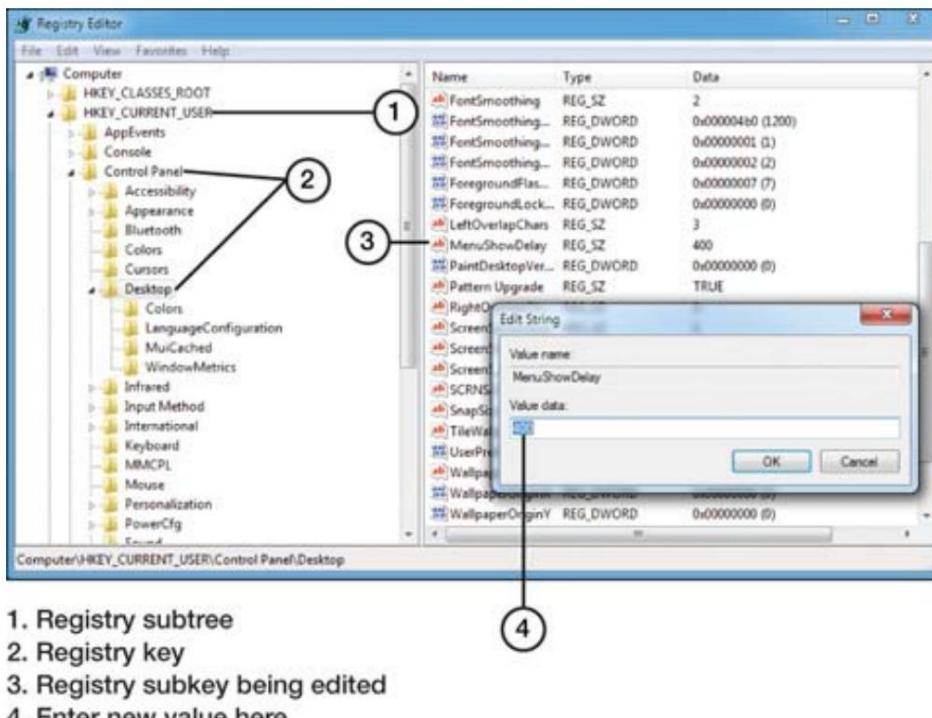


Figura 6-20 Usando o regedit

Sempre faça backup do Registro antes de editá-lo. Siga estas etapas para fazer backup de parte ou de todo o Registro em um arquivo de texto:

Etapa 1. Inicie o regedit.

Etapa 2. Para fazer um backup parcial, selecione a seção do Registro a ser copiada.

Etapa 3. Clique em Arquivo e selecione Exportar.

Etapa 4. Selecione um local para armazenar o backup do Registro.

Etapa 5. Insira um nome para o backup.

Etapa 6. Clique em Todos para fazer backup de todo o Registro. Clique em Filial selecionada para fazer backup apenas da ramificação do Registro selecionada na etapa 2.

Etapa 7. Clique em Salvar.

Utilitários do Painel de Controle do Windows 10

220-1102: Objetivo 1.4: Dado um cenário, use o utilitário apropriado do Painel de Controle do Microsoft Windows 10.

O Painel de Controle é o principal ponto de partida para ajustar as configurações de hardware e interface do usuário no Windows. Embora o Windows 10 inclua Configurações, muitas configurações no Windows são realizadas por meio do Painel de Controle.

Observação

Assim como muitas vezes existem diferentes maneiras de acessar informações no sistema operacional Windows, esta seção repete alguns conteúdos de outros capítulos, mas no contexto do Painel de Controle. Essa repetição é feita para ajudar os leitores que estão rastreando os objetivos do CompTIA A+ Core 2, que possuem elementos de redundância.

Iniciando o Painel de Controle

Para iniciar o Painel de Controle no Windows 10, digite **Painel de Controle** na caixa de pesquisa e selecione o link Painel de Controle. Outra opção é pressionar Windows+R, digitar **control** e pressionar Enter.

Opções da Internet

Acesse o menu Opções da Internet através do Painel de Controle. A [Figura 6-21](#) mostra a caixa de diálogo Propriedades da Internet que aparece, com a guia Segurança selecionada. Observe que essas opções diferem das opções disponíveis na Central de Rede e Compartilhamento.

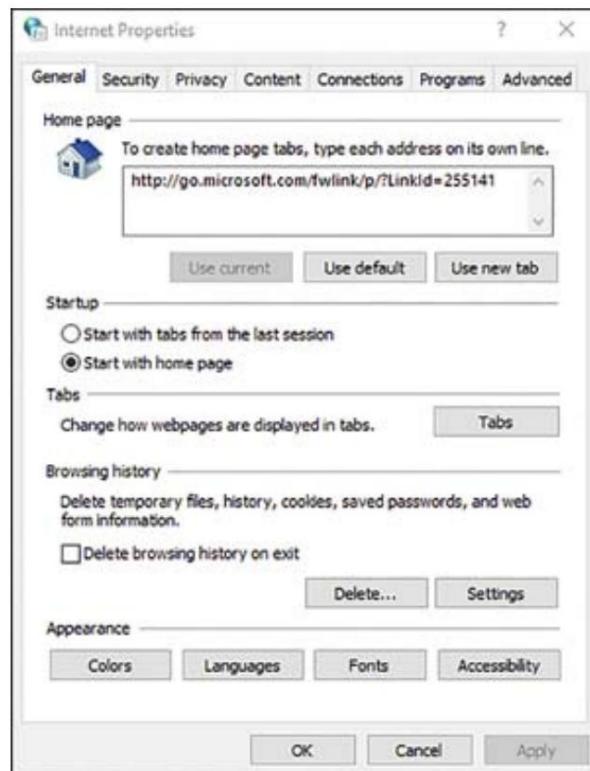


Figura 6-21 Opções da Internet no Painel de Controle

A caixa de diálogo Propriedades da Internet acessada no Painel de controle possui sete guias, que a [Tabela 6-6](#) descreve.



Tabela 6-6 Guias da caixa de diálogo Propriedades da Internet

Aba	Função
Em geral	Definir a página inicial; definir configurações de guia; excluir histórico de navegação, cookies, arquivos temporários e senhas salvas; mudar a aparência; e definir as configurações de acessibilidade
Segurança	Configurar zonas de segurança
Privacidade	Selecionar as configurações de privacidade para a zona atual, configurações de localização, bloqueador de pop-up e configurações de navegação InPrivate
Contente	Definir opções para segurança familiar, gerenciamento de certificado SSL, preenchimento automático e feeds

Aba	Função	
Conexões	Defina opções para VPNs, dial-up, conexões LAN e servidores proxy	
Programas	Selecione o navegador da Web padrão, gerencie complementos, selecione o editor de HTML padrão e defina os aplicativos padrão para e-mail e outros serviços de Internet	
Avançado	Ativar e desativar gráficos acelerados; configurar configurações de acessibilidade, configurações de navegação, configurações de HTTP, configurações internacionais, configurações de multimídia e configurações de segurança; e redefina o Internet Explorer para as configurações padrão	
Muitos dos utilitários do Painel de Controle nos objetivos A+ são discutidos em outros capítulos. A Tabela 6-7 os resume brevemente.		
Tabela 6-7 Utilitários do painel de controle e suas configurações		
Ao controle	Função	Capítulo
Painel		
Utilitário		
Dispositivos e impressoras	Adicionando monitores, câmeras, scanners e assim por diante.	3
Programas e características	Desinstalar e alterar programas.	6
rede e Compartilhamento Centro	Visualização e gerenciamento de conexões de rede.	2
Sistema	Contém muitas das outras configurações no painel de controle. A maioria das configurações que os usuários desejam alterar residem aqui, incluindo Windows Defender, som e exibições.	Vários

Ao controle	Função	Capítulo
Painel		
Utilitário		
Windows Configurando a segurança.		7
Firewall de defesa		
Correspondência	Ajustando as configurações de e-mail para usuários de e-mail do Microsoft Outlook.	3
Som	Configuração de alto-falantes, fones de ouvido e microfones; gerenciamento de sons e temas de eventos.	1

As seções a seguir discutem alguns utilitários menos intuitivos do Painel de controle.

Contas de usuário

No Painel de controle, se você selecionar Contas, poderá gerenciar a conta do usuário e o acesso a outros usuários. A [Figura 6-22](#) mostra as opções de conta do Windows 10 no Painel de controle.

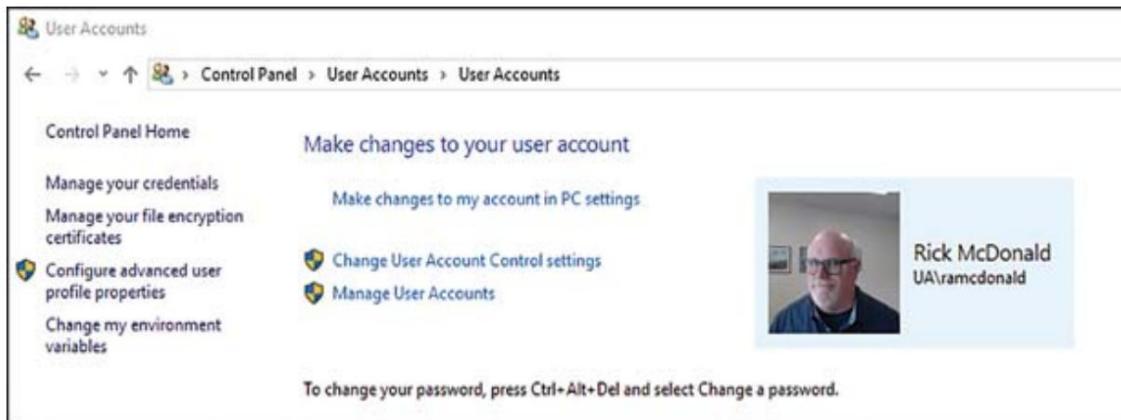


Figura 6-22 Contas de usuário no painel de controle

Gerenciador de Dispositivos

O Gerenciador de Dispositivos acessado no Painel de Controle é o mesmo discutido no MMC, na seção anterior, “Sistema Operacional (SO) Microsoft Windows 10”. É um bom ponto de partida para adicionar e remover dispositivos e solucionar problemas de dispositivos.

Opções de indexação A

página Opções de indexação no Painel de controle gerencia a indexação de dados em um computador. O uso dessas opções pode ajudar a aumentar a facilidade e a velocidade de localização de informações. Assim como o índice no final deste livro o ajuda a localizar um tópico específico, a indexação do computador torna mais fácil para a ferramenta de pesquisa e aplicativos selecionados encontrar informações úteis.

Os arquivos e seu conteúdo de texto são indexados por padrão. Se um usuário estiver procurando por um documento específico e se lembrar de palavras-chave, mas não do nome do documento, a digitação das palavras retornará documentos que usam essas palavras.

A indexação pode ser administrada. Se ativado, ele indexa automaticamente novos documentos e arquivos à medida que são criados.

Ferramentas administrativas

A página Ferramentas Administrativas no Painel de Controle é uma maneira fácil de acessar ferramentas para gerenciar o computador. Algumas dessas ferramentas são familiares da seção anterior, como os utilitários Informações do sistema, Monitor de recursos, Configuração do sistema, Limpeza de disco, Desfragmentação de disco, Editor do registro e Visualizador de eventos. Várias das ferramentas neste painel são discutidas em outras seções.

Opções do Explorador de Arquivos

A folha de propriedades Opções do File Explorer afeta como o Explorer faz o seguinte:

- Exibe informações de arquivos e pastas (guia Exibir)
- Seleciona pastas para indexar para pesquisa (guia Pesquisar)
- Abre pastas (guia Opções gerais)

Por padrão, o File Explorer oculta as seguintes informações do arquivo:

- Extensões de arquivo para tipos de arquivo registrados. Por exemplo, um arquivo chamado letter.docx é exibido como letter porque o Microsoft Word está associado a arquivos .docx.
- O caminho completo para a pasta atual.

- Arquivos ou pastas com atributos ocultos ou do sistema, como a pasta AppData.
- A pasta do Windows.

Ocultar essas informações visa tornar mais difícil para os usuários "quebrar" Windows, mas ter essas informações ocultas também dificulta o gerenciamento e a solução de problemas.

As configurações ocultas padrão podem ser alteradas usando o miniaplicativo File Explorer Options no Painel de Controle. Para alterar os padrões, siga estas etapas:

Etapa 1. Abra o Explorador de Arquivos.

Etapa 2. Clique ou toque na guia **Exibir. Selecione o menu suspenso **Opções** e escolha **Alterar pasta e opções de pesquisa**.**

Etapa 3. Selecione as opções desejadas (consulte a [Figura 6-23](#)). As seguintes alterações são recomendadas para usuários finais experientes:

- Ative a opção Exibir o caminho completo na barra de título
- Para ver todas as extensões de arquivo, desative a opção Ocultar extensões para tipos de arquivo conhecidos.
- Se você estiver mantendo ou solucionando problemas em um sistema, altere o seguinte:
 - Para exibir arquivos ocultos, ative a configuração Mostrar arquivos, pastas e unidades ocultos.
 - Desative a configuração Ocultar arquivos protegidos do sistema operacional.

Etapa 4. Clique em **OK** para fechar a janela Opções de pasta.

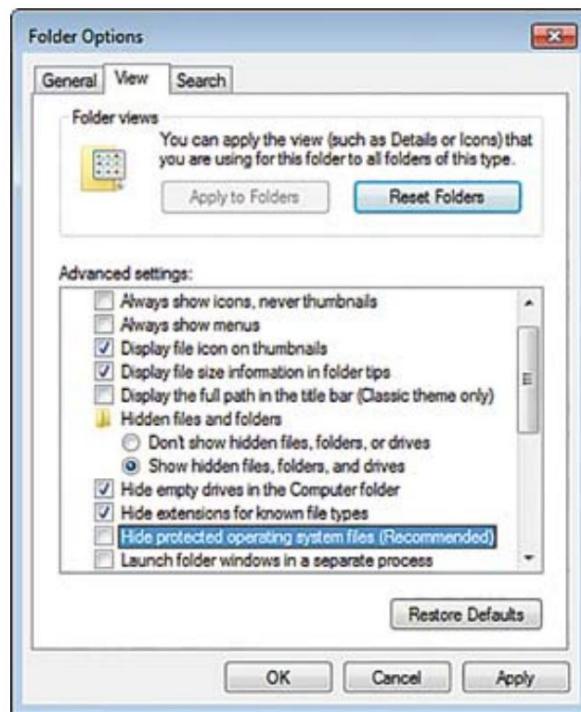


Figura 6-23 A guia Exibir da caixa de diálogo Opções de pasta no Windows com o conjunto de opções recomendadas

Opções de energia

Você pode gerenciar as opções de energia no miniaplicativo Opções de energia do Painel de controle. Se um ícone de Opções de energia estiver disponível na área de notificação da barra de tarefas do Windows, use-o para visualizar a configuração atual da opção de energia e, se desejar, selecione outra opção.

hibernar

A opção Hibernar, originalmente disponível no Windows 7, cria um arquivo de disco especial (hiberfil.sys) que registra os aplicativos abertos, o conteúdo da memória e as posições dos aplicativos na tela. Na verdade, ele “pausa” o sistema para que você possa retornar à direita de onde parou.

No Windows 10, o Hibernate não é uma opção listada para o menu de desligamento; no entanto, ele pode ser adicionado modificando um plano de energia: Selecione o link Escolher a função dos botões de energia em **Configurações de energia e suspensão > Configurações adicionais de energia**. Hibernar é uma opção disponível quando você está escolhendo o que acontece quando você pressiona o botão liga/desliga, pressiona o botão de suspensão ou

feche a tampa. Para despertar um sistema da hibernação, pressione o botão liga/desliga no computador. Se o sistema tiver uma senha definida para acesso, você será solicitado a inserir a senha para reiniciar o sistema.

Observação

As opções de suspensão e hibernação estão disponíveis. São opções de economia de energia semelhantes, mas diferem no local onde armazenam os programas ativos. O modo de suspensão armazena programas em execução na RAM e usa pouca energia. O Hibernate os armazena no disco rígido e permite que a energia seja desligada.

Planos de Energia

As versões padrão do Windows oferecem três planos de energia padrão (com um quarto plano de energia disponível apenas no Windows Pro):

- **Equilibrado:** plano padrão. Equilibra o desempenho com o consumo de energia.
- **Economia de energia:** reduz o desempenho da CPU e o brilho da tela mais do que o plano Balanceado, para maior duração da bateria.
- **Alto desempenho:** oferece o desempenho de CPU mais rápido, tela mais brilhante e menor duração da bateria.
- **Desempenho máximo:** limitado à edição Windows 10 Pro Workstation para computadores de última geração.

Observação

Se o seu computador for compatível com Modern Standby, um plano de gerenciamento de energia do Windows, pode ser que a única opção disponível seja Equilibrado. No entanto, você ainda pode criar um plano personalizado. Computadores de mesa ocultam o Economizador de energia por padrão; os laptops ocultam o Alto desempenho por padrão.

Observação

Alguns fornecedores de dispositivos portáteis oferecem planos adicionais em sistemas com o Windows pré-instalado. Os tablets oferecem apenas o plano de energia Balanceado.

Para alterar um plano, clique ou toque em Alterar configurações do plano. Você pode alterar as configurações de suspensão ou hibernação para tempos de suspensão, tempos de exibição e níveis de bateria. A Figura 6-24 mostra o menu **Opções de energia > Configurações avançadas**.

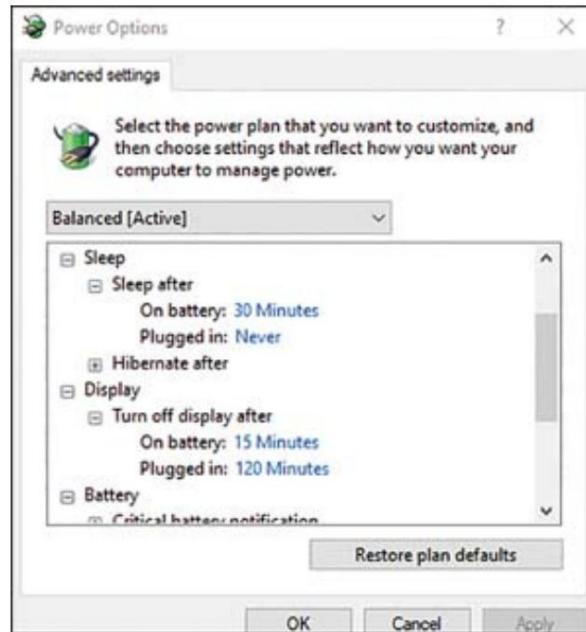


Figura 6-24 Opções avançadas de energia

Para criar um novo plano de energia, clique em Criar um plano de energia na caixa de diálogo Opções de energia. Em seguida, na caixa de diálogo Criar um plano de energia, siga estas etapas:

Etapa 1. Selecione um plano para usar como base para seu plano.

Etapa 2. Insira um nome de plano e clique em **Avançar**.

Etapa 3. Especifique os intervalos para exibição e suspensão e clique em **Criar**.

Suspender/Suspender

O modo de suspensão/suspensão é compatível com o Windows 10. Se o sistema não entrar corretamente no modo de suspensão/espera, os programas de inicialização podem estar interferindo nesse modo. Use o **msconfig** para desativar seletivamente os programas de inicialização até descobrir o aplicativo ofensivo.

Com a maioria dos laptops e muitos desktops, você pode colocar o computador no modo de suspensão pressionando uma tecla especial de suspensão ou pressionando a tecla liga/desliga e soltando-a imediatamente. Para alterar a forma como a tecla de suspensão ou energia funciona, modifique seu plano de energia.

Opções de espera, tampa e inicialização rápida As

configurações de energia, suspensão e fechamento da tampa são gerenciadas nas opções de energia, escolhendo o link What Closing the Lid Does. Isso abre as configurações do sistema para opções de energia. Observe que as opções são definidas com caixas de seleção e menus suspenso, conforme mostrado na [Figura 6-25](#). Esta figura mostra opções para não fazer nada, dormir, hibernar e desligar.

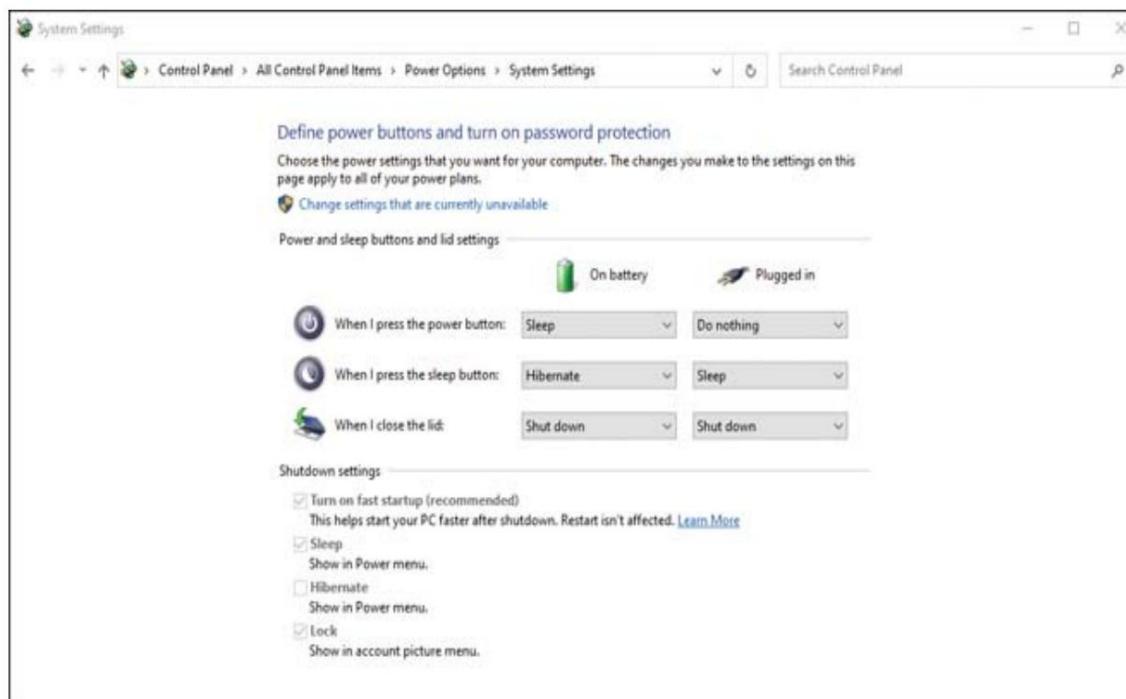


Figura 6-25 Opções avançadas de energia

Universal Serial Bus (USB) Suspensão seletiva

A suspensão seletiva de USB é uma configuração de gerenciamento de energia que permite que um computador saia do modo de suspensão com um sinal via porta USB, como um mouse USB. A configuração é necessária porque, se todas as portas USB forem suspensas, o movimento do mouse não ativará o computador; portas USB seletivas são definidas para responder a um sinal de um dispositivo conectado.

Ocasionalmente, esse recurso, ativado por padrão, pode causar problemas com dispositivos USB. Desativar a configuração pode ajudar porque o modo de suspensão não desliga mais os dispositivos USB.

Para desativar a suspensão seletiva de USB no menu Opções de energia, clique no link Alterar configurações do plano e clique no link Alterar configurações avançadas de energia. Isso abre o menu na [Figura 6-26](#). Abra as configurações de USB e selecione Desativar e, em seguida, selecione OK para salvar a alteração.

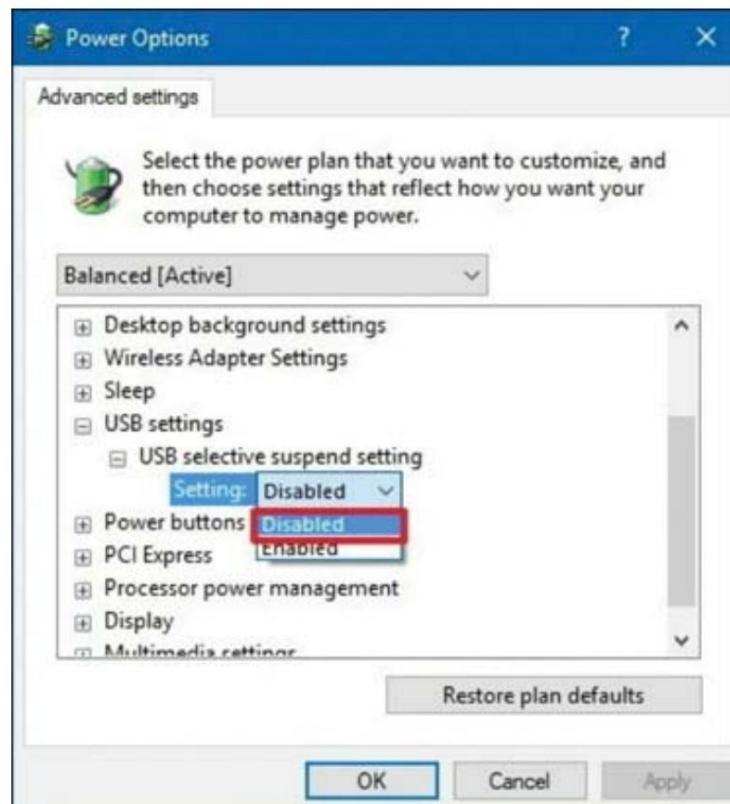


Figura 6-26 Configurações avançadas de suspensão seletiva de USB

Observação

Para que o modo de suspensão/espera funcione corretamente, o sistema precisa suportar a configuração de energia S3 no BIOS/UEFI do sistema.

Facilidade de acesso

As configurações **de facilidade de acesso** são usadas para personalizar as configurações de acordo com as necessidades e gostos do usuário. Pesquise por Facilidade de acesso e selecione o aplicativo. Observe que a coluna à esquerda possui grupos de configurações para Visão, Audição e Interação. Essas configurações ajudam os usuários com habilidades variadas a interagir mais facilmente com o computador.

A [Figura 6-27](#) mostra as configurações disponíveis na seção de teclado do grupo Interação.

Explore todas as configurações para se familiarizar com todas as opções disponíveis.

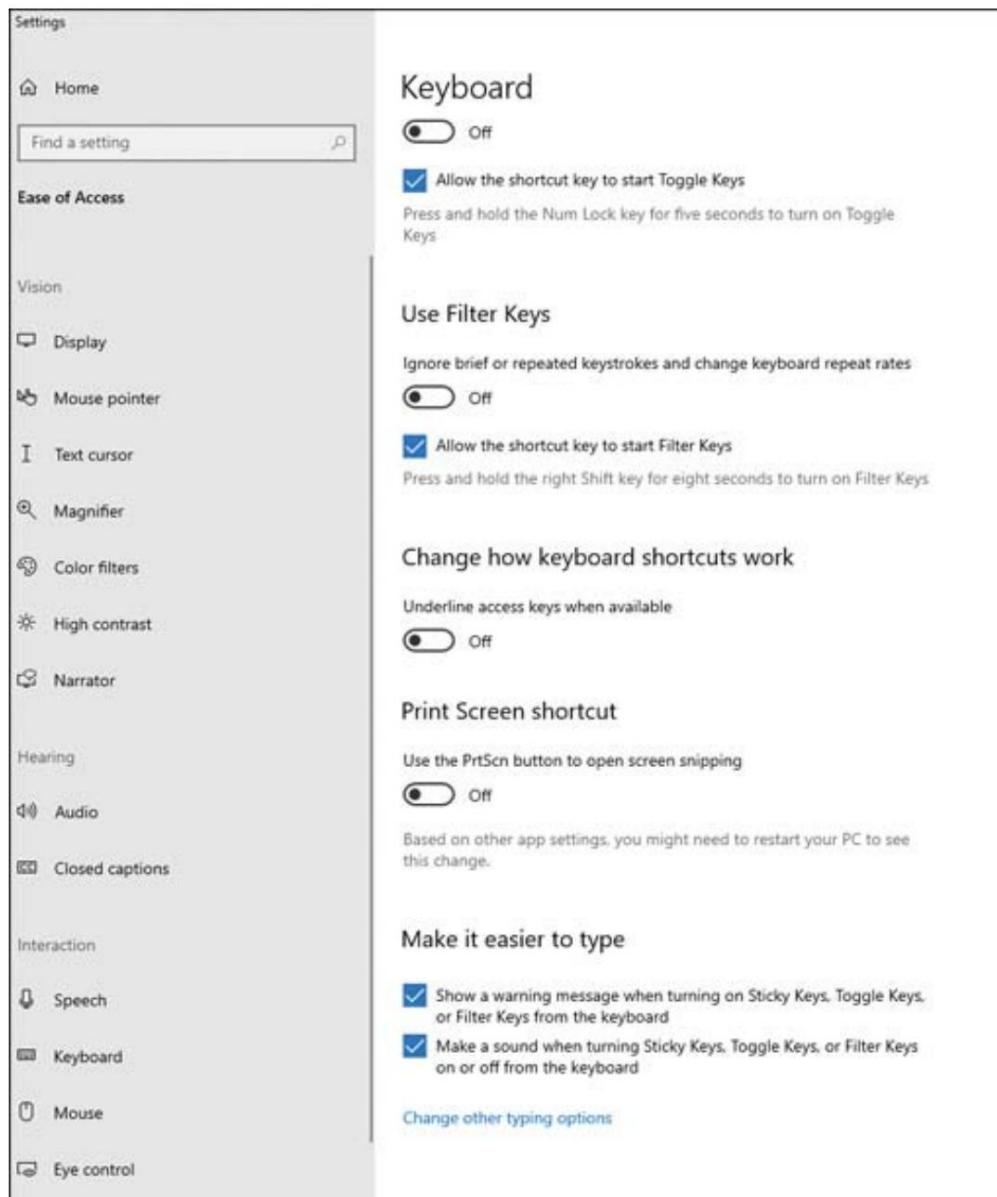


Figura 6-27 Configurações do teclado no menu de configurações de facilidade de acesso

Configurações do Windows



220-1102: Objetivo 1.5: Dado um cenário, use as configurações apropriadas do Windows.

Um entendimento completo do menu Configurações é essencial para um técnico de suporte de TI.

Esta seção fornece uma visão geral básica das principais configurações do Windows.

É recomendável que você explore todas as opções no menu Configurações conforme as seções são realçadas e descritas.

Acesse o menu Configurações usando o atalho Windows+X e selecione Configurações digitando n. Com o mouse, selecione o ícone do Windows e clique na engrenagem Configurações no menu. As opções de configurações têm sua própria barra de pesquisa, que é a maneira mais fácil de encontrar configurações desconhecidas. A seção anterior examinou as configurações de facilidade de acesso, mas há muito mais para explorar.

Observação

Algumas configurações serão exibidas se um computador estiver em uma rede gerenciada.

Hora e Idioma

O menu para Hora e Idioma inclui as seguintes configurações:

- **Data e Hora:** Configurando formatos de hora e data e configurações automáticas de hora
- **Região:** Configurando o país ou região e o formato local de data e hora
- **Idioma:** adicionar idiomas e alterar as opções de idioma do teclado
- **Fala:** Ativando o reconhecimento de voz e escolhendo a voz do computador

Atualização e segurança

O Capítulo 7 aborda a segurança, mas você deve estar familiarizado com as configurações de segurança aqui. Certifique-se de visitar e familiarizar-se com os links listados à esquerda em Windows Update e Segurança no menu Configurações.

Personalização

O menu para Personalização inclui configurações para o seguinte:

- **Plano de fundo:** escolha de uma cor de plano de fundo, imagem ou apresentação de slides
- **Cores:** Cores claras e escuras para menus (como o menu do Windows)
- **Tela de bloqueio:** configurações para bloquear um computador ocioso e a tela bloqueada
- **Temas:** opções de sons de fundo, cores ou imagens
- **Fontes:** opções de fonte para texto do Windows e ferramentas para importar fontes
- **Menu Iniciar (tecla do Windows):** A tecla do Windows indica qual tecla do teclado está sendo configurada
- **Barra de tarefas:** configurações de preferência para exibição de emblema, mostrando ou ocultando a barra de tarefas e definindo o prompt de comando/padrão do PowerShell ao clicar com o botão direito do mouse na barra de tarefas

aplicativos

O menu para Apps inclui as seguintes configurações:

- **Aplicativos e recursos:** instalação de novos aplicativos ou remoção dos antigos
- **Aplicativos padrão:** determinando os aplicativos escolhidos para música, fotos, e-mail, navegador e assim por diante
- **Mapas off-line:** download de mapas para usar quando estiver off-line
- **Aplicativos para sites:** configuração de abertura de sites com um aplicativo ou navegador
- **Reprodução de vídeo:** Configurando a resolução de vídeo e as configurações de energia da bateria
- **Inicialização:** Gerenciando quais aplicativos serão iniciados ao fazer login

Privacidade

As configurações de privacidade geralmente tratam do compartilhamento de suas informações de uso e histórico de dados com a Microsoft para fins de pesquisa. Essas configurações determinam o que é compartilhado e o que não é:

- **Geral:** Compartilhamento de atividades na web e lançamentos de aplicativos, gerenciamento de configurações de publicidade na web
- **Fala:** coletando padrões de fala
- **Personalização de tinta e digitação:** coleta de caligrafia do usuário e padrões de digitação
- **Diagnóstico e Feedback:** Compartilhamento de problemas de software e travamentos com Microsoft
- **Histórico de atividades:** Gerenciando configurações para armazenamento local e compartilhamento externo de atividades
- **Permissões de aplicativos:** Gerenciando configurações de privacidade para cada aplicativo ou dispositivo

Sistema

Este é provavelmente o aplicativo mais importante para estudar. As configurações do sistema são usadas em todo o conteúdo A+ deste livro, e muitas já estarão familiarizadas.

Muitas das configurações afetam o desempenho do computador.

Dispositivos

O menu para Dispositivos inclui as seguintes configurações:

- **Bluetooth e outros dispositivos:** Gerenciando configurações de teclado, mouse, áudio e assim por diante
- **Impressoras e Scanners:** Adicionar e remover impressoras e scanners
- **Mouse:** Gerenciando as configurações do mouse, como as opções de botão principal, rolagem e ponteiro
- **Touchpad:** Gerenciando configurações de sensibilidade, rolagem, zoom e assim por diante
- **Digitação:** Gerenciando configurações para verificação ortográfica, sugestões de texto e opções da barra de espaço
- **Caneta e tinta de janela:** configurações de manipulação para a fonte de escrita manual

- **Reprodução automática:** determinando as configurações padrão para reproduzir vídeos ou músicas de aplicativos
- **USB:** Emitir notificações de carregamento e gerenciar configurações de bateria

Rede e Internet

O menu para Rede e Internet inclui as seguintes configurações:

- **Status:** Gerenciando informações gerais sobre as configurações e atividades atuais da rede
- **Wi-Fi:** Definir configurações específicas de Wi-Fi, lidar com informações de IP e hardware
- **Ethernet:** conceder acesso às configurações de interface Ethernet física e virtual
- **Dial-up:** conceder acesso às configurações de discagem se a linha telefônica e o modem estiverem disponíveis
- **VPN:** Permitir e adicionar acesso à rede privada virtual
- **Modo Avião:** Ativando e desativando dados sem fio, Bluetooth e celular
- **Mobile Hotspot:** Compartilhamento e conexão com a Internet via Bluetooth ou Wi-fi
- **Proxy:** Gerenciando configurações para usar um servidor proxy (não aplicável a VPN)

Jogos

O menu para Gaming inclui as seguintes configurações:

- **Barra de jogos do Xbox:** Configurando atalhos em uma barra de jogos do Xbox
- **Capturas:** Gerenciando as configurações para capturar o áudio e o vídeo do jogo
- **Modo de jogo:** otimizando o PC para jogos
- **Xbox Networking:** Monitorando o status e o desempenho, lidando com o Xbox Conectividade ao vivo

contas

O menu para Contas inclui as seguintes configurações:

- **Suas informações:** Gerenciando configurações de perfil para o usuário
- **E-mail e contas:** adicionar contas usadas por outros aplicativos para facilitar o login
- **Opções de login:** Configurando procedimentos de login com configurações e requisitos de segurança
- **Acessar Trabalho ou Escola:** Manipulando configurações de conexão para computadores gerenciados em um domínio
- **Outros usuários:** Adicionando outras contas ao computador
- **Sincronize suas configurações:** permitindo que as configurações sejam sincronizadas entre dispositivos em um conta Microsoft

Recursos de rede do Microsoft Windows em um

Cliente/área de trabalho



220-1102: Objetivo 1.6: Dado um cenário, configurar os recursos de rede do Microsoft Windows em um cliente/desktop.

A rede do Windows inclui três tipos diferentes de redes, controle remoto e opções de assistência, um firewall integrado e muito mais. As seções a seguir podem ajudá-lo a dominar os conceitos de rede.



Grupo de trabalho vs. Configuração de

domínio O Windows 10 oferece suporte a dois tipos diferentes de redes: grupos de **trabalho** e **domínios**. As seções a seguir descrevem como eles diferem um do outro.

Rede de grupo de trabalho

O Windows 10 oferece suporte a redes de grupo de trabalho. Em uma rede de grupo de trabalho, aplica-se o seguinte:

- Todos os computadores podem compartilhar pastas e dispositivos com outros computadores em um arranjo ponto a ponto. O compartilhamento de arquivos e impressoras (configurado por padrão) é necessário para qualquer computador que compartilhará recursos.
- Todos os computadores devem fazer parte da mesma rede local ou sub-rede. Por exemplo, computadores no intervalo de endereços IP 192.168.1.100– 192.168.1.120 com a sub-rede 255.255.255.0 podem compartilhar recursos entre si, mas não com computadores no intervalo de endereços IP 192.168.2.100–192.168.2.120.
- O grupo de trabalho não possui senha; no entanto, cada computador deve ter uma conta de usuário para cada usuário que acessará esse computador (a menos que o compartilhamento protegido por senha esteja desabilitado). Por exemplo, um computador pode ter uma conta para Mark e uma conta para Mary, e outro computador pode ter uma conta para Mark e uma conta para Jerry. Mark pode se conectar a ambos os computadores, mas Mary e Jerry podem se conectar a apenas um computador. Nessa situação, Mark poderia usar um dos computadores e fazer login via rede em outro computador.

