



# Módulo 3: O sistema operacional Windows



CyberOps Associate v1.0

Prof. Clemilson Oliveira

[clemilson.oliveira@p.ucb.br](mailto:clemilson.oliveira@p.ucb.br)



# Objetivos do módulo

**Título do módulo:** O sistema operacional Windows

**Objetivo do módulo:** Explicar os recursos de segurança do sistema operacional Windows.

Título do Tópico	Objetivo do Tópico
Histórico do Windows	Descrever a história do sistema operacional Windows.
Arquitetura e operações do Windows	Explicar a arquitetura do Windows e sua operação.
Configuração e monitoramento do Windows	Explicar a configuração e o monitoramento do Windows.
Segurança do Windows	Explicar como o Windows pode permanecer seguro.

# 3.1 A história do Windows

# O sistema operacional Windows Sistema operacional de disco

- O sistema operacional de disco (DOS) é um sistema operacional que o computador usa para habilitar os dispositivos de armazenamento de dados para ler e gravar arquivos.
- DOS fornece um sistema de arquivos que organiza os arquivos de uma forma específica no disco.
- MS-DOS, criado pela Microsoft, usou uma linha de comando como interface para as pessoas criarem programas e manipularem arquivos de dados. Os comandos DOS são mostrados em negrito na saída de comando dada.
- Com o MS-DOS, o computador tinha um conhecimento básico de trabalho de acessar a unidade de disco e carregar os arquivos do sistema operacional diretamente do disco como parte do processo de inicialização.

```
Starting MS-DOS...
HIMEM is testing extended memory... done.
C:\> C:\DOS\SMARTDRV.EXE /X
C:\> dir
Volume in drive C is MS-DOS_6
Volume Serial Number is 4006-6939
Directory of C:\
DOS          <DIR>          05-06-17  1:09p
COMMAND     COM           54,645 05-31-94  6:22a
WINA20      386           9,349 05-31-94  6:22a
CONFIG      SYS             71 05-06-17  1:10p
AUTOEXEC    BAT             78 05-06-17  1:10p
              5 file(s)          64,143 bytes
              517,021,696 bytes free
C:\>
```

## Disco do Sistema Operacional Windows (Cont.)

- As primeiras versões do Windows consistiam em uma interface gráfica do usuário (GUI) que executava o MS-DOS, começando com o Windows 1.0 em 1985.
- Em versões mais recentes do Windows, construído em New Technologies (NT), o próprio sistema operacional está no controle direto do computador e seu hardware.
- Hoje, muitas coisas que costumavam ser realizadas através da interface de linha de comando do MS-DOS podem ser realizadas na GUI do Windows.
- Para experimentar um pouco de MS-DOS, abra uma janela de comando digitando **cmd** no Windows Search e pressionando **Enter**.

## Disco do Sistema Operacional Windows (Cont.)

A tabela a seguir lista alguns dos comandos do MS-DOS:

Comando MS-DOS	Descrição
<b>dir</b>	Mostra uma lista de todos os arquivos no diretório atual (pasta)
<i>diretório</i> <b>cd</b>	Altera o diretório para o diretório indicado
<b>cd ..</b>	Muda o diretório para o diretório acima do diretório atual
<b>cd \</b>	Muda o diretório para o diretório raiz (geralmente C:)
<b>copy</b> <i>origem destino</i>	Copia arquivos para outro local
<b>del</b> <i>nome do arquivo</i>	Exclui um ou mais arquivos.
<b>find</b>	Procura texto em arquivos
<b>mkdir</b> <i>diretório</i>	Cria um novo diretório.
<b>ren</b> <i>nome_antigo</i> <i>novo_nome</i>	Renomeia um arquivo
<b>ajuda</b>	Exibe todos os comandos que podem ser usados, com uma breve descrição
<i>comando</i> <b>help</b>	Exibe a ajuda extensa para o comando indicado

## O sistema operacional Windows, versões do Windows

- Desde 1993, houve mais de 20 versões do Windows que são baseadas no sistema operacional NT (SO).
- Muitas edições foram construídas especificamente para estações de trabalho, profissionais, servidores, servidores avançados e servidores de datacenter, para citar apenas algumas das muitas versões criadas para fins específicos.
- O sistema operacional de 64 bits era uma arquitetura totalmente nova. Ele tinha um espaço de endereço de 64 bits em vez de um espaço de endereço de 32 bits.
- Os computadores e sistemas operacionais de 64 bits são compatíveis com programas mais antigos de 32 bits, mas os programas de 64 bits não podem ser executados em hardware mais antigo de 32 bits.
- Com cada versão subsequente do Windows, o sistema operacional tornou-se mais refinado ao incorporar mais recursos.
- A Microsoft anunciou que o Windows 10 é a última versão do Windows. Em vez de comprar novos sistemas operacionais, os usuários apenas atualizarão o Windows 10.

# As versões do Windows do sistema operacional Windows (Cont.)

A tabela a seguir lista versões comuns do Windows:

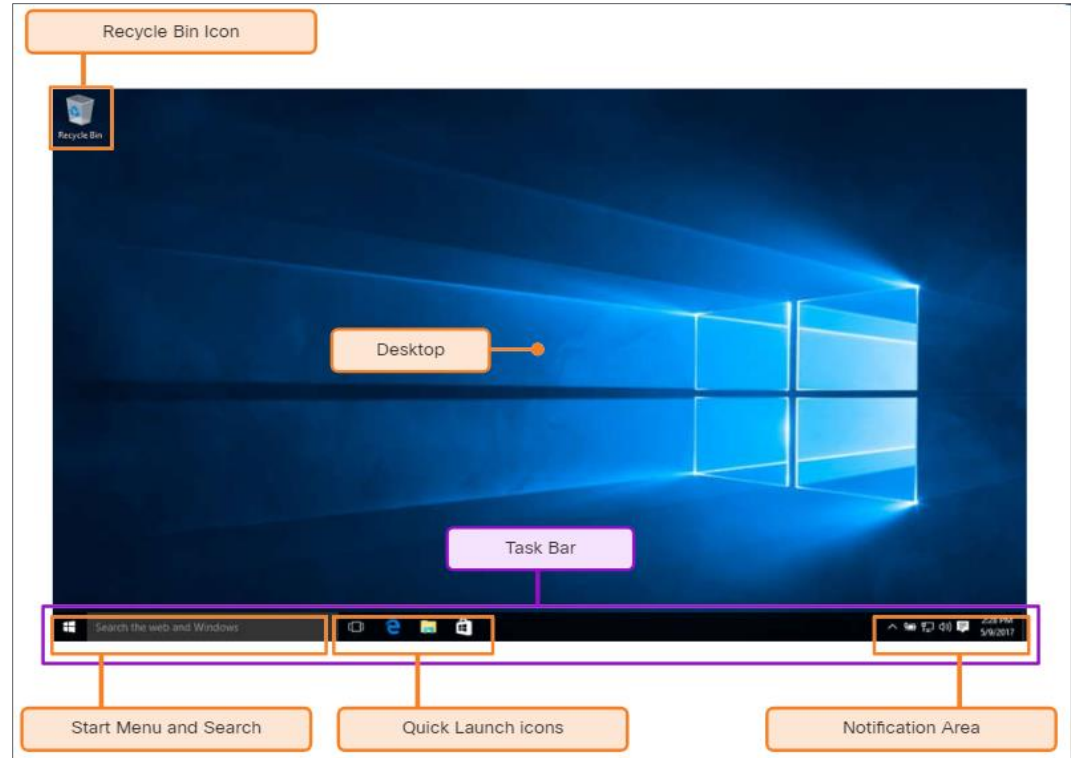
SO	Versões
Windows 7	Starter, Home Basic, Home Premium, Professional, Enterprise, Ultimate
Windows Server 2008 R2	Foundation, Standard, Enterprise, Datacenter, Web Server, HPC Server, Itanium-Based Systems
Windows Home Server 2011	Nenhum
Windows 8	Windows 8, Windows 8 Pro, Windows 8 Enterprise, Windows RT
Windows Server 2012	Foundation, Essentials, Standard, Datacenter
Windows 8.1	Windows 8.1, Windows 8.1 Pro, Windows 8.1 Enterprise, Windows RT 8.1
Windows Server 2012 R2	Foundation, Essentials, Standard, Datacenter
Windows 10	Home, Pro, Pro Education, Enterprise, Education, IoT Core, Mobile, Mobile Enterprise
Windows Server 2016	Essentials, Standard, Datacenter, Multipoint Premium Server, Storage Server, Hyper-V Server



# O sistema operacional Windows

## GUI do Windows

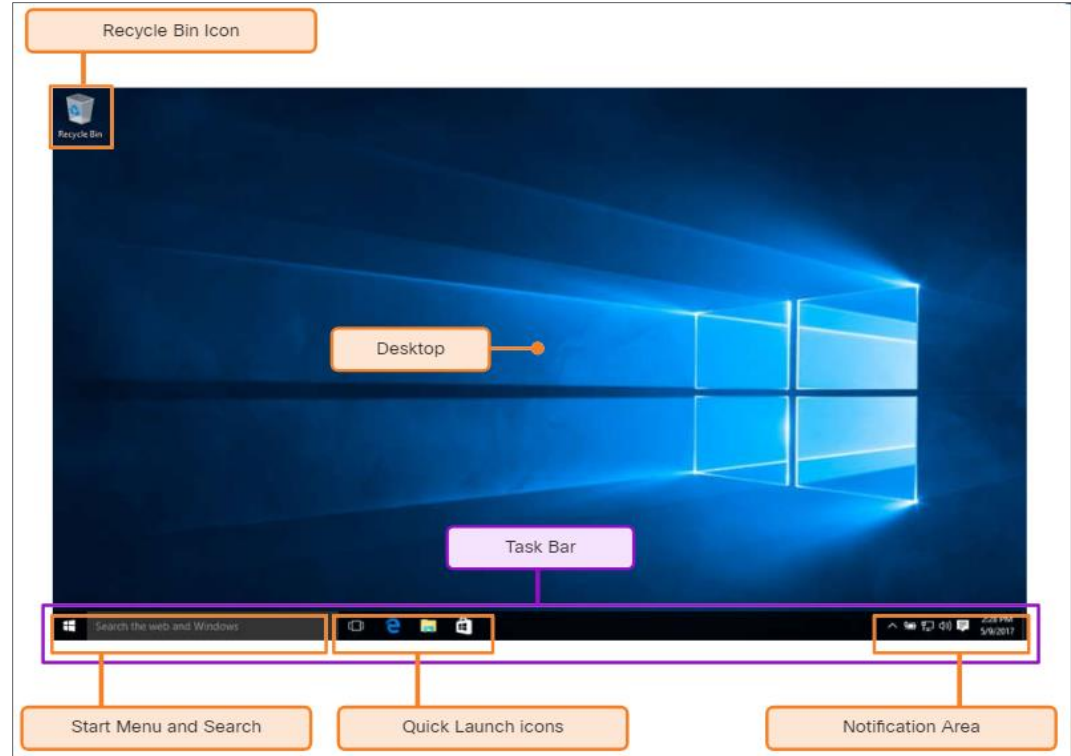
- O Windows tem uma interface gráfica do usuário (GUI) para que os usuários trabalhem com arquivos de dados e software.
- A GUI tem uma área principal que é conhecida como Área de Trabalho. A área de trabalho pode ser personalizada com várias cores e imagens de fundo.
- O Windows oferece suporte a vários usuários, para que cada usuário possa personalizar a Área de Trabalho.
- A Área de Trabalho pode armazenar arquivos, pastas, atalhos para locais e programas e aplicativos.
- A área de trabalho também tem um ícone de lixeira, onde os arquivos são armazenados quando o usuário os exclui. Os arquivos podem ser restaurados da lixeira ou a lixeira pode ser esvaziada de arquivos, o que realmente os exclui.



# O sistema operacional Windows

## GUI do Windows (cont.)

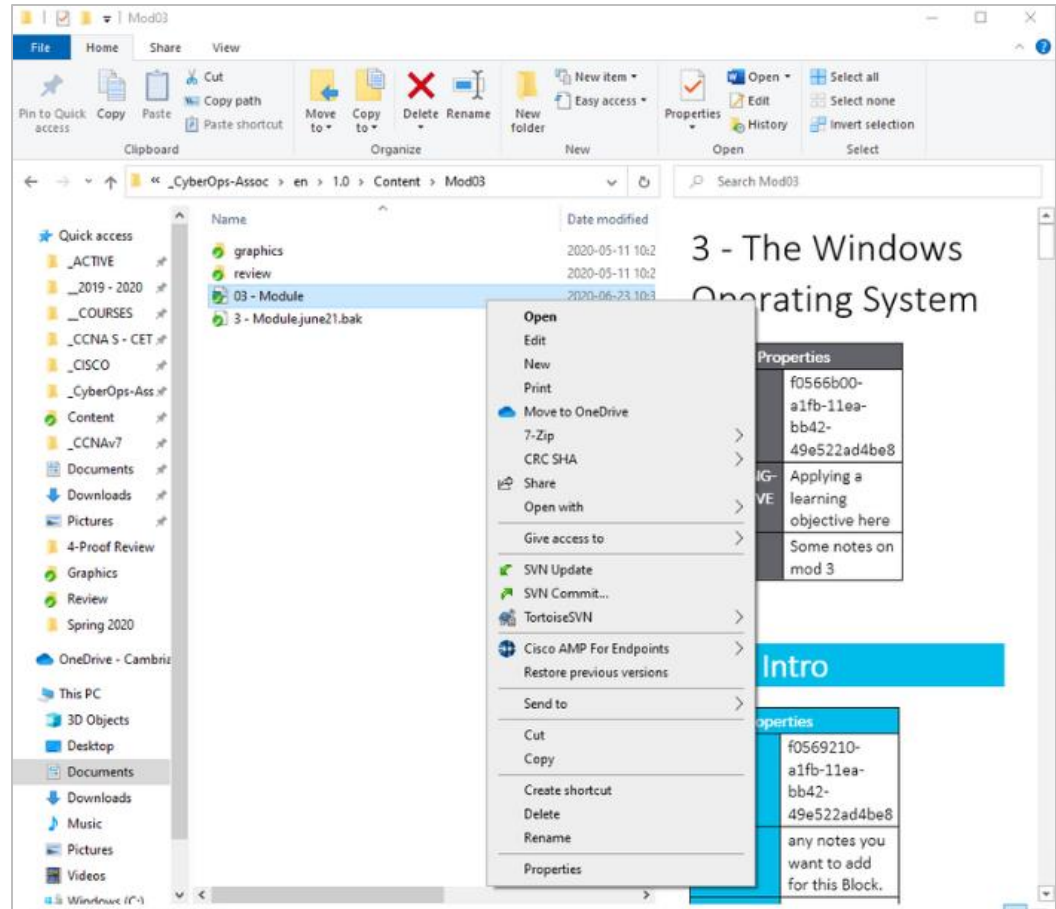
- Na parte inferior da área de trabalho, está a Barra de Tarefas.
- À esquerda está o menu Iniciar que é usado para acessar todos os programas instalados, opções de configuração e o recurso de pesquisa.
- No centro, os usuários colocam ícones de inicialização rápida que executam programas específicos ou abrem pastas específicas quando clicam.
- À direita da Barra de Tarefas está a área de notificação. A área de notificação mostra, em resumo, a funcionalidade de muitos programas e recursos diferentes.



# O sistema operacional Windows

## GUI do Windows (cont.)

- Principalmente clicar com o botão direito do mouse em um ícone trará funções adicionais que podem ser usadas. Esta lista é conhecida como o Menu de Contexto.
- Há Menus de Contexto para os ícones na área de notificação, para ícones de inicialização rápida, ícones de configuração do sistema e para arquivos e pastas.
- O Menu de Contexto fornece muitas das funções mais comumente usadas clicando em.



# Vulnerabilidades do sistema operacional

- Os sistemas operacionais consistem em milhões de linhas de código. Com todo esse código vem vulnerabilidades.
- Uma vulnerabilidade é alguma falha ou fraqueza que pode ser explorada por um invasor para reduzir a viabilidade das informações de um computador.
- Para tirar proveito de uma vulnerabilidade do sistema operacional, o invasor deve usar uma técnica ou uma ferramenta para explorar a vulnerabilidade.
- O invasor pode então usar a vulnerabilidade para fazer com que o computador atue de forma fora do design pretendido.
- Em geral, o objetivo é obter controle não autorizado do computador, alterar permissões ou manipular ou roubar dados.

