Introdução

3.0.1

Por que devo cursar este módulo?

Desde seus humildes começos há mais de 35 anos, em 1985, o sistema operacional Windows tem visto muitas iterações; do Windows 1.0 à versão atual da área de trabalho, Windows 10 e versão do servidor, Windows Server 2019.

Este módulo aborda alguns dos conceitos básicos do Windows, incluindo como o sistema operacional funciona e as ferramentas usadas para proteger endpoints do Windows.

3.0.2

O que vou aprender neste 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. |

3.0.3

Atividade da Classe - Identificar Processos em Execução

Nesta atividade, você usará o TCP/UDP Endpoint Viewer, que é uma ferramenta no Windows Sysinternals Suite, para identificar processos em execução no computador.

# **Histórico do Windows**

3.1.1

## Sistema operacional de disco

Os primeiros computadores não tinham dispositivos de armazenamento modernos, como discos rígidos, unidades ópticas ou armazenamento flash. Os primeiros métodos de armazenamento usavam cartões perfurados, fita de papel, fita magnética e até cassetes de áudio.

Disquetes e armazenamento em disco rígido exigem software para ler, gravar e gerenciar os dados que eles armazenam. O sistema operacional de disco (DOS) é um sistema operacional que o computador usa para habilitar esses 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. A Microsoft comprou o DOS e desenvolveu o MS-DOS.

MS-DOS usou uma linha de comando como a interface para as pessoas criarem programas e manipularem arquivos de dados, como mostrado na saída do comando. Os comandos DOS são mostrados em negrito.

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:\>

Com o MS-DOS, o computador tinha um conhecimento básico de trabalho de como acessar a unidade de disco e carregar os arquivos do sistema operacional diretamente do disco como parte do processo de inicialização. Quando ele foi carregado, o MS-DOS poderia acessar facilmente o disco porque ele foi incorporado no sistema operacional.

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. O DOS ainda controlava o computador e seu hardware. Um sistema operacional moderno como o Windows 10 não é considerado um sistema operacional de disco. Ele é construído no Windows NT, que significa “Novas Tecnologias”. O próprio sistema operacional está no controle direto do computador e seu hardware. NT é um sistema operacional com suporte para vários processos de usuário. Isso é muito diferente do MS-DOS de um único processo e de usuário único.

Hoje, muitas coisas que costumavam ser realizadas através da interface de linha de comando do MS-DOS podem ser realizadas na GUI do Windows. Você ainda pode experimentar como era usar o MS-DOS abrindo uma janela de comando, mas o que você vê não é mais MS-DOS, é uma função do Windows. Para experimentar um pouco do que era trabalhar no MS-DOS, abra uma janela de comando digitando **cmd** na Pesquisa do Windows e pressionando **Enter**. A tabela lista alguns comandos que você pode usar. Digite **help** seguido do comando para saber mais sobre o comando.

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

3.1.2

## Versões do Windows

Desde 1993, houve mais de 20 lançamentos do Windows que são baseados no sistema operacional NT. A maioria dessas versões era para uso pelo público em geral e pelas empresas devido à segurança de arquivos oferecida pelo sistema de arquivos usado pelo sistema operacional NT. As empresas também adotaram sistemas operacionais Windows baseados em SO NT. Isso ocorre porque muitas edições foram criadas especificamente para estações de trabalho, profissionais, servidores, servidores avançados e servidores de datacenter, para citar apenas algumas das muitas versões criadas para fins específicos.