O grupo de trabalho é identificado na seção Especificação do dispositivo da planilha Sobre o sistema. Vá para Configurações, selecione Sistema e selecione Sobre no menu de links à esquerda.

A maneira mais fácil de visualizar o nome do seu computador é digitá-lo na caixa de pesquisa; a opção de visualizar o nome do seu dispositivo está vinculada à página Sobre acima.

Criando um grupo de trabalho

Para criar um grupo de trabalho no Windows, siga estas etapas:



Etapa 1. Configure todos os dispositivos no grupo de trabalho para usar o mesmo intervalo de endereços IP e a mesma sub-rede. Se os dispositivos obtiverem seus endereços IP de um roteador, esta etapa já foi realizada para você.

Etapa 2. Confirme se cada dispositivo possui um nome de computador exclusivo. O nome é gerado automaticamente quando o Windows é instalado em um dispositivo. Para verificar o nome, pressione Windows+R, digite o comando **sysdm.cpl** na caixa de diálogo Executar e pressione Enter. Alternativamente, simplesmente clique com o botão direito do mouse em **Iniciar > Configurações** e selecione **Sistema** para abrir a tela Configuração Sobre. Uma maneira fácil de acessar as Propriedades do Sistema é abrir o Explorador de Arquivos, clicar com o botão direito do mouse em **Este PC** e selecionar **Propriedades**.

Etapa 3. Confirme se cada dispositivo está no mesmo grupo de trabalho. (O nome padrão do grupo de trabalho é WORKGROUP.)

Configuração de domínio

Redes maiores, incluindo redes com usuários em vários locais, usam rede de domínio. Alguns dos recursos especiais da rede de domínio incluem o seguinte:

- **Recursos compartilhados** (arquivos, pastas, impressoras e dispositivos) e contas de usuário são armazenados em servidores. Um servidor Active Directory é usado para autenticar usuários e outros servidores podem ser usados para impressão, arquivo, e-mail e outros serviços.
- As contas de usuário não estão vinculadas a um computador específico. Um usuário em um domínio pode usar qualquer computador ou computadores no domínio e ter acesso a seus arquivos e recursos compartilhados.
- A Diretiva de Grupo pode limitar os recursos disponíveis para um determinado usuário. Por exemplo, as configurações de Diretiva de Grupo podem impedir que um usuário conecte uma unidade flash USB.
- A Diretiva de Grupo também pode limitar as definições de configuração disponíveis para um usuário. Por exemplo, a Diretiva de Grupo pode ser usada para desativar a Reprodução Automática para dispositivos de mídia removível.
- Diferentes redes locais com centenas a milhares de usuários podem fazer parte de um único domínio.

A configuração do domínio para um computador é executada na seção Nome do computador da folha de propriedades do sistema. Para ingressar em um domínio, siga estas etapas:

Etapa 1. Abra a folha de Propriedades do sistema.

Etapa 2. Clique ou toque em **Alterar configurações**.

Etapa 3. Na guia Nome do computador, clique ou toque em **ID da rede**.

Etapa 4. Confirme se a opção Este computador faz parte de uma rede comercial está selecionada. Clique ou toque em **Avançar**.

Etapa 5. Confirme se Minha empresa usa uma rede com um domínio está selecionada. Clique ou toque em **Avançar**.

Etapa 6. Revise as informações necessárias para se conectar a um domínio e clique em **Próximo**.

Etapa 7. Insira o nome de usuário, a senha e o nome de domínio e clique em **Avançar**.

Etapa 8. Clique em **OK** na mensagem “Bem-vindo ao domínio”.



Compartilhamentos de rede

Uma pasta ou unidade compartilhada pode ser acessada por outros computadores na rede.

As ações podem ser fornecidas de três maneiras:

- Em uma rede baseada em cliente/servidor ou em uma rede ponto a ponto com servidores ponto a ponto que oferecem suporte a permissões de usuário/grupo, os compartilhamentos são protegidos por listas de usuários ou grupos autorizados. O Windows 10 suporta controle de acesso de usuário/grupo.
- Uma rede de grupo de trabalho pode oferecer compartilhamento ilimitado (controle total ou somente leitura) para qualquer usuário que se conectar a um sistema se o compartilhamento protegido por senha estiver desabilitado. (Isso não é recomendado.)
- Um compartilhamento de rede pode ser acessado por suas letras de unidade mapeadas ou por seus nomes de pasta no File Explorer.

Quando as permissões baseadas em usuário/grupo são usadas, somente os membros que pertencem a um grupo específico ou que estão listados separadamente na lista de acesso para um determinado compartilhamento podem acessar esse compartilhamento. Depois que os usuários se conectam à rede, eles têm acesso a todos os compartilhamentos que foram autorizados a usar, sem a necessidade de fornecer senhas adicionais. Os níveis de acesso incluem completo e somente leitura; em unidades NTFS, outros níveis de acesso incluem gravação, criação e exclusão.

Ações Administrativas

Compartilhamentos administrativos são compartilhamentos ocultos que podem ser identificados por um \$ no final do nome do compartilhamento. Os usuários padrão que estão navegando para o computador pela rede não podem ver esses compartilhamentos; eles são destinados para uso administrativo.

Todas as pastas compartilhadas que incluem compartilhamentos administrativos podem ser encontradas em **Gerenciamento do computador > Ferramentas do sistema > Pastas compartilhadas >**

Compartilhamentos. Observe que cada volume dentro do disco rígido (C: ou D:, por exemplo) possui um compartilhamento administrativo; por exemplo, C\$ é o compartilhamento administrativo da unidade C:. Embora seja possível removê-los editando o Registro, isso não é recomendado porque pode causar outros problemas de rede. Somente administradores devem ter acesso a esses compartilhamentos.

Compartilhando uma Pasta

Para compartilhar uma pasta com o Windows 10, siga estas etapas:

Etapa 1. Certifique-se de que o compartilhamento de arquivos esteja ativado abrindo o Painel de controle e clicando duas vezes no ícone **Centro de rede e compartilhamento**.

Etapa 2. Abra o Windows File Explorer na barra de tarefas e clique em **Este PC**.

Etapa 3. Na janela Este PC, navegue até a pasta que deseja compartilhar.

Etapa 4. Clique com o botão direito do mouse na pasta que deseja compartilhar e escolha **Compartilhar Com...**

Etapa 5. Se o compartilhamento protegido por senha estiver ativado, clique em **Pessoas selecionadas**; selecione quais usuários terão acesso à pasta compartilhada e selecione seus níveis de permissão. Para permitir todos os usuários, selecione o grupo **Todos** na lista de usuários.

Etapa 6. Quando terminar de configurar as permissões, clique em **Compartilhar e em seguida, clique em Concluído**.

Unidades mapeadas

O Windows permite que pastas compartilhadas e unidades compartilhadas sejam mapeadas para letras de unidade em clientes. No Explorador de Arquivos/Este PC, essas letras de unidade mapeadas aparecem na lista junto com as letras de unidade local. Um recurso compartilhado pode ser acessado por meio da Rede (usando o nome do compartilhamento) ou por meio de uma letra de unidade mapeada.

O mapeamento da unidade oferece os seguintes benefícios:

- Uma pasta compartilhada mapeada como uma unidade pode ser referida pelo nome da unidade em vez de usar um longo caminho UNC (convenção de nomenclatura universal).
- Ao usar programas do MS-DOS, lembre-se de que usar unidades mapeadas é a única maneira de esses programas acessarem pastas compartilhadas.

O mapeamento de unidades e pastas é um procedimento bastante simples:



Etapa 1. Inicie o File Explorer na barra de tarefas e clique com o botão direito do mouse em **Este PC**.

Etapa 2. Selecione **Mapar unidade** de rede no menu suspenso do botão direito para exibir a janela da [Figura 6-28](#).

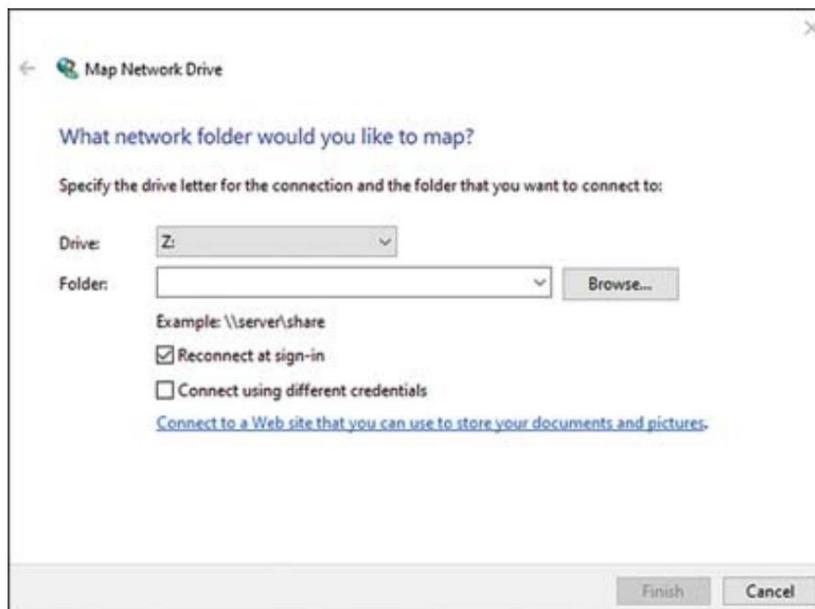


Figura 6-28 A caixa de diálogo Map Network Drive para criar um mapeamento de unidade temporário ou permanente

Etapa 3. Selecione uma letra de unidade na lista de letras de unidade disponíveis; só letras de unidade não usadas por unidades locais são listadas. As letras da unidade já em uso para outras pastas compartilhadas exibem o nome UNC da pasta compartilhada.

Etapa 4. Clique na caixa **Reconectar no login** se desejar usar o dirigir toda vez que você se conectar à rede. Esta opção deve ser usada apenas se o servidor estiver sempre disponível; caso contrário, o cliente receberá mensagens de erro ao tentar acessar o compartilhado recurso.

Etapa 5. Clique na caixa **Conectar usando credenciais diferentes** se desejar usar um nome de usuário/senha diferente para conectar-se ao recurso.

Etapa 6. Clique em **Concluir**.

Compartilhamento de impressora x mapeamento de impressora de rede

As impressoras conectadas a computadores em rede podem ser compartilhadas ou as impressoras podem ser conectadas diretamente a uma rede com conexões Ethernet ou Ethernet sem fio (Wi-Fi).

Para executar o compartilhamento da impressora, siga estas etapas:

Etapa 1. No menu Configurações, abra Dispositivos e clique em **Impressoras e Scanners** à esquerda.

Etapa 2. Clique na impressora a ser compartilhada.

Etapa 3. Clique no botão **Gerenciar** .

Etapa 4. Clique na opção **Propriedades da impressora** .

Etapa 5. Clique na guia **Compartilhamento** .

Etapa 6. Marque a opção **Compartilhar esta impressora** .

Configurações de firewall do sistema

operacional local O **Windows Defender Firewall** fornece proteção contra conexões de entrada indesejadas e também pode ser configurado para filtrar conexões de saída. Use um dos seguintes métodos para abrir o Windows Defender Firewall:

- Clique ou toque no link Windows Defender Firewall no Painel de Controle.
- Pesquise o Firewall do Windows Defender e inicie-o.

Quando o Firewall do Windows Defender é iniciado, ele exibe as configurações do Firewall para a conexão atual (consulte a [Figura 6-29](#)).

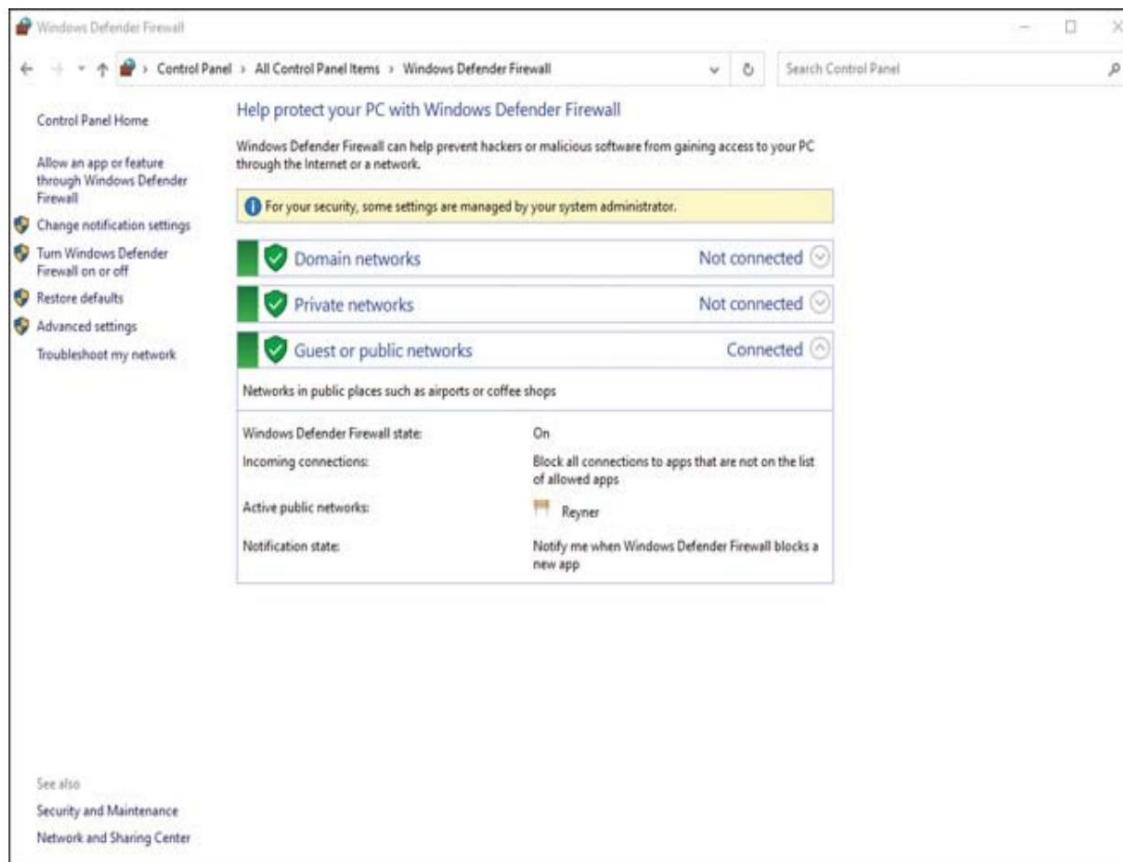


Figura 6-29 Visualizando as configurações de firewall para a conexão atual

Para alterar as configurações de notificação ou ativar ou desativar o firewall, clique ou toque no link Alterar configurações de notificação ou no link Ativar ou desativar o firewall do Windows no painel esquerdo (consulte a [Figura 6-29](#)) para abrir a caixa de diálogo Personalizar (consulte a [Figura 6-30](#)). Qualquer seleção abre a caixa de diálogo Personalizar para configurações em uma rede privada e pública.

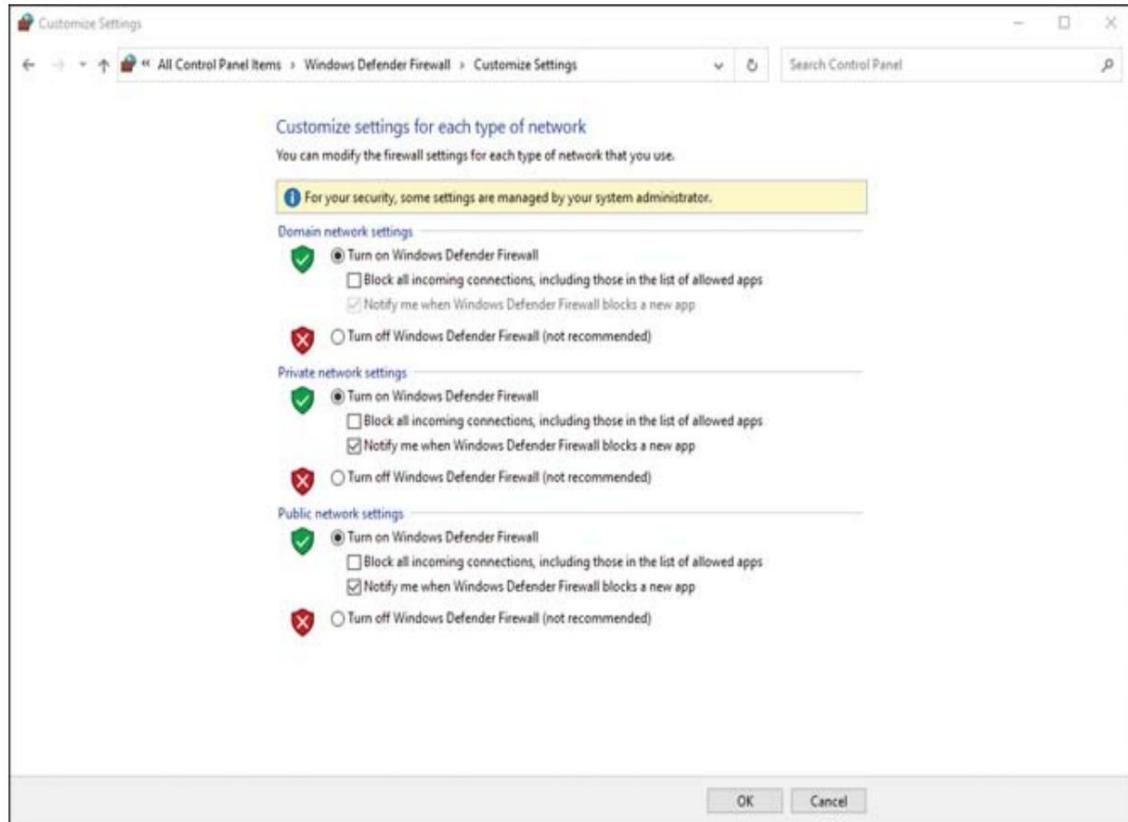


Figura 6-30 Visualizando a Caixa de Diálogo Personalizar Configurações

Nesta caixa de diálogo, as configurações padrão são as mesmas:

- O Firewall do Windows Defender está ativado.
- O usuário é notificado quando o Windows Defender Firewall bloqueia um novo aplicativo.
- Para bloquear todas as conexões de entrada em uma rede pública, clique ou toque na primeira caixa de seleção na seção Configurações de rede pública.
- Se um malware ou erro do usuário tiver desativado o Windows Defender Firewall e nenhum outro firewall estiver presente, clique ou toque em Ativar Windows Defender Firewall em ambas as seções.
- Se o computador usar um firewall de terceiros, clique ou toque em Desativar o Windows Defender Firewall em ambas as seções.
- Se o instalador de um aplicativo recomendar ou exigir que os firewalls sejam desativados, desative o Windows Defender Firewall e ligue-o novamente quando o processo de instalação do aplicativo for concluído.

Para obter mais informações sobre firewalls, consulte o [Capítulo 7](#).

Configuração de rede do cliente Os

computadores que são membros de uma rede local devem ser configurados para que possam se comunicar uns com os outros. Isso geralmente é feito com um **esquema de endereçamento de Protocolo de Internet (IP)**. A Figura 6-31 mostra as configurações necessárias para conectar um dispositivo a uma rede. Você define essas configurações de endereço acessando a interface de rede ativa no Centro de Rede e Compartilhamento. As configurações de endereço de rede atuais podem ser visualizadas acessando a interface de rede ativa em Configurações. Algumas das principais configurações são descritas a seguir. (A maioria deles pode ser acessada rapidamente clicando no ícone de conexão de rede na barra de tarefas e selecionando Propriedades.)

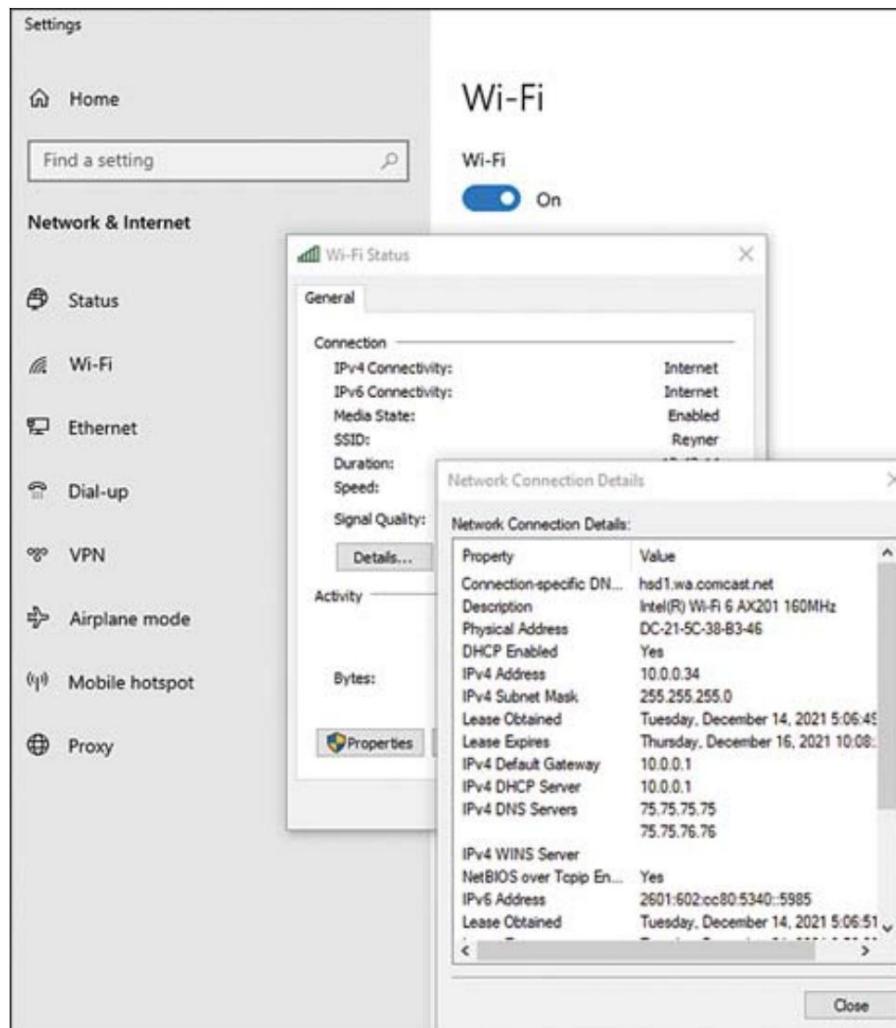


Figura 6-31 Configurações de IP Local

Networking é um tópico amplo digno de sua própria certificação, e muitos livros foram escritos sobre o assunto. Um técnico de suporte de TI encontrará as configurações básicas descritas aqui, portanto, saber o que essas configurações envolvem é importante. Esta seção discute as entradas básicas para que um dispositivo se conecte a uma rede IPv4.

Os computadores em uma rede têm dois tipos de endereços. O endereço MAC é permanente e não muda; ele identifica dispositivos fisicamente em sua própria rede. Os administradores também podem atribuir um endereço IP, o que os ajuda a se comunicar com dispositivos em outras redes além de sua rede local e para a Internet. Os roteadores são os dispositivos que rastreiam os endereços de rede e encaminham a comunicação entre as redes. Isso é feito usando o endereçamento IP. Esta seção descreve os endereços IPv4 e IPv6 dentro do escopo dos objetivos do exame A+.

Ao ler as seções a seguir, consulte a [Figura 6-31](#) para localizar as configurações na saída Network Connection Details.

Esquema de endereçamento de protocolo de Internet (IP)

Um endereço IPv4 é inserido usando um esquema de notação decimal com quatro partes de 8 bits para um endereço. Essas partes são chamadas de octetos porque o número representa 8 bits. Por exemplo, muitos roteadores e dispositivos domésticos têm um endereço de rede IPv4 semelhante a 192.168.1.0. Nesse caso, os três primeiros octetos descrevem a rede; o último octeto, quando atribuído a um dispositivo, possui um número diferente de zero para identificá-lo na rede. Um dispositivo em uma rede pode receber qualquer número de 1 a 254, que é o maior número permitido neste esquema de endereçamento de 8 bits.

máscara de sub-rede

O número de bits que representam as redes e o número que representa o host podem mudar. Olhando apenas para um endereço, não há como saber quais bits ou parte de um bit descrevem o endereço de rede e qual descreve o endereço do host. É aqui que entra a [máscara](#) de sub-rede .

A finalidade de uma máscara de sub-rede é ajudar os roteadores e dispositivos a distinguir os bits de rede dos bits de host. A máscara de sub-rede também tem 32 bits de comprimento e está dividida em grupos de 8 bits. Quando um bit de máscara de sub-rede está “ligado” ou um binário 1, o roteador faz alguns cálculos com o endereço para determinar qual é a rede e

que é o hospedeiro. Um endereço IPv4 não tem sentido para um roteador (e para humanos, aliás), a menos que uma máscara de sub-rede seja configurada.

Por exemplo, um endereço IPv4 de 192.168.1.1 com uma máscara de sub-rede de 255.255.255.0 tem os três primeiros octetos como rede e o último octeto como host. Para uma máscara de sub-rede de 255.255.0.0, os três primeiros octetos definem a rede e os dois últimos definem os hosts. O número aqui é 255 porque representa todos os 8 bits do octeto sendo definido como 1.

Lembre-se de que o roteador também é um dispositivo na rede e a interface que conecta o roteador precisa de um endereço IP na rede. É prática comum reservar o primeiro endereço de host, -xxx1, para o roteador. Isso não é necessário, mas pode facilitar a solução de problemas de gerenciamento de rede.

Configurações do Sistema de Nomes de Domínio (DNS)

Um servidor de nomes de domínio geralmente pertence a um provedor de serviços de Internet (ISP). Os servidores **DNS (Domain Name System)** são computadores especiais que rastreiam os endereços IP de nomes de domínio, como Microsoft.com, IRS.gov e NYT.com. As pessoas usam nomes de domínio em seus navegadores porque são muito mais fáceis de lembrar do que endereços IP (mas você também pode digitar endereços IP em navegadores). Cada nome de domínio possui um endereço IP específico para localizar o servidor na Internet. O trabalho de um servidor DNS é combinar o nome de domínio com o endereço IP correto para que os pacotes possam ser entregues.

Para a rede na [Figura 6-31](#), as informações de DNS podem ser encontradas na janela Network Connection Details. Neste exemplo, o roteador local envia o nome de domínio para o servidor DNS, cujo endereço IPv4 é 75.75.75.75. O servidor responde ao roteador com um endereço IP para Microsoft.com e o usa para encaminhar as informações pela Web. Este é um processo muito rápido que dura milissegundos, de modo que o usuário não notará que a conversa DNS está ocorrendo.

Porta de entrada

Os dispositivos em uma rede local conhecem apenas outros dispositivos na rede local. Eles contam com um dispositivo mais sofisticado (o roteador) para qualquer comunicação externa. Definir um endereço de **gateway**, também conhecido como gateway padrão, garante que, quando um computador estiver enviando comunicação para fora do

rede local, ele vai para o roteador. O gateway padrão é provavelmente a interface local do roteador local. Na [Figura 6-31](#), a interface do roteador é 10.0.0.1.

Estático vs. Dinâmico

Um endereço IP é atribuído a um dispositivo na rede de duas maneiras. Os endereços IP estáticos são configurados por um administrador de rede e não mudam com o tempo. Os endereços dinâmicos são atribuídos ou *alugados* temporariamente e precisam ser renovados após um período de tempo. O administrador da rede pode ajustar quanto tempo se aplica ao aluguel.

A grande maioria dos endereços IP do usuário é atribuída dinamicamente usando o protocolo DHCP (Dynamic Host Configuration Protocol). Um pool de endereços de rede é disponibilizado para o servidor DHCP; sempre que um novo dispositivo ingressa na rede, pode ser atribuído a ele um endereço temporário ou alugado.

Entretanto, nem todos os endereços devem ser dinâmicos. Um administrador de rede pode reservar alguns endereços de rede e não permitir que o DHCP os use. Esses endereços podem ser atribuídos estaticamente a servidores, impressoras e outros recursos importantes que precisam de endereços IP que nunca mudam na rede.

Observe que na [Figura 6-31](#), o gateway padrão (que é o roteador) também é designado para ser o servidor DHCP. A maioria dos roteadores pode ser configurada para executar o protocolo DHCP.

Estabelecer conexões de rede

A página Rede e Internet no Painel de Controle é onde as opções e assistentes são encontrados para os seguintes tipos de conexão:

- Wi-fi
- Ethernet (para conexões com fio)
- Rede privada virtual
- Rede dial-up
- Ponto de acesso
- Proxy

Conexões VPN

Uma **conexão de rede privada virtual (VPN)** cria um túnel seguro em uma rede pública, como a Internet, entre dois computadores. A maioria das VPNs de domínio possui software cliente separado disponível para acesso VPN, mas isso também pode ser configurado no Windows no Painel de controle ou nas Configurações. Uma VPN pode ser configurada tanto no Painel de Controle quanto nas Configurações do Windows. Para configurar uma nova conexão VPN nas configurações do Windows, siga estas etapas:



Etapa 1. Na página **Configurações > Rede e Internet**, selecione **VPN** em a esquerda. Isso abre a caixa de diálogo na [Figura 6-32](#).

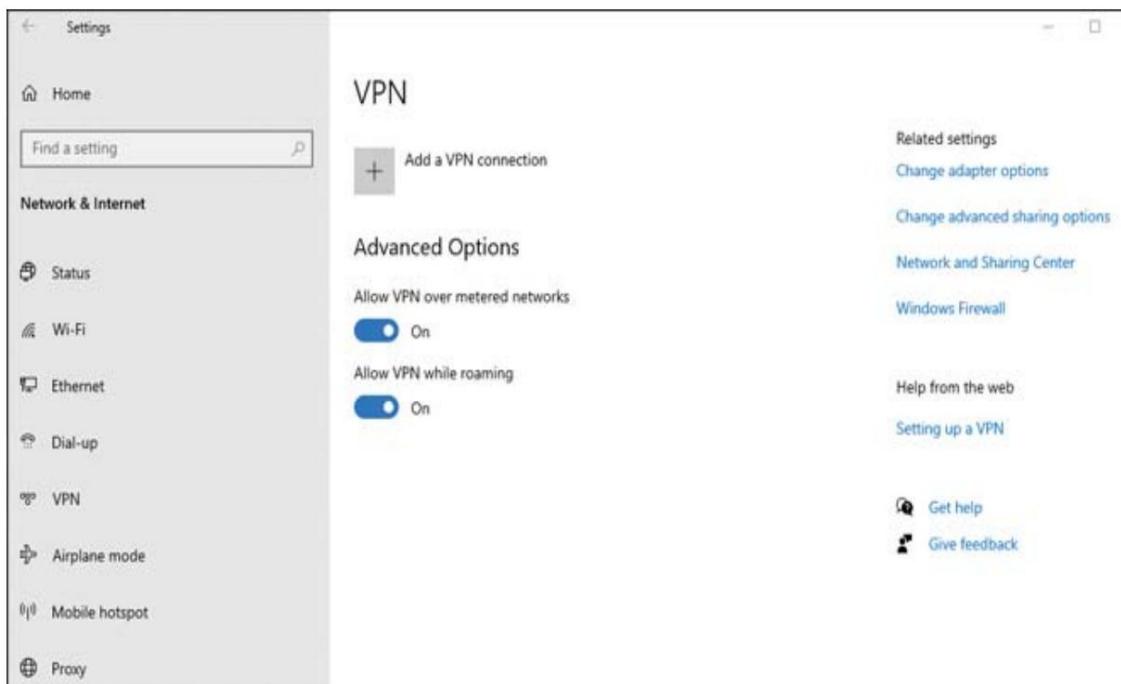


Figura 6-32 Iniciando o processo de criação da conexão VPN no Windows 10

Etapa 2. Clique em Adicionar conexão **VPN** .

Etapa 3. Conclua a conexão VPN na [Figura 6-33](#).

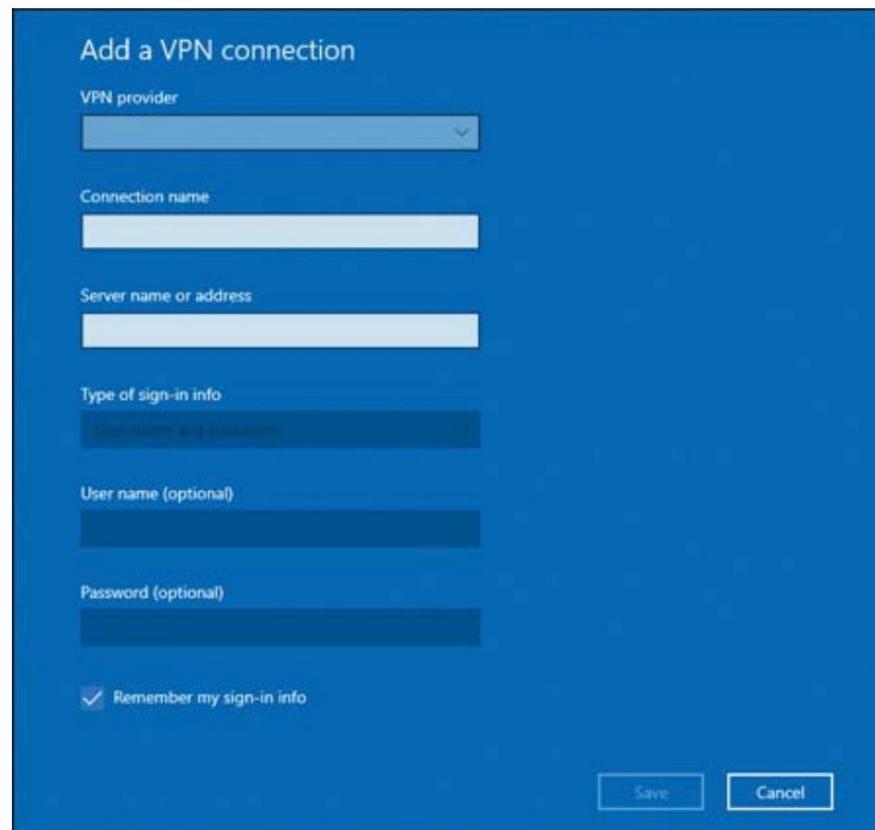


Figura 6-33 Configurando uma conexão VPN

Conexões sem fio

Uma conexão sem fio pode ser configurada quando o usuário clica no SSID na barra de tarefas ou no menu Configurações. No entanto, se você usar a opção Conexão sem fio no Centro de Rede e Compartilhamento na janela do Painel de Controle, poderá especificar mais opções, incluindo tipos de segurança:



Etapa 1. Na caixa de diálogo Configurar uma conexão ou rede, clique ou toque em **Conectar a uma rede sem fio** e clique ou toque em **Avançar**.

Etapa 2. Digite o nome da rede. Selecione o tipo de segurança e digite o chave de segurança. Para iniciar a conexão automaticamente, marque a caixa **Iniciar esta conexão automaticamente**. Clique ou toque em **Avançar**.

Etapa 3. Clique ou toque em **Fechar**. A conexão é adicionada à lista de conexões.

Conexões com fio

Use a opção para configurar uma conexão com fio se estiver configurando uma conexão PPPoE (Point to Point Protocol over Ethernet). Esse tipo de conexão é usado por ISPs a cabo ou DSL que exigem que o usuário faça login na conexão:



Etapa 1. Na caixa de diálogo Configurar uma conexão ou rede, clique ou toque em

Conecte-se à Internet e clique ou toque em **Avançar**.

Etapa 2. Clique ou toque em **Banda larga (PPPoE)** e clique ou toque em **Avançar**.

Etapa 3. Digite o nome de usuário e a senha. Digite o domínio. Verifica a **Lembrar esta** caixa de senha se o usuário não quiser digitar a senha novamente.

Clique ou toque em **Conectar**.

A conexão é armazenada junto com outras conexões de rede.

Conexões WWAN (celular) Uma conexão **de**

rede de longa distância sem fio (WWAN) (celular) aparece na lista de conexões de rede depois que um cartão SIM é instalado e ativado por uma operadora de telefonia móvel. Para usar esse tipo de conexão, selecione-o na lista de conexões de rede exibida ao selecionar o ícone de rede na barra de tarefas ou em Configurações.

Se o nome do ponto de acesso (APN), nome de usuário, senha ou outras informações ainda não tiverem sido armazenadas para a WWAN, o usuário deverá fornecer essas informações durante o primeiro uso da conexão.

Configurações

de proxy Uma rede corporativa pode usar um servidor proxy como intermediário entre um cliente de rede e o destino da solicitação (como uma página da Web) do cliente de rede.

Se um servidor proxy for usado para acesso à Internet e um script de configuração ou detecção automática não estiver disponível, o servidor proxy deverá ser especificado pelo nome do servidor e número da porta. Para definir configurações manuais **de proxy** para uma conexão LAN no Windows:



Etapa 1. Abra as configurações de Rede e Internet no Painel de Controle.

Etapa 2. Clique em **Proxy**.

Etapa 3. Se um script for fornecido, ative a opção **Usar script de configuração** e digite o endereço. Se estiver configurando manualmente, ative a opção **Use Proxy Server** e adicione o endereço e a porta (consulte a [Figura 6-34](#)).