## Vulnerabilidades do sistema operacional (Cont.)

A tabela a seguir lista algumas recomendações comuns de segurança do sistema operacional Windows:

Recomendação	Descrição
<b>Proteção contra vírus ou malware</b>	<ul style="list-style-type: none"><li>• Por padrão, o Windows usa o Windows Defender para proteção contra malware.</li><li>• O Windows Defender fornece um conjunto de ferramentas de proteção incorporadas ao sistema.</li><li>• Se o Windows Defender estiver desativado, o sistema ficará mais vulnerável a ataques e malware.</li></ul>
<b>Serviços desconhecidos ou não gerenciados</b>	<ul style="list-style-type: none"><li>• Há muitos serviços que funcionam nos bastidores.</li><li>• É importante certificar-se de que cada serviço é identificável e seguro.</li><li>• Com um serviço desconhecido em execução em segundo plano, o computador pode ficar vulnerável a ataques.</li></ul>
<b>Criptografia</b>	<ul style="list-style-type: none"><li>• Quando os dados não são criptografados, eles podem ser facilmente coletados e explorados.</li><li>• Isso não é importante apenas para computadores desktop, mas especialmente dispositivos móveis.</li></ul>
<b>Política de segurança</b>	<ul style="list-style-type: none"><li>• Uma boa política de segurança deve ser configurada e seguida.</li><li>• Muitas configurações no controle de Diretiva de Segurança do Windows podem impedir ataques.</li></ul>

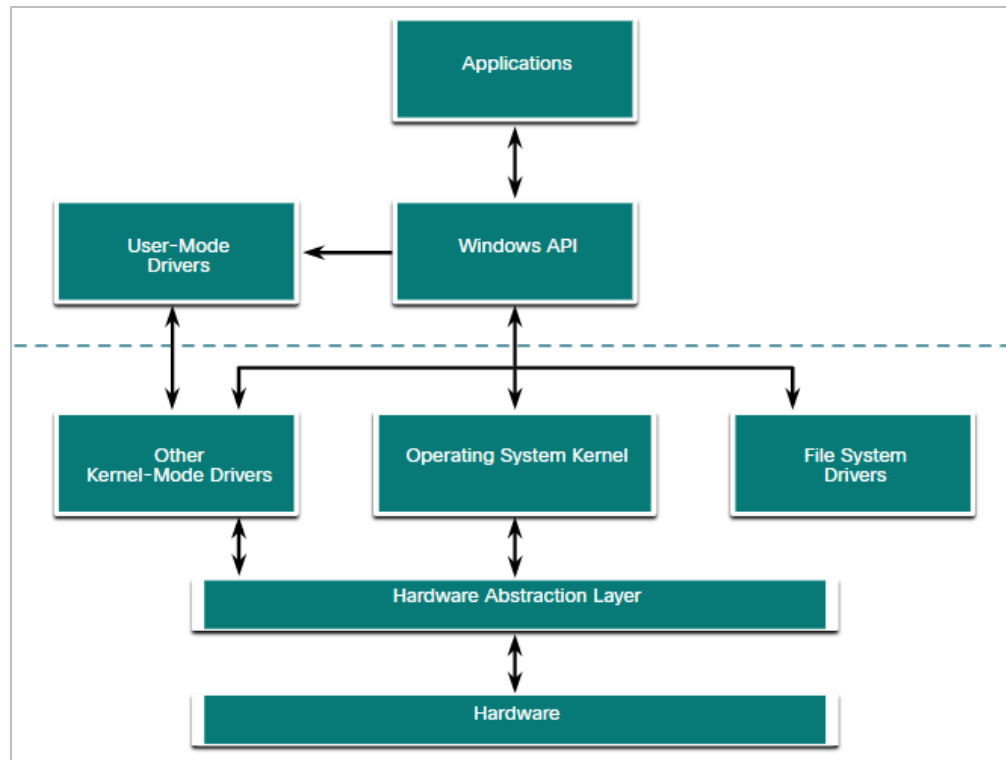
## Vulnerabilidades do sistema operacional (Cont.)

Recomendação	Descrição
<b>Firewall</b>	<ul style="list-style-type: none"><li>• Por padrão, o Windows usa o Firewall do Windows para limitar a comunicação com dispositivos na rede. Com o tempo, as regras podem não se aplicar mais.</li><li>• É importante revisar periodicamente as configurações do firewall para garantir que as regras ainda são aplicáveis e remover as que não se aplicam mais.</li></ul>
<b>Permissões de arquivo e compartilhamento</b>	<ul style="list-style-type: none"><li>• Essas permissões devem ser definidas corretamente. É fácil dar ao grupo “Todos” Controle Total, mas isso permite que todas as pessoas acessem todos os arquivos.</li><li>• É melhor fornecer a cada usuário ou grupo as permissões mínimas necessárias para todos os arquivos e pastas.</li></ul>
<b>Senha fraca ou sem senha</b>	<ul style="list-style-type: none"><li>• Muitas pessoas escolhem senhas fracas ou não usam nenhuma senha.</li><li>• É especialmente importante certificar-se de que todas as contas, especialmente a conta de Administrador, têm uma senha muito forte.</li></ul>
<b>Login como Administrador</b>	<ul style="list-style-type: none"><li>• Quando um usuário faz login como administrador, qualquer programa executado terá os privilégios dessa conta.</li><li>• É melhor fazer login como um Usuário Padrão e usar apenas a senha de administrador para realizar determinadas tarefas.</li></ul>

## 3.2 Arquitetura e operações do Windows

# Camada de abstração de hardware

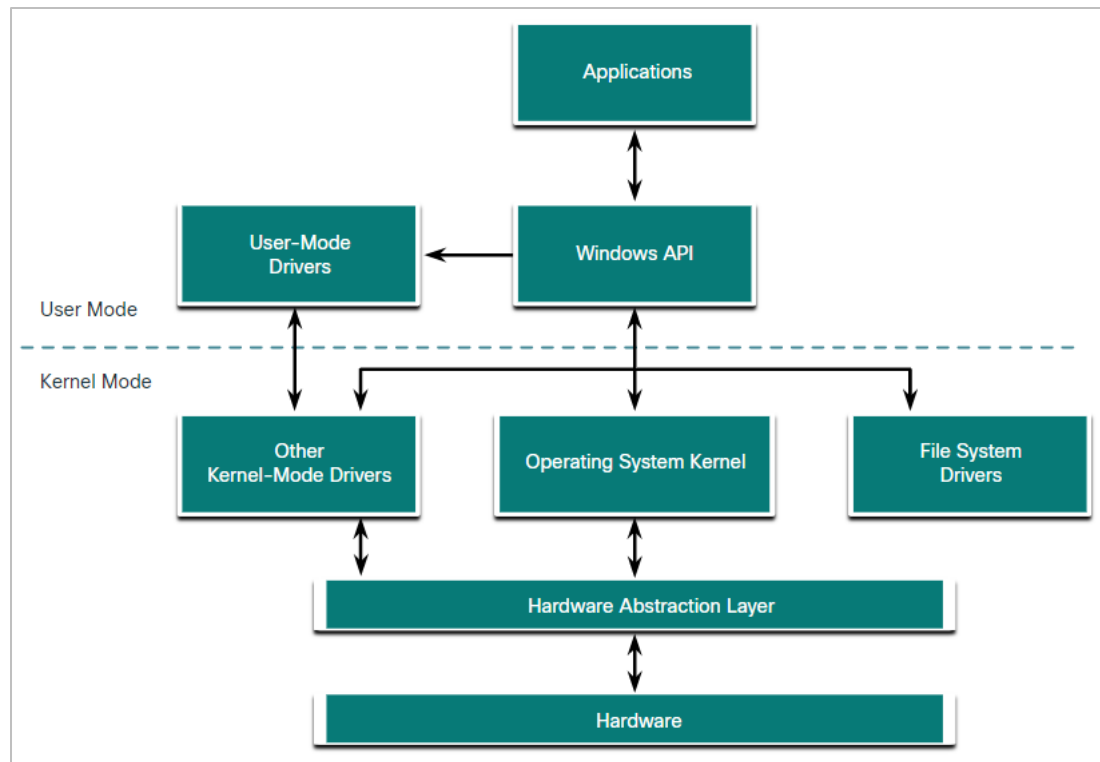
- Uma camada de abstração de hardware (HAL) é um software que lida com toda a comunicação entre o hardware e o kernel.
- O kernel é o núcleo do sistema operacional e tem controle sobre todo o computador.
- O kernel lida com todas as solicitações de entrada e saída, memória e todos os periféricos conectados ao computador.
- A arquitetura básica do Windows é mostrada na figura.





# Modo de usuário e modo de kernel

- Os dois modos diferentes em que uma CPU opera quando o computador tem o Windows instalado são o modo de usuário e o modo kernel.
- Os aplicativos instalados são executados no modo de usuário e o código do sistema operacional é executado no modo kernel.
- Todo o código que é executado no modo kernel usa o mesmo espaço de endereço.
- Quando o código de modo de usuário é executado, ele é concedido seu próprio espaço de endereço restrito pelo kernel, juntamente com um processo criado especificamente para o aplicativo.



## Sistemas de arquivos do Windows

Um sistema de arquivos é uma forma de organizar as informações na mídia de armazenamento. A tabela a seguir lista os sistemas de arquivos suportados pelo Windows:

Sistema de Arquivos Windows	Descrição
<b>exFAT</b>	<ul style="list-style-type: none"><li>• Este é um sistema de arquivos simples suportado por muitos sistemas operacionais diferentes.</li><li>• FAT tem limitações para o número de partições, tamanhos de partições e tamanhos de arquivo que ele pode endereçar, portanto, ele não é mais usado para discos rígidos ou unidades de estado sólido.</li><li>• Tanto o FAT16 quanto o FAT32 estão disponíveis para uso, sendo o FAT32 o mais comum, pois tem muito menos restrições do que o FAT16.</li></ul>
<b>Sistema de Arquivos Hierárquico Plus (HFS+)</b>	<ul style="list-style-type: none"><li>• Este sistema de arquivos é usado em computadores MAC OS X e permite nomes de arquivos muito mais longos, tamanhos de arquivo e tamanhos de partição.</li><li>• Embora não seja suportado pelo Windows sem software especial, o Windows é capaz de ler dados de partições HFS+.</li></ul>

## Sistemas de arquivos do Windows (Cont.)

Sistema de Arquivos Windows	Descrição
<b>Sistema de arquivos estendido (EXT)</b>	<ul style="list-style-type: none"><li>• Este sistema de arquivos é usado com computadores baseados em Linux.</li><li>• Embora não seja suportado pelo Windows, o Windows é capaz de ler dados de partições EXT com software especial.</li></ul>
<b>New Technology File System (NTFS)</b>	<ul style="list-style-type: none"><li>• Este é o sistema de arquivos mais comumente usado ao instalar o Windows. Todas as versões do Windows e Linux suportam NTFS.</li><li>• Computadores Mac-OS X só podem ler uma partição NTFS. Eles são capazes de gravar em uma partição NTFS depois de instalar drivers especiais.</li></ul>

## Sistemas de arquivos do Windows (Cont.)

A formatação NTFS cria estruturas importantes no disco para armazenamento de arquivos e tabelas para gravar os locais dos arquivos:

- **Sector de inicialização de partição:** Este é os primeiros 16 setores da unidade. Ele contém o local da tabela de arquivos mestre (MFT). Os últimos 16 setores contêm uma cópia do setor de inicialização.
- **Tabela de arquivos mestre (MFT):** Esta tabela contém os locais de todos os arquivos e diretórios na partição, incluindo atributos de arquivo, como informações de segurança e carimbos de data/hora.
- **Arquivos do sistema:** são arquivos ocultos que armazenam informações sobre outros volumes e atributos de arquivo.
- **Área de arquivo:** A área principal da partição onde os arquivos e diretórios são armazenados.

**Observação:** Ao formatar uma partição, os dados anteriores ainda podem ser recuperáveis porque nem todos os dados são completamente removidos. Recomenda-se executar um apagamento seguro em uma unidade que está sendo reutilizada. O apagamento seguro grava dados em toda a unidade várias vezes para garantir que não haja dados restantes.

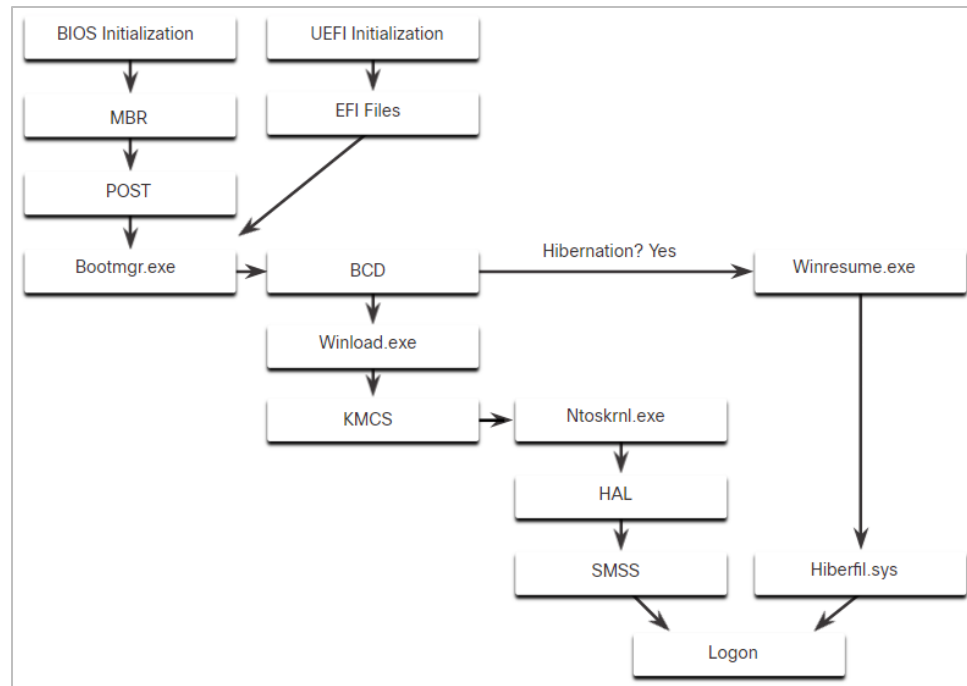
# Streams de dados alternativos

- NTFS armazena arquivos como uma série de atributos, como o nome do arquivo ou um carimbo de data/hora.
- Os dados que o arquivo contém são armazenados no atributo \$DATA, e é conhecido como um fluxo de dados.
- Usando NTFS, os fluxos de dados alternativos (ADSs) podem ser conectados ao arquivo.
- Um invasor pode armazenar código mal-intencionado dentro de um ADS que pode ser chamado de um arquivo diferente.
- No sistema de arquivos NTFS, um arquivo com um ADS é identificado após o nome do arquivo e dois pontos, por exemplo, **Testfile.txt:ADS**. Esse nome de arquivo indica que um ADS chamado ADS está associado ao arquivo chamado **Testfile.txt**.

```
C:\ADS> echo "Alternate Data Here" > Testfile.txt:ADS
C:\ADS> dir
Volume in drive C is Windows
Volume Serial Number is A606-CB1B
Directory of C:\ADS
2020-04-28  04:01 PM    <DIR>          .
2020-04-28  04:01 PM    <DIR>          ..
2020-04-28  04:01 PM                0 Testfile.txt
                1 File(s)                0 bytes
                2 Dir(s)  43,509,571,584 bytes free
C:\ADS> more < Testfile.txt:ADS
"Alternate Data Here"
C:\ADS> dir /r
Volume in drive C is Windows
Volume Serial Number is A606-CB1B
Directory of C:\ADS
2020-04-28  04:01 PM    <DIR>          .
2020-04-28  04:01 PM    <DIR>          ..
2020-04-28  04:01 PM                0 Testfile.txt
                24 Testfile.txt:ADS:$DATA
                1 File(s)                0 bytes
                2 Dir(s)  43,509,624,832 bytes free
C:\ADS>
```

# Processo de inicialização do Windows

- Muitas ações ocorrem entre o botão liga/desliga é pressionado e o Windows está totalmente carregado. Este é o processo de inicialização do Windows. Existem dois tipos de firmware de computador:
  - Sistema básico de entrada-saída (BIOS):** O processo começa com a fase de inicialização do BIOS na qual os dispositivos de hardware são inicializados e um POST é executado. Quando o disco do sistema é descoberto, o POST termina e procura o registro mestre de inicialização (MBR). O BIOS executa o código MBR e o sistema operacional começa a carregar.
  - UEFI (Unified Extensible Firmware Interface):** O firmware UEFI inicializa carregando arquivos de programa EFI (.efi) armazenados em uma partição de disco especial, conhecida como EFI System Partition (ESP).



## Processo de inicialização do Windows (Cont.)

- Se o firmware é BIOS ou UEFI, depois que uma instalação válida do Windows é localizada, o arquivo **Bootmgr.exe** é executado.
- **Bootmgr.exe** lê o banco de dados de configuração de inicialização (BCD).
- Se o computador estiver saindo da hibernação, o processo de inicialização continuará com **Winresume.exe**.
- Se o computador estiver sendo inicializado a partir de um início a frio, o arquivo **Winload.exe** será carregado.
- **Winload.exe** também usa KMCS (Kernel Mode Code Signing) para se certificar de que todos os drivers são assinados digitalmente.
- Depois que os drivers foram examinados, **Winload.exe** executa **Ntoskrnl.exe** que inicia o kernel do Windows e configura a HAL.