A partir do Windows XP, uma edição de 64 bits estava disponível. 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. Isto não é simplesmente o dobro da quantidade de espaço porque estes bits são números binários. Embora o Windows de 32 bits possa endereçar um pouco menos de 4 GB de RAM, o Windows de 64 bits pode, teoricamente, endereçar 16,8 milhões de terabytes. Quando o sistema operacional e o hardware suportam a operação de 64 bits, conjuntos de dados extremamente grandes podem ser usados. Esses grandes conjuntos de dados incluem bancos de dados muito grandes, computação científica e manipulação de vídeo digital de alta definição com efeitos especiais. Em geral, computadores e sistemas operacionais de 64 bits são compatíveis com programas mais antigos de 32 bits, mas 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. O Windows 7 foi oferecido com seis edições diferentes, o Windows 8 com até cinco e o Windows 10 com oito edições diferentes! Cada edição não só oferece diferentes capacidades, mas também diferentes pontos de preço. A Microsoft disse que o Windows 10 é a última versão do Windows, e que o Windows se tornou um serviço em vez de apenas um sistema operacional. Eles dizem que, em vez de comprar novos sistemas operacionais, os usuários apenas atualizarão o Windows 10 em vez disso.

A tabela lista versões comuns do Windows.

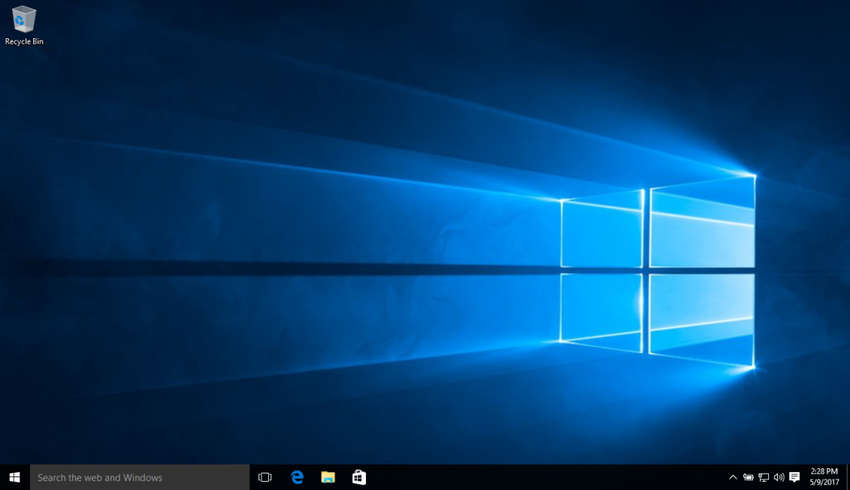
| **SO** | **Versões** |
| --- | --- |
| **Windows 7** | Starter, Home Basic, Home Premium, Professional, Enterprise, Ultimate |
| **Windows Server 2008 R2** | Foundation, Standard, Enterprise, Datacenter, Web Server, HPC Server, Itanium-Based Systems |
| **Windows Home Server 2011** | Nenhum |
| **Windows 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, loT Core, Mobile, Mobile Enterprise |
| **Windows Server 2016** | Essentials, Standard, Datacenter, Multipoint Premium Server, Storage Server, Hyper-V Server |

3.1.3

## 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, mostrada na figura.

A figura mostra a imagem da interface gráfica do usuário do Windows 10 com o ícone Lixeira, a imagem de plano de fundo da área de trabalho e a barra de tarefas na parte inferior da janela que apresenta a ferramenta Menu Iniciar e Pesquisa, os Ícones de Início Rápido e a Área de Notificação formalmente chamada Bandeja do Sistema.