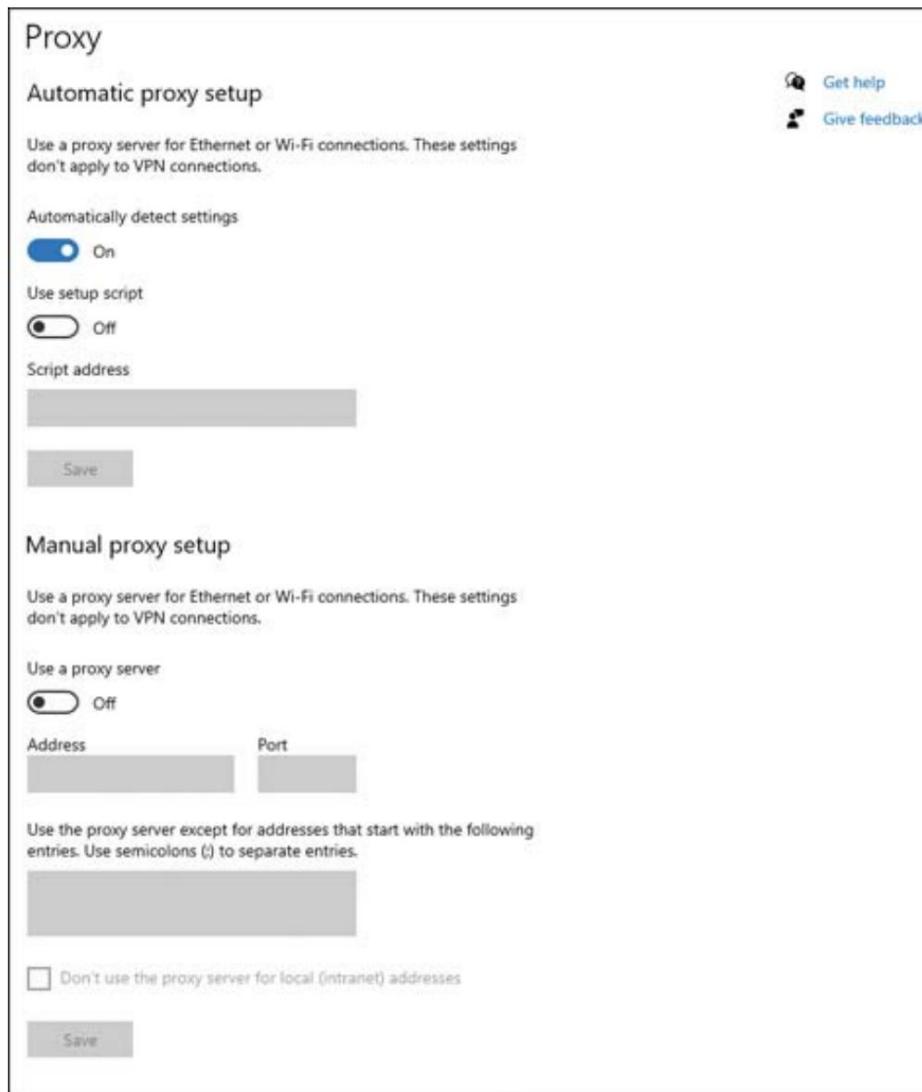


Figura 6-34 Configurando Servidores Proxy

Etapa 4. Clique em **Salvar** para salvar as alterações em cada caixa de diálogo até retornar à exibição do navegador.

Rede pública x rede privada

Ao ingressar em uma rede Wi-Fi, é possível escolher se deseja ser visto por outros usuários ou indetectável por eles.

Por motivos de segurança, pode ser prudente permanecer indetectável em uma rede pública, como uma cafeteria ou outro local público, para evitar a atenção indesejada de usuários desconhecidos.

Se o computador estiver sendo usado em um ambiente de rede privado conhecido, pode ser desejável ser descoberto por outras pessoas para fins de compartilhamento de arquivos e recursos de impressão. Nesse caso, é preferível selecionar uma opção de rede privada.

É possível alternar o status da configuração de privacidade da rede acessando o ícone sem fio na barra de tarefas e clicando no botão Propriedades. A partir daí, basta escolher Public ou Private (consulte a [Figura 6-35](#)).



Figura 6-35 Rede pública/privada e configurações de conexões medidas

Navegação no File Explorer: caminhos de rede

Anteriormente neste capítulo, o File Explorer (o ícone de pasta na barra de tarefas) foi usado para mapear uma unidade de rede. Da mesma forma, as informações de rede podem ser mapeadas usando o File Explorer selecionando o ícone Rede no menu à esquerda.

Para rastrear um caminho para uma rede e para obter outras informações, clique na guia Rede

no canto superior esquerdo para ver a faixa de opções de rede. A partir daqui, você pode visualizar caminhos de rede e adicionar dispositivos à rede.

Conexões Medidas e Limitações

Muitos ISPs e empresas de telefonia móvel têm planos de dados com limites de uso que, quando ultrapassados, podem levar a custos maiores e surpresas desagradáveis em uma fatura. Uma maneira de evitar excessos acidentais é gerenciar o uso nas configurações de **Metered Connection** (consulte a parte inferior da [Figura 6-35](#)).

Quando a configuração Metered Connection está ativada, os detalhes podem ser gerenciados clicando no link Definir um limite de dados para ajudar a controlar o uso de dados nesta rede abaixo da configuração. A [Figura 6-36](#) mostra o resultado. Neste exemplo, o Windows aplica um uso mensal de 1,5 GB de dados na rede Reyner, atualizando no dia 5 de cada mês.

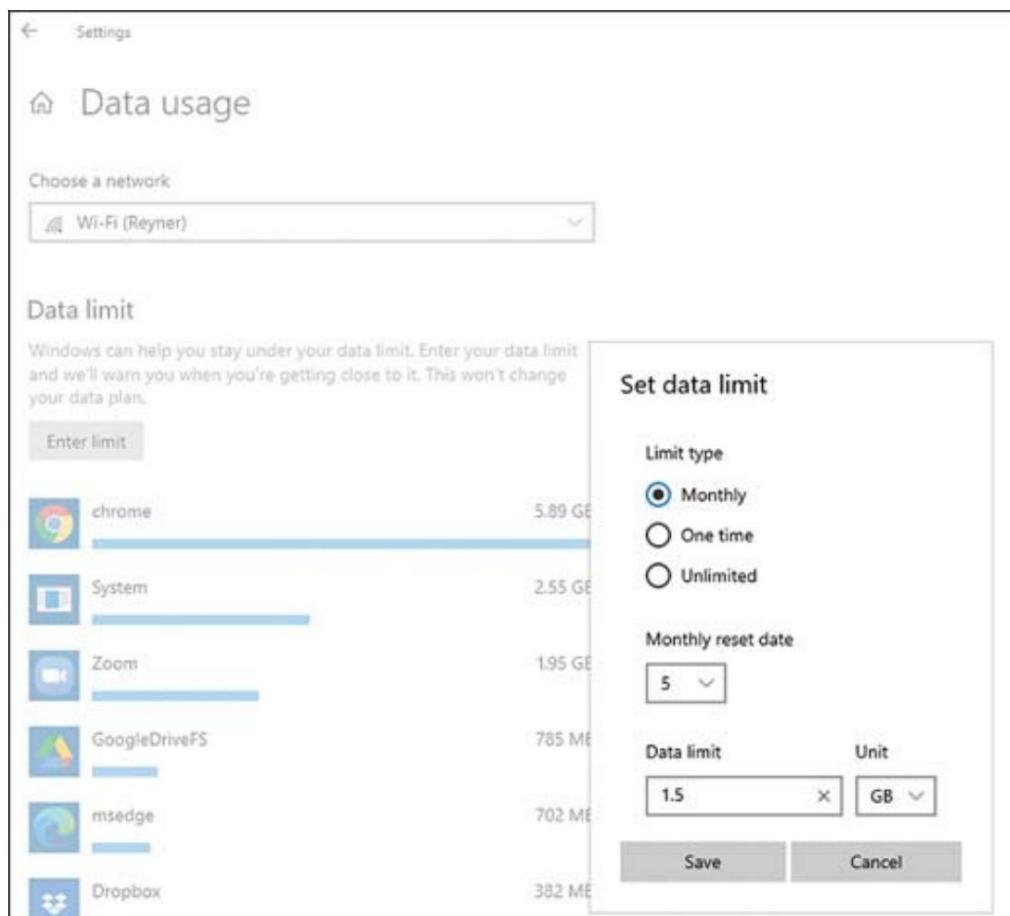


Figura 6-36 Definindo limites de dados para uma conexão medida

Conceitos de instalação e configuração

220-1102:
Exam

220-1102: Objetivo 1.7: Dado um cenário, aplique os conceitos de instalação e configuração de aplicativos.

Key
Topic

Requisitos de sistema para aplicativos Antes de fazer qualquer

alteração em um computador instalando hardware ou software, é essencial entender qual hardware funcionará no computador e qual software funcionará com o hardware instalado. Esta seção é uma revisão básica das considerações ao atualizar o hardware ou instalar o software.

Key
Topic

Sistemas de arquivos de 32 bits versus 64

bits Um dos principais objetivos dos sistemas operacionais é controlar todos os arquivos usados em um computador. Um sistema de arquivos descreve como os dados e as unidades são organizados. No Windows, o sistema de arquivos escolhido para um disco rígido afeta o seguinte:

- As regras para o tamanho de uma unidade lógica (letra de unidade) e se o disco rígido pode ser usado como uma letra de unidade grande ou várias letras de unidade menores, ou se deve ser várias letras de unidade
- A eficiência do armazenamento de dados (quanto menos espaço desperdiçado, melhor)
- A segurança de um sistema contra adulteração
- Se uma unidade pode ser acessada por mais de um sistema operacional

O termo *sistema de arquivos* é um termo geral para a forma como um sistema operacional armazena vários tipos de arquivos. O Windows oferece suporte a três sistemas de arquivos diferentes para disco rígido

unidades e unidades flash USB: FAT32, NTFS e exFAT. Para armazenamento em CD, ele usa CDFS.

FAT32

O FAT32 foi introduzido em 1995 e tem as seguintes características:

- Ele possui uma tabela de alocação de arquivos de 32 bits, que permite 268.435.456 entradas (2³²) por unidade. Uma entrada pode ser uma pasta ou uma unidade de alocação usada por um arquivo.
- O diretório raiz pode estar localizado em qualquer lugar da unidade e pode ter um número ilimitado de entradas, o que é uma grande melhoria em relação ao FAT.
- O FAT32 usa um tamanho de unidade de alocação de 8 KB para unidades de até 16 GB.

O tamanho máximo da partição lógica permitido é 2 TB (ou seja, mais de 2 trilhões de bytes).

Observação

O Windows não pode criar uma partição FAT32 maior que 32 GB. No entanto, se já existir uma partição maior, o Windows poderá usá-la.

O FAT32 tem algumas limitações: ele pode oferecer suporte a arquivos individuais de até 4 GB de tamanho, não pode usar permissões de arquivo e não oferece suporte a sistemas de registro no diário que podem corrigir problemas de corrupção de arquivos. Essas três limitações levaram a indústria além do FAT32, embora ainda seja possível usar o FAT32 para formatar discos rígidos.

Como as limitações não se aplicam à maioria dos cartões SD e flash USB, o FAT32 ainda é usado para formatar cartões de memória flash e unidades flash USB para uso não apenas em estações de trabalho, mas também em players de mídia, smart TVs, impressoras, câmeras e qualquer outra coisa que tem uma porta USB. O FAT32 ainda é compatível com macOS e Linux, então o FAT32 está longe de ser um legado. Mesmo que a capacidade das unidades flash USB esteja aumentando e arquivos de 4 GB precisem ser suportados, o FAT32 provavelmente permanecerá para suportar outros dispositivos.

Observação

Em uma máquina de 32 bits, a quantidade máxima de memória que pode ser usada é de cerca de 4 GB. Em uma máquina de 64 bits, a quantidade máxima de memória é de 264 bytes.

exFAT (FAT64)

exFAT (também conhecido como FAT64) é um sistema de arquivos projetado para permitir que a mídia de armazenamento pessoal móvel seja usada perfeitamente em computadores móveis e de mesa. O exFAT foi projetado para ser tão simples quanto o FAT32, mas com muitas melhorias em capacidade e escalabilidade.

exFAT também é chamado de FAT64 porque suporta endereçamento de 64 bits. As principais características do exFAT incluem o seguinte:

- Ele suporta volumes (letras de unidade) maiores que 32 GB. 512 TB é o tamanho máximo de volume recomendado, mas o tamanho teórico do volume é 64 ZB (zabytes; 1 ZB = 1 bilhão de terabytes).
- Os tamanhos de arquivo recomendado e máximo aumentam para 512 TB e 64 ZB, respectivamente.
- As melhorias na estrutura do sistema de arquivos permitem um melhor desempenho com mídia flash e para gravação de filmes.
- Ele suporta carimbos de data de Coordenada de Tempo Universal (UTC).

A Figura 6-37 ilustra o exFAT como uma opção de formatação para um pen drive USB no Windows.

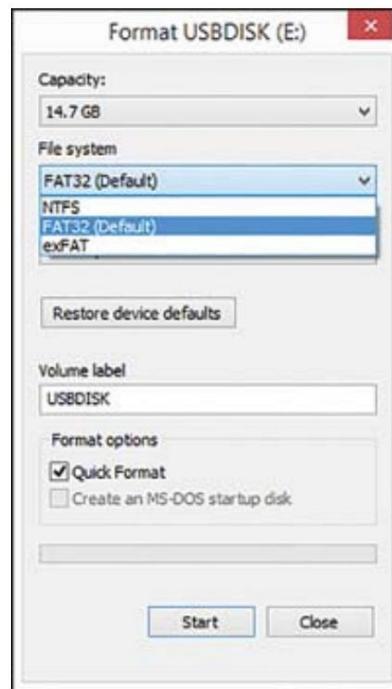


Figura 6-37 Opções de formatação do sistema de arquivos para um Thumb USB de 16 GB Unidade no Windows, incluindo FAT32, NTFS e exFAT

Requisitos de aplicativos dependentes de 32 bits x 64 bits

Lembre-se de que os aplicativos de 32 bits datam da época dos processadores X-86 (consulte o [Capítulo 3, “Hardware”](#)) e, pelos padrões atuais, eram ineficientes para serem executados. Os aplicativos de 64 bits podem aproveitar mais recursos de computação na CPU e na RAM. O Windows 10 executado em uma máquina de 64 bits pode oferecer suporte a programas de 32 bits, mas os processadores de 32 bits em dispositivos móveis menores não podem oferecer suporte a aplicativos de 64 bits. Certifique-se de que o computador está executando e do que o software requer antes de instalar um aplicativo.

A maioria dos softwares executados em desktops hoje é de 64 bits, mas muitos aplicativos de 32 bits ainda estão em uso. Para ver que tipo de software está rodando no Windows, abra o Gerenciador de Tarefas (Ctrl+Alt+Esc); a lista de programas de 32 bits em execução é identificada (consulte a [Figura 6-38](#)). Neste exemplo, observe que o AGS Service e o Bing Wallpaper são de 32 bits.

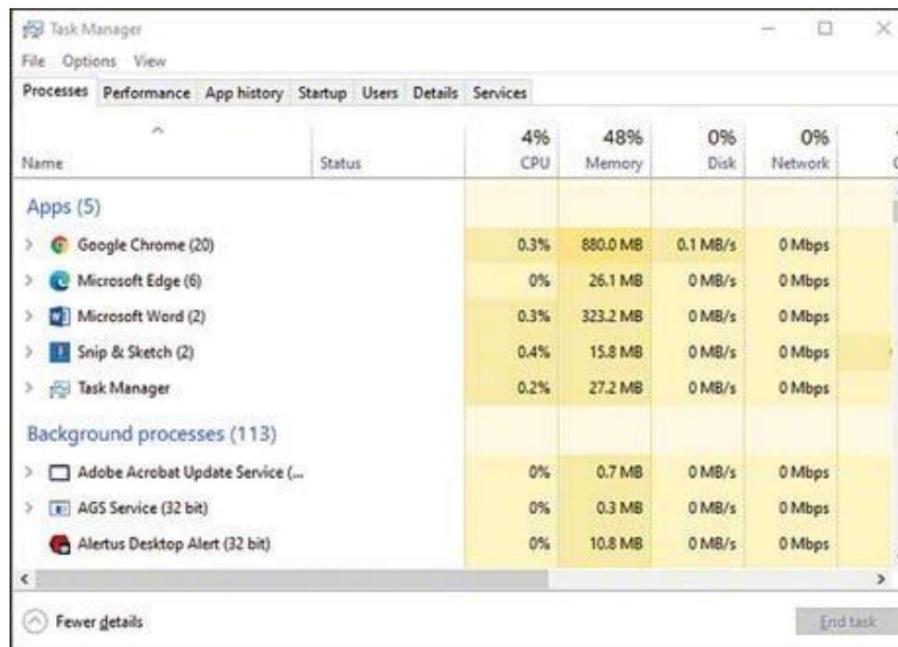


Figura 6-38 Gerenciador de tarefas mostrando software de 32 bits

Placa gráfica dedicada versus placa gráfica integrada

Uma placa gráfica integrada refere-se ao chip gráfico embutido na placa-mãe. É menor e mais eficiente em termos de energia, e os cartões integrados atuais fornecem qualidade suficiente para o usuário médio. Os cartões integrados contam com a RAM do sistema para seu processamento, portanto, eles afetam o desempenho geral do sistema.

No entanto, a placa gráfica integrada não corresponde à qualidade de uma placa dedicada. Os cartões dedicados são projetados para finalidades diferentes, como jogos ou mineração de criptomoedas, mas todos possuem uma unidade de processamento gráfico (GPU), RAM integrada e um ventilador de resfriamento para o processador. A maioria das novas placas dedicadas pode funcionar com os gráficos integrados para melhor eficiência.

Requisitos de memória de acesso aleatório de vídeo (VRAM)

A **memória de acesso aleatório de vídeo (VRAM)** é RAM dedicada ao processamento de exibições gráficas. A VRAM pode ser uma parte atribuída da RAM do sistema, para uma placa gráfica integrada. Por exemplo, um computador pode ter 4 GB de RAM, com 1 GB dedicado ao chip gráfico integrado.

VRAM também se refere à RAM montada em uma placa dedicada para suportar a GPU. Essa RAM fica ao lado da GPU e não consome recursos do sistema para exibição de alta qualidade.

Para a maioria dos usuários, o VRAM integrado é suficiente. Para software e aplicativos que precisam de processamento poderoso, VRAM extra para uma placa dedicada é uma boa solução.

Requisitos de RAM

Antes de instalar o software em um computador, certifique-se de que a quantidade atual de RAM seja compatível com o aplicativo. Use o Gerenciador de Tarefas (consulte a [Figura 6-38](#)) para ver como o computador está usando os recursos de RAM disponíveis no momento. É sensato presumir que máquinas e dispositivos funcionam melhor até o meio de sua faixa de capacidade, portanto, se a RAM estiver acima de 50%, consulte os requisitos de RAM do desenvolvedor de software para garantir que o computador possa lidar com isso.

Quando a RAM estiver instalada e em execução, retorne ao Gerenciador de Tarefas com o software em execução (juntamente com outros aplicativos normais) e verifique o desempenho da memória. Se estiver acima de 60%, considere instalar mais RAM, se possível. Menos melhorias ajudam mais no desempenho de um computador do que adicionar RAM. Consulte o [Capítulo 3](#) para uma discussão mais detalhada sobre RAM.

Requisitos da Unidade Central de Processamento (CPU)

A escolha da CPU deve ocorrer durante a compra de um computador ou outro dispositivo. A atualização de CPUs é bastante incomum porque elas são projetadas para funcionar com a placa-mãe em que estão instaladas. Conhecer a finalidade esperada e as demandas do usuário pode orientar a seleção da CPU. Para uma discussão mais detalhada sobre CPUs, consulte o [Capítulo 3](#).

Tokens de Hardware Externo

A autenticação multifator está em uso muito maior agora do que no passado, mas a necessidade de altos níveis de segurança do computador existe há décadas. Um dos primeiros métodos de autenticação em uma rede era usar um token de hardware externo para acessar um código ou senha para entrar em um computador ou rede para acesso. O token (também conhecido como *dongle* – veja a [Figura 6-39](#)), junto com o servidor de autenticação, gerava um código aleatório a cada minuto para validar um usuário que digitou uma senha. Os dois fatores trabalhando

juntos para proteger a rede sabiam a senha e forneciam um código fisicamente presente.



Figura 6-39 Token de Hardware

A prevalência de smartphones que possuem sua própria segurança permite que os tokens sejam enviados aos usuários em um aplicativo de autenticação. Os usuários agora podem fazer login em seus telefones ou outros dispositivos para aprovar a autenticação multifator.

Requisitos de armazenamento

Ao instalar o software, é importante considerar quais recursos além de RAM e CPU serão necessários para uso. Por exemplo, o software de edição de vídeo pode exigir recursos adicionais para gráficos e VRAM, mas a edição pode gerar arquivos enormes que precisam estar prontamente acessíveis. Certifique-se de que haja armazenamento suficiente disponível nos discos locais e unidades externas ou no armazenamento conectado à rede (NAS). Consulte o [Capítulo 3](#) para obter uma discussão detalhada dessas opções de armazenamento.

Requisitos do sistema operacional para aplicativos

Nem todo aplicativo será executado em todos os sistemas operacionais. Os aplicativos precisam ser especificamente adaptados para funcionar em plataformas Windows, Apple ou Linux. A compatibilidade dentro da plataforma também é uma preocupação; sempre que um sistema operacional é atualizado, o aplicativo também pode precisar de atualização.

Compatibilidade de aplicativo para sistema operacional

Parece bastante fundamental dizer que é importante garantir que a versão do software selecionada será executada com o sistema operacional. No entanto, essa tarefa pode se complicar. As atualizações do sistema operacional acontecem regularmente e os fabricantes de software nem sempre acompanham. Ao instalar o software, certifique-se de verificar as atualizações mais recentes no site do fornecedor.

SO de 32 bits x 64 bits

Conforme mencionado anteriormente nesta seção, o software Windows de 32 bits pode ser executado em uma máquina de 64 bits, mas uma máquina de 64 bits não pode ser executada em uma máquina de 32 bits. A diferença pode não ser perceptível para o usuário, mas uma máquina de 64 bits oferece um ambiente muito mais poderoso para trabalhar. Qualquer máquina atual projetada para executar o Windows 10 ou 11 é uma máquina de 64 bits. Muitas máquinas de 32 bits ainda estão em uso, mas a partir de 2020, novas máquinas com Windows 10 têm processadores de 64 bits. A Microsoft continuará a oferecer suporte a 32 bits, mas a segurança e outros recursos não serão tão robustos quanto nas versões de 64 bits.

O macOS, começando com a versão Catalina 10.15 do macOS em 2019, abandonou o suporte para aplicativos de 32 bits. A execução de aplicativos legados no macOS pode ser complicada, portanto, certifique-se de que os aplicativos legados sejam atualizados se você estiver migrando um macOS mais antigo para uma versão mais recente. As versões mais antigas do macOS listam se um aplicativo é compatível com 64 bits. Para encontrar a lista, vá para **Finder > ícone Apple > Visão geral > Relatório do sistema > Software > Aplicativos**. A janela superior lista todos os aplicativos e indica se eles são de 64 bits.

Métodos de distribuição

Mídia física versus download

Os dias de obter versões de software em mídia física estão quase no fim. A criação de mídia física para instalar o Windows agora envolve o download de um arquivo de imagem (.iso) para uma inicialização USB/eSATA (inicialização a partir de um pen drive USB) ou disco óptico (CD-ROM/DVD/Blu-ray). Use este método para instalar o Windows em um PC individual e para criar um PC mestre a partir do qual as imagens de disco podem ser criadas. A ferramenta de download de USB/DVD do Windows disponível em www.microsoft.com/en-us/download/windows-usb-dvd-download-tool pode criar uma unidade USB inicializável a partir de uma imagem ISO (.iso) do Windows que você baixou. Se necessário, altere a ordem de inicialização no firmware BIOS/UEFI do sistema para permitir a inicialização a partir do USB.

Observação

Esses métodos são discutidos em detalhes posteriormente neste capítulo, na seção “Instalações e atualizações do sistema operacional em um ambiente de sistema operacional diverso”.

Outras considerações para novos aplicativos Uma boa regra no

gerenciamento de redes de computadores é que todo benefício para uma rede tem um custo. Alguns custos são dinheiro, mas outros custos podem ser um sacrifício de desempenho ou capacidade. Às vezes, os custos são desconhecidos até que seja tarde demais e venham na forma de consequências não intencionais – essas podem ser as mais caras e podem até levar a falhas do sistema.

Determinar o custo ou o impacto de uma mudança técnica é uma habilidade importante a ser desenvolvida. Fazer alterações não deve ser feito no vácuo, mas sim por meio de um processo de controle de alterações estabelecido e acordado pelos usuários das máquinas e da rede. Esses processos de controle de alterações permitem que todos os usuários revisem quaisquer alterações ou atualizações para avaliar qualquer impacto negativo que possam ter em seu ambiente de trabalho. A seguir estão apenas alguns exemplos de considerações que o comitê deve ter ao determinar o impacto de uma mudança em um ambiente de rede de computadores. Sinta-se à vontade para debater e adicionar suas próprias perguntas aos exemplos.

- **Impacto no dispositivo:**

- A adição de hardware ou software para um usuário degradará a experiência do usuário para outro usuário?
- A atualização do sistema operacional fará com que o software legado pare de funcionar?

- **Impacto na rede:**

- A adição de novos usuários e dispositivos degradará o desempenho atual da rede?
- Como a adição de armazenamento de rede melhorará ou degradará os recursos de rede?

- **Impacto na operação:**

- As novas atualizações de software desativarão a rede por períodos significativos?
- A migração para a nuvem afetará o tempo de processamento das transações de vendas?
- **Impacto nos negócios:**
 - A adição de software de segurança bloqueará os parceiros de negócios?
 - A empresa pode arcar financeiramente com as atualizações e elas fazem sentido econômico a longo prazo?

Compreendendo os tipos comuns de sistema operacional

220-1102

Exam

220-1102: Objetivo 1.8: Explicar os tipos comuns de SO e suas finalidades.

Diferentes tipos de computadores requerem diferentes funcionalidades de seus sistemas operacionais. Esta seção discute as diferenças entre estações de trabalho e sistemas operacionais móveis e os tipos de arquivo que eles suportam.

Key
Topic

SOs de estação de trabalho

Os sistemas operacionais podem ser classificados como open source, que se refere a software que é efetivamente gratuito para baixar e modificar, e closed source, que se refere a software que não pode ser modificado sem permissão expressa e licenciamento. Outros termos usados para descrever o software de código fechado são *específicos do fornecedor*, o que significa que apenas uma empresa tem acesso ao código-fonte, e *proprietário*, o que significa que o software é de propriedade e patenteado e pode ser usado apenas com permissão (e geralmente mediante o pagamento de um taxa de licenciamento).

janelas

O Microsoft **Windows** é um produto de código fechado e é o sistema operacional mais usado no mundo. Na década de 1980, quando as empresas fizeram a transição para o mundo digital

idade usando PCs compatíveis com IBM, a Microsoft geralmente fornecia o sistema operacional, que era conhecido como Disk Operating System (DOS). O DOS é um sistema operacional de linha de comando, o que significa que os comandos são inseridos como strings de texto. Desde então, o DOS foi substituído pelo Windows, que usa uma interface gráfica do usuário (GUI) para permitir que os comandos sejam inseridos com o clique de um mouse. Mas o legado do DOS sobrevive com muitos dos mesmos comandos usados no PowerShell.

O Windows teve muitas iterações ao longo dos anos, mas o Windows 10 e talvez o 11 são as versões abordadas no exame 220-1102 A+.

Observação

A observação a seguir nos objetivos do exame CompTIA A+ estabelece diretrizes para esse conteúdo do Windows 11 quando os exames 220-1101 e 220-1102 foram lançados. Embora o Windows 11 não seja especificamente detalhado em objetivos separados, aplica-se o seguinte: “Versões do Microsoft Windows que não são o fim do Suporte Mainstream (conforme determinado pela Microsoft), até e incluindo o Windows 11, são áreas de conteúdo pretendido da certificação. Assim, os objetivos em que uma versão específica do Microsoft Windows não é indicada no título do objetivo principal podem incluir conteúdo relacionado ao Windows 10 e Windows 11, no que se refere à função do trabalho.”

SO Apple Macintosh

macOS é o sistema operacional para produtos de desktop da Apple. Assim como no Windows, o macOS é de código fechado e apenas alguns componentes estão abertos aos desenvolvedores. O macOS foi lançado em 2016 e projetado para se integrar a dispositivos que usam o sistema operacional iOS, como iPhone, Apple TV e Apple Watch. A partir desta impressão, a versão mais recente do macOS é Monterey, que é a versão 12. A [Figura 6-40](#) mostra a área de trabalho de Monterey.



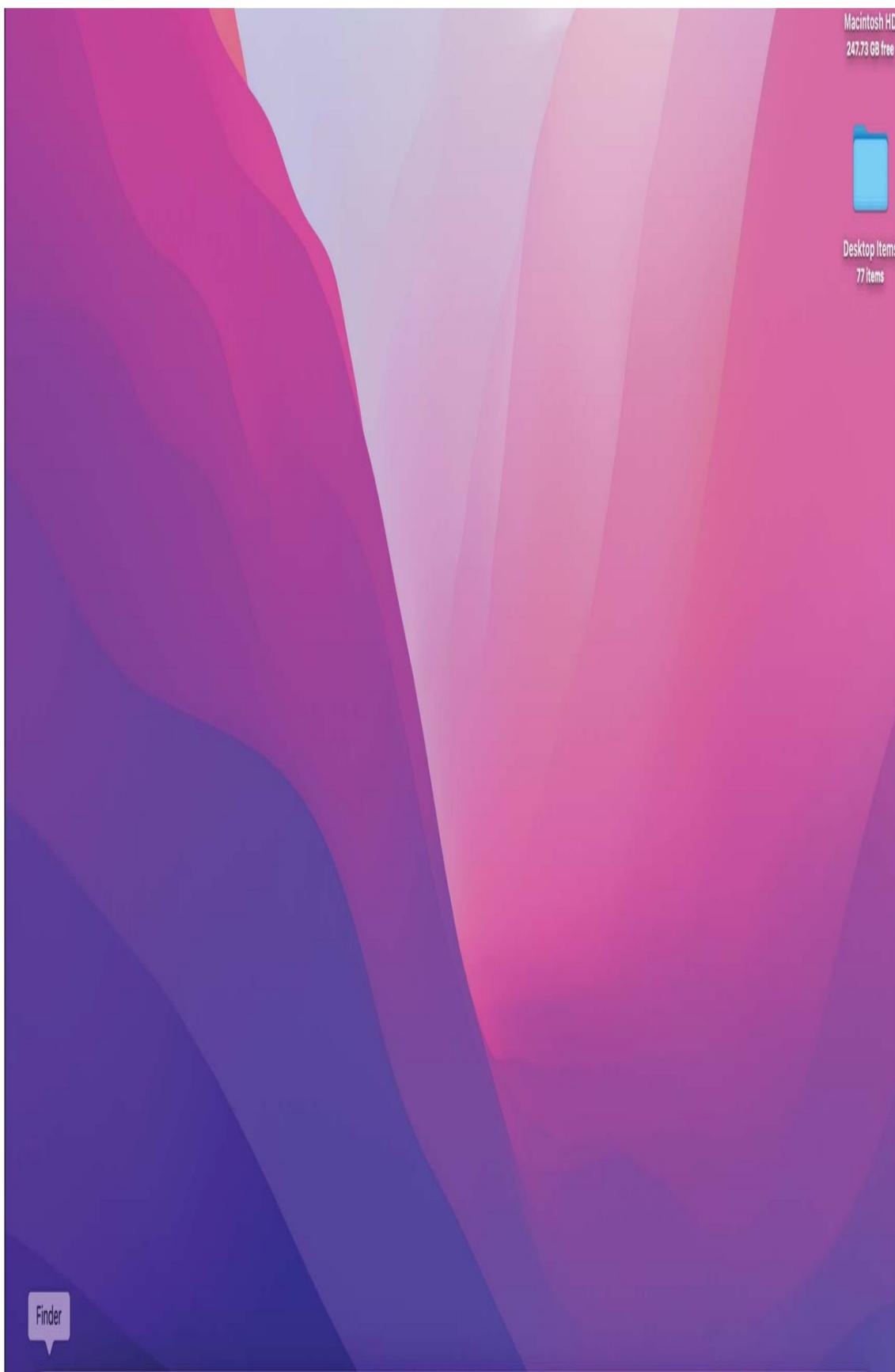




Figura 6-40 macOS Monterey

Linux

O Linux foi derivado do sistema operacional UNIX (usado em computadores mainframe anteriores aos PCs). É nomeado para Linus Torvalds, que desenvolveu o Linux em 1991. Linux é um sistema operacional de código aberto, o que significa que o código-fonte é gratuito. Muitas empresas, como a Red Hat, modificam o código-fonte do Linux e cobram de indivíduos e organizações para dar suporte às modificações.

Como o Linux é de código aberto, ele está disponível gratuitamente na Web na forma de distros (distribuições). O Linux está disponível como distros de linha de comando; e outros são distribuições GUI. Distribuições populares do Linux são Ubuntu, Mint, Kali e Red

A Figura 6-41 mostra um ambiente de desktop Linux Mint.



Figura 6-41 Mint Desktop

Chrome OS

O **Chrome OS** é um sistema operacional relativamente novo desenvolvido pelo Google. É um sistema operacional de código aberto, baseado em um sistema operacional Gentoo Linux de código aberto. A funcionalidade é única, pois o sistema operacional é executado no navegador Google Chrome. O Chrome OS pode ser instalado a partir de uma unidade USB e pode ser executado em um PC ou Mac.

O Chrome pode executar aplicativos do Android, Linux e Windows. Quando lançado pela primeira vez, o Chrome OS executava laptops Chromebook que eram baratos, mas também limitados. Versões mais recentes de Chromebooks e do Chrome OS oferecem melhor desempenho, mas versões baratas ainda estão disponíveis.



Sistemas operacionais para celulares/tablets

Os smartphones geralmente usam sistemas operacionais Android ou iOS.

Algumas diferenças entre smartphones Android e iOS incluem o seguinte:

- As atualizações do sistema operacional são fornecidas pela operadora sem fio para telefones Android.
- As operadoras sem fio fornecem atualizações específicas de rede para iPhones (iOS), mas a Apple fornece as atualizações do sistema operacional.

Android

O **Android**, que é um sistema operacional baseado no kernel do Linux, é um exemplo de software de código aberto. Usado principalmente em smartphones e tablets, o Android é desenvolvido pela Open Handset Alliance, um grupo dirigido pelo Google. O Google libera o código do sistema operacional Android como código aberto, permitindo que os desenvolvedores o modifiquem e criem aplicativos livremente para ele. O Google também encomendou o Android Open Source Project (AOSP), cuja missão é manter e desenvolver o Android.

Versões mais recentes do Android estão em constante desenvolvimento.

Para determinar a versão atual em uso em um dispositivo, comece na tela inicial (ou seja, a tela principal que inicializa por padrão). Toque no botão Menu e depois em Configurações. Role até a parte inferior e toque na opção Sobre o telefone (ou Sobre). Em seguida, toque em Informações do software ou em uma opção semelhante. As versões 1-10 receberam nomes famosos de sobremesas, como Pirulito (versão 5) e Torta (versão 9), mas a partir da versão 10, os codinomes foram descartados. No momento em que este artigo foi escrito, a versão mais recente é a 12.

Ao contrário de outros sistemas operacionais móveis, os contratos de licenciamento do Android permitem uma grande personalização do produto final. Assim, smartphones e tablets Android de diferentes fornecedores provavelmente terão diferentes interfaces de usuário e recursos.

iOS

O Apple **iOS** é um exemplo de software de código fechado.

Conhecido como sistema operacional do iPhone, agora é simplesmente chamado de iOS porque é usado no iPod Touch e no iPhone. O iOS é baseado no macOS (usado em desktops e laptops Mac) e, portanto, tem suas raízes no UNIX.

A [Figura 6-42](#) mostra a tela inicial de um iPad Mini 2 executando o iOS versão 9.0.1.



1. iOS OS update available
2. App updates available
3. Battery charge level

Figura 6-42 Tela inicial do iPad Mini 2

O iPad já rodava no iOS, mas com a versão 13 (2019), era poderoso o suficiente para ter seu próprio [iPadOS](#), que é mais robusto que o iOS e suporta o uso de teclado e multitarefa.

Para determinar a versão do iOS que um dispositivo está executando, vá para a tela inicial e toque **em Configurações > Geral > Sobre**. Por exemplo, a [Figura 6-43](#) mostra um iPhone executando a versão 15.1. O iPad 15 foi lançado no outono de 2021 para iPad Pro, iPad (quinta geração em diante), iPad Mini (quarta geração em diante) e iPad Air (segunda geração em diante).



 General		About
Name	iPhone Example	>
Software Version	15.1	
Model Name	iPhone 11	
Model Number	MWLE2LL/A	
Serial Number	DNPZMJ9YN72Q	
AppleCare Services		>
Songs	395	
Videos	52	
Photos	2,547	
Applications	148	



Figura 6-43 iPhone usando a versão 15.1 do iOS

Ao contrário do Android, o iOS não é de código aberto. Somente o hardware da Apple usa este sistema operacional.

Vários tipos de sistema de arquivos O

que exatamente é um sistema de arquivos? Um sistema de arquivos determina como os dados e as unidades são organizados, mas também é um termo geral para como um sistema operacional armazena vários tipos de arquivos. Conforme discutido anteriormente neste capítulo, o Windows oferece suporte a três sistemas de arquivos diferentes para discos rígidos e unidades flash USB: FAT32, NTFS e exFAT.