**Observação:** Um computador que usa UEFI armazena o código de inicialização no firmware. Isso ajuda a aumentar a segurança do computador no momento da inicialização porque o computador entra diretamente no modo protegido.

- o Ferramenta Msconfig e usada para exibir e alterar todas as opções de inicialização para o sistema. Ela é acessada clicando no ícone de configuração do sistema.



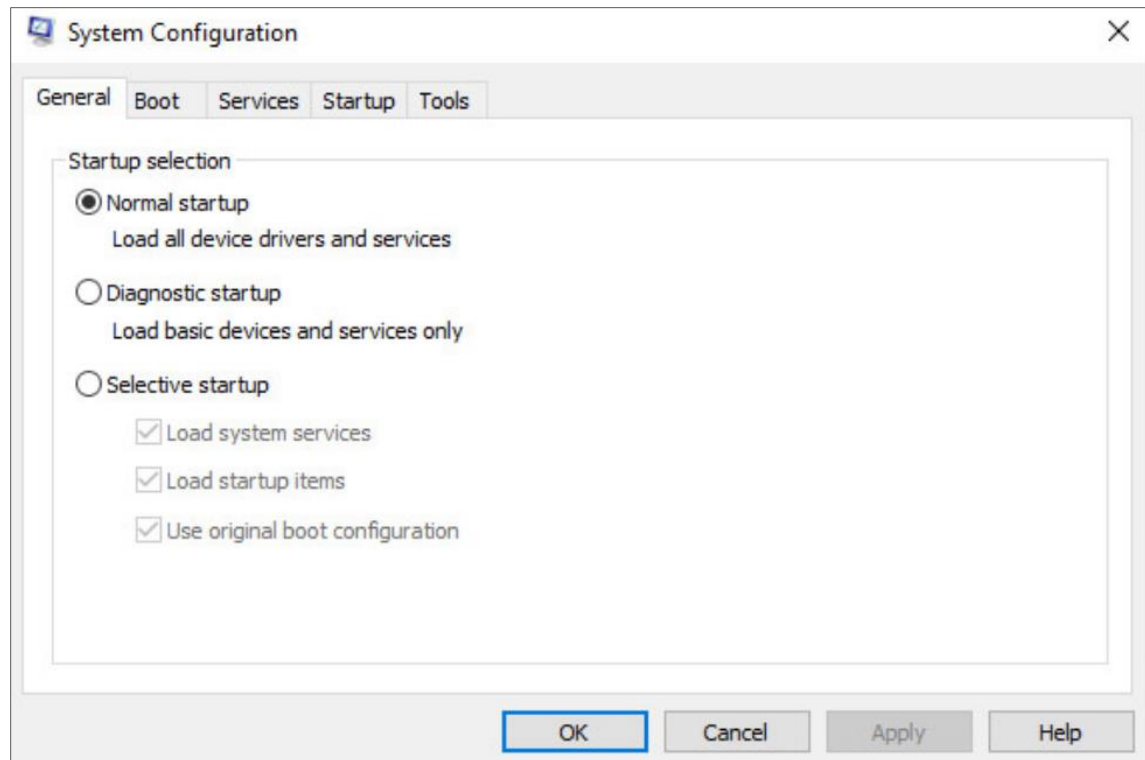
# Inicialização do Windows (Cont.)

Há cinco guias que contêm as opções de configuração.

## Geral

Três tipos de inicialização diferentes podem ser escolhidos aqui:

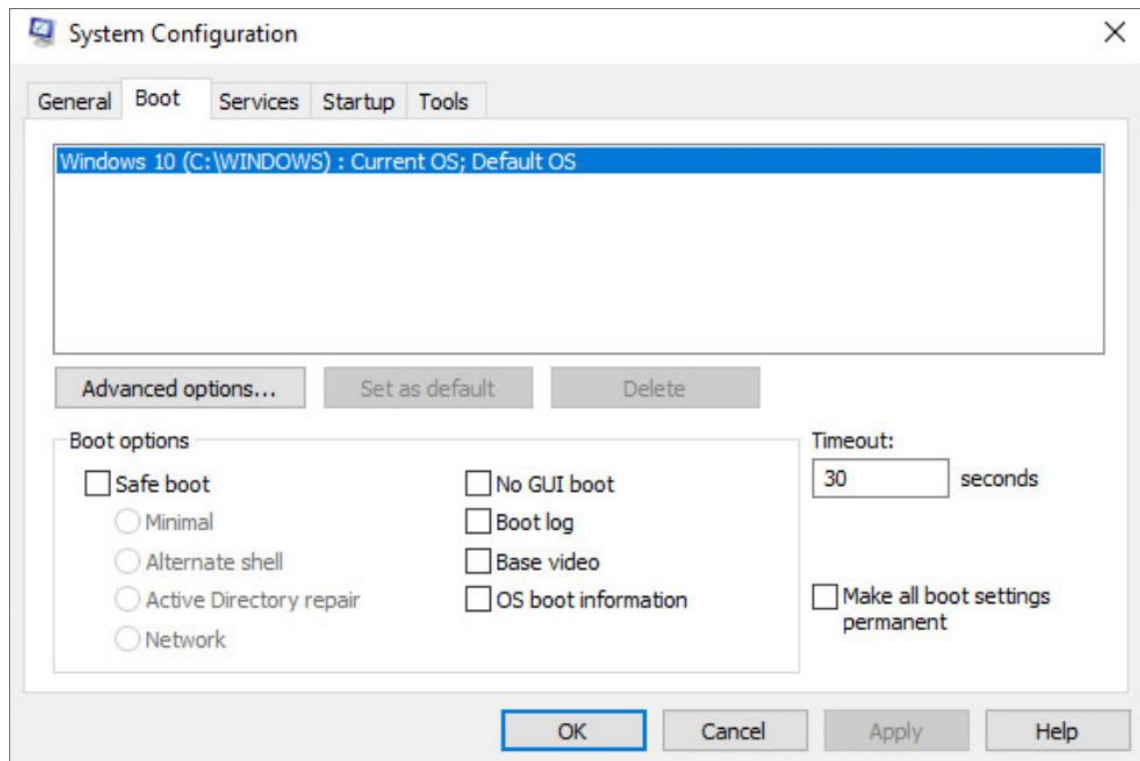
- Normal carrega todos os drivers e serviços.
- O diagnóstico carrega apenas drivers e serviços básicos.
- Seletivo permite que o usuário escolha o que carregar na inicialização.



# Inicialização do Windows (Cont.)

## Inicialização do Sistema

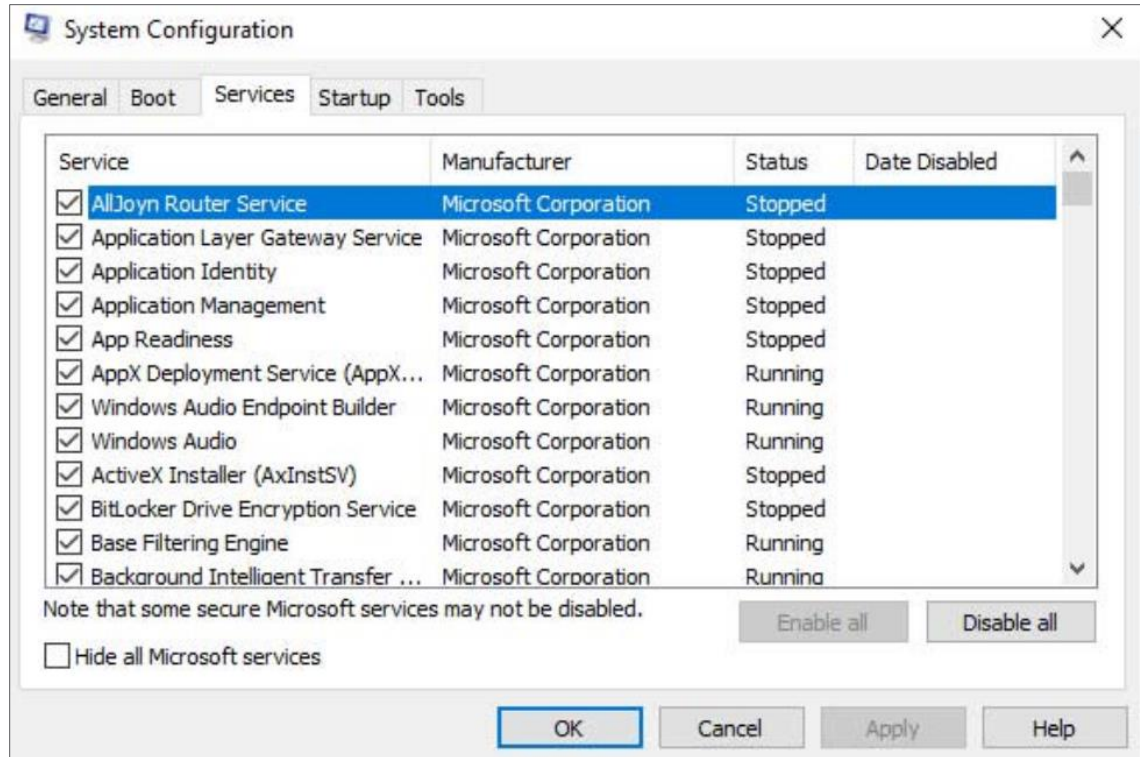
- Qualquer sistema operacional instalado pode ser escolhido aqui para iniciar.
- Existem também opções para a inicialização segura, que é usada para solucionar problemas de inicialização.



# Inicialização do Windows (Cont.)

## Serviços

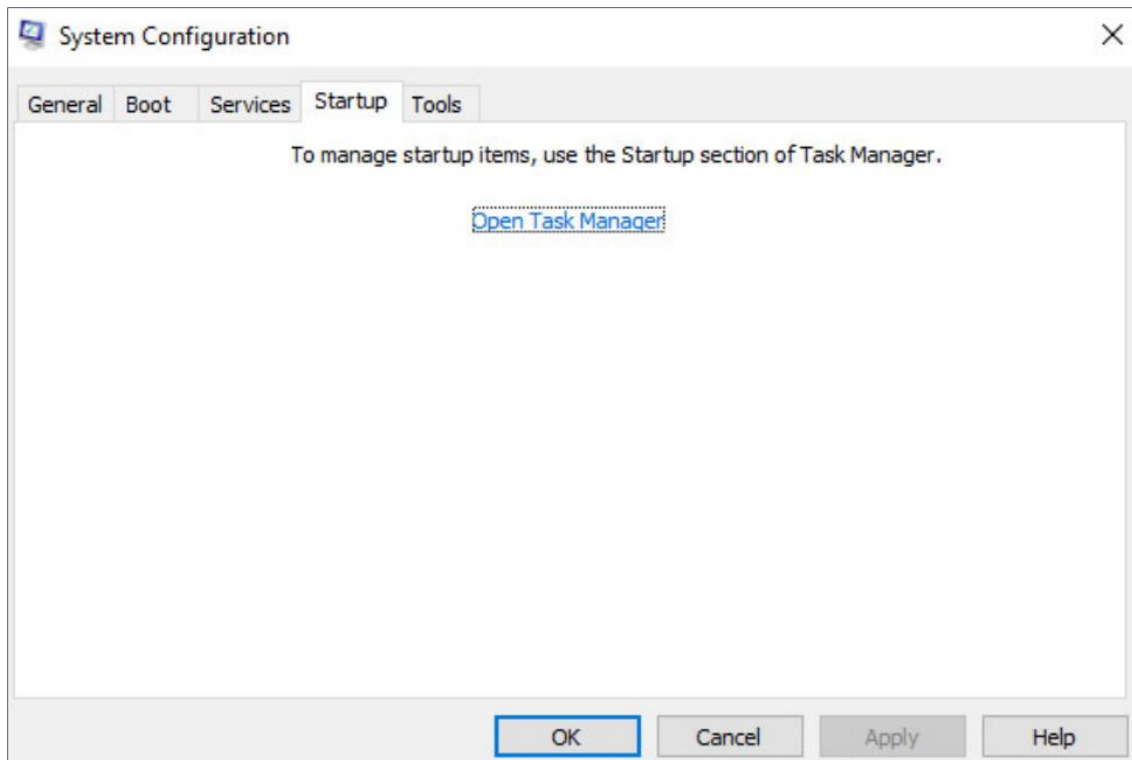
- Todos os serviços instalados estão listados aqui para que possam ser escolhidos para iniciar na inicialização.



# Inicialização do Windows (Cont.)

## Startup

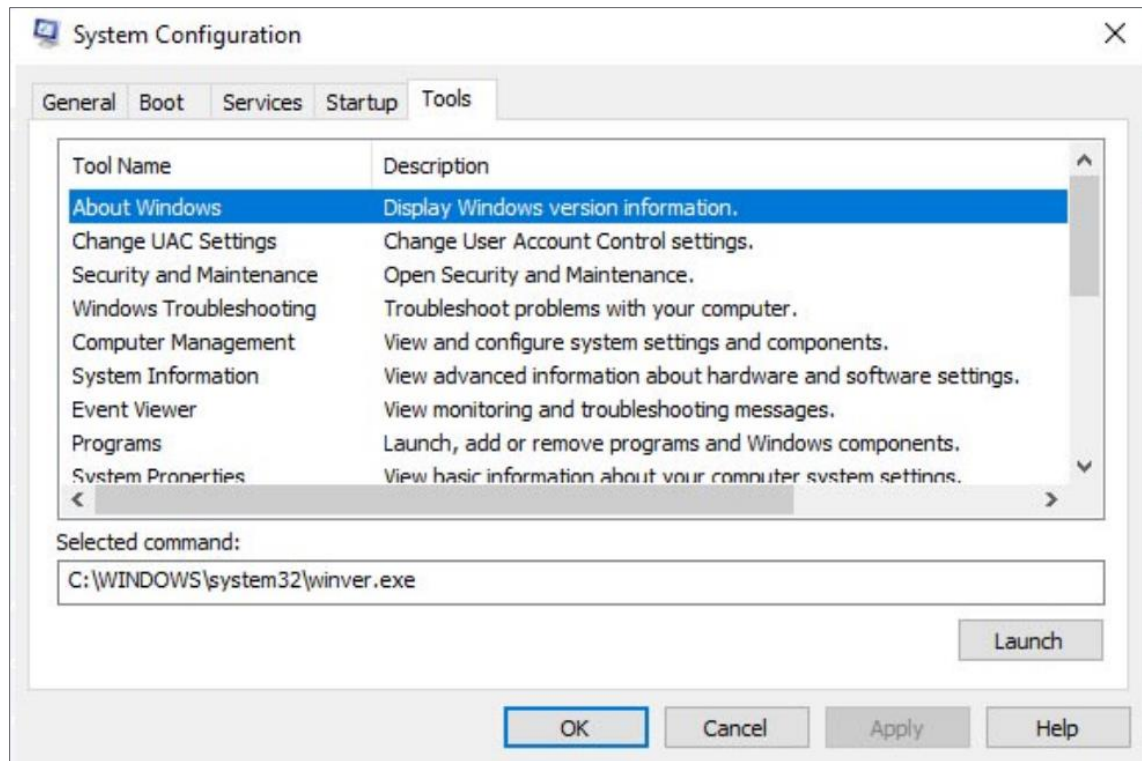
- Todos os aplicativos e serviços configurados para iniciar automaticamente na inicialização podem ser ativados ou desabilitados abrindo o gerenciador de tarefas a partir desta guia.



# Inicialização do Windows (Cont.)

## Ferramentas

- Muitas ferramentas comuns do sistema operacional podem ser iniciadas diretamente a partir desta guia.