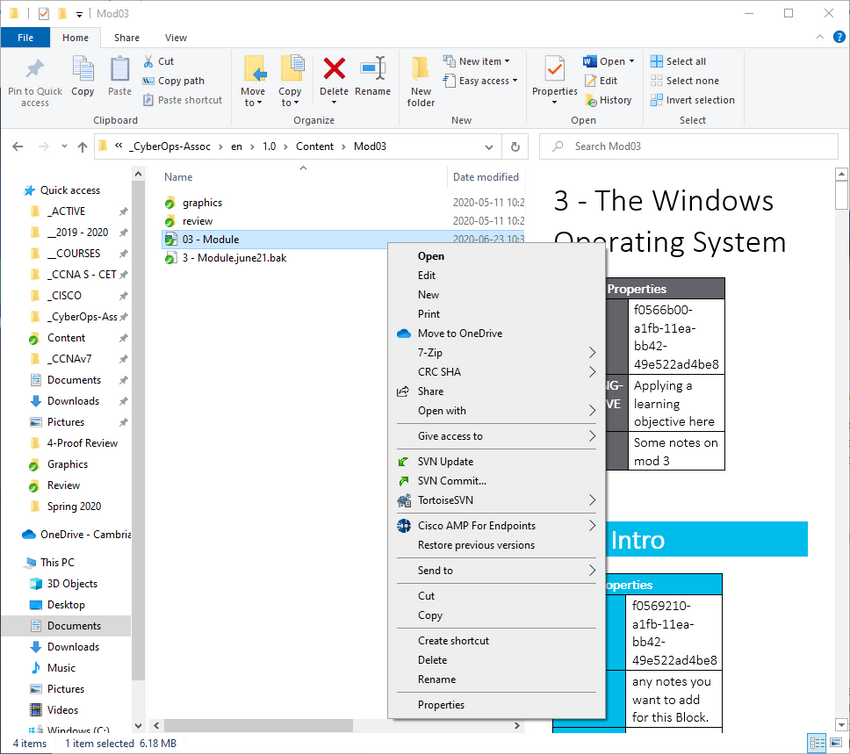


Área de trabalhoÍcones de inicialização rápidaMenu Iniciar e PesquisaÍcone de lixeiraBarra de TarefasArea de Notificação

A área de trabalho pode ser personalizada com várias cores e imagens de fundo. O Windows suporta vários usuários, para que cada usuário possa personalizar a Área de Trabalho ao seu gosto. 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.

Na parte inferior da área de trabalho está a Barra de Tarefas. A Barra de Tarefas tem três áreas que são usadas para diferentes fins. À esquerda está o menu Iniciar. Ele é usado para acessar todos os programas instalados, opções de configuração e o recurso de pesquisa. No centro da Barra de Tarefas, os usuários colocam ícones de inicialização rápida que executam programas específicos ou abrem pastas específicas quando clicam. Finalmente, 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. Por exemplo, um ícone de envelope intermitente pode indicar um novo e-mail ou um ícone de rede com um “x” vermelho pode indicar um problema com a rede.

Muitas vezes, clicar com o botão direito do mouse em um ícone trará funções adicionais que podem ser usadas. Esta lista é conhecida como um Menu de Contexto, mostrado na figura.



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 com apenas um clique. Por exemplo, o Menu de Contexto de um arquivo conterá itens como copiar, excluir, compartilhar e imprimir. Para abrir pastas e manipular arquivos, o Windows usa o Explorador de Arquivos do Windows.

3.1.4

## Vulnerabilidades do sistema operacional

Os sistemas operacionais consistem em milhões de linhas de código. O software instalado também pode conter 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.

A tabela lista algumas recomendações comuns de Segurança do SO Windows.

| **Recomendação** | **Descrição** |
| --- | --- |
| **Proteção contra vírus ou malware** | * Por padrão, o Windows usa o Windows Defender para proteção contra malware. * O Windows Defender fornece um conjunto de ferramentas de proteção incorporadas ao sistema. * Se o Windows Defender estiver desativado, o sistema ficará mais vulnerável a ataques e malware. |
| **Serviços desconhecidos ou não gerenciados** | * Há muitos serviços que funcionam nos bastidores. * É importante certificar-se de que cada serviço é identificável e seguro. * Com um serviço desconhecido em execução em segundo plano, o computador pode ficar vulnerável a ataques. |
| **Criptografia** | * Quando os dados não são criptografados, eles podem ser facilmente coletados e explorados. * Isso não é importante apenas para computadores desktop, mas especialmente dispositivos móveis. |
| **Política de segurança** | * Uma boa política de segurança deve ser configurada e seguida. * Muitas configurações no controle de Diretiva de Segurança do Windows podem impedir ataques. |
| **Firewall** | * 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. * Por exemplo, uma porta pode ser deixada aberta que não deve mais estar prontamente disponível. * É importante revisar periodicamente as configurações do firewall para garantir que as regras ainda são aplicáveis e remover as que não se aplicam mais |
| **Permissões de arquivo e compartilhamento** | * Essas permissões devem ser definidas corretamente. * É fácil dar ao grupo “Todos” Controle Total, mas isso permite que todas as pessoas façam o que quiserem a todos os arquivos. * É melhor fornecer a cada usuário ou grupo as permissões mínimas necessárias para todos os arquivos e pastas. |
| **Senha fraca ou sem senha** | * Muitas pessoas escolhem senhas fracas ou não usam nenhuma senha. * É especialmente importante certificar-se de que todas as contas, especialmente a conta de Administrador, têm uma senha muito forte. |
| **Login como Administrador** | * Quando um usuário faz logon como administrador, qualquer programa executado terá os privilégios dessa conta. * É melhor fazer login como um Usuário Padrão e usar apenas a senha de administrador para realizar determinadas tarefas. |