O **New Technology File System (NTFS)** é o sistema de arquivos nativo do Windows 10.

O NTFS tem muitas diferenças em relação ao FAT32, incluindo o seguinte:



- **Controle de acesso:** Diferentes níveis de controle de acesso, por grupo ou usuário, podem ser configurados tanto para pastas quanto para arquivos individuais.
- **Compactação integrada:** arquivos individuais, pastas ou uma unidade inteira podem ser compactados sem o uso de software de terceiros.
- **Lixeiras individuais:** Ao contrário do FAT32, o NTFS inclui uma Lixeira separada para cada usuário.
- **Suporte para o Sistema de Arquivos com Criptografia (EFS):** O Sistema de Arquivos com Criptografia (EFS) permite que os dados sejam armazenados de forma criptografada. Não requer senha e nenhum acesso aos arquivos.

- **Suporte para montar uma unidade:** a montagem da unidade permite que você enderece o conteúdo de uma unidade de mídia removível, possivelmente como se seu conteúdo estivesse armazenado em seu disco rígido. A letra da unidade de disco rígido é usada para acessar dados tanto na unidade de disco rígido quanto na unidade de mídia removível.
- **Suporte a cota de disco:** o administrador de um sistema pode impor regras sobre quanto espaço em disco cada usuário pode usar para armazenamento.
- **Hot-swapping:** unidades de mídia removível que foram formatadas com NTFS (como USB) podem ser conectadas ou removidas enquanto o sistema operacional está em execução.
- **Indexação:** O serviço de indexação ajuda os usuários a localizar informações mais rapidamente quando a ferramenta de pesquisa é usada.

Siga estas etapas para determinar qual sistema de arquivos foi usado para preparar um Disco rígido do Windows:

Etapa 1. Abra o Windows File Explorer.

Etapa 2. Clique com o botão direito do mouse na letra da unidade na janela do Explorer e selecione **Propriedades**.

A folha de propriedades da unidade lista NTFS para uma unidade preparada com NTFS e FAT32 para uma unidade preparada com FAT32 (consulte a [Figura 6-44](#)).

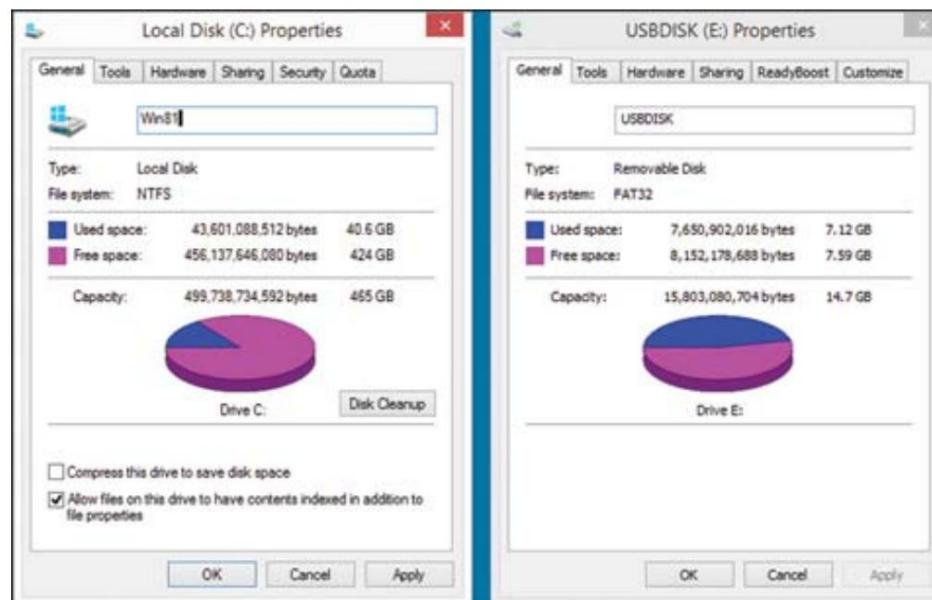


Figura 6-44 Um disco rígido formatado com NTFS versão 5 (esquerda) e um Unidade de memória flash formatada com FAT32 (direita)

Durante a instalação, o Windows 10 formata automaticamente as partições criadas pelo processo de partição com NTFS.

exFAT, FAT32 e NTFS são sistemas de arquivos comuns do Windows. A [Tabela 6-8](#) descreve resumidamente esses e outros sistemas de arquivos que executam as mesmas tarefas, mas em sistemas operacionais diferentes.

Tabela 6-8 Comparação do formato do sistema de arquivos

Sistema	Detalhes do nome completo
Tipo	
exFAT	Estendido
	Sistema de arquivos da Microsoft usado para unidades flash maiores
	Arquivo
	que 32 GB e arquivos maiores que 4 GB.
	Alocação
	Mesa
Arquivo	FAT32
	Formato para unidades flash USB que armazenam arquivos menores
	Alocação
	que 4 GB, consoles de jogos e assim por diante. Funciona com todos
	Mesa
	os sistemas operacionais.
Novo NTFS	Formatação padrão do Windows para discos rígidos.
Tecnologia	
Suporta compartilhamento e registro no diário.	
Sistema de arquivo	
Arquivo	Apple APFS
	Sistema de arquivos Apple do macOS projetado para melhorar o
	Sistema
	desempenho com unidades de estado sólido (SSD) e armazenamento
	flash. Está disponível no macOS 10.13 e superior.
Rede	NFS
	Sistema de código aberto que funciona independentemente do sistema de arquivos
	do sistema operacional, permitindo o acesso ao usuário à rede. Parece local, mas é

Sistema Detalhes do nome completo**Tipo**

ext3 terceiro Versão Linux do NTFS. Permite o registro no diário de

Estendido alterações, para minimizar os danos se ocorrer uma falha.

Arquivo Suporta um máximo de 32.000 subdiretórios.

Sistema

ext4 Quarta Sistema Linux. Suporta tamanhos de arquivo maiores que ext3.

Estendido Pode desabilitar o registro no diário. Suporta um máximo de

Arquivo 64.000 subdiretórios.

Sistema

Limitações do ciclo de vida do fornecedor

O conceito econômico de obsolescência planejada se aplica a computadores e sistemas operacionais ainda mais do que a outros produtos comerciais. Quando uma atualização de CPU, modelo de computador ou sistema operacional é lançada, as chances são muito boas de que seu modelo de substituição esteja no estágio de desenvolvimento. Dois conceitos discutidos nesta seção são o fim da vida útil (EOL) e [o ciclo de vida do produto](#).

Fim da Vida (EOL)

A maioria dos clientes exige que os fabricantes de computadores permaneçam na vanguarda da tecnologia em seus produtos. A qualidade da experiência e as preocupações com a segurança são essenciais para manter a fidelidade dos clientes. Mas o mercado tem capacidade limitada; com cada nova versão de um produto ou sistema operacional, um antigo geralmente recebe o status de “obsoleto” ou “legado”. Quando um novo produto é lançado, como um lançamento de CPU ou placa de GPU, o EOL já está planejado porque a próxima geração geralmente está em desenvolvimento. Isso vale para atualizações de hardware e sistema operacional. Por exemplo, o Windows 7 já é EOL e o Windows 8 EOL está agendado para janeiro de 2023. O Windows 10 EOL está atualmente agendado para outubro de 2025.

Limitações de atualização

Nem todas as atualizações do sistema operacional são viáveis em todos os produtos. Por exemplo, o iOS 15 não pode ser executado na maioria dos modelos de telefone anteriores ao iPhone 6s ou SE. Isso ocorre porque os avanços do software foram além das capacidades físicas do

chipset — pode ser a potência de processamento, a potência do vídeo ou outro fator.

Certifique-se de verificar os sites dos fornecedores antes de atualizar, para garantir que o dispositivo seja compatível com a atualização.

A atualização também pode ter custos ocultos. Se os usuários tiverem acessórios para acompanhar seus dispositivos - cabo de vídeo, adaptadores USB e canetas de escrita, eles também precisam ser substituídos. À medida que os dispositivos migram para interfaces USB-C, muitos dos acessórios antigos se tornam inúteis quando o novo dispositivo chega.

Limitações específicas do fornecedor/preocupações de compatibilidade entre

sistemas operacionais

Quase todos os smartphones nos Estados Unidos usam Android ou iOS. Cada sistema operacional tem usuários leais, e o debate sobre qual é o melhor tem defensores de ambos os lados. Ambos são bons sistemas, mas várias considerações estão envolvidas ao escolher entre o Apple iOS de código fechado específico do fornecedor e o sistema operacional Android de código aberto.

Pode-se argumentar que, como a Apple tem o controle do iOS, ela pode controlar melhor a qualidade e a segurança dos produtos da Apple. Além disso, a Apple pode desenvolver aplicativos melhores, como iMessage, Find My Friends e FaceTime, que funcionam bem porque podem ser projetados com base nas vantagens de uma plataforma de código fechado. Embora seja uma vantagem para uma família ou uma organização usar aplicativos comuns para se comunicar e compartilhar dados facilmente, os usuários que não são do iPhone estão fora do circuito com esses aplicativos.

Pode-se também argumentar que o Android tem certas vantagens porque tem mais aplicativos disponíveis. Além disso, os dispositivos Android tendem a ser muito mais baratos que os iPhones. O Android permite aplicativos de terceiros, mas algumas pessoas veem os aplicativos de terceiros como um problema de segurança em vez de uma vantagem.

A boa notícia é que tanto o iOS quanto o Android são sistemas robustos e confiáveis. A melhor escolha depende, em última instância, dos usuários e de suas necessidades de comunicação. Mais uma boa notícia é que alguns aplicativos que chegam ao mercado facilitam a comunicação e o compartilhamento entre usuários de Android e iOS.

Instalações e atualizações do sistema operacional em um sistema operacional diverso Ambiente

220-1102:
Exam

220-1102: Objetivo 1.9: Dado um cenário, realizar instalações e atualizações de SO em um ambiente de SO diversificado.

Métodos de Inicialização

O processo de inicialização envolve o carregamento dos arquivos necessários do sistema operacional na RAM para que o computador se torne funcional. Dependendo da situação, diferentes **métodos de inicialização** podem ser implantados. O sistema operacional pode ser armazenado no disco rígido local, mas também pode ser armazenado em um CD/DVD, em uma unidade externa USB ou eSATA ou em outro computador na rede. Onde quer que seja armazenado, o computador precisa saber onde ir para encontrar os arquivos do sistema operacional. Isso é feito nas configurações de ordem de inicialização do BIOS/UEFI. Ao inicializar, o PC procura os arquivos no local preferido e os carrega na RAM; o computador torna-se então operacional. Se o PC não conseguir encontrar os arquivos na ordem de inicialização, ele passa para o segundo lugar e continua procurando até encontrar um sistema operacional. A [Figura 6-45](#) mostra a ordem de inicialização no BIOS típico. Lembre-se, porém, de que a tela de ordem de inicialização de cada fornecedor é ligeiramente diferente.



Figura 6-45 Menu de ordem de inicialização do BIOS

Existem muitos métodos para inicializar um sistema durante o processo de instalação:

Key
Topic

- **Disco óptico (CD-ROM/DVD/Blu-ray):** Use este método para instalar o Windows em um PC individual e para criar um PC mestre a partir do qual as imagens de disco podem ser criadas.
- **Inicialização de rede/PXE (ambiente de execução de pré-inicialização):** use este método para instalar o Windows em um ou mais sistemas que tenham conexões de rede em funcionamento. Para usar esse método, os adaptadores de rede devem ser configurados para inicializar usando a ROM de inicialização PXE em um local de rede que contenha uma imagem do sistema operacional.

Observação

Netboot é uma tecnologia de inicialização de rede desenvolvida pela Apple. O Netboot usa o Boot Server Discovery Protocol (BSDP) para localizar e instalar arquivos do sistema operacional.

- **Inicialização USB/eSATA (inicialização a partir de um pen drive USB):** Use este método quando a instalação a partir de um DVD não for possível, como instalar o Windows em um computador sem uma unidade de DVD. A ferramenta de download de USB/DVD do Windows (disponível em www.microsoft.com/en_us/download/windows-usb-dvd-download-tool) pode criar uma unidade USB inicializável a partir de uma imagem ISO (.iso) do Windows que você baixou. Se necessário, altere a ordem de inicialização no firmware BIOS/UEFI do sistema para permitir a inicialização a partir de uma unidade USB.
- **Discos rígidos de estado sólido/flash ou internos (HDD/SSD):** Este é o local mais comum para os arquivos do sistema operacional residirem. Após a instalação do sistema operacional, é importante alterar a ordem de inicialização no BIOS/UEFI para que o computador procure arquivos aqui primeiro e não tente reinstalar a partir do externo fonte.
- **Baseado na Internet:** Baixar e instalar pela Internet é uma opção. Isso envolve o download de um aplicativo de servidor e, em seguida, o download e a criação do arquivo ISO do Windows. É então possível compartilhar a pasta de instalação do Windows e instalar o Windows pela conexão de rede.
- **Unidade externa/hot-swappable:** As unidades hot-swappable são conectadas em baias de unidade especiais que permitem que o disco rígido seja trocado enquanto o

computador está em execução. Quando um computador está em execução, o SO é carregado na RAM para que o SO possa residir em uma unidade hot-swappable e ser trocado, desde que seja devolvido ao compartimento da unidade identificado no BIOS/UEFI como a unidade inicializável .

- **Partição na unidade de disco rígido interna ou SSD:** Esta opção é semelhante à unidade de disco rígido interna acima, mas envolve uma partição designada ou uma seção na unidade reservada para inicialização.

Com cada tipo de unidade, os arquivos de instalação do Windows podem ser extraídos ou o arquivo ISO pode ser usado como fonte de instalação.

Tipos de instalações O

Windows pode ser instalado de várias maneiras. Seguem os métodos mais comuns:



- Como uma atualização local para uma versão existente
- Com a partição de recuperação (que redefine o sistema para seu estado original instalado)
- Como uma instalação limpa em um disco rígido vazio ou na mesma partição da versão atual
- Como inicialização múltipla, o que significa instalar em espaço em disco não utilizado (uma nova partição) para permitir a escolha entre a versão atual e a nova versão, conforme necessário
- Como uma instalação de reparo para corrigir problemas com a instalação atual

As opções de instalação anteriores geralmente usam a mídia de distribuição original ou arquivos de recuperação pré-instalados.

Instalações em grande escala ou personalizadas podem usar os seguintes métodos:

- instalação autônoma
- Instalação de rede remota

- Implantação de imagem

Essas opções de instalação normalmente requerem a criação de um arquivo de imagem.

Instalação autônoma

Em uma instalação assistida, as informações devem ser fornecidas em vários pontos durante o processo. Para executar uma instalação autônoma, crie o tipo apropriado de arquivo de resposta para o tipo de instalação. Atualmente, a Microsoft oferece o Microsoft Deployment Toolkit (MDT) para instalação automatizada do Windows. O MDT cria e atualiza automaticamente o arquivo Unattend.xml (usado para fornecer respostas durante o processo) durante a implantação.

Baixe o MDT do site da Microsoft: <https://docs.microsoft.com/en-us/sccm/mdt/>.

Tipos de Instalações



Atualizações

Para realizar uma atualização do sistema operacional Windows 10/11 para a versão mais recente, recomenda-se uma instalação de *atualização local* do Windows. Inicie o processo de instalação na versão existente do Windows. Essas atualizações no local não excluem instalações anteriores, o que significa que o usuário pode reter aplicativos e configurações, bem como arquivos pessoais.

Observação

Para atualizar do Windows 10 para o Windows 11, use uma atualização local se sua máquina for compatível (as especificações de hardware estão listadas na próxima seção “Considerações de atualização”). Se for compatível, siga estas etapas para atualizar no local: Vá para **Configurações > Atualização e segurança > Windows Update** e clique no botão Verificar atualizações. Se o Windows 11 estiver esperando por você, ele poderá ser instalado. Caso contrário, versões posteriores do Windows 10 podem estar disponíveis.

Os caminhos de atualização exatos entre as versões do Windows variam de acordo com a edição do Windows atualmente em uso. Você pode atualizar para a edição equivalente ou melhor do Windows, mas não para uma edição inferior. As versões de 32 bits podem ser atualizadas apenas para versões de 32 bits; Versões de 64 bits podem ser atualizadas apenas para versões de 64 bits.



Instalação Limpa

Antes de iniciar um processo de **instalação limpa**, verifique o seguinte:

- Certifique-se de que a unidade para instalação seja colocada antes da unidade de disco rígido na sequência de inicialização. O sistema precisa inicializar a partir da mídia de distribuição do Windows se você estiver instalando em um disco rígido vazio. Você pode executar uma instalação limpa do Windows a partir de uma versão mais antiga do Windows se quiser substituir a instalação mais antiga.
- Se você estiver instalando em uma unidade que pode exigir drivers adicionais (SATA, RAID ou adaptadores de host de terceiros na placa-mãe ou em um slot de expansão), tenha os drivers disponíveis em qualquer tipo de mídia removível compatível com o sistema.
- Se você estiver instalando a partir de mídia ótica, de uma imagem de disco (ISO, VXD ou VHDX) ou dentro de uma máquina virtual (VM), depois de reiniciar o sistema com a mídia de CD ou DVD ou arquivo de imagem no lugar, pressione uma tecla quando solicitado a inicializar.

Durante o processo de instalação, esteja preparado para confirmar, inserir, selecionar ou fornecer as seguintes configurações, informações, mídia ou opções quando solicitado:

- **Instalação personalizada:** escolha esta opção se estiver executando uma instalação de “inicialização limpa” em uma parte não utilizada do disco rígido ou apagando a instalação existente em vez de atualizá-la.
- **Edição do Windows que você está instalando:** Se a versão incorreta for inserida, a instalação não poderá ser ativada.
- **Idioma:** o Windows 10 está disponível em mais de 100 idiomas diferentes. Certifique-se de que o pacote de idioma do usuário pretendido esteja selecionado antes da instalação.

- **Local (casa, trabalho/escritório ou público):** As informações de local são usadas para configurar o Firewall do Windows.
- **Configurações de rede:** essas configurações são normalmente detectadas automaticamente para uma conexão com fio. Se sua conexão for sem fio, verifique se o SSID e a senha (chave de criptografia) estão disponíveis.
- **Local da partição, tipo de partição e sistema de arquivos:** consulte a seção “Visão geral do particionamento”, posteriormente neste capítulo, para obter detalhes.
- **Chave do produto:** algumas instalações permitem ignorar isso temporariamente, mas você deve fornecer antes de ativar o Windows.
- **Fuso horário, hora e data:** essas configurações normalmente são detectadas automaticamente, mas você pode defini-las manualmente aqui.
- **Nome de usuário e nome da empresa:** O nome da empresa é opcional.
- **Grupo de trabalho ou nome de domínio:** Este é um grupo de computadores com acesso comum a arquivos e administração e autenticação centralizadas.

Observação

As configurações nesta lista estão em ordem alfabética. Os sistemas operacionais solicitam essas informações em diferentes pontos do processo de instalação.

Ao final do processo, remova a mídia de distribuição. O Windows estará pronto para baixar as últimas atualizações e service packs.

Instalação de reparo

Se uma instalação do sistema operacional Windows for corrompida, use uma instalação de reparo para restaurar os arquivos de trabalho e as entradas do Registro sem perder programas ou informações existentes. Instalações de reparo estão disponíveis no Windows 10. Faça uma cópia de backup de seus arquivos de dados (armazenados em `\Users\Username` para cada usuário do seu PC) antes de executar uma instalação de reparo, em caso de problemas.

Observação

O processo de instalação de reparo também é conhecido como atualização in-loco.

Para executar uma **instalação de reparo** do Windows 10 com uma unidade flash USB (que precisa ser criada antes de iniciar este processo), siga estas etapas:



Etapa 1. Inicialize o computador normalmente e faça login na conta do Administrador.

Desative qualquer software de segurança de terceiros para evitar interrupções na atualização.

Etapa 2. Insira a unidade flash e execute **setup.exe** para iniciar a configuração.

Etapa 3. Quando solicitado, baixe e instale as atualizações.

Etapa 4. Aceite o contrato de licenciamento do usuário final. As atualizações começam.

Etapa 5. Quando as atualizações estiverem prontas, clique em **Instalar** quando solicitado.

Etapa 6. Opte por manter arquivos pessoais, se essa for sua preferência.

Etapa 7. Deixe o processo de instalação do Windows 10 executar e reparar o Windows.

O restante da instalação prossegue como em uma instalação normal.

Instalação de Rede Remota

Uma **instalação de rede remota** (que envolve a instalação do Windows a partir de uma unidade de rede) começa iniciando o computador com um cliente de rede e fazendo logon no servidor para iniciar o processo. Para automatizar o processo, o Windows 10 pode ser instalado automaticamente a partir de uma unidade de rede usando os Serviços de Implantação do Windows. Os Serviços de Implantação do Windows estão incluídos nos sistemas operacionais Windows Server mais recentes.

Os programas baseados em servidor funcionam junto com o Microsoft Development Toolkit ou o programa Windows System Image Manager. Esses programas são usados para criar um arquivo de resposta que fornece as respostas necessárias para a instalação.

Implantação de imagem

Uma **implantação de imagem** é o processo de instalação do Windows a partir de uma imagem de disco de outra instalação. Esse processo também é chamado *de clonagem de disco*. você pode criar

uma imagem de disco usando uma variedade de ferramentas, incluindo Acronis True Image (www.acronis.com) e Seagate DiscWizard (que é parcialmente baseado no Acronis True Image, disponível em www.seagate.com).

Observação

É possível gravar um arquivo de imagem de disco, que geralmente tem uma extensão de nome de arquivo .iso ou .img, em um flash USB ou CD ou DVD gravável usando o Windows Disc Image Burner no Windows 10.

No entanto, se você estiver implantando uma imagem de disco em vários computadores em vez de fazer backup de um único computador, considere estas questões especiais:

- **Diferenças de hardware:** os métodos tradicionais de clonagem de imagem, como aqueles que usam o Acronis True Image, foram projetados para restauração em hardware idêntico (ou seja, a mesma placa-mãe, os mesmos adaptadores de host de armazenamento em massa, a mesma configuração BIOS/UEFI, a mesma camada de abstração de hardware [HAL] e o mesmo arquivo Ntoskrnl.exe [kernel NT]). Para organizações que possuem diferentes tipos e modelos de computadores, isso representa um problema.
- **Mesmo identificador de segurança:** Um sistema clonado é idêntico em todos os aspectos ao original, inclusive tendo o mesmo identificador de segurança (SID). Isso pode causar conflitos em uma rede.

Para superar esses problemas, use programas de clonagem projetados para capturar uma imagem que pode ser implantada em diferentes tipos de computadores (laptops, desktops e tablets) com diferentes hardwares e softwares.

No Windows 10, use a Ferramenta de Preparação do Sistema (Sysprep) para preparar a imagem para instalação em vários computadores. Sysprep carrega arquivos e reinicia o PC. Se você selecionar Generalizar no Sysprep, o Windows removerá as informações exclusivas do PC, incluindo o SID. Quando a instalação for concluída e o computador for reiniciado, um novo SID será gerado.

A Figura 6-46 mostra a janela Sysprep e a opção para generalizar a instalação. Observe a opção de reinicialização no final do processo.



Figura 6-46 Iniciando a ferramenta Sysprep em um sistema Windows 10

Todas as ferramentas de clonagem podem funcionar com uma unidade de destino do mesmo tamanho ou maior que a unidade de sistema clonada original. Alguns também podem funcionar com uma unidade menor; verifique a documentação para obter detalhes.

CUIDADO

Não use a clonagem de disco para fazer cópias ilegais do Windows. Use software de clonagem de disco legalmente para fazer uma cópia de backup de sua instalação. Se você estiver duplicando a instalação em outro PC, certifique-se de clonar um sistema criado com uma licença de volume para Windows e certifique-se de não exceder o número de sistemas cobertos por essa licença; alternativamente, certifique-se de usar o número de licença correto (chave do produto) para cada sistema duplicado. Para obter mais informações sobre o licenciamento do Windows, consulte www.microsoft.com/en-us/licensing/default.aspx.

partição de recuperação

Ao atualizar o Windows ou fazer uma instalação limpa com a Instalação do Windows, uma **partição de recuperação** é criada. A partição de recuperação é um espaço que contém o Windows Recovery Environment (WinRE), que pode reparar alguns erros comuns de inicialização. O WinRE é integrado às versões do Windows 10 para edições de desktop.

Atualizar/Restaurar

Se um PC estiver com baixo desempenho ou parecer estar de alguma forma infectado por um vírus, pode ser uma boa ideia redefinir o PC para as configurações padrão de fábrica. Redefinir um PC no Windows 10 é um processo simples. Vá para **Configurações > Recuperação**

e clique em Começar em Redefinir este PC. Ao clicar em Começar, você tem duas opções: Manter meus arquivos ou Remover tudo. Keep My Files é para uma pequena redefinição; ele permite que arquivos pessoais sejam mantidos durante a remoção de aplicativos e quaisquer configurações que tenham sido alteradas. Remove Everything executa uma redefinição principal, removendo todos os arquivos; antes de escolher esta opção, você precisa fazer backup de arquivos pessoais. A Figura 6-47 mostra a página Recuperação, juntamente com a janela que aparece quando você clica em Começar.

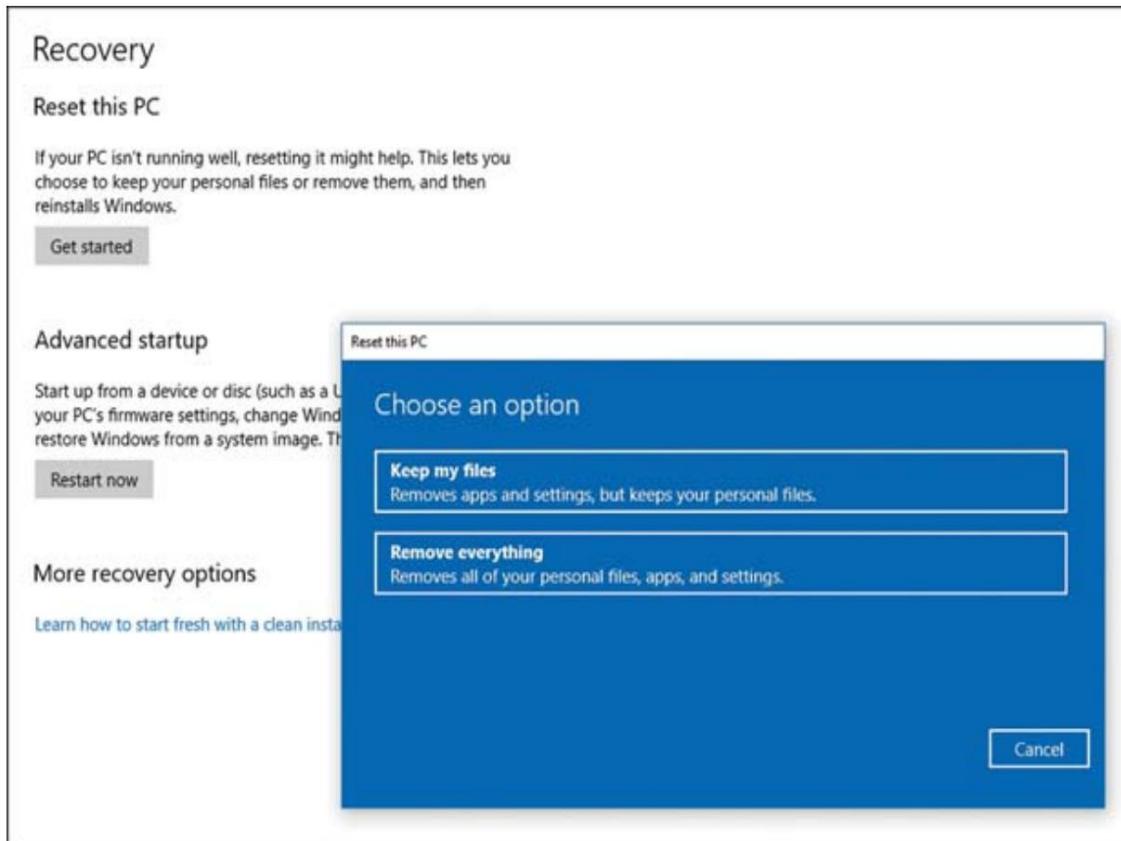


Figura 6-47 A janela de recuperação e a janela Redefinir este PC

Outras considerações/Drivers de terceiros

Ao instalar ou atualizar um sistema operacional, é importante pensar em atualizar os drivers compatíveis com o hardware usado no dispositivo. Por exemplo, um driver corrompido (ou um driver feito para uma versão diferente do sistema operacional) pode causar problemas ou, na pior das hipóteses, travar o sistema. Se um driver de hardware falhar após uma atualização, remover o driver do Gerenciador de dispositivos e reinstalar a versão mais recente do fabricante é uma boa jogada.

Drivers de terceiros referem-se a drivers provenientes de fora do Windows, geralmente de um fabricante de dispositivo. O OD do Windows contém uma biblioteca substancial de drivers padrão para dispositivos, como adaptadores de rede e placas de vídeo e som. Na maioria das vezes, esses drivers funcionam bem, mas a instalação de um driver do fabricante pode aprimorar os recursos ou o desempenho de um dispositivo.

Métodos de particionamento

Se o Windows estiver sendo instalado em um disco rígido vazio ou em um disco rígido com espaço não atribuído (para inicialização múltipla), pelo menos uma nova partição de disco rígido deve ser criada. Para fazer isso com sucesso, você precisa entender as diferenças entre o seguinte:

- Registro mestre de inicialização (MBR) e tabelas [de partição GUID Partition Table \(GPT\)](#)
- Partições primárias e estendidas
- Partições estendidas e unidades de disco lógico
- Discos dinâmicos e básicos

Visão geral do particionamento

Um disco rígido não pode ser usado até que esteja preparado para uso. Duas etapas estão envolvidas na preparação de um disco rígido:

Etapa 1. Crie partições.

Etapa 2. Formate as partições (e atribua letras de unidade).

Uma partição de disco é uma estrutura lógica em um disco rígido que especifica o seguinte:

- Se a unidade pode ser inicializável
- Quantas letras de unidade (uma, duas ou mais) o disco rígido conterá
- Se alguma capacidade do disco rígido será reservada para um sistema operacional futuro ou outro uso

Embora o nome *partição de disco* sugira que a unidade será dividida em duas ou mais seções lógicas, cada disco rígido deve passar por um processo de **particionamento**, mesmo se você quiser usar todo o disco rígido como uma única letra de unidade.

Todas as versões do Windows suportam dois tipos principais de partições de disco:



- **Partição primária:** Uma partição primária pode conter apenas uma única letra de unidade e pode ser ativada (inicializável). Apenas uma partição primária pode estar ativa. Embora uma única unidade física usando MBR possa conter até quatro partições primárias, apenas uma partição primária é necessária em uma unidade que contém um único sistema operacional. Se você estiver instalando um novo sistema operacional em uma configuração de inicialização múltipla com seu sistema operacional atual, instale o novo sistema operacional em uma partição de disco diferente daquela usada para a versão anterior do Windows. Se você estiver usando um sistema operacional diferente do Windows junto com seu sistema operacional atual, ele deverá ser instalado em sua própria partição primária. Uma unidade particionada usando GPT pode ter até 128 partições primárias.

Observação

Dependendo do layout e do conteúdo de suas partições de disco atuais, você pode reduzir o tamanho das partições existentes com o Gerenciamento de disco do Windows, para liberar espaço para uma nova partição primária ou pode precisar usar um software de terceiros, como o Acronis Disk Director ou EaseUS Partition Master.

- **Partição estendida:** Uma partição estendida difere de uma partição primária de duas maneiras importantes:
 - Uma partição estendida não recebe uma letra de unidade, mas pode conter uma ou mais unidades lógicas, cada uma com uma letra de unidade atribuída.
 - Nem uma partição estendida nem qualquer unidade que ela contém podem ser inicializáveis.

Apenas uma partição estendida pode ser armazenada em cada unidade física. As partições estendidas são usadas apenas com unidades MBR.

Tipos de partição MBR x GPT

As partições do **registro mestre de inicialização (MBR)** são suportadas pelo BIOS ROM clássico, bem como pelo firmware UEFI. O MBR suporta um tamanho máximo de unidade de 2 TB e até quatro partições primárias.

Uma **tabela de partição de ID globalmente exclusiva (GPT)** oferece suporte a unidades de até 256 TB e até 128 partições primárias. O GPT também é mais confiável do que o MBR porque protege a tabela de partição com replicação e uma verificação de redundância cíclica (CRC) do conteúdo da tabela de partição. A GPT também fornece uma maneira padrão para os fornecedores de sistemas criarem partições adicionais. As tabelas de partição GPT são suportadas pelo firmware UEFI.

Para inicializar a partir de uma unidade GPT, o sistema deve ter uma versão de 64 bits do Windows. (As versões mais recentes do Windows Server também suportam GPT.) As versões de 32 bits do Windows podem usar unidades GPT para dados.

Preparação de disco usando MBR

Se uma unidade for usada por um único sistema operacional usando uma tabela de partição MBR, uma destas três formas de particionar a unidade é usada:

- **A partição primária ocupa 100 por cento da capacidade da unidade física:** normalmente é assim que o disco rígido em um sistema vendido no varejo é usado e também é o padrão para preparação de disco com o Windows. Esta opção é adequada para a única unidade em um sistema ou uma unidade adicional que pode ser usada para inicializar um sistema, mas não deve ser usada para unidades adicionais em um sistema que será usado para armazenamento de dados.
- **A partição primária ocupa uma parte da capacidade da unidade física e o restante da unidade é ocupado por uma partição estendida:** Isso permite que o sistema operacional seja armazenado na partição primária e os aplicativos e dados sejam armazenados em uma ou mais partições lógicas separadas. unidades (ou seja, letras de unidades criadas dentro da partição estendida). Esta é uma configuração comum para laptops, mas requer que o processo de particionamento seja executado com configurações diferentes dos padrões. Essa configuração é adequada para o único inversor ou para o primeiro inversor em um sistema de vários inversores.

- **A partição estendida ocupa 100% da capacidade da unidade física:** as letras da unidade na partição estendida podem ser usadas para armazenar aplicativos ou dados, mas não o sistema operacional. Uma partição estendida não pode ser ativada (inicializável). Esta configuração é adequada para discos rígidos adicionais em um sistema (não o primeiro disco); uma partição estendida pode conter apenas uma unidade lógica ou várias unidades lógicas.

Você também pode deixar algum espaço não particionado no disco rígido para uso posterior, seja para outro sistema operacional ou para outra letra de unidade.

Depois que um disco é particionado, as letras da unidade devem ser formatadas usando um sistema de arquivos compatível.

Particionando usando GPT

O particionamento GPT cria uma ou mais partições primárias. Não há partições estendidas ou unidades lógicas em uma unidade GPT; cada partição pode receber uma letra de unidade. No entanto, apenas uma partição pode estar ativa.

Discos Dinâmicos e Básicos

O Windows oferece suporte a dois tipos de discos: básicos e dinâmicos. Um disco dinâmico é mais versátil do que um disco básico porque pode abranger duas unidades físicas em uma única unidade lógica, criar matrizes distribuídas ou espelhadas e ajustar o tamanho de uma partição. No entanto, durante a instalação, o Windows cria apenas discos básicos.

Somente discos básicos podem ser inicializáveis.



Criando partições durante a instalação do Windows

Ao instalar o Windows 10 em um disco rígido vazio, você recebe uma solicitação de localização. Para usar todo o espaço no disco, verifique se o disco e a partição desejados estão realçados e clique em Avançar.

Para usar apenas parte do espaço, clique em Opções de unidade (avançadas), clique em Novo, especifique o tamanho da partição e clique em Aplicar. O Windows exibe uma mensagem informando que está criando uma partição adicional. Clique em OK para limpar a mensagem. UMA

partição reservada pelo sistema é criada, seguida pelo tamanho da partição que você selecionou para o Windows usar e o espaço não utilizado (não alocado).

Para usar uma partição existente, realce a partição desejada e clique em Avançar.

CUIDADO

Tenha cuidado: qualquer partição que você selecionar para a instalação será formatada e todos os dados dessa partição serão apagados.

Formatação A

formatação rápida é uma opção em todas as versões do Windows. Com novos discos rígidos ou discos existentes sem erros, você pode usar a opção de formatação rápida para limpar rapidamente as áreas do disco rígido que armazenam registros de localização de dados.

Com a opção de formato completo, o Windows deve reescrever as estruturas do disco em toda a superfície do disco. Isso pode levar vários minutos com os grandes discos rígidos de hoje.

Observação

Se você estiver preocupado com a condição de um disco rígido usado que está sendo reutilizado com o Windows, use Windows chkdsk se a unidade tiver sido formatada para verificar seu estado. O programa utilitário de diagnóstico de disco do fornecedor da unidade também verifica a condição de uma unidade.

Considerações sobre atualização

Algumas definições de configuração do Windows são feitas durante a instalação; outros são feitos depois. As seções a seguir descrevem os principais problemas a serem considerados para concluir o processo de atualização.

Arquivos de backup e preferências do usuário

Antes de atualizar, uma boa estratégia é fazer backup de todo o conteúdo do computador em uma unidade selecionada ou em outro local ou local de rede. UMA

O programa de backup pode criar um arquivo compactado para armazenar informações de backup e preferências do usuário.

O Windows pergunta durante uma atualização o que fazer com os arquivos atuais. Eles devem migrar bem, mas um backup é sempre uma boa ideia, mesmo em operações normais.

Suporte a aplicativos e drivers/compatibilidade com versões anteriores

Após a instalação do Windows, ele deve ser atualizado com os drivers mais recentes. Para PCs individuais, a maneira mais fácil de executar essas etapas é configurar o Windows Update para atualizações automáticas.