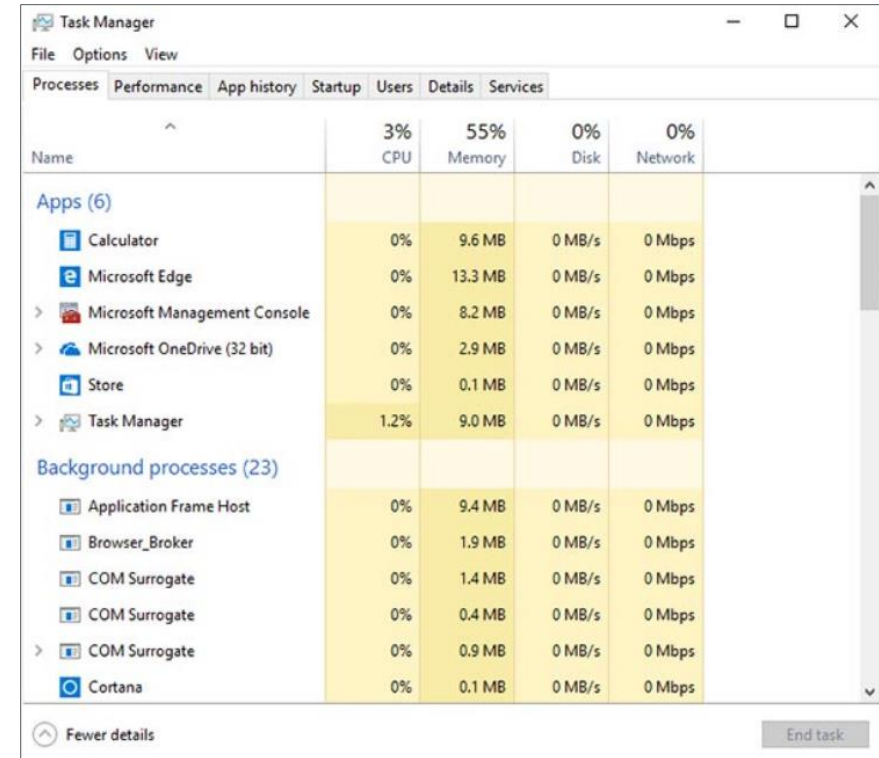


## Desligamento do Windows

- É sempre melhor executar um desligamento adequado para desligar o computador. O computador precisa de tempo para fechar cada aplicativo, desligar cada serviço e registrar quaisquer alterações de configuração antes que a energia seja perdida.
- Durante o desligamento, o computador fechará os aplicativos do modo de usuário primeiro, seguido pelos processos do modo kernel.
- Existem várias maneiras de desligar um computador Windows: Opções de energia do menu Iniciar, o **desligamento** comando da linha de comando e usando **Ctrl+Alt+Delete** clicando no ícone de energia.
- Existem três opções diferentes para escolher ao desligar o computador:
  - **Desligamento:** Desliga o computador (desliga).
  - **Reiniciar:** Reinicializa o computador (desligar e ligar).
  - **Hibernate:** registra o estado atual do ambiente do computador e do usuário e o armazena em um arquivo. A hibernação permite que o usuário continue de onde parou muito rapidamente com todos os seus arquivos e programas ainda abertos.

# Processos, threads e serviços

- Um aplicativo do Windows é composto de processos. Um processo é qualquer programa em execução no momento.
- Cada processo que é executado é composto de pelo menos um thread. Um thread é uma parte do processo que pode ser executado.
- Para configurar processos do Windows, procure o Gerenciador de Tarefas. A guia Processos do Gerenciador de Tarefas é mostrada na figura.
- Todos os threads dedicados a um processo estão contidos dentro do mesmo espaço de endereço, o que significa que esses threads podem não acessar o espaço de endereço de qualquer outro processo. Isso evita a corrupção de outros processos.

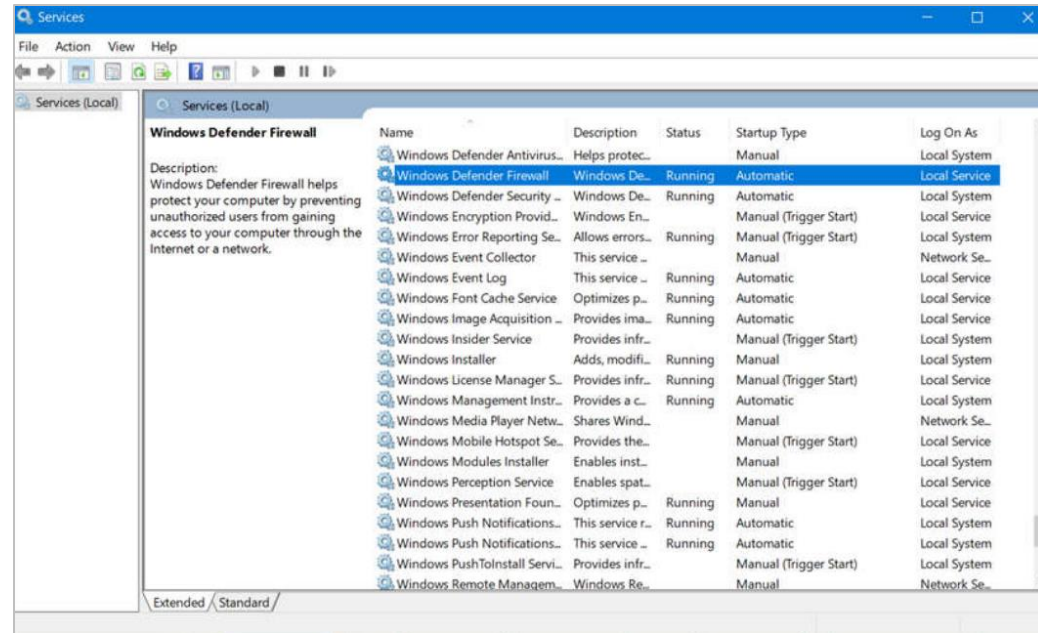


Name	3% CPU	55% Memory	0% Disk	0% Network
<strong>Apps (6)</strong>				
Calculator	0%	9.6 MB	0 MB/s	0 Mbps
Microsoft Edge	0%	13.3 MB	0 MB/s	0 Mbps
> Microsoft Management Console	0%	8.2 MB	0 MB/s	0 Mbps
> Microsoft OneDrive (32 bit)	0%	2.9 MB	0 MB/s	0 Mbps
Store	0%	0.1 MB	0 MB/s	0 Mbps
> Task Manager	1.2%	9.0 MB	0 MB/s	0 Mbps
<strong>Background processes (23)</strong>				
Application Frame Host	0%	9.4 MB	0 MB/s	0 Mbps
Browser_Broker	0%	1.9 MB	0 MB/s	0 Mbps
COM Surrogate	0%	1.4 MB	0 MB/s	0 Mbps
COM Surrogate	0%	0.4 MB	0 MB/s	0 Mbps
> COM Surrogate	0%	0.9 MB	0 MB/s	0 Mbps
Cortana	0%	0.1 MB	0 MB/s	0 Mbps



# Processos, threads e serviços (Cont.)

- Alguns dos processos executados pelo Windows são serviços. Estes são programas que são executados em segundo plano para suportar o sistema operativo e as aplicações.
- Os serviços fornecem funcionalidade de longa execução, como sem fio ou acesso a um servidor FTP.
- Para configurar os Serviços do Windows, procure serviços. O miniaplicativo do painel de controle dos Serviços do Windows é mostrado na figura.
- Tenha muito cuidado ao manipular as configurações desses serviços. Encerrar um serviço pode afetar negativamente aplicativos ou outros serviços.



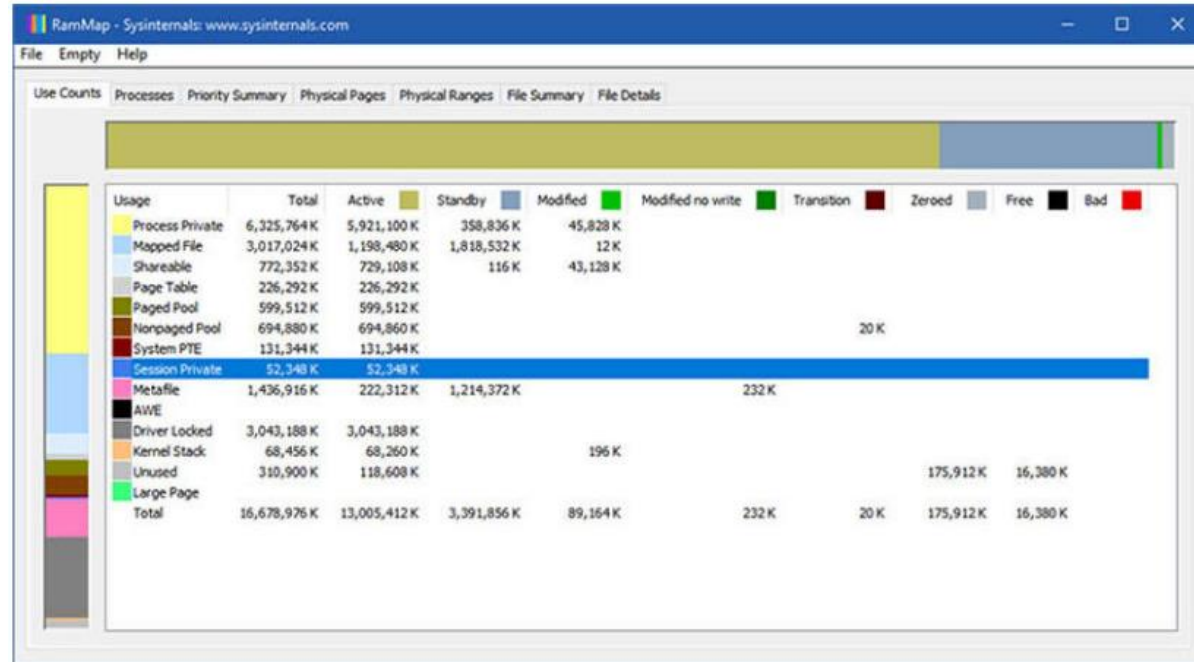


# Alocação de memória e controles

- O espaço de endereço virtual para um processo é o conjunto de endereços virtuais que o processo pode usar.
- O endereço virtual não é o local físico real na memória, mas uma entrada em uma tabela de página que é usada para traduzir o endereço virtual para o endereço físico.
- Cada processo em um computador Windows de 32 bits suporta um espaço de endereço virtual que permite endereçar até 4 gigabytes.
- Cada processo num computador Windows de 64 bits suporta um espaço de endereço virtual de 8 terabytes.
- Cada processo de espaço do usuário é executado em um espaço de endereço privado, separado de outros processos de espaço do usuário.
- Quando o processo de espaço do usuário precisa acessar recursos do kernel, ele deve usar um identificador de processo.
- Como o processo de espaço do usuário não tem permissão para acessar diretamente esses recursos do kernel, o identificador do processo fornece o acesso necessário para o processo de espaço do usuário sem uma conexão direta com ele.

# Alocação de memória e controles (Cont.)

- Uma ferramenta poderosa para visualizar a alocação de memória é RAMMap, que é mostrado na figura.
- RAMMap faz parte do conjunto de ferramentas do Windows Sysinternals. Ele pode ser baixado da Microsoft.
- RAMMap fornece informações sobre como o Windows alocou memória do sistema para o kernel, processos, drivers e aplicativos.



# O Registro do Windows

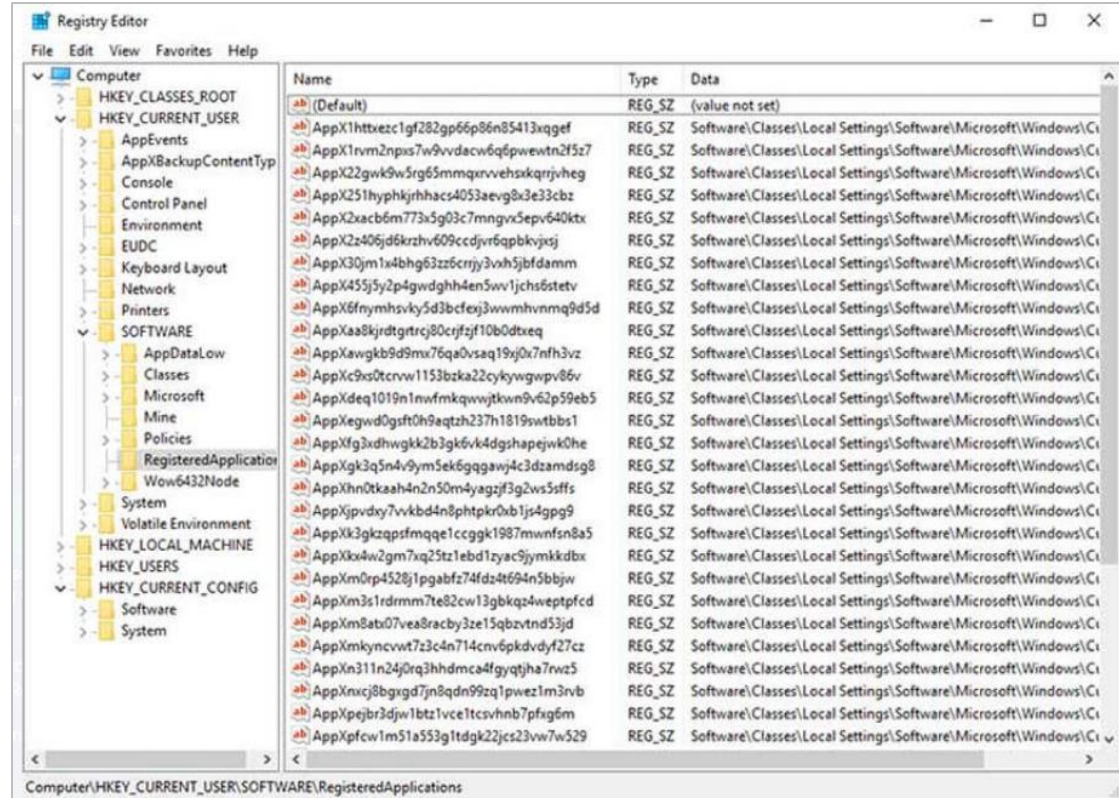
- O Windows armazena todas as informações sobre hardware, aplicativos, usuários e configurações do sistema em um banco de dados grande conhecido como o Registro.
- O registro é um banco de dados hierárquico onde o nível mais alto é conhecido como um ramo, abaixo que existem chaves, seguido por subchaves.
- Os valores armazenam dados e são armazenados nas chaves e subchaves. Uma chave do Registro pode ter até 512 níveis de profundidade.
- A tabela a seguir lista os cinco hives do registro do Windows:

Hive do Registro	Descrição
HKEY_CURRENT_USER (HKCU)	Contém informações sobre o usuário conectado no momento.
HKEY_USERS (HKU)	Contém informações relativas a todas as contas de usuário no host.
HKEY_CLASSES_ROOT (HKCR)	Contém informações sobre registros OLE (vinculação e incorporação de objetos). Ele permite que os usuários incorporem objetos de outros aplicativos em um único documento.
HKEY_LOCAL_MACHINE (HKLM)	Contém informações relacionadas ao sistema.
HKEY_CURRENT_CONFIG (HKCC)	Contém informações sobre o perfil de hardware atual.

# Arquitetura e operações do Windows

## O Registro do Windows (Cont.)

- Novas colmeias não podem ser criadas. As chaves do Registro e os valores nas seções podem ser criados, modificados ou excluídos por uma conta com privilégios administrativos.
- Como mostrado na figura, a ferramenta **regedit.exe** é usada para modificar o registro.
- Tenha muito cuidado ao usar esta ferramenta. Alterações menores no registro podem ter efeitos maciços ou mesmo catastróficos.



## O Registro do Windows (Cont.)

- A navegação no registro é muito semelhante ao explorador de arquivos do Windows.
- Use o painel esquerdo para navegar nas colmeias e na estrutura abaixo dele e use o painel direito para ver o conteúdo do item realçado no painel esquerdo.
- O caminho é exibido na parte inferior da janela para referência.
- As chaves do Registro podem conter uma subchave ou um valor. Os diferentes valores que as chaves podem conter são os seguintes:
  - **REG\_BINARY:** Números ou valores booleanos
  - **REG\_DWORD:** Números maiores que 32 bits ou dados brutos
  - **REG\_SZ:** Valores de string
- O registro também contém a atividade que um usuário executa durante o uso diário normal do computador.
- Isso inclui o histórico de dispositivos de hardware, incluindo todos os dispositivos que foram conectados ao computador, incluindo o nome, o fabricante e o número de série.

# Laboratório - Explorando processos, threads, manipuladores e registro do Windows

Neste laboratório, você completará os seguintes objetivos:

- Explore os processos, threads e manipuladores usando o Process Explorer no Sysinternals Suite.
- Use o Registro do Windows para alterar uma configuração.

## 3.3 Configuração e monitoramento do Windows

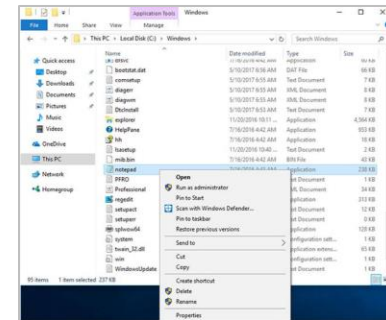
# Configuração e Monitoramento do Windows

## Executar como Administrador

- Como prática recomendada de segurança, não é aconselhável fazer logon no Windows usando a conta de Administrador ou uma conta com privilégios administrativos.
- Há duas maneiras diferentes de executar ou instalar um software que requer os privilégios do Administrador.

### Administrador

- Clique com o botão direito no comando no Explorador de Arquivos do Windows e escolha Executar como Administrador no Menu de Contexto.