# **Arquitetura e operações do Windows**

3.2.1

## Camada de abstração de hardware

Computadores Windows usam muitos tipos diferentes de hardware. O sistema operacional pode ser instalado em um computador comprado ou em um computador que é montado pelo usuário. Quando o sistema operacional está instalado, ele deve ser isolado das diferenças no hardware. A arquitetura básica do Windows é mostrada na figura.

A figura mostra a arquitetura básica do Windows com os aplicativos na parte superior, os drivers do modo de usuário e a API do Windows abaixo deles, Outros drivers do modo kernel, kernel do sistema operacional e drivers do sistema de arquivos abaixo deles, a camada de abstração de hardware abaixo deles e, na parte inferior, o hardware.

AplicaçõesAPI do WindowsDrivers de modo  
de usuárioOutros drivers  
de modo kernelKernel do sistema operacionalDrivers  
do sistema de arquivosCamada de abstração de hardwareHardware

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. Ele lida com todas as solicitações de entrada e saída, memória e todos os periféricos conectados ao computador.

Em alguns casos, o kernel ainda se comunica diretamente com o hardware, portanto não é completamente independente do HAL. O HAL também precisa do kernel para executar algumas funções.

3.2.2

## Modo de usuário e modo kernel

Conforme identificado na figura, existem dois modos diferentes em que uma CPU opera quando o computador tem o Windows instalado: o modo de usuário e o modo kernel.

Esta figura é a mesma que a página anterior, mas mostra que os Aplicativos, Drivers de Modo de Usuário e a API do Windows compõem o Modo de Usuário, enquanto os Outros Drivers de Modo Kernel, o Kernel do Sistema Operacional e os Drivers de Sistema de Arquivos, a Camada de Abstração de Hardware e o Hardware compõem o Modo Kernel.

AplicaçõesAPI do WindowsDrivers de modo  
de usuárioOutros drivers  
de modo kernelKernel do sistema operacionalDrivers  
do sistema de arquivosCamada de abstração de hardwareHardwareModo de usuárioModo Kernel

Os aplicativos instalados são executados no modo de usuário e o código do sistema operacional é executado no modo kernel. O código que está sendo executado no modo kernel tem acesso irrestrito ao hardware subjacente e é capaz de executar qualquer instrução de CPU. O código do modo kernel também pode referenciar qualquer endereço de memória diretamente. Geralmente reservado para as funções mais confiáveis do sistema operacional, falhas no código em execução no modo kernel param a operação de todo o computador. Por outro lado, programas como aplicativos de usuário são executados no modo de usuário e não têm acesso direto a locais de hardware ou memória. O código do modo de usuário deve passar pelo sistema operacional para acessar recursos de hardware. Devido ao isolamento fornecido pelo modo de usuário, as falhas no modo de usuário são restritas apenas ao aplicativo e são recuperáveis. A maioria dos programas no Windows são executados no modo de usuário. Drivers de dispositivo, peças de software que permitem que o sistema operacional e um dispositivo se comuniquem, podem ser executados no modo kernel ou usuário, dependendo do driver.