No entanto, se você estiver instalando o Windows pela primeira vez e o sistema ou a placa-mãe tiver um disco de driver, execute a instalação do driver antes de executar o Windows Update.

Pré-requisitos e compatibilidade de hardware e aplicativos

Antes de tentar instalar qualquer versão de qualquer sistema operacional, é importante ter certeza de que o hardware e os aplicativos a serem usados funcionarão com (ou seja, são compatíveis com) o sistema operacional. Esta seção descreve resumidamente o processo que os fabricantes usam para garantir a conformidade e as etapas que os técnicos de PC executam para garantir a conformidade dos produtos.

Pré-requisitos

Ao fazer uma instalação limpa, é importante certificar-se de que seu hardware atenda aos pré-requisitos para trabalhar com o software - geralmente uma quantidade mínima de RAM e um certo nível de poder de processamento. No entanto, os pré-requisitos são mínimos; não ter poder de processamento suficiente e não ter RAM suficiente são as causas mais comuns de problemas de desempenho. Certifique-se de exceder os mínimos para que o sistema operacional possa operar sem problemas.

A lista a seguir é um resumo dos requisitos atuais para Windows 10 e Windows 11.

Windows 10

- **Processador:** Processador de 1 GHz ou mais rápido ou System on a Chip (SoC)

- **RAM:** 1 GB para SO de 32 bits ou 2 GB para SO de 64 bits
- **Espaço no disco rígido:** 16 GB para SO de 32 bits ou 32 GB para SO de 64 bits
- **Placa gráfica:** DirectX 9 ou posterior com driver WDDM 1.0
- **Exibição:** 800 × 600
- Conexão com a Internet : conectividade com a Internet para realizar atualizações e aproveitar alguns recursos

Windows 11

- **Processador:** Dois ou mais núcleos em um processador compatível de 64 bits ou System on a Chip (SoC).
- **RAM:** 4 GB.
- **Espaço no disco rígido:** dispositivo de armazenamento de 64 GB ou maior.
- **Placa gráfica:** Compatível com DirectX 12 ou posterior com driver WDDM 2.0.
- **Monitor:** Monitor de alta definição (720p) com mais de 9 polegadas na diagonal; 8 bits por canal de cor.
- **Conexão com a Internet:** o Windows 11 Home Edition requer conectividade com a Internet e uma conta da Microsoft. A troca de um dispositivo do Windows 11 Home no modo S também requer conectividade com a Internet.

Qualquer coisa abaixo dessas recomendações provavelmente resultará em uma instalação difícil e desempenho insatisfatório. A atualização para esses padrões ou acima é altamente recomendada.

Programa de Compatibilidade do Windows

Os fabricantes têm interesse em garantir que seus produtos possam ser usados pelo maior público de sistemas operacionais do mundo, portanto, eles projetam seus produtos de acordo com os padrões do Programa de Compatibilidade do Windows. Isso permite que eles testem seus produtos de hardware e software para garantir que funcionem quando o cliente os comprar e instalar.

Compatibilidade de hardware e aplicativos

Para um consumidor, a maneira mais fácil de verificar a compatibilidade com um sistema operacional Windows é consultar a Microsoft. Por muitos anos, a Microsoft manteve a lista de compatibilidade de hardware (HCL), também chamada de lista de produtos de compatibilidade do Windows. A HCL fornece informações sobre fabricantes e drivers que podem ser usados (e não usados) com o Windows. Com o Windows 10, a maioria dos equipamentos anteriores deve funcionar. O verificador de compatibilidade de hardware da Microsoft corresponde a produtos compatíveis para Windows e macOS (consulte <https://docs.microsoft.com/en-us/windows-hardware/drivers/dashboard/windows-certified-products-list>).

Os fabricantes mais populares enviam drivers para o Windows para permitir o recurso plug and play, mas os drivers geralmente precisam ser atualizados em algum ponto do ciclo de vida do dispositivo. Sempre que você estiver instalando um dispositivo ou aplicativo, é aconselhável verificar no site do fabricante a atualização mais recente.

Um programa é escrito para funcionar em um determinado sistema operacional e, com cada atualização do sistema operacional, existe a possibilidade de que um programa esteja executando mal ou não. Se você estiver executando programas escritos para versões anteriores do Windows, poderá verificar a compatibilidade com o Windows 10 usando a ferramenta Solucionador de problemas de compatibilidade. No Windows File Explorer, clique com o botão direito do mouse no programa a ser executado e selecione Propriedades. Clique na guia Compatibilidade, marque Executar este programa no modo de compatibilidade e selecione o sistema operacional usado anteriormente.

Outra opção no Windows 10 é digitar **Executar Programas** na barra de pesquisa e selecionar Executar Programas Criados para Versões Anteriores do Windows.

Atualizações de recursos

O Windows inclui um recurso que mantém o software atualizado com correções e patches de segurança. A página pode ser encontrada em **Configurações > Atualização e segurança > Windows Update** (consulte a [Figura 6-48](#)).

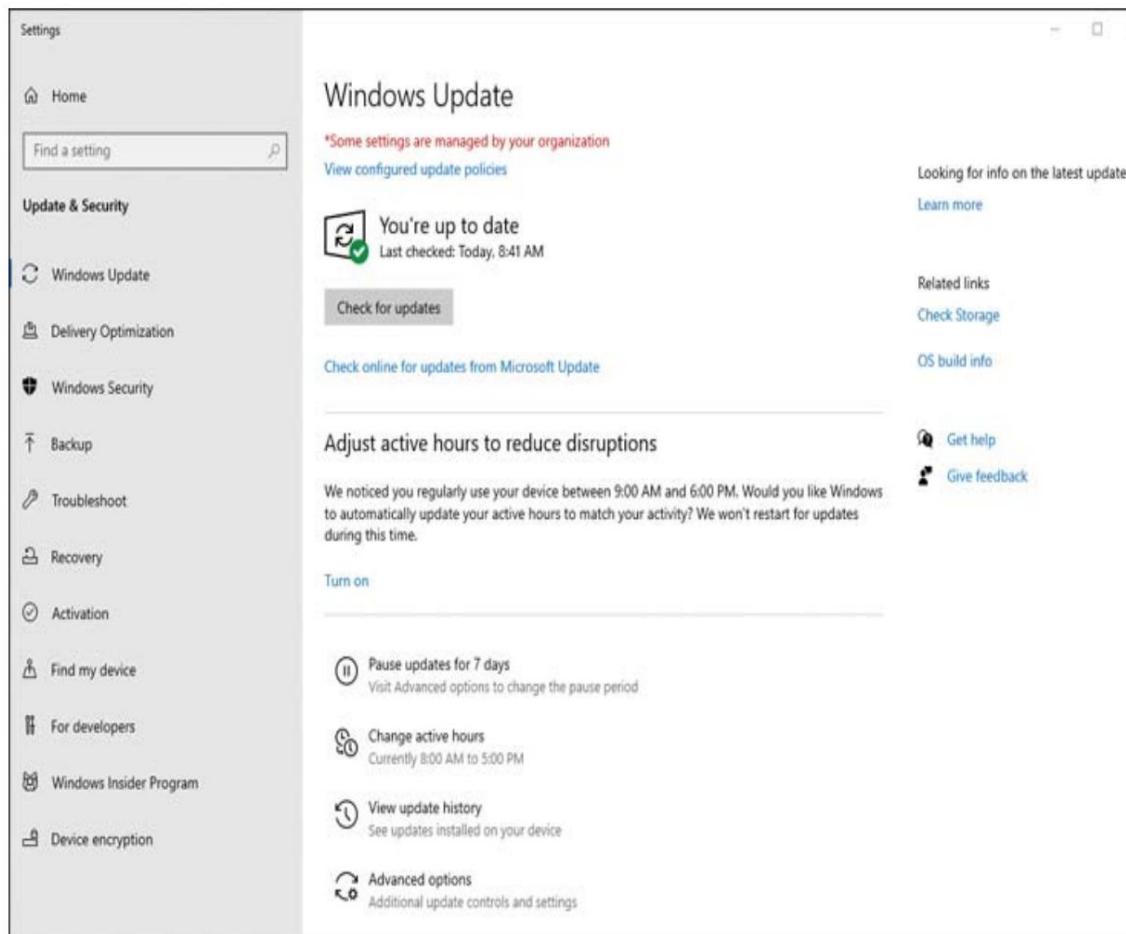


Figura 6-48 A página de atualização do Windows

As atualizações podem ser feitas manualmente clicando no botão Verificar atualizações ou pode ser criada uma programação de atualização.

Atualizar ciclo de vida

Versões mais recentes do sistema operacional Windows são lançadas a cada outono e primavera. O ciclo de vida dessas versões do Windows Update é de 18 meses, quando a Microsoft encerra o suporte a essa atualização. Quando o ciclo de suporte termina, é necessário atualizar para uma versão compatível para continuar recebendo patches de segurança e não relacionados à segurança.

Recursos e ferramentas comuns do sistema operacional macOS/Desktop

220-1102:
Exam

220-1102: Objetivo 1.10: Identificar recursos e ferramentas comuns do sistema operacional macOS/desktop.

Embora o macOS seja muito menos comum que o Windows em alguns ambientes corporativos, o macOS é muito popular em locais de trabalho educacionais e criativos. Para ser um técnico de informática completo, é importante entender como o sistema operacional difere do Windows e ser capaz de executar comandos básicos e procedimentos de manutenção.

Instalação e desinstalação de aplicativos Os processos de instalação e desinstalação de aplicativos macOS são bastante simples. As seções a seguir descrevem os tipos de arquivo e as etapas do processo.

Tipos de arquivo

O Mac usa um processo bastante direto para instalar e desinstalar arquivos que difere do assistente de instalação encontrado no Windows. Os tipos de arquivo de instalação usados no macOS são os seguintes:

- Arquivos .dmg (**imagem de disco**): o download de um arquivo .dmg é semelhante ao download de um kit de instalação completo para um aplicativo — semelhante a um arquivo ISO no Windows. Tudo o que é necessário está contido no arquivo, incluindo scripts de instalação e arquivos de aplicativos. Simplesmente arrastar um arquivo para o disco rígido garante que todos os arquivos necessários estejam presentes. Essa ação de arrastar e soltar conclui todas as tarefas de instalação, semelhante ao assistente de instalação no ambiente Windows. Quando a instalação estiver concluída, o arquivo .dmg pode ser excluído com segurança.
- **.pkg**: são arquivos e scripts de instalação compactados, semelhantes aos arquivos .zip que o macOS usa para instalações de software Mac. Os arquivos de instalação estão no arquivo .pkg e não há necessidade de arrastá-los e soltá-los.
- **.app**: esta extensão de arquivo indica que um arquivo contém um aplicativo executável que será executado no macOS. A pasta também contém informações como ícones e outras propriedades que o sistema operacional usa para torná-lo funcional.

Loja de aplicativos

A App Store é a plataforma de mercado online para aplicativos aprovados pela Apple. Um usuário pode comprar e baixar aplicativos para o computador ou iPhone e tablets e ter certeza de que a Apple examinou o código quanto à qualidade e segurança.

O macOS tem uma variedade de opções para atualizações do sistema na seção App Store das Preferências do Sistema. A App Store pode ser configurada para verificar automaticamente atualizações de aplicativos e macOS, instalar atualizações automaticamente e baixar aplicativos instalados em outros dispositivos macOS sob o mesmo usuário conta.

Para evitar confusão, observe que a Apple Store é um local para compra de hardware (telefones, computadores, acessórios e serviços); a App Store é para comprar aplicativos.

Processo de desinstalação

Desinstalar aplicativos de um computador Mac não é um processo complicado. No menu Finder, acesse a pasta Aplicativos. Localize o aplicativo a ser excluído e arraste-o para a lixeira.

Outro método é selecionar o Launchpad no Dock. Isso exibe todos os aplicativos na área de trabalho; aqueles que podem ser excluídos rapidamente mostram um X no canto superior esquerdo de seu ícone. Simplesmente clique no X e confirme (veja [a Figura 6-49](#)).

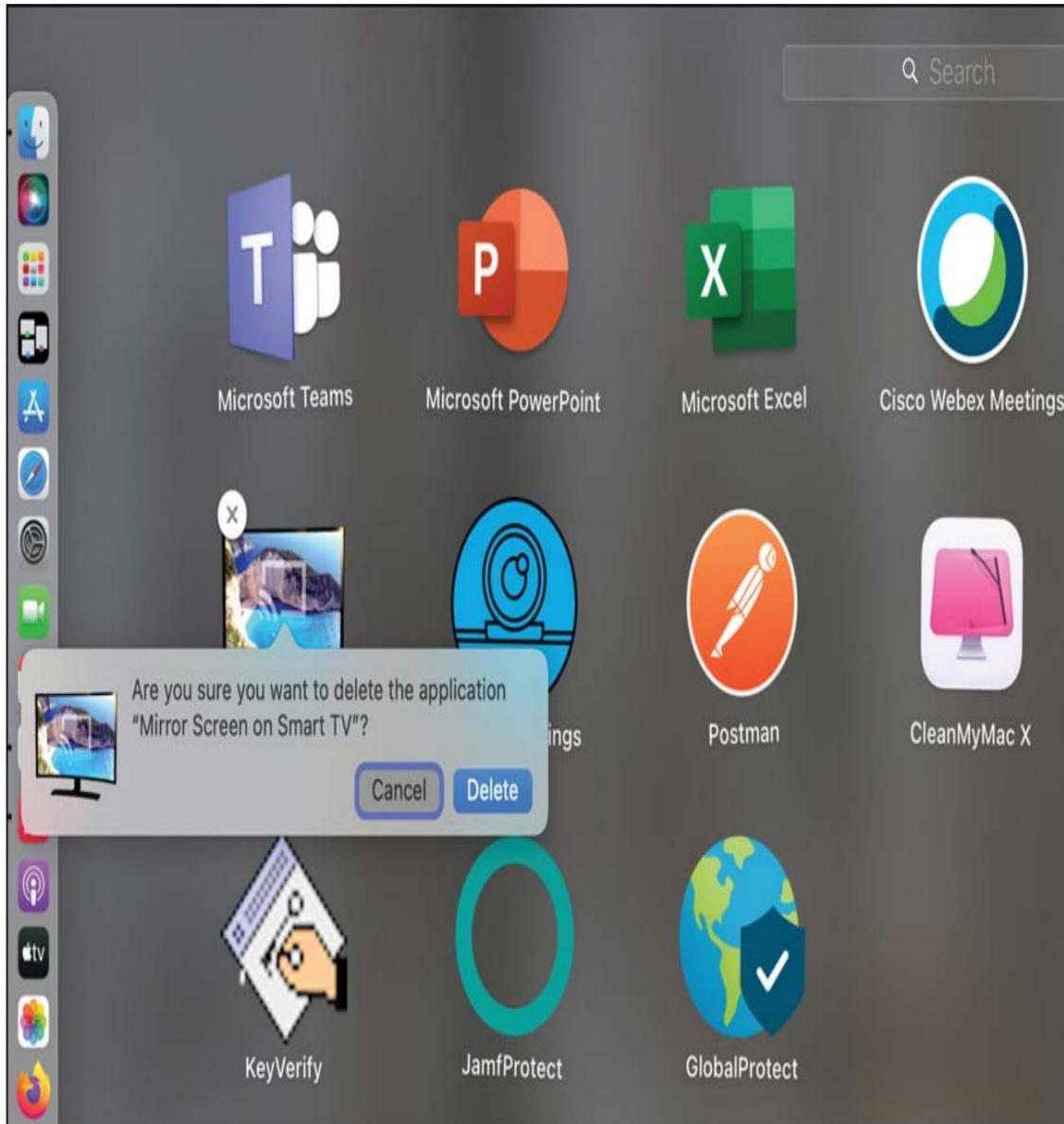


Figura 6-49 Desinstalando do Mac Launchpad (terceiro ícone do topo na doca)

Esses métodos rápidos não desinstalam completamente os arquivos dos vários lugares onde as informações do aplicativo são armazenadas. A maneira mais fácil de fazer isso é com um software de terceiros, como o CleanMyMac.

ID Apple e restrições corporativas O ID

Apple é o processo de autenticação usado para garantir que usuários autorizados acessem a App Store e façam compras de software. O ID da Apple

cruza plataformas e uma conta de usuário pode ser usada para compras e acesso em um iPhone, iPad ou computador Mac.

As empresas também podem ter contas de ID Apple que podem ser atribuídas aos funcionários. A principal diferença entre a conta pessoal e a conta corporativa é que um administrador no ambiente corporativo pode restringir o acesso ao software e aos serviços quando o usuário estiver trabalhando no ambiente corporativo.

Melhores Práticas

As melhores práticas em um Mac não são diferentes das de qualquer outro sistema operacional. Antigamente, pensava-se que os computadores da Apple eram menos vulneráveis a infecções por vírus, mas isso não é mais verdade. Essas etapas devem parecer familiares agora.

backups

Um backup completo faz backup de todo o conteúdo do computador ou da unidade selecionada em outro local ou local de rede. Um programa de backup pode criar um arquivo compactado para armazenar informações de backup. Com esse tipo de backup, o programa de backup deve executar um utilitário de restauração para tornar os arquivos utilizáveis novamente.

Outro tipo de programa de backup simplesmente copia os arquivos de backup para um local diferente, onde podem ser abertos pelo sistema operacional.

A maioria dos programas de backup também pode executar um backup incremental, que faz backup apenas dos arquivos que foram criados ou alterados após o último backup completo.

Os recursos de backup a serem procurados incluem o seguinte:



- **Compactação:** Isso reduz a quantidade de espaço de arquivo e também diminui o tempo necessário para fazer um backup.
- **Supporte para backups incrementais e completos:** Boas práticas de backup exigem backups completos periódicos, seguidos de backups de arquivos que foram alterados desde o último backup completo (backups incrementais).
- **Destinos de backup local e de rede:** alguns utilitários de backup requerem configuração adicional antes que um backup de rede possa ser

realizada.

O macOS inclui o utilitário de backup **Time Machine** que deve ser configurado e executado para ser útil em caso de perda de dados.

Para ativar e configurar o Time Machine, siga estas etapas:



Etapa 1. Conecte um disco externo adequado a um sistema macOS.

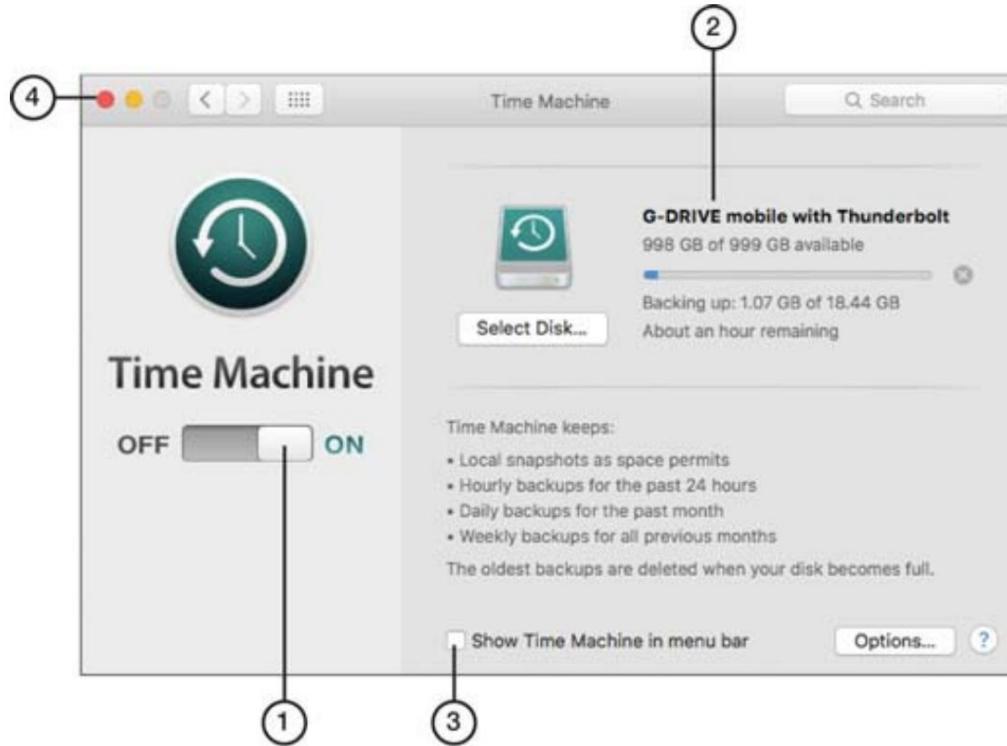
Etapa 2. Quando solicitado, clique em **Usar como disco de backup**. Você também pode verificar a caixa **Criptografar disco de backup** para proteger o backup (consulte a [Figura 6-50](#)).



1. Create and confirm password for encrypted Time Machine drive
2. Enter a password hint
3. Click to start encryption of Time Machine drive

Figura 6-50 Selecionando um disco externo para uso com o Time Machine

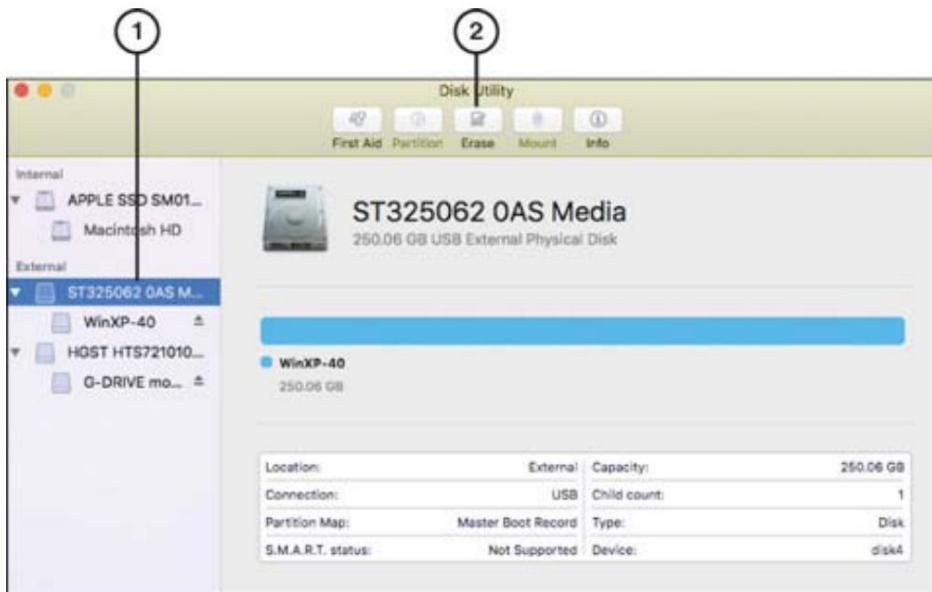
Etapa 3. Se você selecionou a opção de criptografar seu backup na etapa 2, insira uma senha, confirme-a e insira uma dica de senha. Clique em **Criptografar disco** (consulte a [Figura 6-51](#)).



1. Time Machine turned on
2. Progress bar and backup disk information
3. Check box to put Time Machine on menu bar at top of screen
4. Click to close (Red) or minimize (Yellow) Time Machine menu

Figura 6-51 Criptografando o disco do Time Machine

Etapa 4. Certifique-se de que o Time Machine esteja ativado (consulte a [Figura 6-52](#)). Depois que o disco selecionado é criptografado, o backup é iniciado.



1. Click drive to erase
2. Click Erase to start process

Figura 6-52 Criando um backup com o Time Machine

O Time Machine foi projetado para fazer backup dos arquivos do usuário automaticamente. No entanto, para criar uma imagem de disco que possa ser restaurada em caso de desastre, use o Utilitário de Disco.

Atualizações de antivírus/antimalware

Antigamente, acreditava-se amplamente que o macOS era imune a vírus e malware. Embora o macOS não seja tão visado quanto o Windows, um computador macOS desprotegido pode ser usado como um vetor de infecção para máquinas Windows que se conectam a ele.

ClamAV (www.clamav.net) é um aplicativo antivírus de código aberto disponível para macOS e Linux. Varreduras e atualizações podem ser automatizadas com cron, e um front-end GUI conhecido como ClamTK está disponível. O software antivírus conhecido geralmente possui versões macOS, bem como versões Linux e Windows.

Os aplicativos antivírus e antimalware devem ser atualizados pelo menos diariamente.

Atualizações/Correções

O macOS tem uma variedade de opções para atualizações do sistema na seção Atualização de software das Preferências do sistema (consulte a [Figura 6-53](#)). As preferências podem ser configuradas para verificar automaticamente se há atualizações para aplicativos e macOS,

instalar atualizações automaticamente e baixar aplicativos instalados em outros dispositivos macOS na mesma conta de usuário.



Figura 6-53 O aplicativo de atualização de software nas preferências do sistema Cardápio

Ao atualizar o software, o Mac ou outro dispositivo deve estar conectado à alimentação CA. Depois de baixar e instalar a atualização, uma senha, impressão digital ou identificação facial é necessária após a reinicialização.

Preferências do Sistema

As configurações de Preferências do Sistema em um Mac podem ser acessadas selecionando o ícone de roda dentada no Dock ou usando o menu Apple e selecionando Preferências do Sistema. A Figura 6-54 mostra um exemplo do menu Preferências do Sistema.

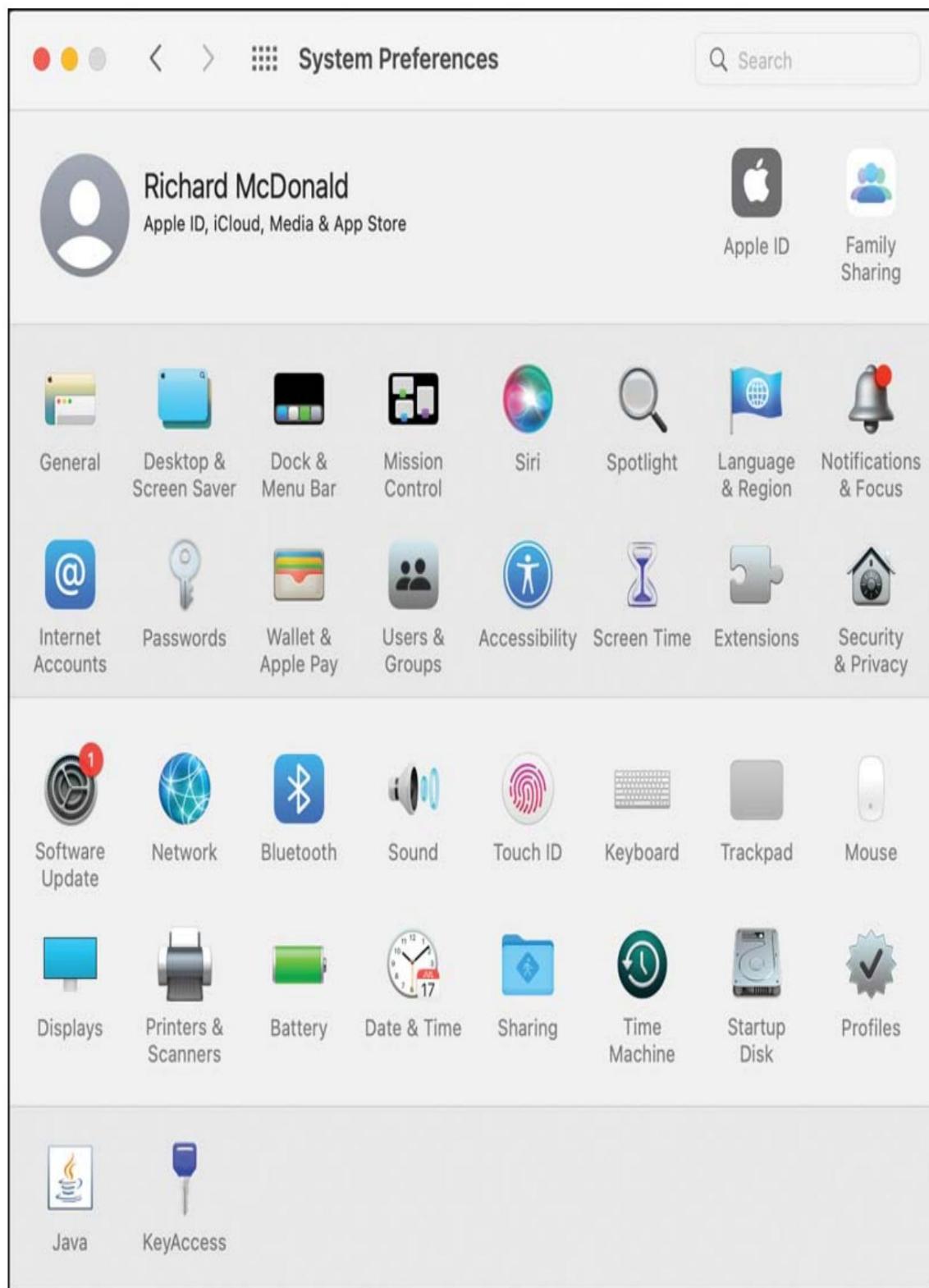


Figura 6-54 O Menu de Preferências do Sistema. O número vermelho sobre a atualização de software indica que uma nova atualização está disponível (e que

As atualizações automáticas ainda não foram configuradas).

O menu Preferências do Sistema varia, dependendo do usuário e dos aplicativos instalados. No entanto, encontrar uma configuração específica é bastante simplificado com o menu de pesquisa no canto superior direito. Este menu é intuitivo: basta digitar uma ou duas letras de uma configuração para destacar a preferência que precisa ser aberta para alterar as configurações.

Algumas das principais preferências destacadas nos objetivos A+ são as seguintes:

- **Monitores:** configuração das configurações de um monitor, como brilho e Night Shift, que aquece as cores de um monitor à noite para melhorar o sono.
- **Rede:** configurações para gerenciamento de Wi-Fi, TCP/IP, DNS e outras configurações de rede. Também possui configurações de ingresso automático para redes comumente acessadas.
- **Impressoras e Scanners:** Preferências para impressoras, compartilhamento de impressão e digitalização.
- **Segurança e privacidade:** controle sobre os serviços de localização (consulte a [Figura 6-55](#)). Quando ativado, as configurações indicam quais aplicativos usaram serviços de localização nas últimas 24 horas. Os serviços de segurança incluem configurações de firewall, FileVault (que criptografa dados automaticamente no disco) e controles de senha.

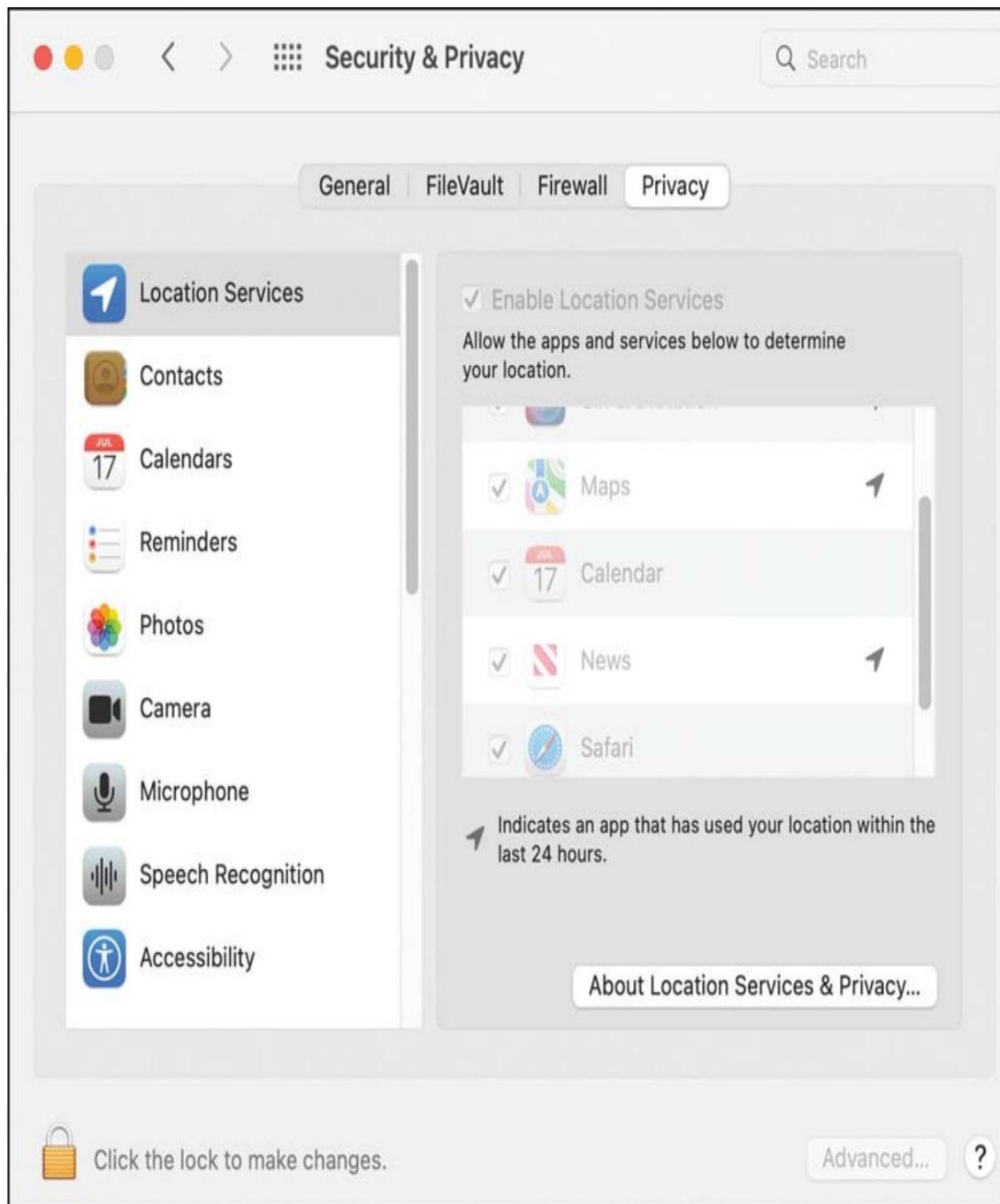


Figura 6-55 Configurações de privacidade no menu Segurança e privacidade

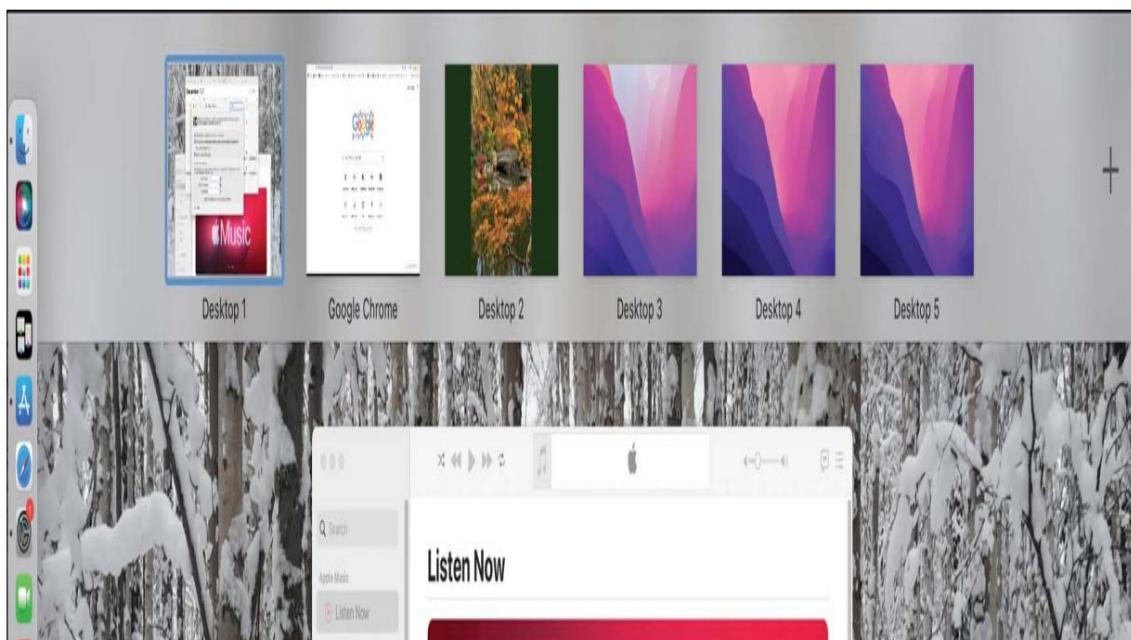
Para alterar as configurações ou acessar as configurações avançadas, a fechadura no canto inferior esquerdo deve ser desbloqueada com uma senha (ou biométrica) antes que você possa fazer alterações; ele deve então ser travado novamente para aplicar as configurações.

- **Acessibilidade:** configurações para configurar o Mac para se adaptar à visão, audição, motor e outros requisitos do usuário para facilidade de uso.
- **Time Machine:** consulte a cobertura do Time Machine na seção anterior.

Recursos

O macOS tem seguidores dedicados de usuários, e um dos motivos são os muitos atalhos e recursos incluídos na experiência de desktop. Os objetivos A+ apresentam os nove discutidos aqui, mas há muitos mais a serem descobertos:

- **Vários desktops:** os usuários não estão limitados a um desktop para trabalhar. Vários podem estar em uso ao mesmo tempo, com áreas de trabalho executando diferentes aplicativos (consulte a parte superior da [Figura 6-55](#)). Essas áreas de trabalho podem ser navegadas deslizando para cima com três ou quatro dedos no trackpad, usando a tecla Control com as setas para a esquerda ou para a direita ou usando o Mission Control.
- **Controle de Missão: O Controle** de Missão facilita a exibição de todas as janelas abertas, áreas de trabalho disponíveis e outras configurações. Entre essas configurações está a capacidade de usar cantos quentes, em que o mouse sobre um canto escolhido da tela abre um atalho para um recurso pré-selecionado, como o Launchpad ou Quick Notes. A [Figura 6-56](#) representa o Mission Control (aberto com o atalho Ctrl+seta para cima).