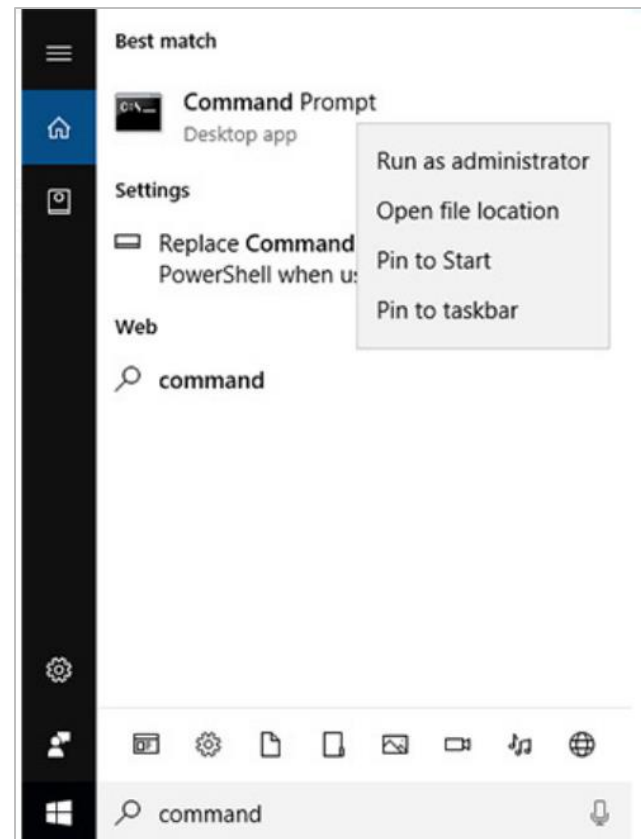




# Executar como Administrador (Cont.)

### Prompt de comando do administrador

- Procure por **comando**, clique com o botão direito do mouse no arquivo executável e escolha Executar como administrador no Menu de contexto.
- Cada comando executado a partir desta linha de comando será realizado com os privilégios de Administrador, incluindo a instalação de software.



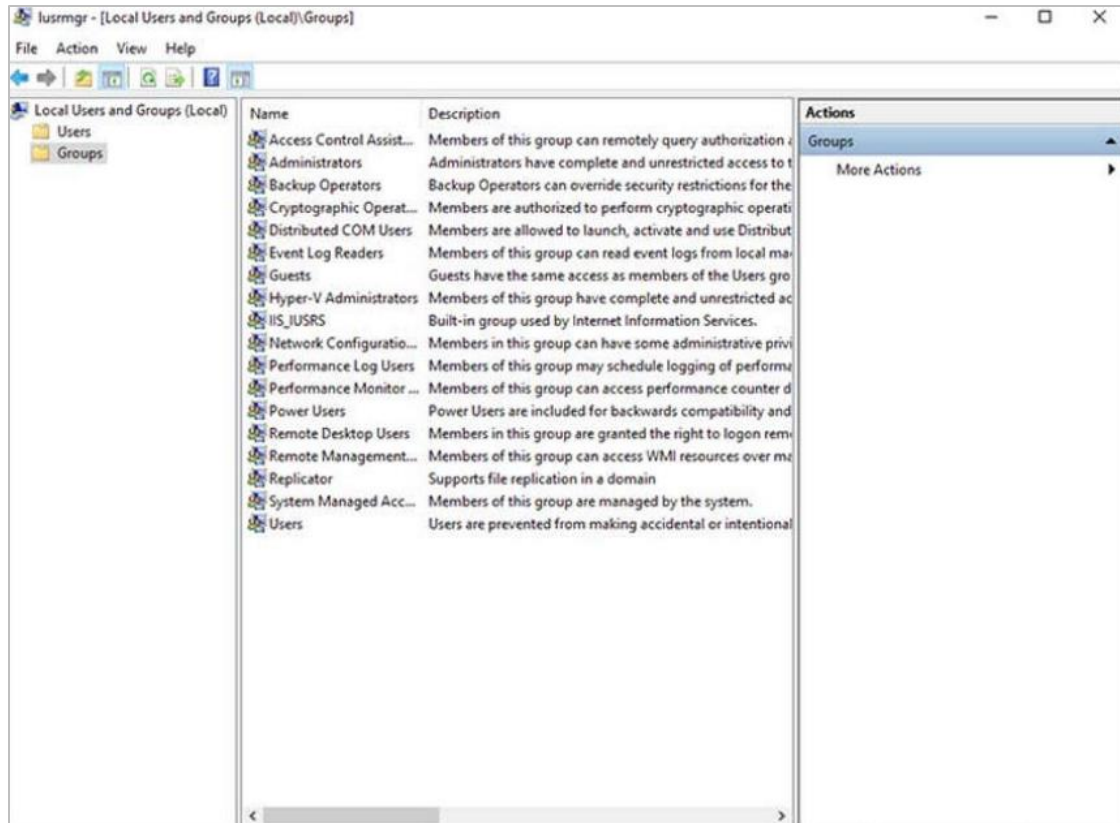
# Usuários e domínios locais

- Quando um novo computador é iniciado pela primeira vez ou o Windows estiver instalado, haverá um prompt para criar uma conta de usuário. Isso é conhecido como um usuário local.
- Esta conta contém todas as configurações de personalização, permissões de acesso, locais de arquivos e muitos outros dados específicos do usuário.
- Para facilitar a administração de usuários, o Windows usa grupos. Um grupo terá um nome e um conjunto específico de permissões associadas a ele.
- Quando um usuário é colocado em um grupo, as permissões desse grupo são dadas a esse usuário.
- Um usuário pode ser colocado em vários grupos para ser fornecido com muitas permissões diferentes. Quando as permissões se sobrepõem, certas permissões, como “negar explicitamente”, substituirão a permissão fornecida por um grupo diferente.
- Há muitos grupos de usuários diferentes incorporados no Windows que são usados para tarefas específicas.

# Configuração e monitoramento do Windows

## Usuários e domínios locais (Cont.)

- Usuários e grupos locais são gerenciados com o applet do painel de controle **lusrmgr.msc**, conforme mostrado na figura.
- O Windows também usa domínios para definir permissões. Um domínio é um tipo de serviço de rede onde todos os usuários, grupos, computadores, periféricos e configurações de segurança são armazenados e controlados por um banco de dados.



# CLI e PowerShell

- A interface de linha de comando (CLI) do Windows pode ser usada para executar programas, navegar no sistema de arquivos e gerenciar arquivos e pastas.
- Para abrir a CLI do Windows, procure **cmd.exe** e clique no programa. Estas são algumas coisas a serem lembradas ao usar a CLI:
  - Os nomes de arquivo e caminhos não diferenciam maiúsculas de minúsculas, por padrão.
  - Os dispositivos de armazenamento recebem uma letra para referência. Isto seguido por dois pontos e barra invertida (\).
  - Comandos que têm opções opcionais usam a barra (/) para delinear entre o comando e a opção switch.
  - Você pode usar a tecla **Tab** para completar automaticamente comandos quando diretórios ou arquivos são referenciados.
  - O Windows mantém um histórico dos comandos inseridos durante uma sessão da CLI. Acesse comandos inseridos anteriormente usando as teclas de seta para cima e para baixo.
  - Para alternar entre dispositivos de armazenamento, digite a letra do dispositivo, seguida de dois pontos e pressione **Enter**.

# CLI e PowerShell (Cond.)

- Outro ambiente, chamado Windows PowerShell, pode ser usado para criar scripts para automatizar tarefas que a CLI normal não consegue criar.
- O PowerShell também fornece uma CLI para iniciar comandos.
- O PowerShell é um programa integrado no Windows.
- Assim como a CLI, o PowerShell também pode ser executado com privilégios administrativos.
- Estes são os tipos de comandos que o PowerShell pode executar:
  - **cmdlets**- Esses comandos executam uma ação e retornam uma saída ou objeto para o próximo comando que será executado.
  - **Scripts do PowerShell**- São arquivos com uma extensão **.ps1** que contêm comandos do PowerShell executados.
  - **Funções do PowerShell**- São partes de código que podem ser referenciadas em um script.

# Configuração e Monitoramento do Windows CLI e PowerShell (Cond.)

- Para ver mais informações sobre o PowerShell e começar a usá-lo, digite **help**, conforme mostrado na saída do comando.
- Há quatro níveis de ajuda no Windows PowerShell:
  - **get-help** *PS comando* - Exibe ajuda básica para um comando
  - **get-help** *PS comando* [-examples] - Exibe ajuda básica para um comando com exemplos
  - **get-help** *PS comando* [-detailed] - Exibe ajuda detalhada para um comando com exemplos
  - **get-help** *PS comando* [-full] - Exibe todas as informações de ajuda de um comando com exemplos em maior profundidade

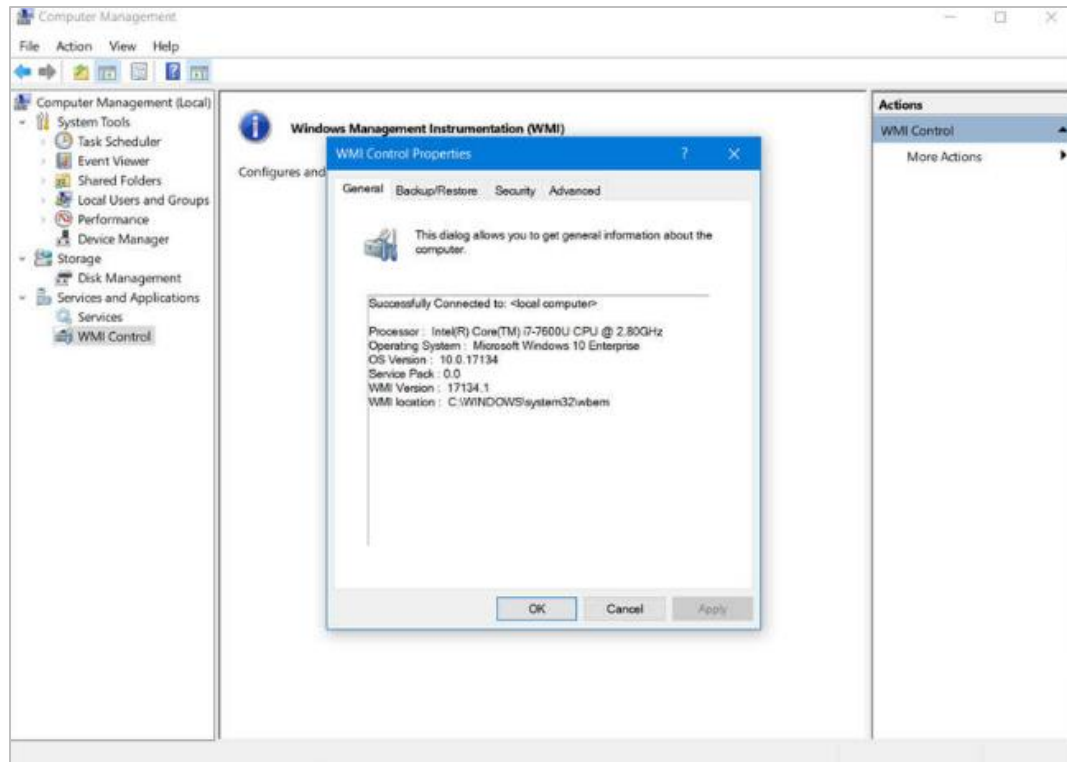
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\WINDOWS\system32> help
TOPIC
    Windows PowerShell Help System
SHORT DESCRIPTION
    Displays help about Windows PowerShell cmdlets and concepts.
LONG DESCRIPTION
    Windows PowerShell Help describes Windows PowerShell cmdlets,
    functions, scripts, and modules, and explains concepts, including
    the elements of the Windows PowerShell language.
    Windows PowerShell does not include help files, but you can read the
    help topics online, or use the Update-Help cmdlet to download help files
    to your computer and then use the Get-Help cmdlet to display the help
    topics at the command line.
    You can also use the Update-Help cmdlet to download updated help files
    as they are released so that your local help content is never obsolete.
    Without help files, Get-Help displays auto-generated help for cmdlets,
    functions, and scripts.
ONLINE HELP
    You can find help for Windows PowerShell online in the TechNet Library
    beginning at http://go.microsoft.com/fwlink/?LinkID=188518.
    To open online help for any cmdlet or function, type:
        Get-Help <cmdlet-name> -Online
UPDATE-HELP
    To download and install help files on your computer:
        1. Start Windows PowerShell with the "Run as administrator" option.
        2. Type:
            Update-Help
    After the help files are installed, you can use the Get-Help cmdlet to
    display the help topics. You can also use the Update-Help cmdlet to
    download updated help files so that your local help files are always
    up-to-date.
    For more information about the Update-Help cmdlet, type:
        Get-Help Update-Help -Online
-- More --
```

# Instrumentação de gerenciamento do Windows

- A Instrumentação de Gerenciamento do Windows (WMI) é usada para gerenciar computadores remotos.
- Ele pode recuperar informações sobre componentes de computador, estatísticas de hardware e software e monitorar a integridade de computadores remotos.
- Para abrir o controle WMI a partir do Painel de Controle, clique duas vezes em **Ferramentas Administrativas > Gerenciamento do Computador** para abrir a janela Gerenciamento do Computador, expanda a árvore **Serviços e Aplicativos** e clique com o botão direito do mouse no **ícone Controle WMI** Propriedades.

# Instrumentação de gerenciamento do Windows (Cont.)

- A janela Propriedades de Controle WMI é mostrada na figura. Quatro guias na janela Propriedades de Controle WMI são:
  - **Geral**- Informações resumidas sobre o computador local e o WMI
  - **Backup/Restore**- Permite backup manual de estatísticas coletadas pelo WMI
  - **Segurança**- Configurações para configurar quem tem acesso a diferentes estatísticas WMI
  - **Avançado**- Configurações para configurar o namespace padrão para WMI





# O Comando da Rede

- O comando **net** é usado na administração e manutenção do sistema operacional.
- O comando **net** suporta muitos subcomandos que o seguem e pode ser combinado com switches para focar na saída específica.
- Para ver uma lista de muitos comandos **net**, digite **net help** no prompt de comando.
- A saída do comando mostra os comandos que o comando **net** pode usar.
- Para ver ajuda detalhada sobre qualquer um dos comandos **net**, digite **C:\>net help**.