Todo o código que é executado no modo kernel usa o mesmo espaço de endereço. Os drivers de modo kernel não têm isolamento do sistema operacional. Se ocorrer um erro com o driver em execução no modo kernel e ele gravar no espaço de endereço errado, o sistema operacional ou outro driver de modo kernel pode ser afetado negativamente. A este respeito, o driver pode falhar, fazendo com que todo o sistema operacional falhe.

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. A razão para essa funcionalidade é principalmente para impedir que aplicativos alterem o código do sistema operacional que está sendo executado ao mesmo tempo. Ao ter seu próprio processo, esse aplicativo tem seu próprio espaço de endereço privado, tornando outros aplicativos incapazes de modificar os dados nele. Isso também ajuda a evitar que o sistema operacional e outros aplicativos falhe se esse aplicativo falhar.

3.2.3

## Sistemas de arquivos Windows

Um sistema de arquivos é como as informações são organizadas na mídia de armazenamento. Alguns sistemas de arquivos podem ser uma melhor opção para usar do que outros, dependendo do tipo de mídia que será usado. A tabela lista os sistemas de arquivos suportados pelo Windows.

| **Sistema de Arquivos Windows** | **Descrição** |
| --- | --- |
| **exFAT** | * Este é um sistema de arquivos simples suportado por muitos sistemas operacionais diferentes. * O FAT tem limitações para o número de partições, tamanhos de partições e tamanhos de arquivo que pode resolver, portanto, não é mais usado para discos rígidos (HDs) ou unidades de estado sólido (SSDs). * Tanto o FAT16 quanto o FAT32 estão disponíveis para uso, sendo o FAT32 o mais comum porque tem muito menos restrições do que o FAT16. |
| **Sistema de Arquivos Hierárquico Plus (HFS+)** | * Este sistema de arquivos é usado em computadores MAC OS X e permite nomes de arquivos, tamanhos de arquivo e tamanhos de partição muito mais longos do que os sistemas de arquivos anteriores. * Embora não seja suportado pelo Windows sem software especial, o Windows é capaz de ler dados de partições HFS+. |
| **Sistema de arquivos estendido (EXT)** | * Este sistema de arquivos é usado com computadores baseados em Linux. * Embora não seja suportado pelo Windows, o Windows é capaz de ler dados de partições EXT com software especial. |
| **New Technology File System (NTFS)** | * Este é o sistema de arquivos mais comumente usado ao instalar o Windows. Todas as versões do Windows e Linux suportam NTFS. * Computadores Mac-OS X só podem ler uma partição NTFS. Eles são capazes de gravar em uma partição NTFS depois de instalar drivers especiais. |

O NTFS é o sistema de arquivos mais utilizado para Windows por muitas razões. NTFS suporta arquivos e partições muito grandes e é muito compatível com outros sistemas operacionais. O NTFS também é muito confiável e oferece suporte a recursos de recuperação. Mais importante ainda, ele suporta muitos recursos de segurança. O controle de acesso a dados é alcançado através de descritores de segurança. Esses descritores de segurança contêm permissões e propriedade do arquivo até o nível do arquivo. O NTFS também controla muitos carimbos de data/hora para controlar a atividade do arquivo. Às vezes referido como MACE, os carimbos de data/hora Modificar, Access (acesso), Create (criar) e Entry Modified (entrada modificada) são frequentemente usados em investigações forenses para determinar o histórico de um arquivo ou pasta. O NTFS também suporta criptografia do sistema de arquivos para proteger toda a mídia de armazenamento.

Antes que um dispositivo de armazenamento, como um disco, possa ser usado, ele deve ser formatado com um sistema de arquivos. Por sua vez, antes que um sistema de arquivos possa ser colocado em prática em um dispositivo de armazenamento, o dispositivo precisa ser particionado. Um disco rígido é dividido em áreas denominadas partições. Cada partição é uma unidade lógica de armazenamento que pode ser formatada para armazenar informações, como arquivos de dados ou de aplicações. Durante o processo de instalação, a maioria dos sistemas operacionais particiona e formata automaticamente o espaço disponível na unidade com um sistema de arquivos como o NTFS.