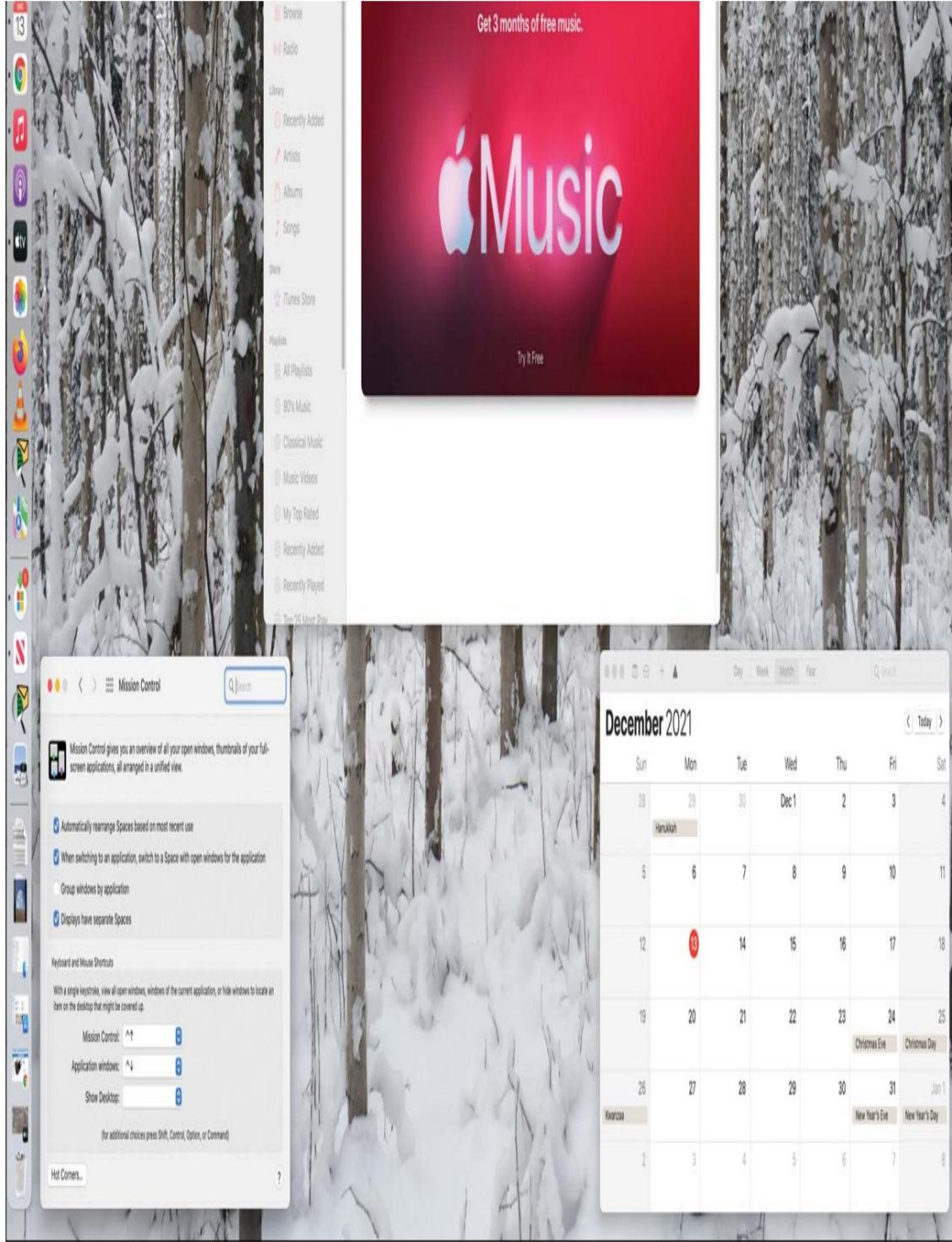


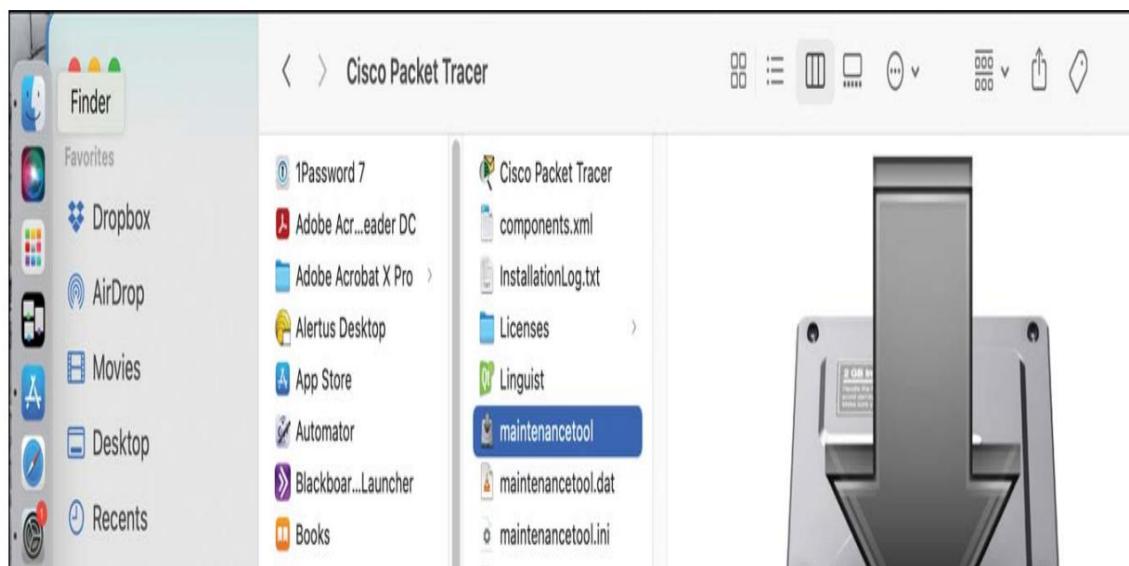
Figura 6-56 Privacy Mission Control, exibindo as áreas de trabalho disponíveis, o Dock e todas as janelas abertas

- **Chaveiro:** Este contêiner criptografado no Mac armazena senhas, nomes de usuário, números de contas e outras informações privadas. Ele fornece

segurança e facilidade no acesso a sites que requerem autenticação.

O Keychain funciona em várias plataformas, portanto, uma atualização em um Mac atualiza as informações em um iPhone na mesma conta.

- **Spotlight:** Este é um mecanismo de pesquisa altamente intuitivo para documentos, referências de texto e muito mais. Ele não reside na área de trabalho, mas você pode acessá-lo instantaneamente pressionando Cmd+barra de espaço. O Spotlight pode ser configurado para pesquisar até 18 tópicos e áreas diferentes, como aplicativos, documentos, bibliotecas de música e definições. Também pode ser configurado para não pesquisar itens nas configurações de privacidade.
- **iCloud:** iCloud é o produto de armazenamento em nuvem compartilhado da Apple. Por uma taxa mensal ou anual, os usuários podem armazenar documentos e fotos. O iCloud não se limita a usuários de Mac; ele também está disponível para usuários de Windows e Linux.
- **Gestos:** esse recurso permite uma experiência aprimorada de mouse tátil ou baseado em toque, com diferentes respostas configuráveis para deslizar com um, dois ou três dedos; usando movimentos de beliscar; e assim por diante. Os gestos são configurados nas configurações do Track Pad nas Preferências do Sistema.
- **Finder:** o Finder é a principal ferramenta de gerenciamento de arquivos no macOS. Ele fornece uma visão das pastas e subpastas (consulte a [Figura 6-57](#)). Na figura, o ícone do Finder é destacado no Dock e, em seguida, aberto em Aplicativos. As subpastas do aplicativo exibem informações e um arquivo .dmg de instalação para o aplicativo.



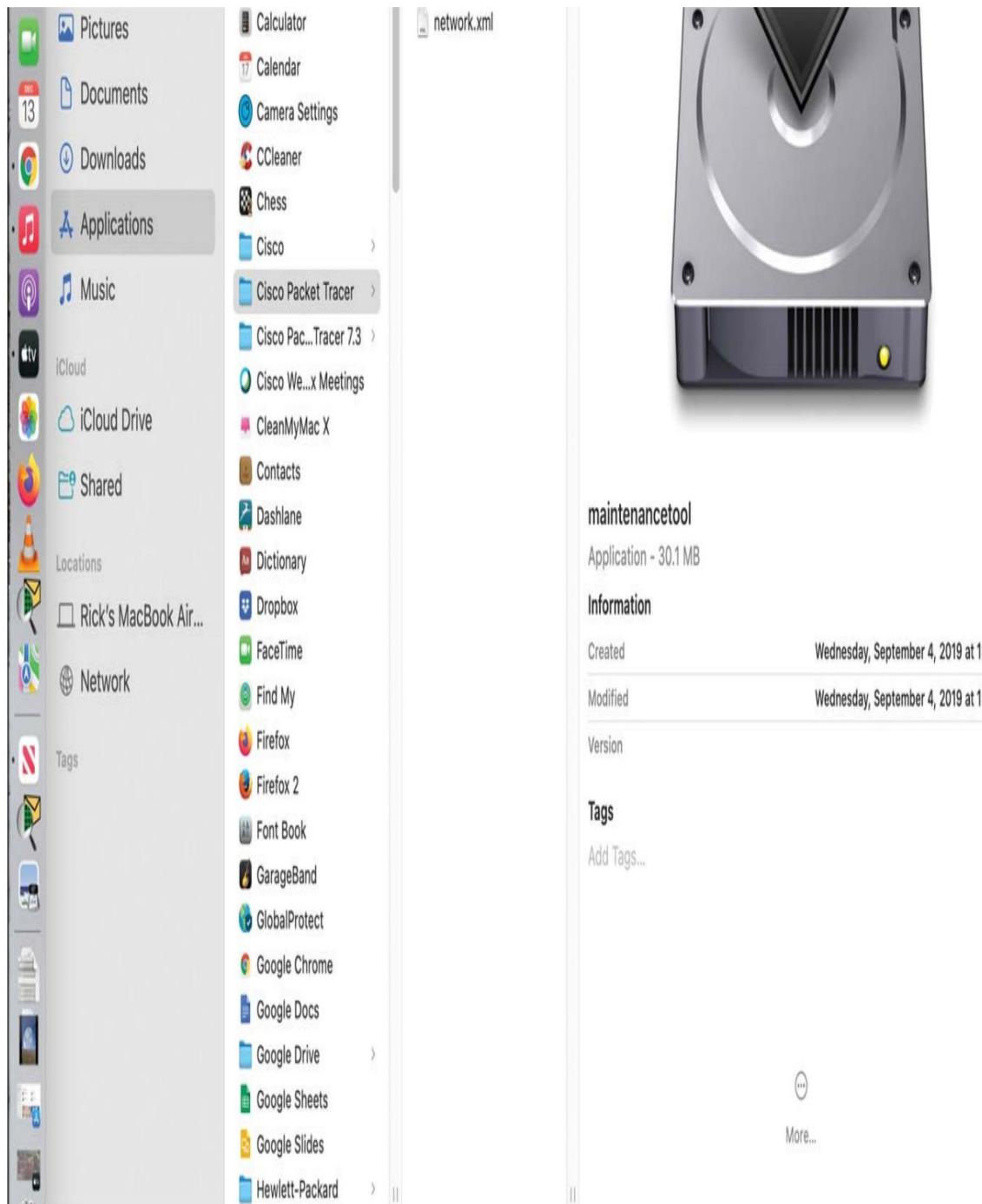


Figura 6-57 O Localizador

- **Disco remoto:** em Macs anteriores, esse recurso permitia que um dispositivo sem uma unidade óptica acessasse uma unidade óptica em outro computador. Ele foi removido em 2019 com a atualização do macOS Catalina 10.15. Em Macs mais antigos com o recurso Remote Disc, use o Finder para abrir o Remote Disc

Disco e selecione o computador Mac ou Windows que está compartilhando a unidade óptica. Ele toca como se estivesse conectado localmente.

- **Dock:** O Dock é a barra de inicialização rápida em um Mac, semelhante à barra de tarefas do Windows. Ele pode ser configurado para iniciar aplicativos ou abrir pastas ou documentos. Ele pode ser posicionado em qualquer lado ou na parte inferior da área de trabalho. A [Figura 6-57](#) tem o Dock à esquerda, acessando subpastas na pasta Aplicativos. Quando o cursor estiver sobre os ícones do Dock, as informações do ícone serão exibidas.

Utilitário *de*

Disco O Utilitário de Disco, mostrado na [Figura 6-58](#), permite o gerenciamento de disco e arquivo no macOS. Ele cria imagens de disco em branco que podem ser usadas como contêineres para outros arquivos, incluindo backups de imagem. Ele também apaga as unidades que não são do macOS e as prepara para uso com o macOS. Também é possível reparar, restaurar e montar discos. O particionamento pode acontecer aqui, mas desde o iOS 10.13, os volumes formatados do Apple File System (APFS) se ajustam automaticamente conforme necessário.



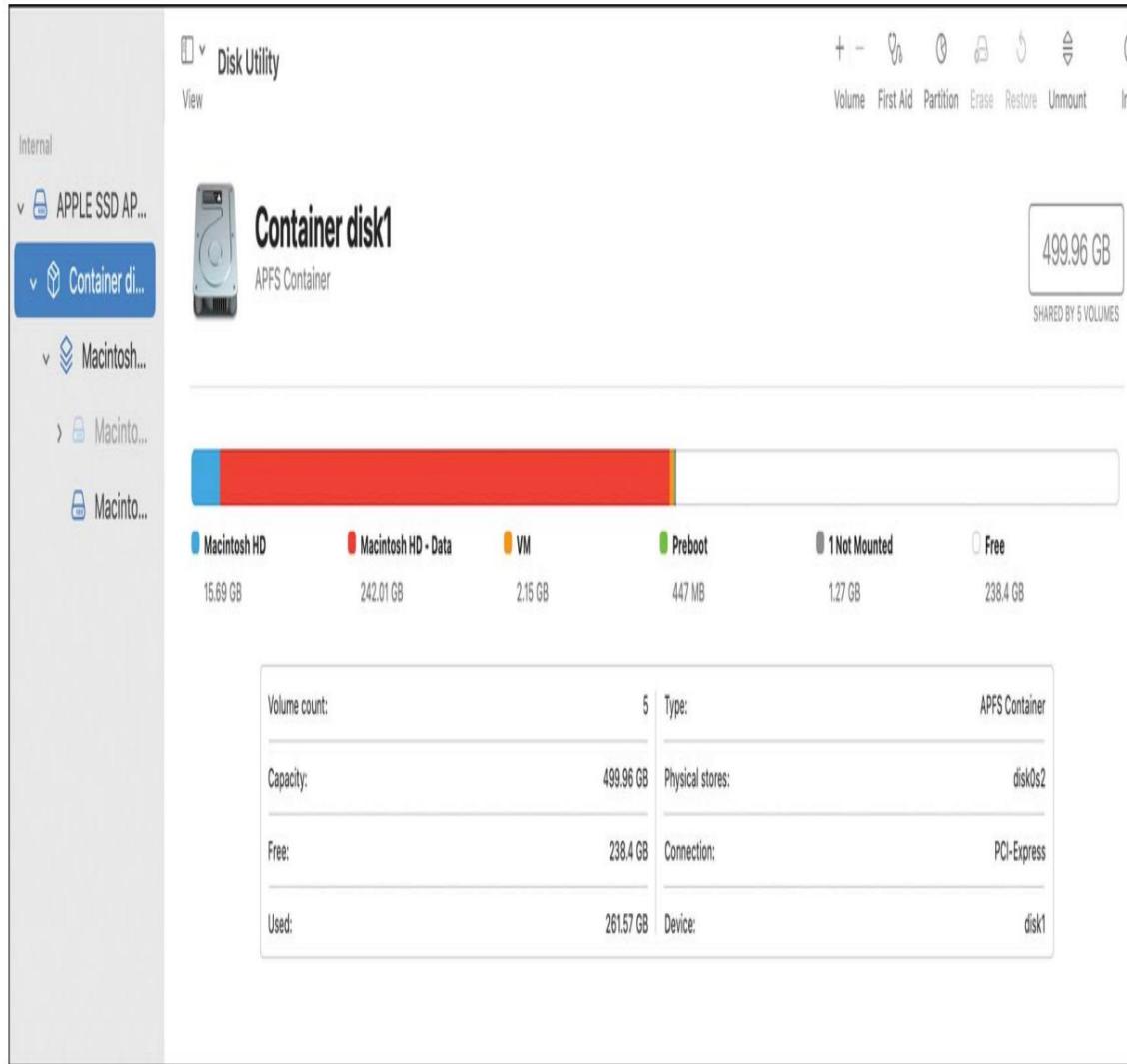


Figura 6-58 Utilitário de Disco APFS

O Utilitário de Disco é acessado com mais facilidade usando o Spotlight, o Launchpad ou o Finder e pesquisando o Utilitário de Disco. Para iniciar o Utilitário de Disco na inicialização, pressione e segure Cmd+R até iniciar.

FileVault

A guia **FileVault** ativa e desativa (com uma senha ou autenticação biométrica) a criptografia automática de dados no computador (consulte a [Figura 6-55](#)).

Durante a configuração, uma chave de recuperação é criada caso a senha seja perdida. Se a senha e a chave forem perdidas, os dados também serão perdidos permanentemente.

terminal

O macOS inclui um poderoso aplicativo **Terminal** que abre um ambiente de linha de comando. O utilitário macOS Terminal é usado para executar comandos, scripts e programas sem uma GUI. Terminal tem suas raízes em um shell UNIX e pode ser usado para gerenciar outros computadores em uma rede. A Figura 6-59 mostra o Terminal monitorando os principais processos em um Mac em execução.

The screenshot shows a terminal window titled "ramcdonald - top - 97x34". The window displays system statistics and a detailed list of processes. The statistics include:

- Processes: 631 total, 4 running, 627 sleeping, 2729 threads
- Load Avg: 2.67, 2.80, 2.65 CPU usage: 20.63% user, 12.47% sys, 66.89% idle
- SharedLibs: 676M resident, 113M data, 46M linkedit.
- MemRegions: 164592 total, 3841M resident, 238M private, 1920M shared.
- PhysMem: 16G used (2771M wired), 117M unused.
- VM: 22T vsize, 3083M framework vsize, 7689523(0) swapins, 7971241(0) swapouts.
- Networks: packets: 4108870/3450M in, 1750928/501M out.
- Disks: 4026044/75G read, 2404564/56G written.

The process list is as follows:

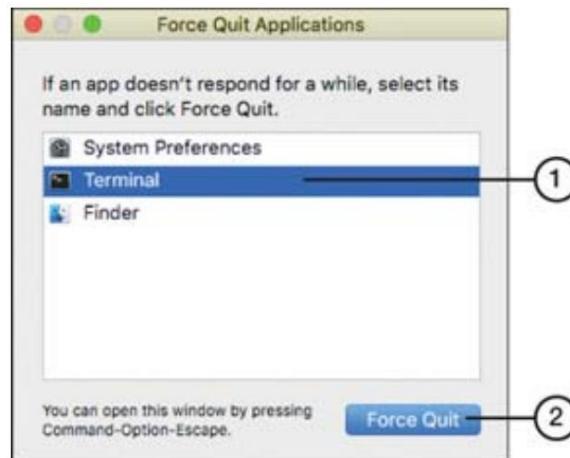
PID	COMMAND	%CPU	TIME	#TH	#WQ	#PORT	MEM	PURG	CMPRS	PGRP	PPID	STATE
52010	SymDaemon	47.6	02:32:15	21/1	4	172	12M	0B	0B	52010	1	running
165	WindowServer	29.2	69:12.45	13/1	5	3385-	1096M-	19M+	52M-	165	1	running
86408	top	13.5	00:13.82	1	0	23	6936K	0B	0B	86408	86395	sleeping
86545	top	8.6	00:03.57	1/1	0	28	7420K	0B	0B	86545	86536	running
85881	top	8.1	00:29.29	1	0	23	6640K	0B	0B	85881	85873	sleeping
0	kernel_task	6.2	47:42.49	201/4	0	0	348M-	0B	0B	0	0	running
86557	screencaptur	3.8	00:00.56	2	1	62	3816K+	620K	0B	2304	2304	sleeping
33167	com.apple.Ap	2.5	03:43.10	4	3	168	608K	0B	80K	33167	1	sleeping
84303	Terminal	2.1	00:34.37	7	2	495	110M-	22M-	0B	84303	1	sleeping
2272	Google Chrom	1.1	52:13.08	37	1	1387-	338M-	0B	67M	2272	1	sleeping
2456	Google Chrom	1.0	21:25.74	10	1	236	66M	0B	15M	2272	2272	sleeping
44543	Google Chrom	0.6	02:33.94	17	1	709	159M	0B	30M	2272	2272	sleeping
86558	screencaptur	0.4	00:00.11	4	2	155	3516K	0B	0B	86558	1	sleeping
120	launchservic	0.4	00:49.73	4	3	715	3900K	0B	580K	120	1	sleeping
85877	Google Chrom	0.2	00:01.89	13	1	266	46M	4096B	0B	2272	2272	sleeping
2540	Google Chrom	0.2	02:32.32	13	1	122	20M	0B	16M	2272	2272	sleeping
85098	Activity Mon	0.2	00:20.54	5	3	524	42M-	3320K+	0B	85098	1	sleeping
80	karl	0.1	00:09.35	8	1	57	4960K	0B	2640K	80	1	sleeping
84	configd	0.1	03:12.03	7	1	534	3764K	0B	660K	84	1	sleeping
2268	AXVisualSupp	0.1	01:08.70	3	1	179	7180K	0B	3584K	2268	1	sleeping
2305	Finder	0.1	07:06.38	8	5	1335	341M	2712K	12M	2305	1	sleeping
86	powerd	0.1	01:20.08	3	2	132	2152K	0B	268K	86	1	sleeping
2454	Google Chrom	0.1	35:32.23	12	1	650-	807M-	1244K	200M	2272	2272	sleeping
231	airportd	0.1	10:13.25	11	9	445	13M-	0B	660K	231	1	sleeping

Figura 6-59 Terminal no Mac

O recurso **Force Quit** no macOS permite que o usuário desligue um aplicativo com defeito.

Para abrir o aplicativo Forçar encerramento no teclado, pressione Cmd+Option+Esc.

Forçar encerramento também pode ser iniciado a partir da barra de menus: Abra o menu Apple e selecione Forçar encerramento. Você também pode apontar para o ícone do aplicativo no Dock (na parte inferior da tela) e clicar com o botão direito do mouse ou clicar e segurar para abrir um menu com a opção Sair. No menu Forçar encerramento, selecione o aplicativo a ser interrompido (consulte a Figura 6-60).



1. Select an app to force quit
2. Click Force Quit to close it

Figura 6-60 Usando Forçar Encerramento no macOS

Recursos e ferramentas comuns do Linux SO do cliente/desktop



220-1102: Objetivo 1.11: Identificar recursos e ferramentas comuns do SO cliente/desktop Linux.

Os sistemas operacionais Linux são muito menos comuns que o Windows em desktops organizacionais; no entanto, eles têm uma presença cada vez maior como sistema operacional em servidores e outros computadores de nível empresarial.



Comandos comuns do Linux

Com mais sistemas Linux aparecendo em redes corporativas, os técnicos de informática precisam entender os comandos básicos do Linux. As seções a seguir revisam os comandos que podem aparecer no exame A+.

Para usar esses comandos, abra uma sessão do Terminal. Alguns comandos devem ser executados como usuário root. (Para executar comandos como root, faça login como root ou use **sudo**.)

ls

ls é o macOS e Linux equivalente ao **diretório** de comando do Windows . Use **ls -l** para listar o conteúdo de um diretório (pasta), incluindo permissões e outras informações (consulte a [Figura 6-61](#)).

```

msoper@localhost:/etc
File Edit View Search Terminal Help
-rw-r--r--. 1 root root 375 Sep 17 2015 trusted-key.key
drwxr-xr-x. 4 root root 4096 Oct 29 16:24 udev
drwxr-xr-x. 2 root root 4096 Jun 30 2015 udisks2
drwxr-xr-x. 2 root root 4096 Oct 29 16:23 unbound
-rw-r--r--. 1 root root 587 Jun 17 2015 updatedb.conf
drwxr-xr-x. 2 root root 4096 Oct 29 16:23 UPower
-rw-r--r--. 1 root root 1018 Jul 16 2015 usb_modeswitch.conf
drwxr-xr-x. 2 root root 20480 Oct 29 16:23 usb_modeswitch.d
-rw-rw-r--. 1 root root 28 Mar 2 19:19 vconsole.conf
-rw-r--r--. 1 root root 51 Aug 31 2015 vdpa_wrapper.cfg
-rw-r--r--. 1 root root 1982 Aug 20 2015 virrc
drwxr-xr-x. 5 root root 4096 Oct 29 16:23 vmware-tools
drwxr-xr-x. 2 root root 4096 Oct 29 16:23 vpnc
-rw-r--r--. 1 root root 4925 Jun 18 2015 wgetrc
drwxr-xr-x. 2 root root 4096 Oct 29 16:23 wpa_supplicant
-rw-r--r--. 1 root root 0 Jun 18 2015 wvdial.conf
drwxr-xr-x. 6 root root 4096 Oct 29 16:24 X11
-rw-r--r--. 1 root root 589 Sep 14 2015 xattr.conf
drwxr-xr-x. 7 root root 4096 Oct 29 16:23 xdg
drwxr-xr-x. 2 root root 4096 Sep 10 2015 xinetd.d
drwxr-xr-x. 2 root root 4096 Oct 29 16:22 xml
drwxr-xr-x. 3 root root 4096 Oct 29 16:23 yum
drwxr-xr-x. 2 root root 4096 Oct 29 16:21 yum.repos.d
[msoper@localhost etc]$ ls -l

```

1. Directories are listed in blue
2. Press the up-arrow key to repeat the last command; press it again to repeat the previous one, and so on

Figura 6-61 Usando **ls -l** no Fedora 23 Workstation

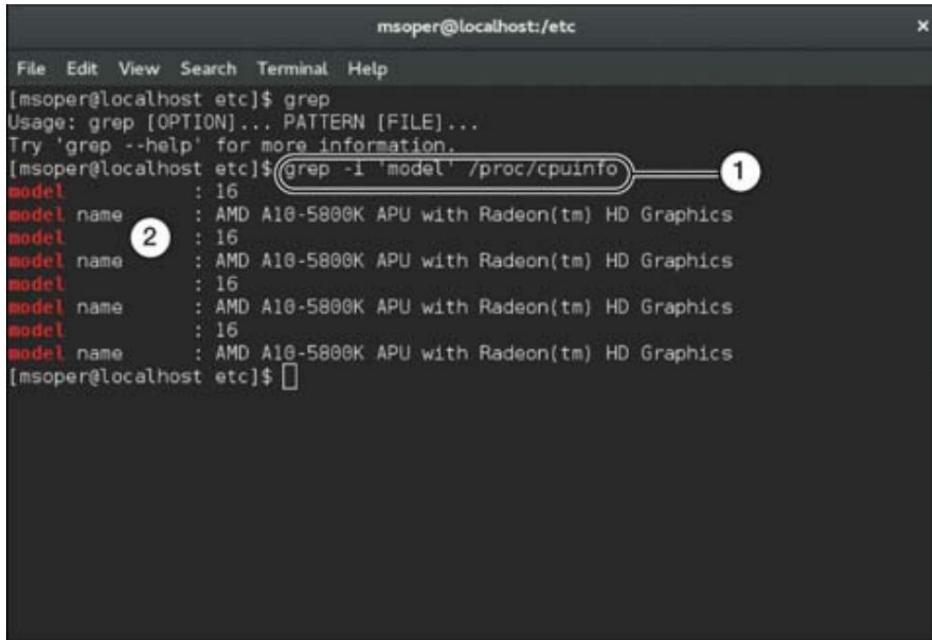
grep

Use o **grep** para realizar pesquisas de texto. A linha de comando **grep** especifica o que pesquisar e onde pesquisar.

grep pode ser usado para localizar uma palavra especificada em um ou mais arquivos especificados. **grep** normalmente procura correspondências exatas (Linux e macOS diferenciam maiúsculas de minúsculas), mas pode ser configurado para ignorar maiúsculas e minúsculas com **-i**.

O **grep** oferece suporte à pesquisa recursiva - ou seja, pesquisa em todos os arquivos em diretórios (pastas) abaixo do diretório atual.

A Figura 6-62 mostra **grep** sendo usado para procurar a palavra *model* no diretório */proc/cpuinfo* (pasta).



```
msoper@localhost:~$ grep -i 'model' /proc/cpuinfo
Usage: grep [OPTION]... PATTERN [FILE]...
Try 'grep --help' for more information.
[msoper@localhost ~]$ grep -i 'model' /proc/cpuinfo
model : 16
model name : AMD A10-5800K APU with Radeon(tm) HD Graphics
model : 16
model name : AMD A10-5800K APU with Radeon(tm) HD Graphics
model : 16
model name : AMD A10-5800K APU with Radeon(tm) HD Graphics
model : 16
model name : AMD A10-5800K APU with Radeon(tm) HD Graphics
[msoper@localhost ~]$
```

1. Searching for the word *model*
2. Matches

Figura 6-62 Procurando um texto específico em uma pasta usando **grep**

cd

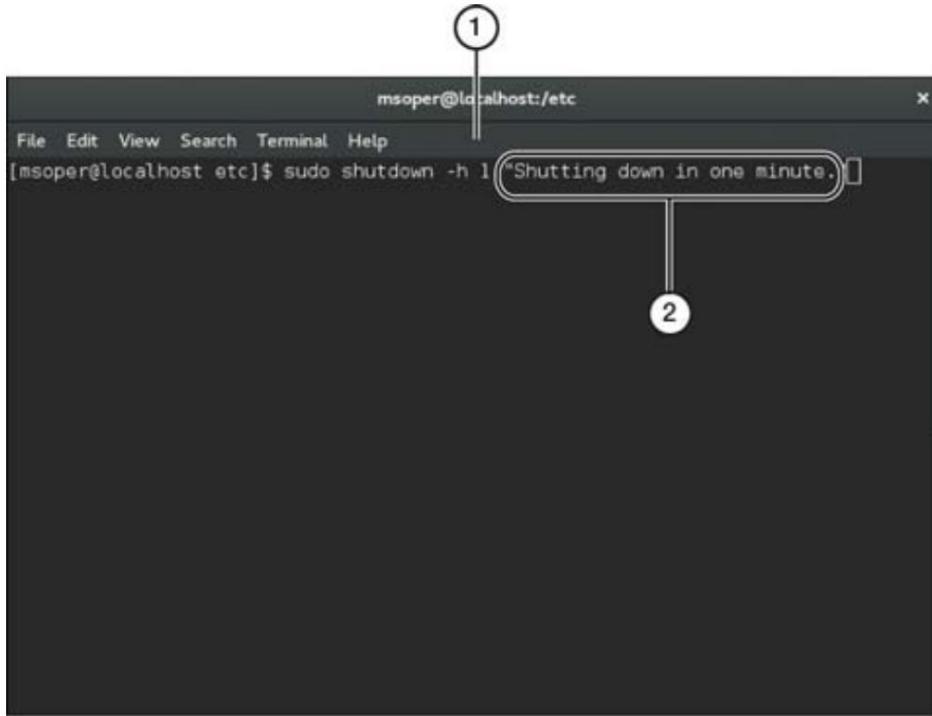
Use **cd** para alterar diretórios (pastas). A sintaxe é diferente da linha de comando do Windows: o Linux usa a barra /, enquanto o Windows usa a barra \.

Use **cd /etc** para mudar para a pasta /etc.

Use **cd..** para subir um nível.

desligar

Use **desligamento** para desligar o sistema. A Figura 6-63 mostra o **desligamento** usado junto com as opções para especificar quando desligar e quando transmitir uma mensagem de aviso. Observe que o comando **sudo** é usado com este comando porque o **desligamento** requer acesso root.



1. One minute (1) to shutdown
2. Message broadcast to all systems logged in to this computer

Figura 6-63 Preparando para desligar um sistema

pwd

pwd exibe o nome do diretório atual/de trabalho.

mv

Use **mv** para mover arquivos para um local especificado, como neste exemplo:

mv thisfile.ext pasta de destino

cp

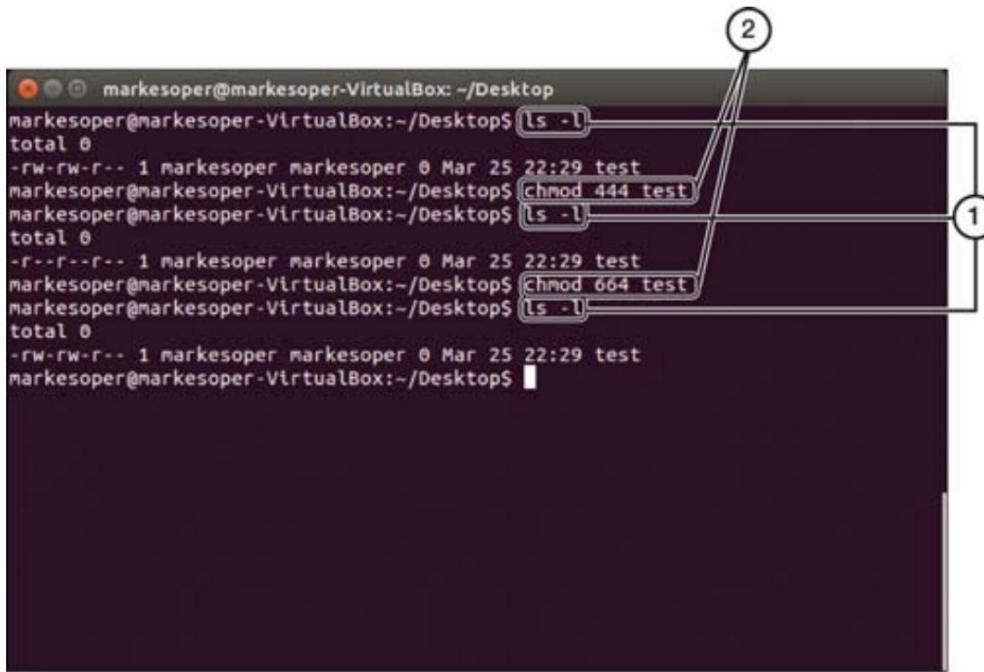
Use **cp** para copiar arquivos para um local especificado (usando a sintaxe **cp filename / folder/subfolder**) ou para um nome diferente na mesma pasta (por exemplo, **cp -i origfile copyfile**). Use a opção **-i** para ser avisado caso o comando substitua um arquivo.

rm

Use ***rm*** para remover (excluir) arquivos do sistema (***rm filename***).

chmod

Use ***chmod*** para alterar as permissões de arquivos e diretórios usando a sintaxe ***chmod permissions filename***. Na [Figura 6-64](#), ***chmod*** é usado para alterar as permissões no arquivo test. Os números usados representam diferentes permissões. Para saber mais sobre esses valores, consulte a Calculadora Chmod em <https://chmod-calculator.com>. Observe também que, na [Figura 6-64](#), o comando ***ls -l*** é usado para exibir as permissões de arquivo e o nome do arquivo.



The screenshot shows a terminal session on an Ubuntu system. The user, markesoper, is in their home directory (~). They first run `ls -l` (1), which shows a file named "test" with permissions `-rw-rw-r--`. Then, they run `chmod 444 test` (2), changing the permissions to `-r--r--r--`. Finally, they run `ls -l` again, which shows the updated permissions for the "test" file.

```

markesoper@markesoper-VirtualBox: ~/Desktop
markesoper@markesoper-VirtualBox:~/Desktop$ ls -l
total 0
-rw-rw-r-- 1 markesoper markesoper 0 Mar 25 22:29 test
markesoper@markesoper-VirtualBox:~/Desktop$ chmod 444 test
markesoper@markesoper-VirtualBox:~/Desktop$ ls -l
total 0
-r--r--r-- 1 markesoper markesoper 0 Mar 25 22:29 test
markesoper@markesoper-VirtualBox:~/Desktop$ chmod 664 test
markesoper@markesoper-VirtualBox:~/Desktop$ ls -l
total 0
-rw-rw-r-- 1 markesoper markesoper 0 Mar 25 22:29 test
markesoper@markesoper-VirtualBox:~/Desktop$ 
```

1. Using the `ls -l` command to see the file permissions changes made with `chmod`
2. Changing file permissions with `chmod`

Figura 6-64 Alterando permissões para o teste de arquivo usando o Ubuntu

chown

Use ***chown*** para alterar a propriedade do arquivo usando a sintaxe ***sudo chown newowner filename***.