```
C:\> net help
The syntax of this command is:
NET HELP
command
-or-
NET command /HELP
Commands available are:
NET ACCOUNTS          NET HELPMSG          NET STATISTICS
NET COMPUTER          NET LOCALGROUP       NET STOP
NET CONFIG            NET PAUSE            NET TIME
NET CONTINUE          NET SESSION          NET USE
NET FILE              NET SHARE            NET USER
NET GROUP             NET START            NET VIEW
NET HELP
NET HELP NAMES explains different types of names in NET HELP syntax lines.
NET HELP SERVICES lists some of the services you can start.
NET HELP SYNTAX explains how to read NET HELP syntax lines.
NET HELP command | MORE displays Help one screen at a time.
C:\>
```

## O Comando da Rede (Cont.)

A tabela a seguir lista alguns comandos de rede comuns:

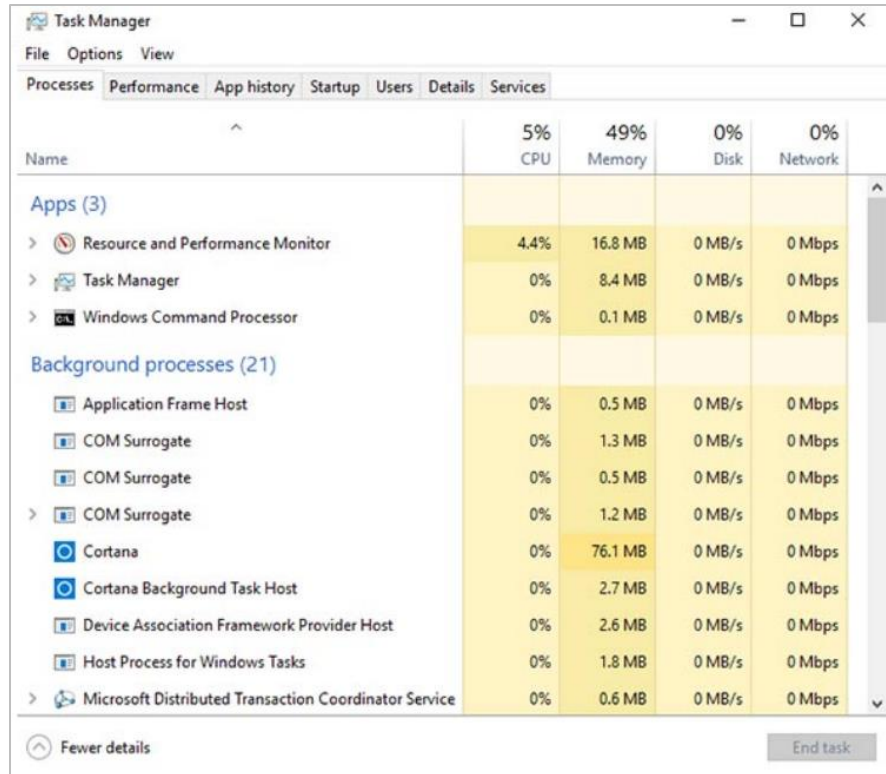
Comando	Descrição
<b>net accounts</b>	Define os requisitos de senha e logon para usuários
<b>net session</b>	Lista ou desconecta sessões entre um computador e outros computadores na rede
<b>net share</b>	Cria, remove ou gerencia recursos compartilhados
<b>net start</b>	Inicia um serviço de rede ou lista os serviços de rede em execução
<b>net stop</b>	Para um serviço de rede
<b>net use</b>	Conecta, desconecta e exibe informações sobre recursos de rede compartilhados
<b>net view</b>	Mostra uma lista de computadores e dispositivos de rede na rede

# Gerenciador de Tarefas e Monitor de Recursos

Existem duas ferramentas úteis para ajudar um administrador a compreender os diferentes aplicativos, serviços e processos que estão sendo executados em um computador Windows.

## Gerenciador de Tarefas

- O Gerenciador de Tarefas, que é mostrado na figura, fornece muitas informações sobre o software em execução e o desempenho geral do computador.
- O Gerenciador de Tarefas possui sete guias.



The screenshot shows the Windows Task Manager window with the 'Performance' tab selected. The window title is 'Task Manager'. The menu bar includes 'File', 'Options', and 'View'. The tabs at the top are 'Processes', 'Performance', 'App history', 'Startup', 'Users', 'Details', and 'Services'. The 'Performance' tab displays a table of system resource usage. The table has four columns: 'Name', 'CPU', 'Memory', 'Disk', and 'Network'. The 'CPU' column shows 5% usage, 'Memory' shows 49%, 'Disk' shows 0%, and 'Network' shows 0%. The table is divided into two sections: 'Apps (3)' and 'Background processes (21)'. The 'Apps (3)' section lists 'Resource and Performance Monitor' (4.4% CPU, 16.8 MB Memory), 'Task Manager' (0% CPU, 8.4 MB Memory), and 'Windows Command Processor' (0% CPU, 0.1 MB Memory). The 'Background processes (21)' section lists various system processes, including 'Application Frame Host', 'COM Surrogate', 'Cortana', 'Cortana Background Task Host', 'Device Association Framework Provider Host', 'Host Process for Windows Tasks', and 'Microsoft Distributed Transaction Coordinator Service'. The 'Cortana' process is highlighted with a yellow background, showing 76.1 MB of memory usage. At the bottom of the window, there is a 'Fewer details' button and an 'End task' button.

Name	5% CPU	49% Memory	0% Disk	0% Network
<b>Apps (3)</b>				
> Resource and Performance Monitor	4.4%	16.8 MB	0 MB/s	0 Mbps
> Task Manager	0%	8.4 MB	0 MB/s	0 Mbps
> Windows Command Processor	0%	0.1 MB	0 MB/s	0 Mbps
<b>Background processes (21)</b>				
Application Frame Host	0%	0.5 MB	0 MB/s	0 Mbps
COM Surrogate	0%	1.3 MB	0 MB/s	0 Mbps
COM Surrogate	0%	0.5 MB	0 MB/s	0 Mbps
> COM Surrogate	0%	1.2 MB	0 MB/s	0 Mbps
Cortana	0%	76.1 MB	0 MB/s	0 Mbps
Cortana Background Task Host	0%	2.7 MB	0 MB/s	0 Mbps
Device Association Framework Provider Host	0%	2.6 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks	0%	1.8 MB	0 MB/s	0 Mbps
> Microsoft Distributed Transaction Coordinator Service	0%	0.6 MB	0 MB/s	0 Mbps

## Gerenciador de Tarefas e Monitor de Recursos (Cont.)

A tabela a seguir descreve as sete guias no Gerenciador de Tarefas:

Guias do gerenciador de tarefas	Descrição
Processos	<ul style="list-style-type: none"><li>• Lista todos os programas e processos que estão em execução no momento.</li><li>• Exibe a utilização da CPU, da memória, do disco e da rede de cada processo.</li><li>• As propriedades podem ser examinadas ou terminadas se não estiver se comportando corretamente ou tiver parado.</li></ul>
Desempenho	<ul style="list-style-type: none"><li>• Uma exibição das estatísticas de desempenho fornece uma visão geral do desempenho da CPU, memória, disco e rede.</li><li>• Clicar em cada item no painel esquerdo irá mostrar estatísticas detalhadas desse item no painel direito.</li></ul>
Histórico do aplicativo	<ul style="list-style-type: none"><li>• O uso de recursos por aplicativo ao longo do tempo fornece informações sobre aplicativos que estão consumindo mais recursos.</li><li>• Clique em <b>Opções</b> e <b>Mostrar histórico de todos os processos</b> para ver o histórico de todos os processos executados desde que o computador foi iniciado.</li></ul>
Startup	<ul style="list-style-type: none"><li>• Todos os aplicativos e serviços que iniciam quando o computador é inicializado são mostrados nesta guia.</li><li>• Para desativar o início de um programa na inicialização, <b>clique com o botão direito do mouse</b> no item e escolha <b>Desativar</b>.</li></ul>

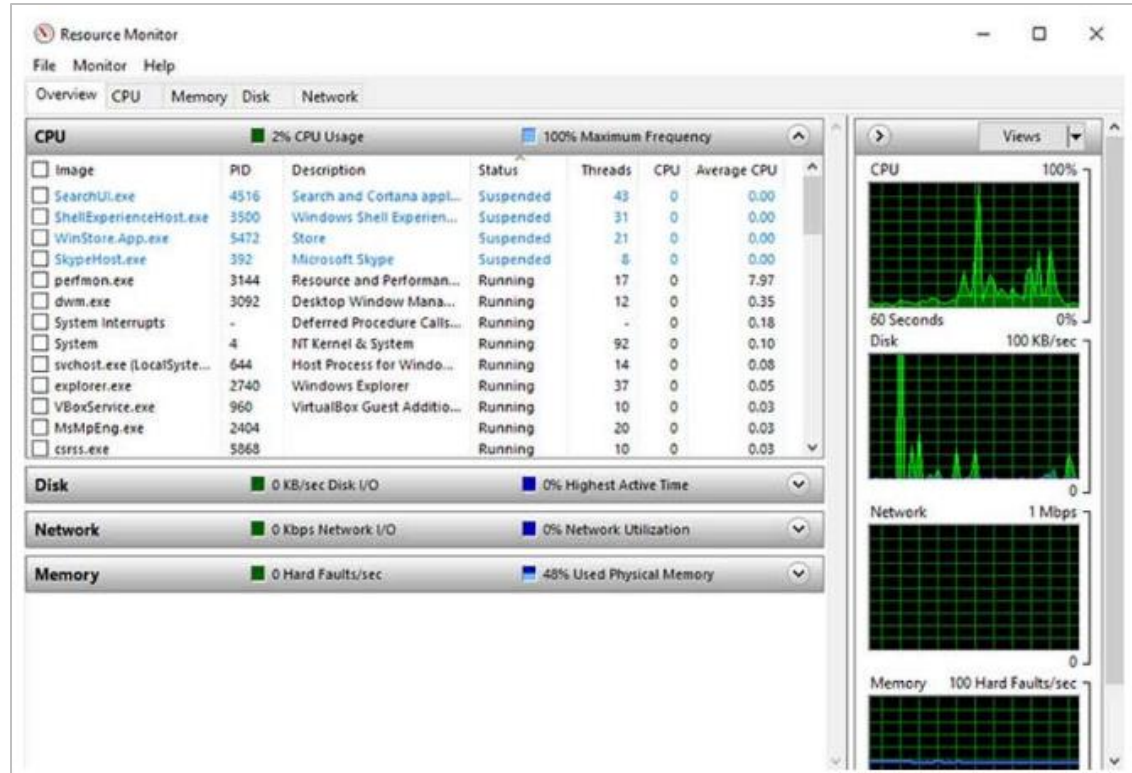
# Gerenciador de Tarefas e Monitor de Recursos (Cont.)

Guias do gerenciador de tarefas	Descrição
<b>Usuários</b>	<ul style="list-style-type: none"><li>• Todos os usuários que estão conectados ao computador e todos os recursos que os aplicativos e processos de cada usuário estão usando são mostrados nesta guia.</li><li>• Nesta guia, um administrador pode desconectar um usuário do computador.</li></ul>
<b>Detalhes</b>	<ul style="list-style-type: none"><li>• Esta guia fornece opções de gerenciamento adicionais para processos, como definir uma prioridade para que o processador dedique mais ou menos tempo a um processo.</li><li>• A afinidade da CPU também pode ser definida, o que determina qual núcleo ou CPU um programa usará.</li><li>• Um recurso útil chamado Analisar cadeia de espera mostra qualquer processo para o qual outro processo está aguardando. Esse recurso ajuda a determinar se um processo está simplesmente aguardando ou está parado.</li></ul>
<b>Serviços</b>	<ul style="list-style-type: none"><li>• Todos os serviços que são carregados são mostrados nesta guia.</li><li>• O ID do processo (PID) e uma breve descrição também são mostrados juntamente com o status de Executando ou Parado.</li><li>• Na parte inferior, há um botão para abrir o console Serviços que fornece gerenciamento adicional de serviços.</li></ul>

# Gerenciador de Tarefas e Monitor de Recursos (Cont.)

## Monitor de recursos

- Quando informações mais detalhadas sobre o uso de recursos são necessárias, o Monitor de recursos pode ser usado.
- Ao procurar o motivo pelo qual um computador pode estar agindo de forma irregular, o Monitor de Recursos pode ajudar a encontrar a origem do problema.
- O Monitor de Recursos tem Cinco guias.



## Gerenciador de Tarefas e Monitor de Recursos (Cont.)

A tabela a seguir descreve as cinco guias do Monitor de Recursos:

Guias do Monitor de Recursos	Descrição
Visão geral	A guia exibe o uso geral de cada recurso.
CPU	<ul style="list-style-type: none"><li>• O PID, o número de threads, que o processo está usando e o uso médio da CPU de cada processo é mostrado.</li><li>• Informações adicionais sobre quaisquer serviços e os identificadores e módulos associados podem ser vistas expandindo as linhas inferiores.</li></ul>
Memória	Todas as informações estatísticas sobre como cada processo usa memória são mostradas nesta guia e uma visão geral do uso de toda a RAM é mostrada abaixo da linha Processos.
Disco	Todos os processos que estão usando um disco são mostrados nesta guia, com estatísticas de leitura/gravação e uma visão geral de cada dispositivo de armazenamento.
Captura de dados	<ul style="list-style-type: none"><li>• Todos os processos que estão usando a rede são mostrados nesta guia, com estatísticas de leitura/gravação.</li><li>• É muito útil ao tentar determinar quais aplicativos e processos estão se comunicando pela rede. Além disso, informe se um processo não autorizado está acessando a rede.</li></ul>

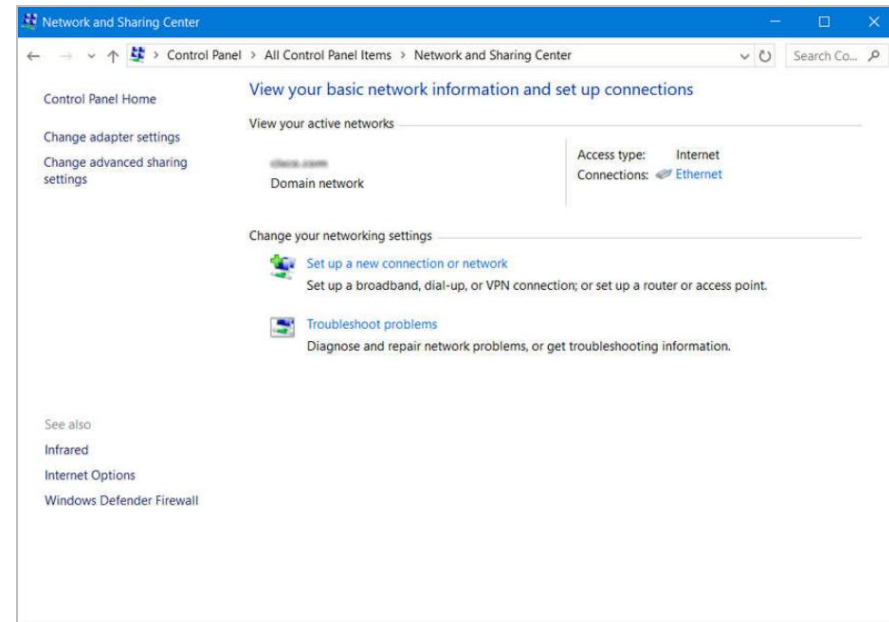
# Configuração e monitoramento do Windows

## Redes

- Um dos recursos mais importantes de qualquer sistema operacional é a capacidade do computador se conectar a uma rede.
- Para configurar as propriedades de rede do Windows e testar as configurações de rede, o Centro de Rede e Compartilhamento é usado.

### Central de Rede e Compartilhamento

- Ele é usado para verificar ou criar conexões de rede, configurar o compartilhamento de rede e alterar as configurações do adaptador de rede.
- A visualização inicial mostra uma visão geral da rede ativa.
- Na janela, você pode ver o Grupo Doméstico ao qual o computador pertence ou criar um caso ainda não faça parte de um Grupo Doméstico. Observe que o Grupo Doméstico foi removido do Windows 10 na versão 1803.





# Configuração e monitoramento do Windows

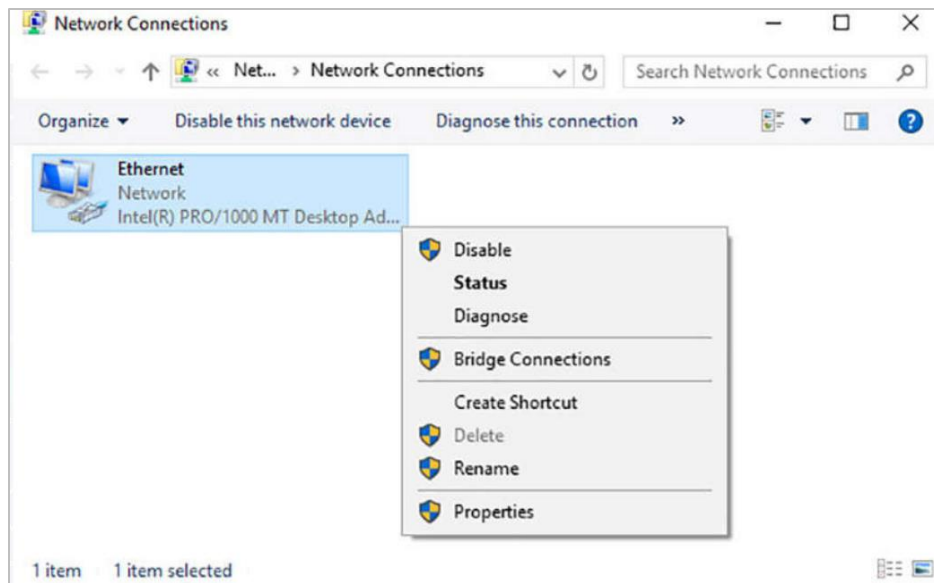
## Redes (Cont.)

### Alterar as configurações do adaptador

- Para configurar um adaptador de rede, escolha **Alterar configurações do adaptador** no Centro de Rede e Compartilhamento para mostrar todas as conexões de rede disponíveis. Selecione o adaptador a ser configurado.
- A seguir estão os passos para alterar um adaptador Ethernet para adquirir seu endereço IPv4 automaticamente da rede:

### Etapa 1: Propriedades do adaptador de acesso

Clique com o botão direito do mouse no adaptador que deseja configurar e escolha **Propriedades**, conforme mostrado na figura.

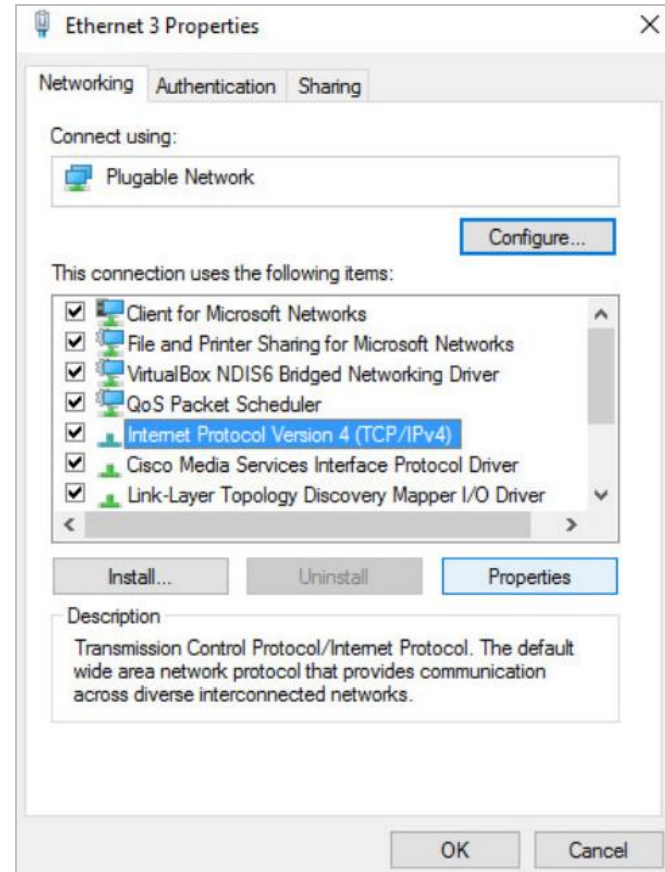


# Configuração e monitoramento do Windows

## Redes (Cont.)

### Etapa 2: Acessar propriedades de TCP/IPv4

- Esta conexão usa o **protocolo Internet versão 4 (TCP/IPv4)** ou o **protocolo Internet versão 6 (TCP/IPv6)** dependendo da versão que o usuário deseja usar.
- Na figura, IPv4 está sendo selecionado.

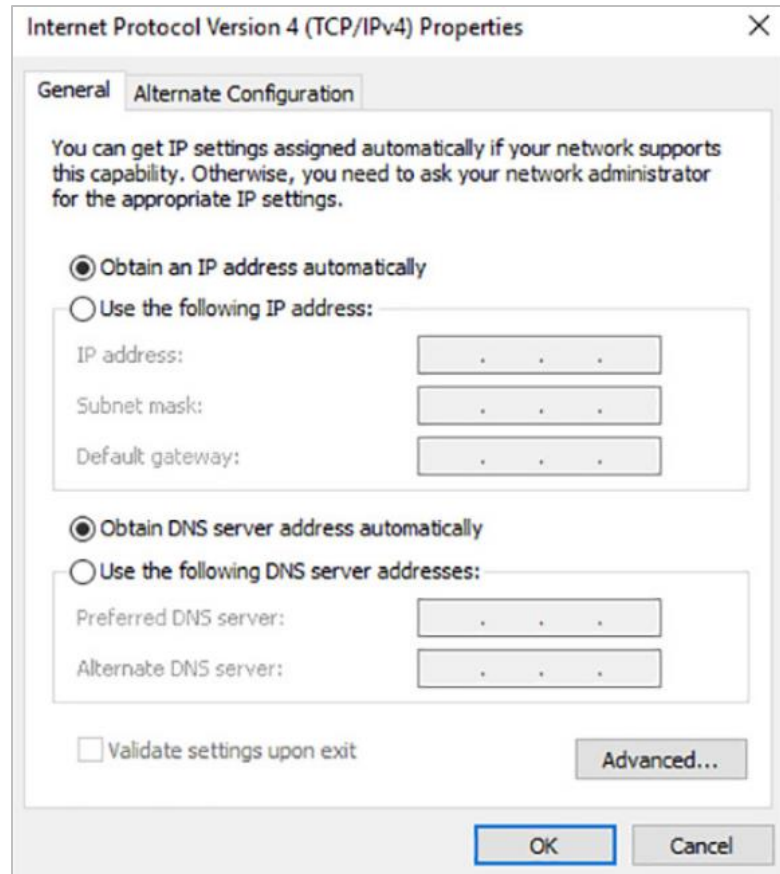


# Configuração e monitoramento do Windows

## Redes (Cont.)

### Etapa 3: Alterar configurações

- Clique em **Propriedades** para configurar o adaptador.
- Na caixa de diálogo **Propriedades**, escolha **Obter um endereço automaticamente** se houver um servidor DHCP disponível na rede ou se o usuário desejar configurar o endereçamento manualmente, preencha o endereço, a sub-rede, o gateway padrão e os servidores DNS.
- Clique em **OK** para aceitar as alterações.
- Você também pode usar a ferramenta **netsh.exe** para configurar parâmetros de rede a partir de um prompt de comando.
- Este programa pode exibir e modificar a configuração de rede.
- Digite **netsh/?** no prompt de comando para ver uma lista de todas as opções.



## Redes (Cont.)

### nslookup e netstat

- O Sistema de Nomes de Domínio (DNS) também deve ser testado porque é essencial encontrar o endereço dos hosts traduzindo-o a partir de um nome, como uma URL.
- Use o comando **nslookup** para testar o DNS.
- Digite **nslookup cisco.com** no prompt de comando para localizar o endereço do servidor Web Cisco. Se o endereço for retornado, o DNS está funcionando corretamente.
- Digite **netstat** na linha de comando para ver detalhes das conexões de rede ativas.