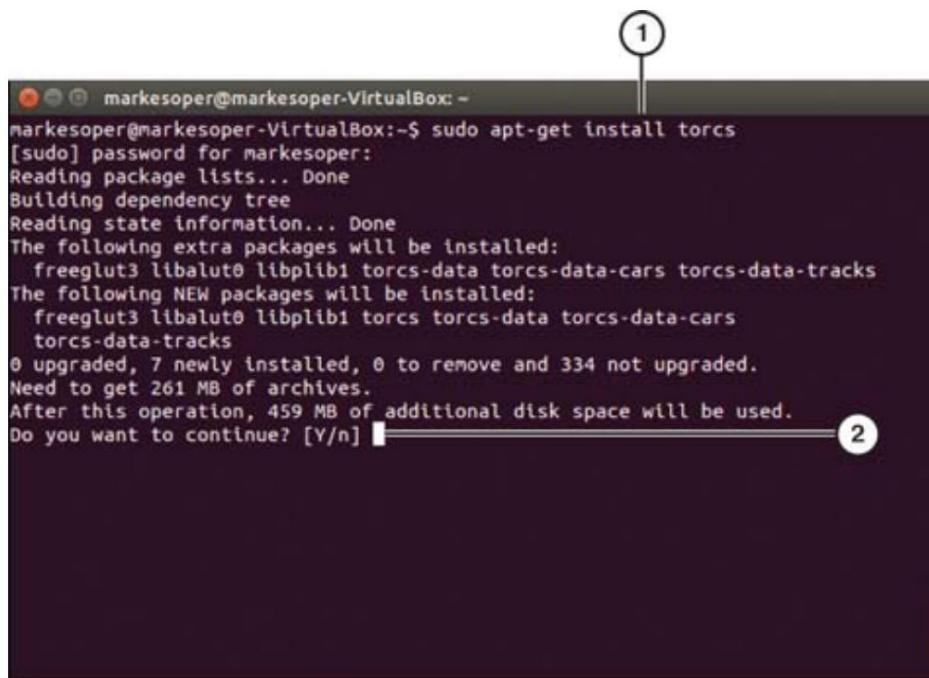
su/sudo

Use ***sudo*** para executar um comando como outro usuário. É mais comumente usado por um usuário para executar um comando como root.

Use **su** para alternar entre contas. Inserir **su** sem especificar opções muda para root e solicita a senha root.

apt-get

Use **apt-get** para instalar ou gerenciar pacotes de software Advanced Packaging Tool (APT), que são comuns em distribuições baseadas em Debian, como o Ubuntu (consulte a Figura 6-65). O comando **apt-get** deve ser usado com **sudo**. Use esta sintaxe: **sudo apt-get function appname**.



```
markesoper@markesoper-VirtualBox:~$ sudo apt-get install torcs
[sudo] password for markesoper:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  freeglut3 libalut0 libplib1 torcs-data torcs-data-cars torcs-data-tracks
The following NEW packages will be installed:
  freeglut3 libalut0 libplib1 torcs torcs-data torcs-data-cars
  torcs-data-tracks
0 upgraded, 7 newly installed, 0 to remove and 334 not upgraded.
Need to get 261 MB of archives.
After this operation, 459 MB of additional disk space will be used.
Do you want to continue? [Y/n] 1
```

1. The function to perform is install
2. Answer Y to continue

Figura 6-65 Instalando torques (The Open Racing Car Simulator) com **apt get** no Ubuntu

YUM (Yellowdog Updater, Modificado)

YUM é um utilitário de código aberto que fornece atualizações automáticas e gerenciamento de pacotes no Linux.

ip

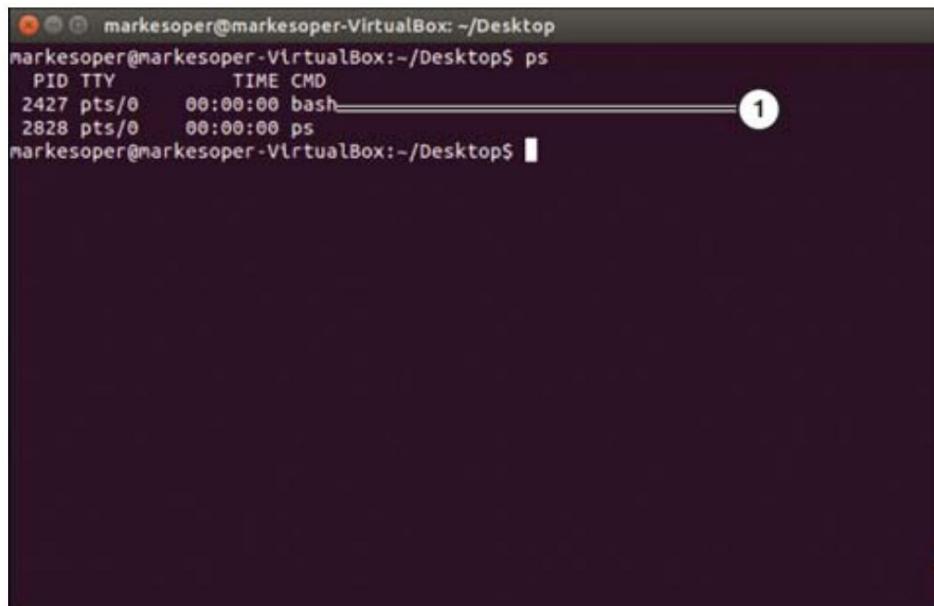
O comando **ip** é usado para gerenciar interfaces de rede. Ele pode ativar as interfaces de rede ou desligá-las, gerenciar endereços IP e examinar as tabelas de roteamento e ARP.

df (disco livre)

O comando **df** é usado para exibir o espaço usado e livre em discos. O comando também possui opções para visualizar o tamanho do sistema de arquivos.

PS

Use o comando **ps** para listar os processos e tarefas em execução no sistema operacional (consulte a Figura 6-66).



A screenshot of a terminal window titled "markesoper@markesoper-VirtualBox: ~/Desktop". The window displays the output of the "ps" command. The output shows two processes: process ID 2427, which is a bash shell running on TTY pts/0 for 00:00:00, and process ID 2828, which is a ps command also running on TTY pts/0 for 00:00:00. A callout bubble with the number "1" points to the first line of the output, which lists the current processes by name and PID.

```
markesoper@markesoper-VirtualBox: ~/Desktop
markesoper@markesoper-VirtualBox:~/Desktop$ ps
  PID TTY      TIME CMD
 2427 pts/0    00:00:00 bash
 2828 pts/0    00:00:00 ps
markesoper@markesoper-VirtualBox:~/Desktop$
```

1. Current processes listed by name and PID.

Figura 6-66 Listando processos para o usuário atual com **ps**

cara

As distribuições Linux (distros) contêm um manual (manpages) com opções para cada comando. Para visualizar ou imprimir a página de manual de um comando, use o comando **man**. Para saber mais, consulte www.linfo.org/man.xhtml. Para visualizar páginas de manual do Ubuntu (uma das distros mais populares) online, consulte <https://manpages.ubuntu.com>.

principal

O comando **top** fornece informações resumidas sobre o uso de recursos para tarefas e processos na forma de um painel. Também pode ser usado para monitorar o uso da CPU e da memória.

achar

O comando **find** é usado para localizar arquivos e diretórios e informações sobre eles. Você pode pesquisar por nome, data, proprietários e assim por diante.

DIG (Rastreador de Informações de Domínio)

O comando **dig** fornece informações úteis sobre servidores DNS para solucionar problemas de DNS.

gato

cat é um comando utilitário para escrever texto em arquivos e imprimir o conteúdo do arquivo.

nano

nano é um editor de texto de linha de comando com atalhos de teclado e funções para editar arquivos.

Melhores Práticas

Para manter qualquer sistema de computador, você deve seguir as práticas recomendadas relacionadas ao seguinte:

- backups agendados
- Manutenção de disco programada
- Atualizações do sistema e App Store
- Gerenciamento de patches
- Atualizações de driver e firmware
- Atualizações de antivírus e antimalware

As seções a seguir discutem as práticas recomendadas nessas áreas para macOS e Linux.

Backups agendados

Os backups programados ajudam a evitar grandes perdas de dados em caso de falha do sistema, acidente ou perda. Os backups podem ser usados para proteger o seguinte:

- Contatos
- O email
- Arquivos de mídia (fotos, vídeos e músicas)
- Documentos

O aplicativo de backup padrão no macOS é o Time Machine. O Linux inclui vários utilitários que podem ser usados para backups. Isso inclui os utilitários tar e rsync de linha de comando. Outros, incluindo grsync (GUI para rsync) e duplicidade (linha de comando e GUI disponíveis como Déjà Dup), estão disponíveis no repositório para uma distribuição Linux ou nos fornecedores.

Observação

A página BackupYourSystem na Ajuda do Ubuntu Linux (<https://help.ubuntu.com/community/BackupYourSystem>) fornece uma longa lista de ferramentas de backup baseadas em linha de comando e GUI que também funcionam com outras distribuições do Linux.

Os backups agendados devem ser executados nos horários em que o sistema estiver ocioso, como durante a noite e nos finais de semana.

Tipos de backup

Um backup completo faz backup de todo o conteúdo do computador ou da unidade selecionada em outro local ou local de rede. Um programa de backup pode criar um arquivo compactado para armazenar informações de backup. Com esse tipo de backup, o programa de backup deve executar um utilitário de restauração para tornar os arquivos utilizáveis novamente.

Outro tipo de programa de backup simplesmente copia os arquivos de backup para um local diferente, onde podem ser abertos pelo sistema operacional.

A maioria dos programas de backup também pode executar um backup incremental, que faz backup apenas dos arquivos que foram criados ou alterados após o último backup completo.

Os recursos de backup a serem procurados incluem o seguinte:



- **Compactação:** Isso reduz a quantidade de espaço de arquivo e, muitas vezes, também diminui a quantidade de tempo necessária para fazer um backup.
- **Supporte para backups incrementais e completos:** Boas práticas de backup exigem backups completos periódicos, seguidos de backups de arquivos que foram alterados desde o último backup completo (backups incrementais).
- **Destinos de backup local e de rede:** alguns utilitários de backup podem exigir configuração adicional antes que um backup de rede possa ser executado.

Configurando um aplicativo de backup no Linux

As distribuições do Ubuntu têm um aplicativo de backup pré-instalado que é executado semanalmente e também pode ser configurado para ser executado diariamente. Os backups podem ser mantidos enquanto o espaço permitir ou por pelo menos 6 meses ou um ano. Este utilitário de backup foi projetado para novos usuários.

Os utilitários de backup baseados em tar, rdiff e outros aplicativos do Linux podem exigir muitos scripts. Um utilitário de backup que ajuda a criar scripts de backup preenchendo os espaços em branco é o Backupninja. Mais informações sobre o Backupninja podem ser encontradas em <https://linux.die.net/man/1/backupninja>.



antivírus

Acredita-se amplamente que o Linux é imune a vírus e malware. Embora o Linux não seja tão visado quanto o Windows, um Linux desprotegido

computer pode ser usado como um vetor de infecção para máquinas Windows que se conectam a ele.

ClamAV (www.clamav.net) é um aplicativo antivírus de código aberto disponível para macOS e Linux. Varreduras e atualizações podem ser automatizadas com o cron, e um front-end GUI conhecido como ClamTK também está disponível. O software antivírus conhecido geralmente possui versões para Linux e macOS, bem como versões para Windows.

Aplicativos antivírus e antimalware para Linux devem ser atualizados pelo menos diariamente.

Atualizações e Patches

Se uma organização tiver apenas alguns sistemas Linux, executar atualizações manuais do sistema com yum ou apt-get pode ser suficiente para o gerenciamento de patches. No entanto, à medida que o número de sistemas Linux aumenta e quando os sistemas Linux são usados para funções de missão crítica, como servidores da Web, métodos melhores de gerenciamento de patches são desejáveis.

Se você usar um script para verificar e instalar atualizações para Linux ou aplicativos instalados, o utilitário crontab pode ser usado para definir a tarefa em um agendamento executado pelo utilitário cron.

Ferramentas

Assim como no Windows e no macOS, as principais ferramentas adicionam facilidade e funcionalidade ao sistema operacional. Duas ferramentas importantes no Linux são discutidas aqui.

shell/terminal

As ferramentas de **terminal** e **shell** no Linux são semelhantes ao shell de comando (prompt) e às ferramentas do PowerShell no Windows. A linha de comando é o acesso mais direto e eficiente ao centro do sistema operacional, e o PowerShell foi projetado para estender o poder do shell de comando, adicionando funções de script e interoperabilidade. O mesmo se aplica ao Linux. O comando do terminal abre um shell para digitar comandos. Os shells Linux, dos quais existem vários, adicionam funcionalidade semelhante ao terminal Linux. O shell Linux mais popular é o Bash (Bourne Again Shell), mas outros estão em uso; isso inclui o PowerShell, que agora é uma linguagem de script multiplataforma totalmente funcional que funciona no Linux, macOS e Windows 10 e 11.

Para abrir o Terminal no Linux, basta pressionar Ctrl+Alt+T ou digitar **terminal** na caixa de pesquisa.

Samba

As máquinas Linux e Windows podem trabalhar juntas em uma rede, graças ao **Samba**. Samba é um software de código aberto que permite que máquinas Linux funcionem em um ambiente Windows para compartilhamento de arquivos e impressão. O Samba também permite que máquinas Linux participem do Windows Active Directory como controlador ou membro. Mais informações sobre o Samba estão disponíveis em www.samba.org/.

Tarefas de preparação para exames

Conforme mencionado na Introdução, você tem várias opções para se preparar para o exame: os exercícios aqui; [Capítulo 10, “Preparação Final”](#); e as questões de simulação de exame no software de teste prático Pearson Test Prep.

Revise todos os tópicos principais

Revise os tópicos mais importantes do capítulo, indicados pelo ícone Tópico principal na margem externa da página. A [Tabela 6-9](#) lista esses tópicos principais e o número da página em que cada um é encontrado.



Tabela 6-9 Tópicos-chave para o [Capítulo 6](#)

Tópico principal Elemento	Descrição	Página Número
Tabela 6-2	Edições e recursos do Windows 10	436
Seção	Ferramentas de linha de comando da Microsoft	438
Tabela 6-4	Comandos do prompt de comando do Windows	440
Seção	formato	443

Tópico principal Elemento	Descrição	Página Número
Seção	cópia de	445
Seção	xcopy	446
Seção	robocopy	446
Seção	diskpart	447
Seção	sfc	448
Seção	chkdsk	449
Seção	gpupdate	450
Seção	Gerenciador de Dispositivos	456
Figura 6-14 Resumo do sistema msinfo32		464
Seção	Utilitário de configuração do sistema	467
Seção	Editor do Registro	469
Tabela 6-6	Guias de Diálogo de Propriedades da Internet	472
Seção	Grupo de trabalho vs. configuração de domínio	484
Lista	Criando um grupo de trabalho no Windows	485
Seção	Compartilhamentos de rede	486
Lista	Mapeamento de unidades e pastas	488
Degraus	conexões VPN	495
Degraus	Configurando uma conexão sem fio	496
Degraus	Configurando uma conexão com fio	497
Degraus	Configurações de proxy	497
Seção	Requisitos do sistema para aplicativos Sistemas	501
Seção	de arquivos de 32 bits x 64 bits	501
Seção	SOs de estação de trabalho	509
Seção	Sistemas operacionais para celulares/tablets	511

Tópico principal Elemento	Descrição	Página Número
Lista	NTFS x FAT32	515
Lista	Métodos para inicializar um sistema durante o processo de instalação	519
Lista	Tipos de instalações do Windows	520
Seção	Atualizações	521
Seção	Instalação Limpa	521
Degraus	Reparar a instalação	523
Lista	Métodos de particionamento	527
Seção	Criando partições durante o Windows Instalação	529
Lista	Recursos de backup	536
Degraus	macOS: configurando o Time Machine	537
Figura 6-58 Utilitário de Disco APFS		544
Figura 6-60 Usando Forçar Encerramento no macOS		546
Seção	Comandos comuns do Linux	546
Lista	Sistema operacional Linux: recursos de backup	554
Seção	antivírus	555

Complete as tabelas e listas da memória

Imprima uma cópia do [Apêndice C, “Tabelas de Memória”](#) (encontrado online), ou pelo menos a seção deste capítulo, e complete as tabelas e listas de memória.

O [Apêndice D, “Respostas das tabelas de memória”](#), também on-line, inclui tabelas e listas preenchidas para verificar seu trabalho.

Definir termos-chave

Defina os seguintes termos-chave deste capítulo e verifique suas respostas no glossário:

acesso ao domínio

grupo de trabalho

Protocolo de Área de Trabalho Remota (RDP)

BitLocker

cd de

atualização no local

gpedit.msc

dir

md

rmdir

ipconfig

ping

hostname

netstat

nslookup

chkdsk

usuário da rede

uso da net

tracert

formato

xcopy

copiar

robocopy

gpupdate

gpresult

shutdown

sfc

[nome do comando] /?

pathping diskpart

vencedor

Gerenciador de

Tarefas Microsoft Management Console (MMC)

Visualizador de eventos (eventvwr.msc)

Gerenciamento de disco (diskmgmt.msc)

Agendador de Tarefas (taskschd.msc)

Gerenciador de dispositivos (devmgmt.msc)

Gerenciador de certificados (certmgr.msc)

Usuários e grupos locais (lusrmgr.msc)

Monitor de desempenho (perfmon.msc)

Editor de Diretiva de Grupo (gpedit.msc)

Informações do sistema (msinfo32.exe)

Monitor de recursos (resmon.exe)

Configuração do sistema (msconfig.exe)

Limpeza de Disco (cleanmgr.exe)

Editor do Registro (regedit.exe)

facilidade de acesso

domínio do grupo

de trabalho

recursos compartilhados

Firewall do Windows Defender

Máscara de sub-rede do esquema de endereçamento de
protocolo de Internet (IP)

Sistema de nomes de domínio (DNS)

gateway

rede privada virtual (VPN) rede de longa

distância sem fio (WWAN) configurações de proxy

conexões limitadas

memória de acesso aleatório de vídeo (VRAM)

janelas

Mac OS

Linux

Chrome OS

Android

iOS

iPadOS

Sistema de arquivos de nova tecnologia (NTFS)

Tabela de alocação de arquivos extensível (exFAT)

Tabela de Alocação de Arquivos 32 (FAT32)

Sistema de arquivos da Apple (APFS)

Terceiro Sistema de Arquivo Estendido (ext3)

Métodos de inicialização do quarto sistema de

arquivos estendidos (ext4) do ciclo de vida do produto

instalação limpa

reparar instalação

instalação de rede remota

imagem implantação

recuperação partição

particionamento registro

mestre de inicialização

GUID Partition Table (GPT)

Arquivos .dmg Arquivos .pkg

Arquivos .app Time Machine

Controle da missão

Chaveiro

Destaque

iCloud

gestos

localizador

Disco Remoto

Doca

Utilitário de Disco

FileVault

terminal

Forçar Encerramento

grep

pwd

mv

cp

rm

chmod

chown

su/sudo

apt-get

yum

ip df

grep

PS

cara

melhor

achado

escavação

gato

nano

terminal

Concha

Samba

Responder a perguntas de revisão

1. Qual das seguintes afirmações melhor descreve um grupo de trabalho? (Escolher tudo o que se aplica.)

a. Todos os computadores em um grupo de trabalho devem estar na mesma sub-rede. **b.**

O compartilhamento de arquivos e impressoras deve ser ativado em cada computador em um grupo de

trabalho. **c.** O grupo de trabalho deve ter uma senha. **d.** Cada

computador em um grupo de trabalho deve ter uma conta de usuário para cada do utilizador.

- 2.** Mark está reimplantando uma estação de trabalho para um novo usuário em outro prédio. Foi determinado que o computador precisa ser renomeado para fins de gerenciamento. Qual das opções a seguir permitirá que ele faça a alteração? **a.** Abrindo as Propriedades do Sistema **b.** Digitando Msinfo32 na linha de comando **c.** Abrindo o utilitário de configuração do sistema **d.** Acessando as propriedades da unidade

- 3.** Na tabela a seguir, indique qual comando deve ser usado para executar cada tarefa.

Tarefa	Comando
uma. Abra um prompt de comando b.	
Exibir todos os diretórios em um local especificado	
c. Criar uma nova pasta	
d. Remover uma pasta vazia	
e. Remova um ou mais arquivos	
f. Parar de executar uma tarefa especificada	
g. Copie um ou vários arquivos	
h. Verifique se há erros e repare o disco rígido	
eu. Fechar um prompt de comando	
j. Criar novas partições	
k. Exibir os arquivos de ajuda para um comando específico	

1. chkdsk

2. cmd ou comando

3. comando/?

4. del

5. dir .

6. parte do disco

7. sair

8. md ou mkdir

9. rd ou rmdir

10. taskkill

11. xcopy, robocopy

4. Um cliente pode navegar na Web, mas não pode imprimir em uma impressora de rede.

Qual das seguintes afirmações descreve melhor a causa mais provável? **uma.** As

opções de compartilhamento para o perfil de rede precisam ser reconfiguradas. **b.**

O adaptador de rede está configurado para usar o modo half-duplex.

c. O Wi-Fi está desativado.

d. Uma configuração de IP alternativa não está completa.

5. Seu adaptador de rede está desativado. Como isso é indicado no Windows

Gerenciador de Dispositivos?

uma. O dispositivo não está listado.

b. Um ! é exibido sobre o ícone do dispositivo. **c.**

Um ícone de seta para baixo é exibido sobre o ícone do dispositivo.

d. UMA ? é exibido sobre o ícone do dispositivo.

6. Um cliente relata que o sistema está inicializando muito lentamente. Qual dos seguintes

utilitários é melhor para determinar o que está acontecendo? **uma.** Dispositivos e

Impressoras

b. Programas e características

c. Proteção do sistema **d.**

Configuração do sistema

7. Qual das etapas a seguir é necessária para ativar o compartilhamento de arquivos?

uma. Abra o aplicativo Firewall **b.** Abra as

Propriedades do sistema **c.** Abra o Centro

de Rede e Compartilhamento **d.** Abra o utilitário de

configuração do sistema

8. Você criou uma pasta compartilhada em um servidor de rede. Você atribuiu uma designação de carta à pasta e a disponibilizou a todos os membros do departamento de Pesquisa. Essa pasta agora aparece como uma letra de unidade no computador de cada usuário. Que tipo de pasta você criou?

uma. Compartilhamento administrativo

b. Compartilhamento na nuvem

c. Unidade de rede mapeada

d. VPN

9. Na tabela a seguir, escreva o comando usado para abrir o respectivo

Serviços de utilidade pública.

Utilitário	Comando
uma. Registro	
b. Informações do sistema	
c. Configuração do sistema d.	
Consola de gestão da Microsoft	
	1. mmc
	2. msconfig
	3. msinfo32
	4. regedit

10. Qual dos seguintes utilitários é usado para criar uma VPN?

- uma.** Central de Rede e Compartilhamento
- b.** Opções da Internet **c.** Propriedades do sistema **d.** Firewall do Windows

11. Qual dos seguintes utilitários você usa para ver os itens que estão definidos para executar automaticamente em um determinado momento?

- uma.** Agendador de tarefas
- b.** Serviços
- c.** Gerenciador de Dispositivos
- d.** Desempenho

12. Antonio está usando seu laptop em um restaurante e definiu seu perfil de rede como Público. Qual dos seguintes não está disponível para ele? (Escolha todas as que se aplicam.) **a.** Compartilhamento de arquivos e impressoras

- b.** Acesso a documentos baixados
- c.** Descoberta de rede **d.** Transmissão de mídia

13. Qual das seguintes afirmações melhor descreve um firewall?

- uma.** Um firewall é uma barreira especialmente construída na sala do servidor que destina-se a limitar a propagação do fogo.
- b.** Um firewall é uma tecnologia de supressão de incêndio que usa cabeamento em dutos e espaços no teto.
- c.** Um firewall é um servidor proxy com uma conexão VPN. **d.** Um firewall é um software ou hardware que controla o fluxo de informações entre um computador e a Internet ou outra rede.

14. Quais das opções a seguir podem ser configuradas como exceções no Windows Defender Firewall? (Escolha todas as que se aplicam.) **a.** Aplicativos que devem ser permitidos através do firewall **b.** Portas e números de porta a serem abertos

- c. O endereço IP a ser usado
- d. A máscara de sub-rede a ser usada

15. Qual é a finalidade de uma máscara de sub-rede?

- uma.** Ele permite que os computadores escondam seus endereços IP de outros.
- b. Traduz endereços entre IPv4 e IPv6.
- c. Ele define quais bits de endereço IPv4 são bits de rede e quais são bits do host.
- d. Ele oculta o gateway padrão da rede local.

16. Qual dos seguintes é o utilitário de backup para o sistema operacional macOS sistema?

- uma.** alcatrão
- b. crontab
- c. Máquina do tempo
- d. YUM

17. Qual é a finalidade do Utilitário de Disco no macOS?

- uma.** Ele prepara um disco para ser usado para armazenar backups de imagens e outros arquivos.
- b. Ele gerencia a conexão de rede com a Internet.
- c.** Ele ejeta um disco.
- d.** Ele gerencia o armazenamento remoto na nuvem.

18. No terminal macOS ou Linux, qual dos seguintes é usado para forçar sair de um aplicativo usando seu número PID?

- uma.** matar
- b. Ctrl+Alt+Del
- c. fim
- d. fq

19. O que não é verdade sobre o Samba?

- uma.** É de código aberto.
- b. Ele permite que máquinas Linux ingressem no Active Directory.

- c.** Ele permite o compartilhamento de impressão entre máquinas Linux e Windows. **d.** É um utilitário de backup para Windows e Linux.
- 20.** Compartilhamento de tela, compartilhamento de arquivo e compartilhamento de impressora são configurados por meio de qual utilitário macOS? **uma.** Painel de controle
b. Preferências do sistema **c.** Aplicativo de compartilhamento
d. Tela
- 21.** Qual função o Mission Control desempenha no macOS?
uma. Ele exibe todos os aplicativos abertos em vários desktops. **b.** Ele instala um sistema operacional em uma máquina virtual. **c.** Ele gerencia o fluxo de entrada e saída de dados em uma rede.
d. Ele gerencia o fluxo de dados através de um firewall.
- 22.** Qual dos seguintes aplicativos macOS é usado para compartilhar fotos e documentos e para armazenamento de dados?
uma. Máquina do tempo
b. iCloud
c. Assistência da Apple **d.** Holofote
- 23.** Qual é o nome do gerenciador de arquivos usado pelo macOS?
uma. Explorador
b. Procurar
c. localizador
d. Explorador de arquivos
- 24.** Qual das opções a seguir se refere à linha de ícones de aplicativos em execução no momento na parte inferior da tela do macOS?
uma. barra de tarefas
b. Barra de menu

c. localizador

d. Doca

25. Combine os seguintes comandos de usuário do Linux com suas descrições.

a. su

b. iwconfigapt-get

c. cd

d. ls

e. chmod

f. ps

g. rm

h. grep

i. pwd

j. bom

k. chown

Opções de resposta:

1. Altere a propriedade do arquivo

2. Altere as pastas

3. Altere as permissões

4. Exclua arquivos ou pastas

5. Instalar ou gerenciar ferramentas avançadas de empacotamento

6. Listar os processos atualmente em execução

7. Realize pesquisas de texto/palavra

8. Imprimir (exibir) diretório de trabalho

9. Executar comandos como um usuário diferente (geralmente root)

10. Mostra o conteúdo de um diretório ou pasta

11. Utilitário de código aberto para atualizações automáticas no Linux

Capítulo 7

Segurança

Este capítulo aborda os 10 objetivos do exame A+ 220-1102 relacionados à segurança. Esses objetivos podem abranger 25 por cento das questões do exame:

- **Núcleo 2 (220-1102): Objetivo 2.1:** Resumir várias medidas de segurança e seus propósitos.
- **Núcleo 2 (220-1102): Objetivo 2.2:** Comparar e contrastar protocolos de segurança sem fio e métodos de autenticação.
- **Núcleo 2 (220-1102): Objetivo 2.3:** Dado um cenário, detectar, remover e prevenir malware usando ferramentas e métodos apropriados.
- **Núcleo 2 (220-1102): Objetivo 2.4:** Explicar ataques, ameaças e vulnerabilidades comuns de engenharia social.
- **Núcleo 2 (220-1102): Objetivo 2.5:** Dado um cenário, gerenciar e definir configurações básicas de segurança no sistema operacional Microsoft Windows.
- **Núcleo 2 (220-1102): Objetivo 2.6:** Dado um cenário, configurar uma estação de trabalho para atender às melhores práticas de segurança.
- **Núcleo 2 (220-1102): Objetivo 2.7:** Explicar métodos comuns para proteger dispositivos móveis e integrados.
- **Núcleo 2 (220-1102): Objetivo 2.8:** Dado um cenário, use métodos comuns de destruição e descarte de dados.
- **Núcleo 2 (220-1102): Objetivo 2.9:** Dado um cenário, definir as configurações de segurança apropriadas em redes sem fio e com fio de pequenos escritórios/escritórios domésticos (SOHO).
- **Núcleo 2 (220-1102): Objetivo 2.10:** Dado um cenário, instale e configure navegadores e configurações de segurança relevantes.

O ativo mais importante que a maioria das empresas possui são seus dados. Os dados se tornaram tão importantes para o sucesso dos negócios que são o que a maioria dos ladrões procura. Devido à natureza interconectada da Internet, uma violação de segurança de um único dispositivo ou rede pode levar ao roubo de dados, incluindo o roubo de dados financeiros de clientes que podem afetar significativamente a vida de milhões de pessoas. Violações de dados em larga escala levaram grandes empresas à falência, portanto, a segurança dos dados está entre as principais preocupações da liderança empresarial. Neste capítulo, você aprenderá sobre as ameaças multifacetadas à segurança no ambiente de computação moderno e como mitigá-las por meio do estudo desses objetivos do CompTIA A+ Core 2. Este capítulo abrange os seguintes tópicos:

- **Medidas de segurança física:** Práticas de segurança física e sua implementação
- **Conceitos lógicos de segurança:** medidas de segurança baseadas em software
- **Autenticação e protocolos de segurança sem fio:** Tipos de segurança e autenticação sem fio
- **Remoção e prevenção de malware:** métodos e protocolos para detecção e prevenção
- **Ameaças e vulnerabilidades de engenharia social:** os vários tipos de ameaças
- **Configurações de segurança do sistema operacional Microsoft Windows:** as configurações importantes de segurança da Microsoft
- **Práticas recomendadas de segurança para proteger uma estação de trabalho:** Implementação de práticas recomendadas
- **Segurança de dispositivos móveis:** métodos de implementação para proteger dispositivos
- **Destrução e descarte de dados:** métodos e técnicas para descartar hardware com segurança
- **Configuração de segurança em redes SOHO:** Métodos para configurar a segurança SOHO
- **Configurações de segurança do navegador:** configurações e práticas seguras em navegadores

“Eu já sei disso?” Questionário

O “Eu já sei disso?” questionário permite avaliar se você precisa ler o capítulo inteiro. A [Tabela 7-1](#) lista os principais títulos deste capítulo e a seção “Eu já sei disso?” perguntas do questionário que cobrem o material desses títulos para que você possa avaliar seu conhecimento nessas áreas específicas. As respostas para a pergunta “Eu já sei disso?” questionário aparecem no Apêndice A, “Respostas para a pergunta ‘Eu já sei disso?’ Questionários e perguntas de revisão.

Tabela 7-1 “Eu já sei disso?” Mapeamento de seção para pergunta

Seção de Tópicos Fundamentais	Perguntas
Medidas de segurança	1–2
Protocolos de segurança sem fio e autenticação	3
Remoção e Prevenção de Malware	4
Ameaças e vulnerabilidades de engenharia social	5
Configurações de segurança do sistema operacional Microsoft Windows	6
Práticas recomendadas de segurança para proteger uma estação de trabalho	7
Protegendo dispositivos móveis	8
Destruição e descarte de dados	9
Configurando a segurança em redes SOHO	10
Configurando o navegador e as configurações de segurança relevantes	11

CUIDADO

O objetivo da autoavaliação é avaliar seu domínio dos tópicos deste capítulo. Se você não souber a resposta a uma pergunta ou tiver certeza apenas parcial da resposta, marque essa pergunta como errada para fins de autoavaliação. Dar a si mesmo crédito por uma resposta que você adivinhou corretamente distorce os resultados de sua autoavaliação e pode lhe dar uma falsa sensação de segurança.

1. Que tipo de violação de segurança é um vestíbulo de controle de acesso (anteriormente mantrap) projetado para frustrar?

- uma.** biométrico
- b.** Utilização não autorizada
- c. Guarda**
- d. surf de ombro**

2. Diga que você foi solicitado a melhorar a segurança adicionando um sistema que examina pacotes de rede para determinar se eles devem ser encaminhados ou bloqueados. Qual função você provavelmente adicionaria?

- uma.** Filtragem de endereços
- MAC b.** Clonagem de endereços
- MAC c.** firewall de software
- d. autenticação multifator**

3. Qual dos seguintes é o protocolo sem fio mais seguro em uso hoje?

- uma.** WEP
- b.** WEP3
- c.** TKIP
- d. WPA3**

4. Um usuário baixou inadvertidamente um malware enquanto também baixava um aplicativo gratuito em um site de jogos. Qual termo geral descreve o arquivo baixado acidentalmente?

- uma.** Verme
- b.** troiano
- c.** ransomware
- d. botnet**

5. Vários computadores em uma rede foram comandados para lançar um ataque a um servidor na Web. Qual termo descreve melhor essa situação?

- a. Phishing**
b. DoS
c. Falsificação
d. DDoS
- 6.** Qual configuração permite ao usuário mais privilégios em um Windows rede?
- a. Modificar**
b. Ler e Executar
c. Uso final
d. Escreva
- 7.** Qual é o melhor exemplo de senha forte? **a. dr0wssap**
b. Senha9
c. Pa5SwordRd5
d. pA55wrds
- 8.** Qual das opções a seguir não é um exemplo de autenticação biométrica?
- a. Inserindo uma senha e respondendo a uma pergunta secreta**
b. ID FACE da Apple **c. Windows Hello**
d. ID de toque
- 9.** Qual método apaga a mídia de armazenamento, mas deixa o dispositivo intacto?
- a. Destruição de dados** **b. Desmagnetização** **c. BitLocking** **d. Incineração**
- 10.** Para ajudar a ocultar a identidade de um roteador sem fio, o que deve ser alterado da configuração padrão?
- a. endereço IP privado**

b. Filtro de endereço MAC

c. Gateway IP padrão **d.**

Identificador do conjunto de serviços

11. Quais dos seguintes são considerados gerenciadores de senhas? (Selecione dois.)

a. Fontes confiáveis

b. Hash do arquivo

c. Gerente de credenciais **d.**

Chaveiro

Tópicos Fundamentais

Medidas de segurança



220-1102: Objetivo 2.1: Resumir várias medidas de segurança e suas finalidades.

Existem duas categorias básicas de segurança: física e lógica. Esta seção fornece uma visão aprofundada de ambos os aspectos deste tópico vital.

Segurança física A

segurança física do equipamento de TI é um primeiro fator fundamental em uma rede segura. Conforme mencionado anteriormente, os dados geralmente são o ativo mais valioso de uma empresa; deixá-lo em uma área destrancada é perigoso de duas maneiras. Primeiro, o equipamento de computador é valioso. Um ladrão pode querer o equipamento por seu valor de face, não se importando com os dados valiosos que ele contém ou com o dano que sua liberação pode causar aos clientes. Em segundo lugar, uma porta destrancada é um convite para alguém instalar um equipamento de detecção e obter acesso aos ativos de rede da empresa que estão muito além da sala física deixada sem vigilância. no reino

de segurança física, um profissional de TI deve entender e praticar várias medidas de proteção.

Vestíbulo de Controle de Acesso

Algumas áreas seguras incluem um **vestíbulo de controle de acesso** (anteriormente conhecido como mantrap), que é uma área com duas portas trancadas. Uma pessoa pode passar pela primeira porta por meio da utilização não autorizada, mas provavelmente terá dificuldade em passar pela segunda porta, especialmente se houver um guarda entre as duas portas. Um vestíbulo de controle de acesso essencialmente retarda o processo de entrada, na esperança de que qualquer pessoa que se esgueire atrás de outras seja impedida antes de conseguir entrar na área segura. Se alguém não tiver a autenticação adequada, essa pessoa ficará presa no vestíbulo de controle de acesso até a chegada das autoridades.

Leitor de crachás

Os leitores de crachás são dispositivos que podem interpretar os dados de um determinado tipo de ID. Embora os IDs com foto ainda sejam melhor avaliados por humanos, outros tipos de IDs adicionam segurança extra que os leitores de crachás podem controlar.

Crachás de identificação e leitores podem usar uma variedade de métodos de segurança física, incluindo o seguinte:

- **Fotos:** Se o portador do cartão não se parece com a pessoa do cartão, o portador pode estar usando o cartão de outra pessoa e deve ser detido.
- **Códigos de barras e tarjas magnéticas:** Os códigos embutidos nesses cartões carregam uma série de informações sobre os portadores e podem limitar o acesso dos indivíduos apenas a áreas autorizadas dos edifícios. Esses cartões podem ser lidos rapidamente por um leitor de código de barras ou dispositivo de furto.
- **Tecnologia RFID:** Assim como os crachás com código de barras, os cartões com chips de identificação por radiofrequência (RFID) podem ser usados para abrir apenas portas que correspondam ao chip RFID. Eles também podem rastrear o movimento dentro de um prédio e fornecer outros dados de acesso exigidos por um oficial de segurança.

Para evitar adulteração não detectada, os crachás de identificação devem ser revestidos com uma camada externa inviolável.

Video vigilância

As câmeras são onipresentes, graças ao crescimento explosivo da Internet das Coisas (IoT). Eles são acessíveis e podem facilmente armazenar gravações para segurança e referência histórica. A vigilância por vídeo de áreas seguras é essencial.

Sistemas de Alarme

Os alarmes são comuns em muitas áreas de segurança, desde alarmes de unidade com falha em computadores até tentativas de hacking em firewalls. Menos sofisticados, mas igualmente essenciais, são os alarmes físicos que alertam o pessoal de segurança quando as portas são abertas ou os cabos são movidos.

Sensores de movimento

Quando usados com sistemas de alarme e vídeo, os sensores de movimento podem fornecer boa segurança física. Os detectores de movimento podem ativar alarmes e eventos de registro de data e hora para rastreamento em gravações de vídeo.

guardas

Um ladrão determinado e habilidoso pode frustrar até mesmo os melhores planos de segurança. A melhor maneira de deter um ladrão é usar uma mistura de barreiras técnicas e interação humana. Os guardas podem ser implantados de diferentes maneiras. Quando os funcionários entram na área de trabalho na presença de um guarda, as melhores práticas provavelmente serão seguidas e todos farão a varredura e serão autenticados. Sem um guarda, as pessoas podem manter a porta aberta para outras pessoas que reconhecem, mas que dizem ter perdido suas identidades. Saber que alguém está observando atentamente mantém as pessoas honestas honestas e dissuade as pessoas desonestas.

Outra maneira de implantar guardas é fazer com que eles vigiem várias áreas por meio de câmeras de segurança que registram o acesso para dentro e para fora dos prédios. Embora esse método não seja tão eficaz quanto colocar um guarda em cada porta, ele permite que menos guardas de segurança examinem áreas diferentes em busca de comportamentos de tráfego que justifiquem mais atenção.

Fechaduras

Obviamente, a maneira mais fácil de proteger uma área é trancar as portas. Isso parece uma afirmação óbvia, mas é surpreendentemente comum que as pessoas simplesmente entrem em áreas não autorizadas. Algumas organizações escreveram políticas explicando como, quando e onde trancar as portas. Além das entradas principais, você também deve sempre trancar salas de servidores, armários de fiação, laboratórios e outras salas técnicas quando não estiverem em uso. Fechaduras físicas podem parecer uma solução simples, mas não podem ser invadidas por hackers.

Fechaduras de equipamento

A maioria dos desktops, laptops e outros dispositivos móveis, como projetores e estações de encaixe, possui um slot de segurança. Em um laptop, o slot geralmente está localizado próximo a um canto traseiro (consulte a [Figura 7-1](#)).



1. Security slot

Figura 7-1 Um slot de segurança em um laptop

Esse slot é usado com uma trava de cabo de laptop, como a mostrada na [Figura 7-2](#). As travas de laptop usam uma combinação ou fechadura com chave e são projetadas para travar um laptop (ou outro dispositivo seguro) em um local fixo, como uma mesa. Lembre-se de que muitos tipos de fechaduras de equipamentos podem ser usados para armários ou até mesmo sistemas de rack de servidor.



Figura 7-2 Uma trava de segurança combinada para laptop

postes de amarração

Os postes de **amarração** são postes curtos de madeira, metal ou concreto instalados em calçadas e calçadas para permitir a passagem de pedestres e bicicletas, mantendo os veículos maiores afastados. Eles geralmente são removíveis com acesso chave, para permitir que os veículos de manutenção e outro tráfego necessário cheguem perto dos edifícios. Os postes de amarração são uma maneira passiva de manter os veículos que podem estar ouvindo sinais longe de centros de dados sensíveis. Pessoas entrando e saindo de edifícios também são mais fáceis de acompanhar com câmeras de vídeo.

Cercas

Claro, o dispositivo de segurança mais fundamental é uma cerca. As cercas geralmente estão sujeitas a códigos de construção, portanto, um projeto eficaz é importante. Elas

deve ser o mais alto possível, robusto e monitorado.

Segurança física para funcionários

Esta seção destaca os métodos e práticas de segurança que permitem o acesso a quem precisa e ajudam a impedir a entrada de pessoas (e de seus softwares) que tentem comprometer as áreas seguras de uma organização.

Porta-chaves

Os chaveiros podem ser usados com uma variedade de dispositivos de segurança. Os chaveiros podem conter chips RFID e muitos são usados como parte de um processo de autenticação em duas etapas que funciona da seguinte maneira:

- O usuário carrega um chaveiro que gera um código a cada 30 a 60 segundos. Sempre que o código muda no fob, ele também é correspondido no servidor de autenticação. Em alguns casos, o usuário também deve fazer login no fob para ver o código de acesso, para uma camada extra de segurança.
- O usuário então faz login no sistema ou na área restrita, usando o código de acesso gerado aleatoriamente e exibido no display LCD do chaveiro. O servidor de autenticação corresponde ao código atual e permite Acesso.

Um chaveiro usado dessa maneira geralmente é chamado de *token de hardware*.

Cartão inteligente

Um **cartão inteligente** é um cartão do tamanho de um cartão de crédito que contém informações armazenadas e possivelmente também um microprocessador simples ou um chip RFID. Os cartões inteligentes podem ser usados para armazenar informações de identificação para uso em aplicações de segurança e para armazenar valores para uso em telefones pré-pagos ou serviços de cartão de débito, acesso a quartos de hóspedes de hotéis e outras funções. Os cartões inteligentes estão disponíveis em formatos de contato e sem contato.

Os cartões sem contato também são conhecidos como *cartões de proximidade*. Os leitores desses cartões geralmente são montados na parede para que os usuários possam digitalizar seus cartões a até 6 polegadas de um leitor.

Um sistema de segurança baseado em cartão inteligente inclui cartões inteligentes, leitores de cartão projetados para funcionar com cartões inteligentes e um sistema de back-end que contém um banco de dados que armazena uma lista de cartões inteligentes aprovados para cada local seguro. Os sistemas de segurança baseados em cartões inteligentes também podem proteger computadores pessoais individuais.

Para aumentar ainda mais a segurança, os sistemas de segurança de cartão inteligente podem ser multifatoriais, exigindo que o usuário insira um PIN ou senha de segurança e, em seguida, forneça o cartão inteligente em pontos de verificação seguros, como a entrada de uma sala de computadores.

Chaves

Manter o controle das chaves é essencial. Se as chaves forem confiadas a uma pessoa descuidada ou, pior ainda, a um funcionário desonesto, todo o plano de segurança pode falhar. Documente quem tem as chaves das salas de servidores e armários de fiação e troque periodicamente as fechaduras e chaves. Os bloqueios cifrados que usam códigos perfurados também aumentam a segurança. O uso de uma combinação desses métodos oferece maior proteção.

biometria

A **segurança biométrica** refere-se ao uso das informações biológicas de uma pessoa, coletadas a partir de varreduras. Os seguintes tipos principais estão atualmente em uso:

- Varredura de **retina (íris)**: essa tecnologia altamente precisa é quase impossível de ser frustrada, mas requer equipamento especializado e pode ser cara.
- **Digitalização de impressão digital**: assim como a digitalização de íris, a digitalização de impressão digital é altamente precisa, mas esse tipo de digitalização biométrica é muito mais acessível de implementar. A varredura reúne dados sobre impressões digitais e compara suas características com os dados armazenados para correspondência. Mais de uma impressão digital pode ser armazenada para referência.
- Digitalização de impressão digital : esta digitalização é menos precisa do que a digitalização de impressão digital porque o scanner de palma não analisa a estrutura das impressões digitais; apenas coleta dados sobre o tamanho da mão.

O reconhecimento facial não está listado nos objetivos A+, mas pode se tornar mais comum à medida que a tecnologia melhora, os custos caem e as práticas de higiene se tornam mais difundidas desde a chegada do COVID-19. Reconhecimento facial

envolve o armazenamento de fotografias, no entanto, e questões de privacidade estão surgindo como resultado.

Illuminação

Manter áreas bem iluminadas é importante, por muitas razões óbvias e não tão óbvias. Com o advento da iluminação LED, uma boa iluminação não é mais a preocupação de custo e energia que costumava ser. Áreas bem iluminadas podem fornecer segurança para os trabalhadores, melhor legibilidade de pequenas etiquetas ao trabalhar com racks de equipamentos e melhor qualidade para câmeras de vídeo e outras medidas de segurança.

Magnetômetros

O termo **magnetômetro** é simplesmente outro nome para um detector de metais, comum a todos os aeroportos e muitas áreas públicas. Áreas altamente sensíveis geralmente têm restrições de armas; um magnetômetro pode identificar armas escondidas, para fazer cumprir as regras e reduzir a probabilidade de um incidente violento.

Tela de privacidade As

questões de privacidade são importantes para qualquer empresa que lida com dados confidenciais. Quando esses dados estão sendo usados na tela de uma estação de trabalho ou dispositivo móvel, eles precisam ser protegidos contra visualização não intencional. Os dados em uma tela de computador podem ser facilmente protegidos com a instalação de uma tela de privacidade, que é uma cobertura transparente para um monitor de PC ou laptop. Ele reduz o cone de visão, geralmente para cerca de 30 graus, de modo que apenas a pessoa diretamente na frente da tela possa ver o conteúdo. Muitas dessas telas também são antirreflexo, para reduzir o cansaço visual do usuário.

Conceitos de Segurança Lógica

Um computador é uma combinação de sistemas físicos e lógicos, e as práticas de segurança devem abordar esses dois lados da computação. Os componentes físicos de segurança abordados na seção anterior são apenas parte de um bom plano de segurança e serão ineficazes se as políticas de segurança pararem por aí.

Abordar as práticas de segurança (lógica) de software também é essencial.

Princípio do Menor Privilégio

Aplicar o **princípio do menor privilégio** significa dar aos usuários acesso apenas ao que eles precisam para realizar seus trabalhos. A maioria dos usuários em um ambiente de negócios não precisa de acesso administrativo aos computadores e deve ser restringida de funções que possam comprometer a segurança.

O princípio do menor privilégio parece ser senso comum básico, mas não deve ser considerado levianamente. Quando as contas de usuário são criadas localmente em um computador, especialmente em um domínio, deve-se tomar muito cuidado ao atribuir usuários a grupos. Além disso, muitos programas perguntam durante a instalação quem pode usar e fazer modificações no programa; geralmente o padrão é "todos os usuários". Alguns técnicos apenas aceitam os padrões ao instalar programas apressadamente, sem perceber que estão dando aos usuários o controle total do programa. É uma prática importante dar aos clientes tudo o que eles precisam, mas limitar seu acesso apenas ao que eles precisam.

Listas de controle de acesso

Listas de controle de acesso (ACLs) são listas de permissões ou regras de restrição para acesso a um objeto, como um arquivo ou pasta. As ACLs controlam quais usuários ou grupos podem executar operações específicas em arquivos ou pastas especificados.

autenticação multifator

Um sistema de **autenticação multifator (MFA)** usa dois ou mais métodos de autenticação e é muito mais seguro do que a autenticação de fator único. Por exemplo, considere uma pessoa obtendo acesso a um sistema usando um código digital de um chaveiro e digitando um nome de usuário e uma senha. A combinação da senha e do token digital torna muito difícil para os impostores obter acesso a um sistema. A autenticação multifator é mais segura do que versões anteriores de tokens de software, que podem ser roubados.

Os fatores de autenticação geralmente são divididos em algo que um usuário é (biometria), algo que um usuário possui (um token ou cartão de acesso), algo que um usuário sabe (um número de identificação pessoal [PIN]) e onde o usuário está localizado (geolocalização). Por exemplo, caixas eletrônicos (ATMs) usam um exemplo comum de um sistema de autenticação multifator, exigindo tanto um

chave física “algo que você tem” (seu cartão do caixa eletrônico) e um PIN “algo que você conhece”.

O email

O e-mail é a forma mais comum de atacar uma organização porque seus funcionários podem cair em ataques de phishing (descritos na seção “Ameaças e vulnerabilidades de engenharia social”). A filtragem pode organizar automaticamente o e-mail em pastas, mas, do ponto de vista da segurança, sua função mais importante é bloquear spam e mensagens potencialmente perigosas.

A filtragem de e-mail pode ser executada no ponto de entrada de uma rede com um servidor ou dispositivo de filtragem de e-mail especializado, bem como habilitando os recursos de detecção de spam e ameaças incorporados aos clientes de e-mail ou software de segurança.

Os usuários podem descartar ou colocar em quarentena spam ou e-mails suspeitos, bem como recuperar falsos positivos que são realmente mensagens legítimas da pasta de spam e colocá-los de volta na caixa de entrada normal.

Os protocolos de e-mail devem ser protegidos para garantir que o e-mail seja criptografado. Por exemplo, por padrão, os protocolos de e-mail POP e IMAP não são seguros. O uso de protocolos seguros como POP3S (porta 995) ou IMAPS (porta 993) permite que os dados recebidos do cliente sejam criptografados porque eles usam uma sessão SSL/TLS.

Tokens rígidos

Um **hard token** é qualquer dispositivo físico que um usuário deve carregar para obter acesso a um sistema específico. Exemplos são cartões inteligentes, cartões RFID, tokens USB e chaveiros. (Os tokens de hardware do chaveiro são explicados anteriormente nesta seção.)

Tokens flexíveis

Assim como os chaveiros, mencionados na seção anterior sobre segurança física, os *tokens de software* (ou **soft tokens**) fazem parte de um processo de autenticação multifatorial. A diferença é que os tokens de software existem no software e geralmente são armazenados em dispositivos. Por exemplo, fazer login em um sistema seguro pode exigir o envio de um soft token via mensagem SMS para um smartphone para

autenticação de código. Tanto os hard tokens quanto os soft tokens podem ser usados na autenticação multifator, conforme descrito anteriormente nesta seção.

Serviço de mensagens curtas

Short Message Service (SMS) é o formato padrão de mensagens de texto entre dispositivos. Os produtos podem ter seus próprios formatos de mensagem (por exemplo, a Apple usa o iMessage em seus dispositivos), mas o SMS é um padrão. O SMS geralmente é usado para tokens multifatoriais, descritos anteriormente.

Chamada de voz

Os soft tokens podem ser autenticados com um retorno de chamada de voz. Quando um usuário faz login em um site, ele pode ter que se autenticar com uma chamada de voz e pressionar uma tecla fornecida pelo aplicativo de serviço no telefone. Isso é semelhante ao login do SMS que acabamos de descrever.

Aplicativo de Autenticação

Os serviços de autenticação multifator fornecem aplicativos que podem ser baixados para telefones e outros dispositivos. Essa é uma maneira fácil de fornecer autenticações de segundo fator após o login. Ao fazer login em um site restrito, o serviço envia um token para o dispositivo registrado do usuário. Basta tocar em um botão de confirmação para um login rápido e seguro.

Gerenciamento de dispositivos móveis

As organizações que possuem muitos dispositivos móveis precisam administrá-los para que todos os dispositivos e usuários cumpram as práticas e políticas de segurança em vigor. Isso geralmente é feito com um conjunto de software conhecido como [**gerenciamento de dispositivo móvel \(MDM\)**](#). O mercado de MDM é bastante competitivo e várias soluções estão disponíveis em empresas como VMware (AirWatch), Citrix (XenMobile) e SOTI MobiControl. Esses produtos enviam atualizações e permitem que um administrador configure muitos dispositivos móveis a partir de um local central. Um bom software de MDM protege, monitora, gerencia e oferece suporte a vários dispositivos móveis diferentes em toda a empresa.

Active Directory

O **Active Directory** é uma solução da Microsoft para gerenciar usuários, computadores e acesso a informações em uma rede. É baseado em um banco de dados de todos os recursos e usuários que serão gerenciados dentro da rede. As informações no banco de dados determinam o que as pessoas podem ver e fazer dentro da rede. Um entendimento completo do Active Directory está além do escopo deste livro, mas toda pessoa de suporte de TI deve saber o básico sobre o que é e como funciona. Aqui estão os princípios:



- **Script de login:** quando um usuário faz logon na rede, o Active Directory sabe quem é esse usuário e executa um script de login para disponibilizar os recursos atribuídos. Exemplos de tarefas de login incluem atualizações de vírus, mapeamentos de unidade e atribuições de impressora.
- **Domínio:** O domínio é uma rede de computadores ou um grupo de redes de computadores sob uma única administração. Os usuários fazem logon no domínio do Active Directory para acessar recursos de rede dentro do domínio.
- **Diretiva de Grupo:** Este é um conjunto de regras e instruções que definem o que um usuário ou grupo de usuários pode ou não fazer quando conectado ao domínio. Um objeto de política de grupo (GPO) é um conjunto de instruções atribuídas a um grupo de usuários ou a determinadas máquinas na rede.
- **Unidade Organizacional (OU):** OUs são grupos lógicos que ajudam a organizar usuários e computadores para que GPOs possam ser atribuídos a eles. Por exemplo, uma equipe de contadores pode ser atribuída a uma UO e seu GPO pode conceder a eles acesso especial a registros financeiros.
- **Pasta Home:** Esta pasta, acessível ao administrador da rede, é onde os dados e arquivos do usuário são mantidos localmente.
- **Redirecionamento de pasta:** permite que o trabalho feito por uma UO seja salvo em uma pasta comum no domínio, conforme orientado pelo administrador em vez do usuário. Por exemplo, uma política pode determinar que todo o trabalho seja mantido em uma pasta comum para que todos os membros de uma equipe possam ver o trabalho e as atualizações mais recentes.
- **Grupos de segurança:** fornecem uma maneira eficiente de atribuir direitos e permissões de usuário a usuários aprovados que acessam recursos no

rede. A Diretiva de Grupo (anteriormente na lista) pode ser usada para atribuir direitos a grupos de segurança. As permissões podem ser atribuídas a um grupo de segurança para recursos compartilhados em níveis específicos de acesso.

Protocolos de segurança sem fio e autenticação



Objetivo 2.2: Comparar e contrastar protocolos de segurança sem fio e métodos de autenticação.

A segurança sem fio evoluiu nos últimos anos para se adaptar às ferramentas cada vez mais disponíveis que podem invadir uma rede sem fio. Um administrador não pode instalar com segurança uma rede sem fio usando as configurações padrão. As seções a seguir descrevem as opções de segurança disponíveis em uma rede sem fio.

Protocolos e criptografia Uma rede

sem fio criptografada depende da troca de uma senha entre o cliente e o ponto de acesso sem fio (WAP) ou roteador antes que o cliente possa se conectar à rede. Vários padrões de criptografia foram usados, pois os métodos de criptografia foram aprimorados para se manter à frente dos hackers.

Os protocolos atuais são conhecidos como Wired Equivalent Privacy (WEP). A primeira versão do WEP usava o **Temporal Key Integrity Protocol (TKIP)**, que agora é considerado obsoleto. As versões atuais são descritas a seguir:



- **Wi-Fi Protected Access 2 (WPA2)** foi lançado em 2004 e usa **criptografia AES (Advanced Encryption Standard)**. A criptografia AES do WPA2 é muito mais forte do que a versão anterior: usa blocos de 128 bits e suporta comprimentos de chave variáveis de 128, 192 e 256 bits. Permite até 63 caracteres alfanuméricos (incluindo sinais de pontuação e outros caracteres) ou 64 caracteres hexadecimais. O WPA2 também suporta o uso de um servidor de **autenticação RADIUS** em ambientes corporativos.

- **O Wi-Fi Protected Access 3 (WPA3)**, lançado em 2018, usa criptografia de 128 bits (192 bits em uma versão corporativa) e possui um método diferente para compartilhar chaves de segurança dos outros tipos de criptografia. O WPA3 foi projetado para adicionar melhor privacidade e proteção contra ataques em redes Wi-Fi públicas.

A criptografia TKIP e AES são bem diferentes. O TKIP é um pouco parecido com o WEP em design, de modo que pode operar em hardware herdado que carece de poder de computação. O TKIP não é mais considerado suficientemente seguro. AES é muito mais seguro e foi adotado pelo governo dos EUA como padrão de criptografia. Alguns pontos importantes a serem lembrados são que existem duas versões do WPA2: WPA2-Personal e WPA2-Enterprise. O WPA2-Personal protege o acesso não autorizado à rede por meio de uma senha. O WPA2-Enterprise verifica os usuários da rede por meio de um servidor. O WPA2 Personal usa chaves pré-compartilhadas. O WPA3 também inclui uma versão pessoal e uma versão corporativa. O WPA3 mantém força criptográfica equivalente por meio do uso obrigatório de AES de 192 bits para a versão Enterprise e AES opcional de 192 bits para a versão pessoal. O WPA3 ajuda a evitar ataques de senha offline usando a autenticação simultânea de iguais (SAE). Isso ainda permite que os usuários escolham senhas mais fáceis de lembrar e, por meio do sigilo de encaminhamento, não compromete o tráfego já transmitido, mesmo que a senha seja comprometida.

Autenticação

Quatro métodos de autenticação diferentes são usados para acessar uma rede sem fio: fator único, multifator, RADIUS e TACACS+. Esses métodos também se aplicam a redes com fio.

Fator Único

A autenticação de fator único é o acesso básico de nome de usuário e senha a um computador ou rede. Durante anos, isso foi suficiente - e ainda é usado em muitos ambientes. Mas a ascensão do banco e das compras on-line atraiu métodos de hacking mais avançados, e a autenticação de fator único agora é rara no comércio on-line.

Multifator

Um sistema de autenticação multifator usa dois ou mais métodos de autenticação e é muito mais seguro do que a autenticação de fator único.

RAIO

O **Remote Authentication Dial-In User Service (RADIUS)** remonta aos dias de acesso por modem dial-up às redes no início dos anos 90. Foi amplamente distribuído e ainda está em uso, embora tenha sido atualizado ao longo dos anos. Um usuário que deseja acessar uma rede ou um serviço online pode entrar em contato com um servidor RADIUS e inserir informações de nome de usuário e senha quando solicitado. O servidor autentica (ou recusa) o usuário e avisa a rede ou serviço para permitir (ou não) a entrada do cliente.

TACACS+

Terminal Access Controller Access Control System (TACACS+) resolveu um problema que ocorreu quando o uso da rede se expandiu na década de 1980. O nome e o acrônimo parecem complicados, mas descrevem muito bem a função e o processo. No início da computação em rede, quando um usuário se conectava a uma rede, cada vez que acessava um recurso ou host diferente nessa rede, o usuário precisava se autenticar novamente. A discagem era lenta e o login era um processo demorado. Com o TACACS+, um usuário que já foi autenticado na rede também foi automaticamente logado em outros recursos do sistema. O sistema de controle de acesso à rede cuidava do acesso do usuário ao terminal.

Em sua forma original, o TACACS é bastante inseguro, mas a Cisco o atualizou e relançou de forma proprietária como TACACS+.

Kerberos

Kerberos é um protocolo de autenticação padrão aberto que é usado entre dois clientes (ou um cliente e um servidor) e um servidor Kerberos Key Distribution Center de terceiros. Os clientes adquirem uma chave Kerberos e podem se autenticar mutuamente em uma rede não segura ou na Internet.

A versão do Kerberos da Microsoft é o método padrão para autenticação do Windows para ingressar em domínios. As versões também estão disponíveis no macOS, Linux e outros sistemas operacionais.

Remoção e Prevenção de Malware

220-1102

Exam

Objetivo 2.3: Dado um cenário, detectar, remover e prevenir malware usando ferramentas e métodos apropriados.

A segurança sem fio evoluiu nos últimos anos para se adaptar às ferramentas cada vez mais disponíveis que podem ser usadas para invadir uma rede sem fio. Um administrador não pode instalar com segurança uma rede com ou sem fio usando as configurações padrão. As seções a seguir descrevem algumas ameaças de segurança e opções disponíveis para atenuar essas ameaças.

Key
Topic

Malware

Software malicioso, ou **malware**, é um software projetado para se infiltrar em um sistema de computador e possivelmente danificá-lo sem o conhecimento ou consentimento do usuário. *Malware* é um termo amplo usado por profissionais de informática para incluir vírus, worms, cavalos de Tróia, spyware, rootkits, keyloggers, adware e outros tipos de software indesejado. As seções a seguir descrevem alguns tipos de malware com mais detalhes.

troiano

O malware **Trojan**, também conhecido como cavalo de Tróia, é um programa de malware disfarçado de “presente” – geralmente vídeos populares ou links de sites – que induz o usuário a baixar um vírus que pode ser usado para interceptar pressionamentos de tecla ou transmitir informações confidenciais. Os troianos são nomeados apropriadamente para a famosa história do cavalo de Tróia de madeira, um presente aparente que escondeu soldados invasores e permitiu que eles se esgueirassem para dentro dos portões da cidade de Tróia.

Rootkit

Um **rootkit** é um conjunto de ferramentas de hacking que penetra profundamente no sistema operacional ou nos aplicativos do computador e se prepara para assumir o controle

o computador. Alguns rootkits fazem keylogging, alguns escutam informações bancárias e outros mais complexos assumem completamente o controle de um computador. Um rootkit é um tipo complexo de malware difícil de detectar e remover com o software antivírus de malware padrão. Às vezes, limpar a unidade e reinstalar o sistema operacional é a única solução certa.

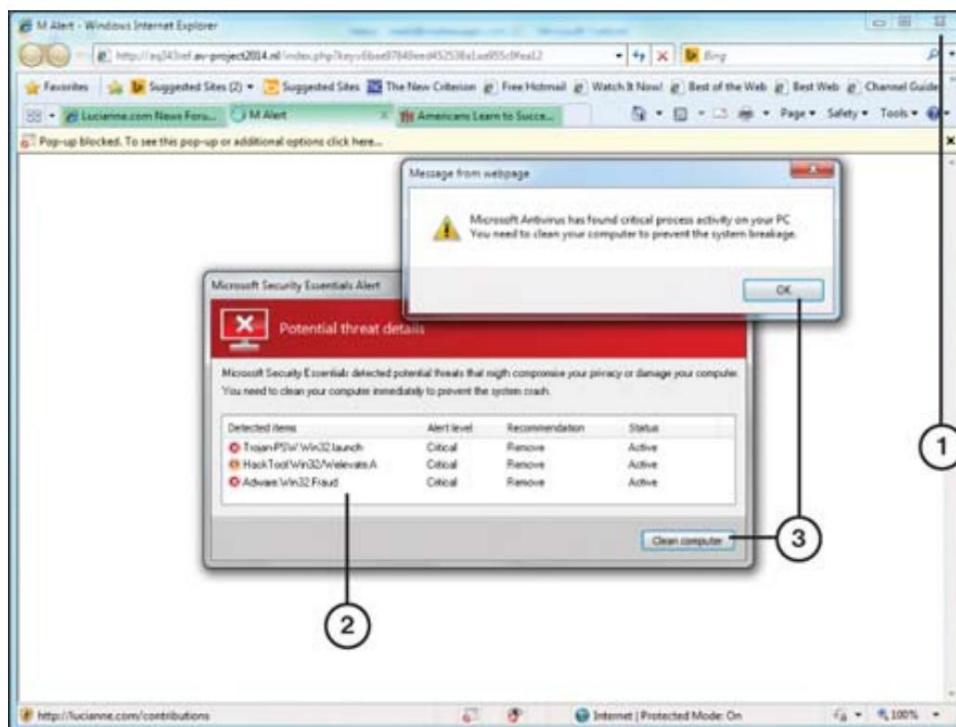
Vírus

Assim como os vírus biológicos podem infectar humanos e causar todo tipo de doença, os vírus de computador podem infectar e danificar computadores. **Vírus** é um termo genérico para qualquer software malicioso que pode se espalhar para outros computadores e causar problemas. Alguns vírus são mais maliciosos do que outros, mas todos precisam ser protegidos com atualizações de antivírus. A maioria dos ataques de vírus se espalha com assistência humana quando os usuários são vítimas de phishing e abrem anexos descuidadamente. (O phishing é discutido na seção “Ameaças e vulnerabilidades da engenharia social”, posteriormente neste capítulo.)

Spyware

Spyware é um software que espia as atividades do sistema e transmite detalhes de pesquisas na web ou outras atividades para computadores remotos. Obter várias janelas pop-up indesejadas ao navegar na Internet é um bom indicador de spyware. Algumas janelas pop-up exibem falsos alertas de segurança (como na [Figura 7-3](#)), na esperança de que o usuário clique em algo e adquira um software antivírus desonesto ou falso ou apenas baixe mais malware.

Spyware pode causar lentidão no desempenho do sistema.



1. The only safe place to click is the close browser button.
2. Fictitious threats.
3. Clicking either of these buttons might launch malware or spyware.

Figura 7-3 Um alerta de segurança falso que pretende vir de Microsoft

ransomware

Ransomware usa malware para criptografar os arquivos do computador de destino. O pedido de resgate pode ser apresentado depois que você liga para um número de suporte técnico falso exibido por uma mensagem de erro falsa do ransomware, ou o pedido de resgate pode ser exibido na tela. O resgate deve ser pago dentro de um período de tempo especificado ou os arquivos não serão descriptografados.

Um exemplo recente famoso de ransomware é o vírus WannaCry, que se espalhou pelo mundo em 2017. Ele afetou máquinas Windows que não foram atualizadas com patches de segurança que impediriam a propagação do ataque.

Um ataque ainda maior é tecnicamente conhecido como UNC2452, mas mais comumente conhecido pela forma como foi espalhado: através de grandes redes pegando carona no software de rede Solar Winds. Esse vírus é tão

exceptionalmente complicado que se pensa ser obra de um governo desconhecido.

Keylogger

Os vírus **keylogger** são especialmente perigosos porque rastreiam as teclas digitadas e podem capturar nomes de usuário e senhas de usuários involuntários. Um keylogger pode ser entregue por meio de um cavalo de Tróia, phishing ou um anexo de e-mail falso que o usuário abre. Uma maneira de evitar esses ataques é exigir autenticação multifator porque o segundo fator de autenticação muda, tornando a senha roubada inválida.

Vírus do setor de inicialização

Um **vírus do setor de inicialização** é semelhante a um vírus rootkit, pois está profundamente incorporado no computador. Nesse caso, o vírus se insere no código inicial do setor de inicialização de um disco rígido. Uma vez lá, ele pode ser carregado na memória do sistema na inicialização e inicializar o vírus oculto em outras unidades da rede. As versões atuais do BIOS e UEFI possuem proteção integrada contra vírus do setor de inicialização, e esses vírus são menos comuns do que nas décadas anteriores.

Criptomineradores

Criptomineradores são vírus que se apoderam dos recursos de um computador infectado para minerar criptomoedas, geralmente bitcoin. Essa prática também é conhecida como cryptojacking. A mineração de Bitcoin é amplamente legal na maioria dos países, mas é cara em termos de uso de energia e recursos de computador. Assim, os mineradores às vezes tentam forçar alguém a pagar os custos da mineração enquanto colhem o benefício de ganhar criptomoedas. Os vírus podem ser transmitidos em cavalos de Tróia, durante phishing e em ataques baseados em navegador, nos quais um código malicioso é inserido em uma página da Web e executado quando o navegador visita a página.

Desempenho lento, alto uso de CPU e tráfego de rede mais alto são sintomas de que um vírus criptográfico pode estar a bordo.

Ferramentas e Métodos

A indústria de antivírus/antimalware tem trabalhado arduamente para acompanhar a ameaça de hackers e vírus cada vez mais sofisticados. As seções a seguir discutem algumas das ferramentas e métodos usados para impedir hackers.

Antivírus/Antimalware

A proteção contra vírus e malware é necessária para todos os tipos de dispositivos de computação, de dispositivos móveis a servidores. Conjuntos de proteção de computador que incluem proteção antivírus, antimalware, antiadware e antiphishing estão disponíveis em muitos fornecedores, mas alguns usuários preferem uma abordagem “melhor da categoria” e escolhem o melhor produto disponível em cada categoria.

Os programas antivírus/antimalware podem usar algumas ou todas as técnicas a seguir para proteger usuários e sistemas:



- Proteção em tempo real para bloquear infecções
- Varreduras periódicas para ameaças conhecidas e suspeitas
- Atualização automática com frequência (geralmente diariamente)
- Assinaturas renováveis para obter assinaturas de ameaças atualizadas
- Links para enciclopédias de vírus e ameaças
- Inoculação de arquivos do sistema
- Acesso baseado em permissões à Internet
- Verificação de arquivos baixados e e-mails enviados/recebidos

Ao tentar se proteger contra vírus e malware, a consideração mais importante é manter seu aplicativo antimalware atualizado.

A segunda consideração mais importante é ficar atento a dados desconhecidos, sejam eles provenientes de e-mail, unidade flash USB, dispositivo móvel ou algum outro mecanismo.

Modo de recuperação

O modo de recuperação permite que você reinicie seu PC ou inicialize a partir de um disco de recuperação. Se redefinir o PC não for suficiente, você pode inicializar a partir de um disco de recuperação para remover os arquivos infectados e restaurar os arquivos originais. Acesse as ferramentas de recuperação no Windows 10 acessando **Configurações > Atualização e segurança > Recuperação**. A Figura 7-4 mostra a página de ferramentas de recuperação no Windows 10.

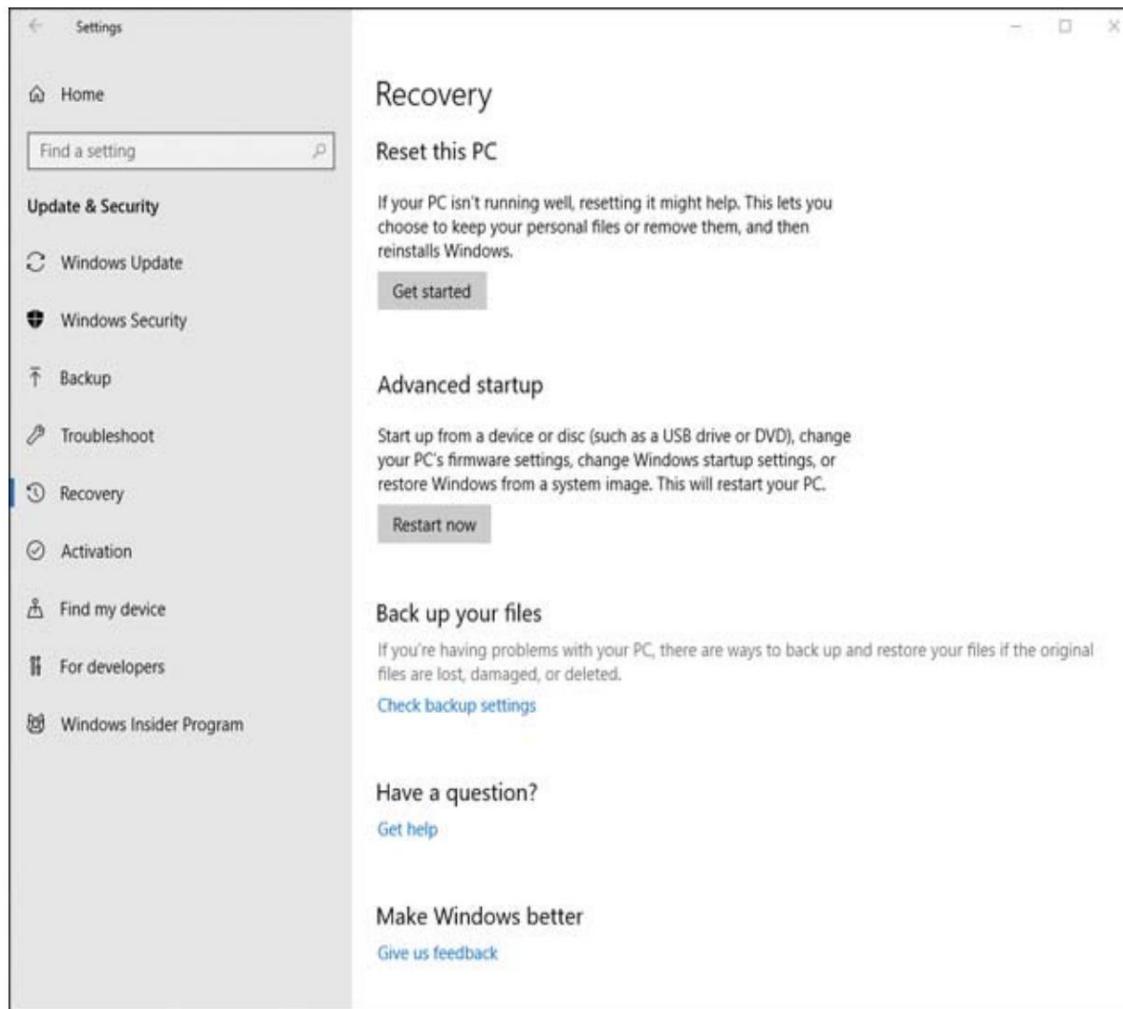


Figura 7-4 Opções de recuperação do Windows 10

Educação do usuário

Independentemente da sofisticação das medidas de segurança física ou digital, a falta de educação do usuário pode levar a problemas de segurança. Os usuários devem ser instruídos sobre como fazer o seguinte:

- Peça uma identificação quando for abordado pessoalmente por alguém que afirme ser do help desk, da companhia telefônica ou de uma empresa de serviços.
- Peça um nome e o nome do supervisor quando contatado por telefone por alguém que afirma ser do help desk, da companhia telefônica ou de uma empresa de serviços.
- Use apenas informações de contato oficiais para o suporte técnico, companhia telefônica e empresas de serviço autorizadas e ligue para a pessoa de contato autorizada para verificar se uma chamada de serviço ou solicitação de informações por telefone é legítima.
- Faça login nos sistemas primeiro e, em seguida, forneça o computador ao técnico (em vez de fornecer ao técnico todas as informações de login).
- Altere as senhas imediatamente após as chamadas de serviço.
- Relate qualquer possível chamada de engenharia social ou contatos pessoais, mesmo que nenhuma informação tenha sido trocada. Especialistas em engenharia social podem coletar informações aparentemente inócuas de vários usuários e criar uma história convincente para obter acesso a sistemas restritos.
- Mantenha os programas antivírus, antispyware e antimalware atualizados.
- Examine os sistemas em busca de vírus, spyware e malware.
- Entenda os principais tipos e técnicas de malware.
- Verifique as unidades de mídia removível (como discos ópticos e unidades USB) em busca de vírus e malware.
- Desative a execução automática e a reprodução automática.
- Configure programas de varredura para operação programada.
- Responda a notificações de que vírus, spyware ou malware foram detectados.
- Colocar arquivos suspeitos em quarentena.
- Relate arquivos suspeitos ao help desk.
- Remover malware.