```
C:\Users\USER>netstat

Active Connections


```

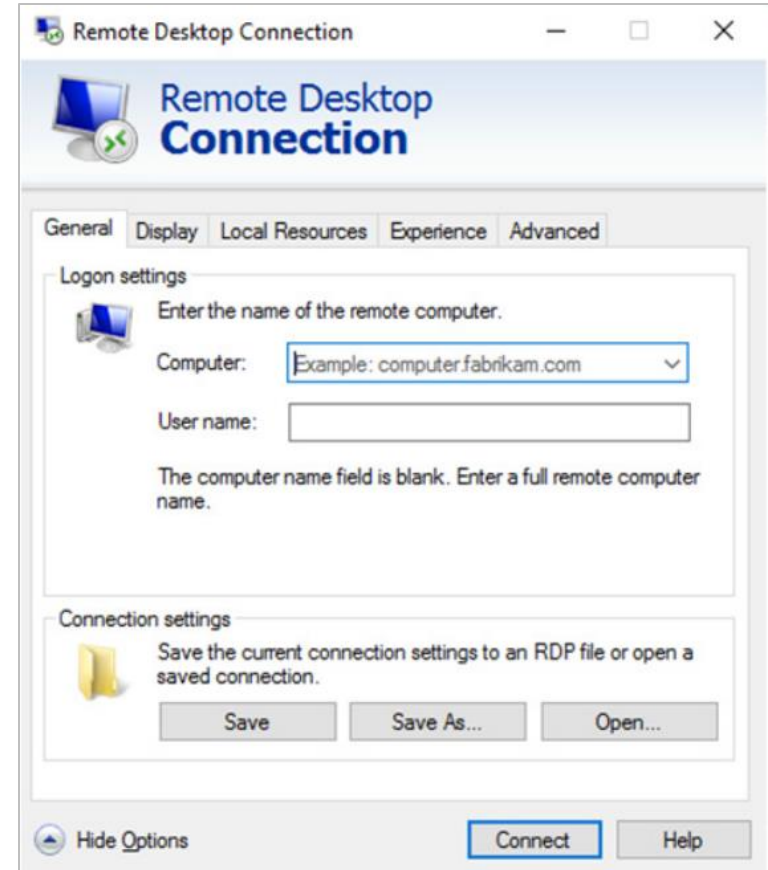
Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:3030	USER-VGFFA:58652	ESTABLISHED
TCP	127.0.0.1:3030	USER-VGFFA:62114	ESTABLISHED
TCP	127.0.0.1:3030	USER-VGFFA:62480	TIME_WAIT
TCP	127.0.0.1:3030	USER-VGFFA:62481	TIME_WAIT
TCP	127.0.0.1:3030	USER-VGFFA:62484	TIME_WAIT

# Acessando recursos de rede

- O Windows usa a rede para muitos aplicativos diferentes, como serviços da Web, de email e de arquivo.
- O protocolo Server Message Block (SMB) é usado para compartilhar recursos de rede. Ele é usado principalmente para acessar arquivos em hosts remotos.
- O formato UNC (Universal Naming Convention) é usado para se conectar a recursos como **\\servername\sharename\file**.
- No UNC, servername é o servidor que está hospedando o recurso. O nome do compartilhamento é a raiz da pasta no sistema de arquivos no host remoto, enquanto o arquivo é o recurso que o host local está tentando encontrar.
- Ao compartilhar recursos na rede, a área do sistema de arquivos que será compartilhada precisará ser identificada. O controle de acesso pode ser aplicado aos arquivos para restringir usuários e grupos a funções específicas.
- Há também compartilhamentos especiais que são criados automaticamente pelo Windows. Essas ações são chamadas de ações administrativas e são identificadas por um cifrão (\$) que vem após o nome da ação.

# Acessando Recursos de Rede (Cond.)

- Além de acessar compartilhamentos em hosts remotos, o usuário também pode fazer login em um host remoto e manipular esse computador, como se fosse local, para fazer alterações de configuração, instalar software ou solucionar um problema.
- No Windows, esse recurso usa o protocolo RDP (Remote Desktop Protocol). A janela Remote Desktop Connection é mostrada na figura.
- Como o Protocolo de Área de Trabalho Remota (RDP) foi projetado para permitir que usuários remotos controlem hosts individuais, ele é um alvo natural para atores de ameaças.



## Servidor Windows

- A maioria das instalações do Windows são executadas como instalações de área de trabalho em desktops e laptops.
- Há outra edição do Windows que é usada principalmente em data centers chamados Windows Server. Esta é uma família de produtos Microsoft que começou com o Windows Server 2003.
- O Windows Server hospeda muitos serviços diferentes e pode desempenhar funções diferentes dentro de uma empresa.
- Estes são alguns dos serviços que o Windows Server fornece:
  - **Serviços de rede:** DNS, DHCP, serviços de terminal, controlador de rede e virtualização de rede Hyper-V
  - **Serviços de Arquivo:** SMB, NFS e DFS
  - **Serviços Web:** FTP, HTTP e HTTPS
  - **Gerenciamento:** diretiva de grupo e controle de serviços de domínio do Active Directory

**Nota:** Embora exista um Windows Server 2000, é considerada uma versão cliente do Windows NT 5.0. O Windows Server 2003 é um servidor baseado no NT 5.2 e inicia uma nova família de versões do Windows Server.

## Laboratório - Criar contas de usuário

Neste laboratório, você criará e modificará contas de usuário no Windows.



# Laboratório - Usando o Windows PowerShell

Neste laboratório, você explorará algumas das funções do PowerShell.

# Laboratório de configuração e monitoramento do Windows - Gerenciador de tarefas do Windows

Neste laboratório, você vai explorar o Gerenciador de Tarefas e administrar processos nele.

# Laboratório - Monitorar e gerenciar recursos do sistema no Windows

Neste laboratório, você usará ferramentas administrativas para monitorar e gerenciar recursos do sistema.

# 3.4 Segurança do Windows

# O Comando netstat

- O comando **netstat** é usado para procurar conexões de entrada ou saída que não estão autorizadas.
- O comando **netstat** exibirá todas as conexões TCP ativas.
- Examinando essas conexões, é possível determinar os programas que estão escutando conexões que não estão autorizadas.
- Quando um programa é suspeito de ser malware, o processo pode ser encerrado com o Gerenciador de Tarefas e o software de remoção de malware pode ser usado para limpar o computador.
- Para facilitar esse processo, as conexões podem ser vinculadas aos processos em execução que foram criados por eles no Gerenciador de Tarefas.

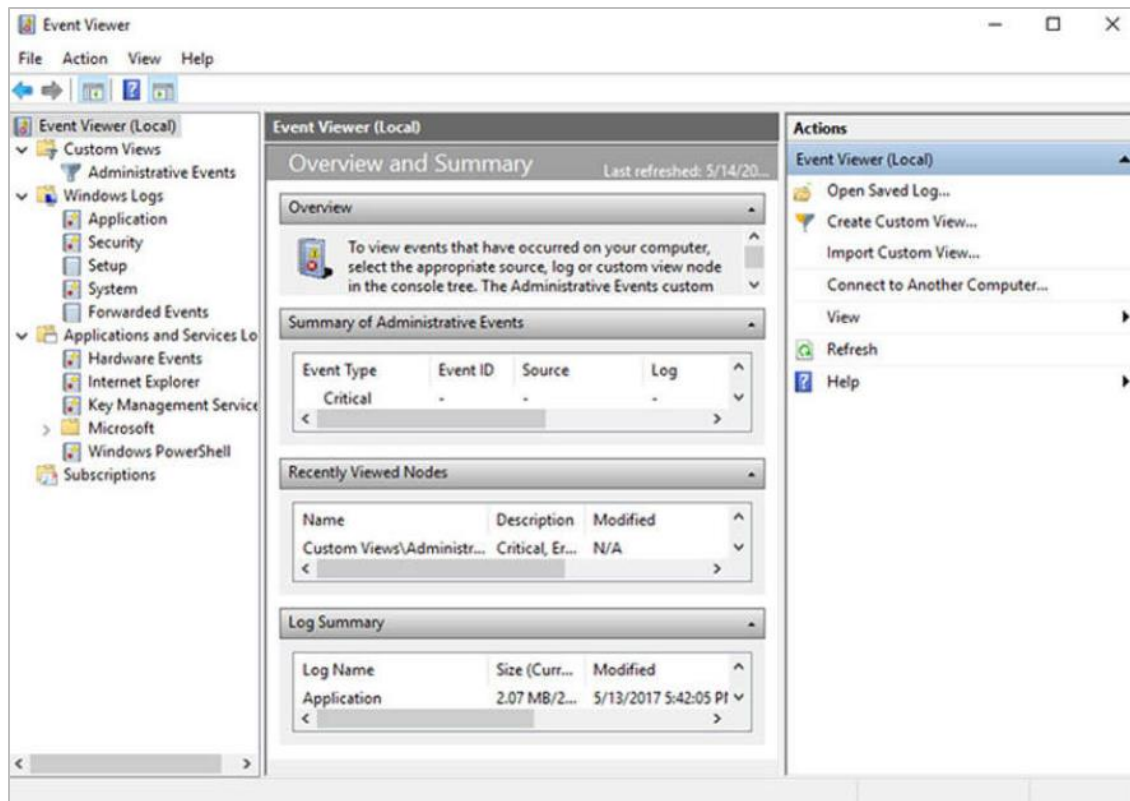
# O Comando netstat (Cont.)

- Para fazer isso, abra um prompt de comando com privilégios administrativos e digite o comando **netstat -abno**.
- Examinando as conexões TCP ativas, um analista deve ser capaz de determinar se há algum programa suspeito que esteja escutando conexões de entrada no host.
- Pode haver mais de um processo listado com o mesmo nome. Se esse for o caso, use o PID exclusivo para encontrar o processo correto. Para exibir os PIDs dos processos no Gerenciador de Tarefas, abra o Gerenciador de **Tarefas**, clique com o botão direito do mouse no cabeçalho da tabela e selecione **PID**.

```
Microsoft Windows [Version 10.0.18363.720]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32> netstat -abno
Active Connections
  Proto Local Address           Foreign Address         State       PID
  TCP    0.0.0.0:80               0.0.0.0:0               LISTENING   4
  Can not obtain ownership information
  TCP    0.0.0.0:135              0.0.0.0:0               LISTENING   952
  RpcSs
  [svchost.exe]
  TCP    0.0.0.0:445              0.0.0.0:0               LISTENING   4
  Can not obtain ownership information
  TCP    0.0.0.0:623              0.0.0.0:0               LISTENING   14660
  [LMS.exe]
  TCP    0.0.0.0:3389             0.0.0.0:0               LISTENING   1396
  TermService
  [svchost.exe]
  TCP    0.0.0.0:5040             0.0.0.0:0               LISTENING   9792
  CDPSvc
  [svchost.exe]
  TCP    0.0.0.0:5357             0.0.0.0:0               LISTENING   4
  Can not obtain ownership information
  TCP    0.0.0.0:5593             0.0.0.0:0               LISTENING   4
  Can not obtain ownership information
  TCP    0.0.0.0:8099             0.0.0.0:0               LISTENING   5248
  [SolarWinds TFTP Server.exe]
  TCP    0.0.0.0:16992             0.0.0.0:0               LISTENING   14660
```

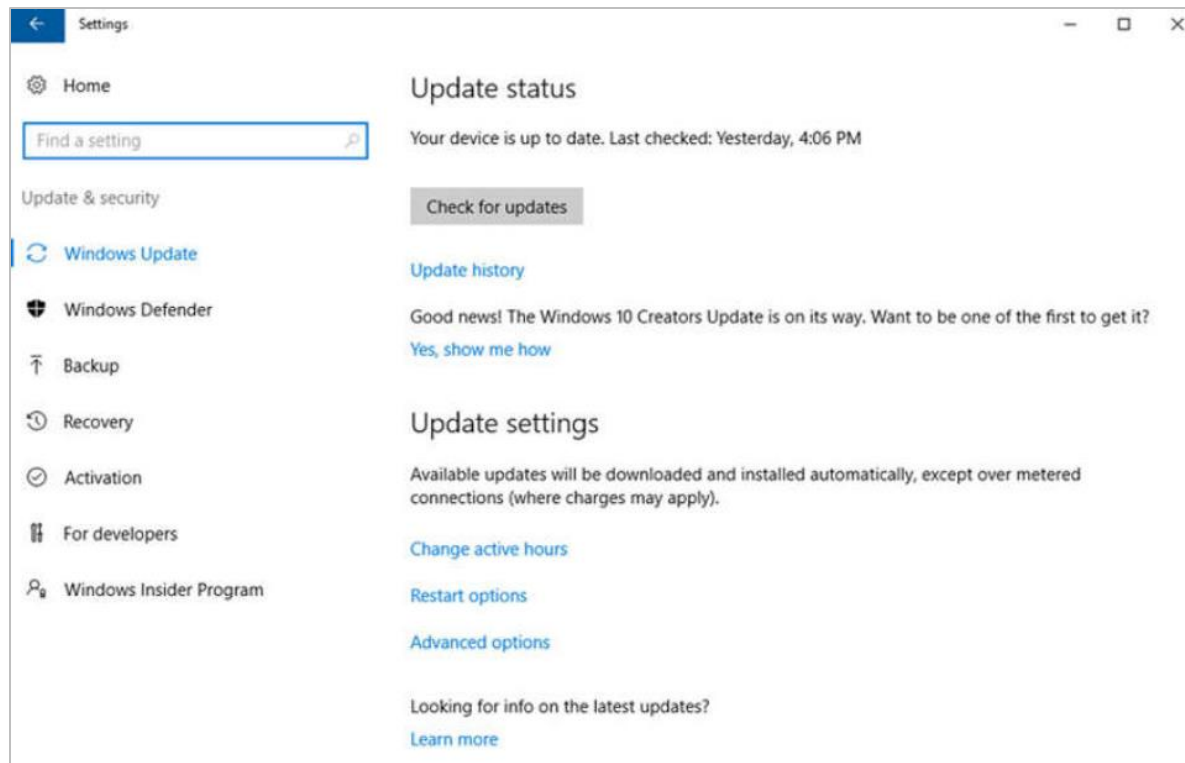
# Visualizador de eventos

- O Visualizador de Eventos do Windows registra o histórico de eventos de aplicativos, segurança e sistema.
- Esses arquivos de log são uma ferramenta de solução de problemas, pois fornecem as informações necessárias para identificar um problema.
- O Windows inclui duas categorias de logs de eventos: Logs do Windows e Logs de Aplicativos e Serviços.
- Uma exibição personalizada interna chamada Eventos administrativos mostra todos os eventos críticos, de erro e de aviso de todos os logs administrativos.
- Os logs de eventos de segurança são encontrados em Logs do Windows. Eles usam IDs de evento para identificar o tipo de evento.



# Gerenciamento do Windows Update

- Para garantir o mais alto nível de proteção contra os ataques, certifique-se sempre de que o Windows esteja atualizado com os service packs e patches de segurança mais recentes.
- O status da atualização, mostrado na figura, permite que você verifique as atualizações manualmente e veja o histórico de atualizações do computador.
- Os patches são atualizações de código que os fabricantes fornecem para evitar que um vírus ou um worm recém-descoberto façam um ataque bem-sucedido.



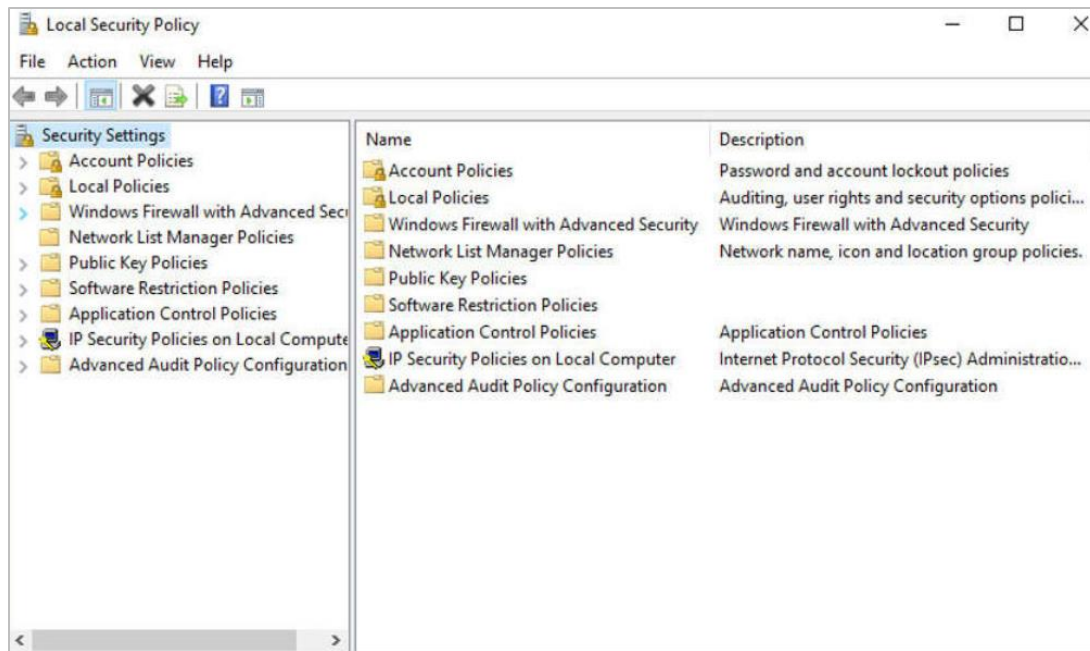


# Gerenciamento do Windows Update (Cont.)

- De tempos em tempos, os fabricantes combinam patches e atualizações em uma aplicação completa de atualização chamada de service pack.
- Muitos ataques devastadores de vírus poderiam ter sido muito menos graves, se mais usuários tivessem baixado e instalado o service pack mais recente.
- É altamente desejável que as empresas utilizem sistemas que distribuam, instalam e rastreiam automaticamente as atualizações de segurança.
- O Windows verifica, regularmente, o site Windows Update, por atualizações de alta prioridade e que podem ajudar a proteger o computador contra as mais recentes ameaças de segurança.
- Há também configurações para as horas em que o computador não será reiniciado automaticamente, por exemplo, durante o horário comercial regular.
- Opções avançadas também estão disponíveis para escolher como as atualizações são instaladas como outros produtos da Microsoft são atualizados.

# Política de segurança local

- Uma política de segurança é um conjunto de objetivos que garante a segurança de uma rede, dos dados e dos sistemas de computador em uma organização.
- Na maioria das redes que usam computadores Windows, o Active Directory é configurado com domínios em um servidor Windows. Computadores Windows ingressam no domínio.
- A diretiva de segurança local do Windows pode ser usada para computadores independentes que não fazem parte de um domínio do Active Directory.



# Política de segurança local (Cont.)

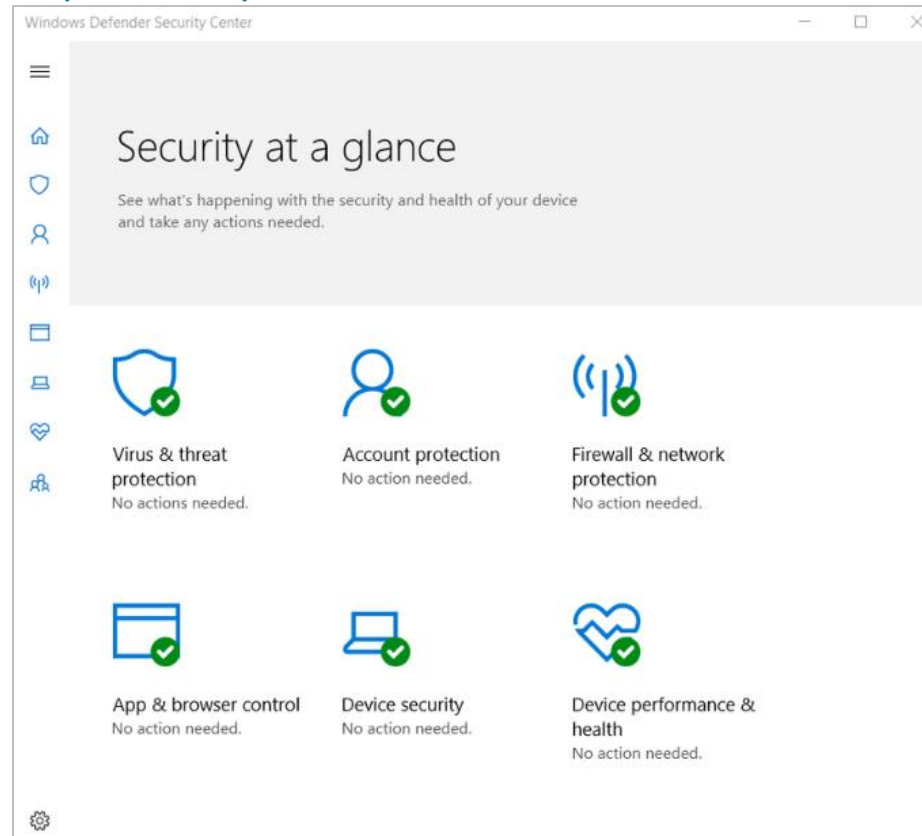
- As diretrizes de senha são um componente importante de uma política de segurança.
- Na Política de Segurança Local, a Política de Palavra-passe é encontrada em Políticas de Conta e define os critérios para as palavras-passe para todos os utilizadores no computador local.
- Use a Diretiva de Bloqueio de Conta em Diretivas de Conta, para impedir tentativas de login por força bruta.
- É importante garantir que os computadores estejam seguros quando os usuários estiverem ausentes. Uma política de segurança deve conter uma regra sobre exigir que um computador seja bloqueado quando o protetor de tela for iniciado.
- Se a política de segurança local em cada computador autônomo for a mesma, use o recurso Exportar política. Isso é particularmente útil quando o administrador precisa configurar diretivas locais abrangentes para direitos de usuário e opções de segurança.
- O miniaplicativo Diretiva de Segurança Local contém configurações de segurança que se aplicam especificamente ao computador local. O usuário pode configurar Direitos de Usuário, Regras de Firewall e a capacidade de restringir os arquivos que os usuários ou grupos têm permissão para executar com o AppLocker.

# proteção do Windows

- Malware inclui vírus, worms, cavalos de Troia, keyloggers, spyware, e adware. Eles são projetados para invadir a privacidade, roubar informações, danificar o computador ou corromper dados.
- É importante proteger os computadores e dispositivos móveis com software antimalware de qualidade. Estão disponíveis os seguintes tipos de programas antimalware:
  - **Proteção antivírus:** este programa monitora continuamente a existência de vírus. Quando um vírus é detectado, o usuário é avisado e o programa tenta colocar o vírus em quarentena ou excluí-lo.
  - **Proteção de adware:** Este programa procura continuamente programas que exibam anúncios no computador.
  - **Proteção contra phishing:** Este programa bloqueia os endereços IP de sites de phishing conhecidos e avisa o usuário sobre sites suspeitos.
  - **Proteção contra spyware:** Este programa procura keyloggers e outros spywares.
  - **Fontes confiáveis \ não confiáveis:** Este programa avisa sobre programas inseguros prestes a serem instalados ou sites inseguros.

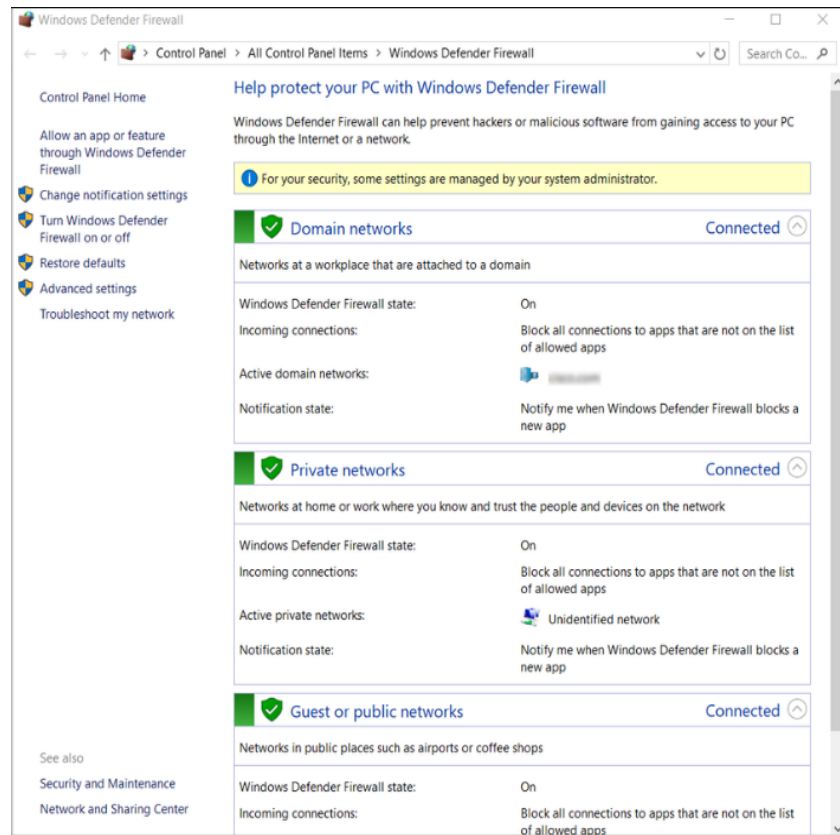
# Windows Defender de Segurança (Cond.)

- Podem ser necessárias várias varreduras para remover completamente todos os softwares maliciosos. Execute apenas um programa de proteção contra malware por vez.
- Diversas organizações de segurança, como McAfee, Symantec e Kaspersky, oferecem proteção completa contra malware para computadores e dispositivos móveis.
- O Windows tem proteção interna contra vírus e spyware chamada Windows Defender.
- O Windows Defender está ativado por padrão para fornecer proteção em tempo real contra infecções.
- Embora o Windows Defender funcione em segundo plano, o usuário pode realizar varreduras manuais do computador e dispositivos de armazenamento.



# Firewall do Windows Defender

- Um firewall nega, seletivamente, o tráfego a um computador ou a um segmento de rede.
- Para permitir o acesso ao programa através do Firewall do Windows Defender, procure por **Painéis de Controle**. Em **Sistemas e Segurança**, localize o **Firewall do Windows Defender**. Clique em **Permitir um aplicativo ou recurso por meio do Firewall do Windows Defender**, conforme mostrado na figura.
- Para desativar o Firewall do Windows e usar um firewall de software diferente, clique em **Ativar ou desativar o Firewall do Windows**.
- Muitas configurações adicionais podem ser encontradas em **Configurações avançadas**. Aqui, regras de tráfego de entrada ou saída podem ser criadas e diferentes aspectos do firewall podem ser monitorados.



# 3.5 O resumo do sistema operacional Windows

## O que aprendi neste módulo?

- Os primeiros computadores precisaram de um sistema operacional de disco (DOS) para criar e gerenciar arquivos.
- A Microsoft desenvolveu o MS-DOS como uma interface de linha de comando (CLI) para acessar a unidade de disco e carregar os arquivos do sistema operacional. As versões anteriores do Windows consistiam em uma interface gráfica do usuário (GUI) que executava o MS-DOS.
- Windows consiste em uma camada de abstração de hardware (HAL) que lida com toda a comunicação entre o hardware e o kernel.
- O Windows opera em dois modos diferentes, o modo de usuário e o modo kernel. A maioria dos programas do Windows são executados no modo de usuário. O modo kernel permite o acesso direto do código do sistema operacional ao hardware do computador.
- Um computador funciona armazenando instruções na RAM até que a CPU os processe.
- Cada processo em um computador Windows de 32 bits suporta um espaço de endereço virtual que permite endereçar até quatro gigabytes. Cada processo num computador Windows de 64 bits suporta um espaço de endereço virtual de até oito terabytes.



## O que aprendi neste módulo? (Continuação)

- O Windows armazena todas as informações sobre hardware, aplicativos, usuários e configurações do sistema em um banco de dados grande conhecido como o Registro.
- O registro é um banco de dados hierárquico onde o nível mais alto é conhecido como um ramo, abaixo que existem chaves, seguido por subchaves.
- Existem cinco hives de registro que contêm dados relativos à configuração e operação do Windows. Existem centenas de chaves e subchaves.
- Por razões de segurança, não é aconselhável iniciar sessão no Windows utilizando a conta de Administrador ou uma conta com privilégios administrativos.
- Use grupos do Windows para facilitar a administração de usuários. Usuários e grupos locais são gerenciados com o applet do painel de controle lusrmgr.msc.
- Você pode usar a CLI ou o Windows PowerShell para executar comandos. O PowerShell pode ser usado para criar scripts para automatizar tarefas que a CLI normal não consegue automatizar.
- A Instrumentação de Gerenciamento do Windows (WMI) é usada para gerenciar computadores remotos.

## O que aprendi neste módulo? (Continuação)

- O comando **net** pode ser combinado com switches para focar na saída específica.
- O Gerenciador de Tarefas fornece muitas informações sobre o que está sendo executado e o desempenho geral do computador. O Monitor de Recursos fornece informações mais detalhadas sobre o uso de recursos.
- O protocolo SMB (Server Message Block) é usado para compartilhar recursos de rede, como arquivos em hosts remotos.
- O comando **netstat** do Windows exibe todas as portas de comunicação abertas em um computador e também pode exibir os processos de software associados às portas.
- O Visualizador de Eventos do Windows fornece acesso a vários eventos registrados em relação à operação de um computador.
- É muito importante manter o Windows atualizado para se proteger contra novas ameaças à segurança.
- O Windows deve ser configurado para baixar e instalar atualizações automaticamente à medida que elas se tornarem disponíveis.