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

* **Setor de inicialização de partição** - Este é o primeiro 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 de 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. O espaço livre pode ser examinado e os arquivos podem ser recuperados, o que pode comprometer a segurança. 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.

3.2.4

## Fluxos 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, você pode conectar fluxos de dados alternativos (ADSs) ao arquivo. Às vezes, isso é usado por aplicativos que estão armazenando informações adicionais sobre o arquivo. O ADS é um fator importante ao discutir malware. Isso ocorre porque é fácil ocultar dados em um ADS. 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**. Um exemplo de ADS é mostrado na saída do comando.

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>

Na saída:

* O primeiro comando coloca o texto “Dados Alternativos Aqui” em um ADS do arquivo Testfile.txt chamado “ADS”.
* Depois disso, **dir**, mostra que o arquivo foi criado, mas o ADS não está visível.
* O próximo comando mostra que há dados no Testfile.txt \* O último comando mostra o ADS do arquivo Testfile.txt porque a opção **r** **dir** foi usada com o.

3.2.5

## Processo de Inicialização do Windows

Muitas ações ocorrem entre o momento em que o botão liga/desliga do computador é pressionado e o Windows está totalmente carregado, como mostrado na figura. Isso é conhecido como o processo de inicialização do Windows.

A figura mostra um fluxograma do processo de inicialização do Windows. O processo começa com a inicialização do BIOS ou inicialização UEFI. No caso da inicialização do BIOS, o próximo passo é o POST, seguido pelo MBR. No caso da inicialização do UEFI, a próxima etapa são os Arquivos EFI. Os próximos passos para ambos os caminhos são o Boot m g r ponto e x e, seguido pelo B C D. Se o computador estiver retomando da hibernação, o próximo passo é o win resume ponto e x e, seguido por hiberfil ponto s y s e, em seguida, para o início de sessão. A partir de uma inicialização fria, após B C D, os próximos passos são win load ponto e x e, K M C S, n t o s k r n l ponto e x e, H A L, S M S S S e, finalmente, logon.

Inicialização UEFIPOSTArquivos EFIBCDMBRBootmgr.exeWinload.exeKMCSWinresume.exeNtoskrnl.exeHALSMSSHiberfil.sysLogonHibernação? SimInicialização do BIOS

Existem dois tipos de firmware de computador:

* **Sistema básico de entrada-saída (BIOS)** - o firmware do BIOS foi criado no início da década de 1980 e funciona da mesma forma que quando foi criado. À medida que os computadores evoluíram, tornou-se difícil para o firmware do BIOS suportar todos os novos recursos solicitados pelos usuários.
* **UEFI (Unified Extensible Firmware Interface)** - O UEFI foi projetado para substituir o BIOS e suportar os novos recursos.

No firmware do BIOS, o processo começa com a fase de inicialização do BIOS. Isso ocorre quando os dispositivos de hardware são inicializados e um POST (Power On Self-Test) é executado para garantir que todos esses dispositivos estejam se comunicando. Quando o disco do sistema é descoberto, o POST termina. A última instrução no POST é procurar o registro mestre de inicialização (MBR).

A MBR contém um pequeno programa que é responsável por localizar e carregar o sistema operacional. O BIOS executa esse código e o sistema operacional começa a carregar.

Em contraste com o firmware do BIOS, o firmware UEFI tem muita visibilidade sobre o processo de inicialização. O UEFI inicializa carregando arquivos de programa EFI, armazenados como arquivos.efi em uma partição de disco especial, conhecida como EFI System Partition (ESP).

**Nota**: 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.

Se o firmware é BIOS ou UEFI, depois que uma instalação válida do Windows é localizada, o arquivo **Bootmgr.exe** é executado. **Bootmgr.exe** alterna o sistema do modo real para o modo protegido para que toda a memória do sistema possa ser usada.

**Bootmgr.exe** lê o Banco de Dados de Configuração de Inicialização (BCD). O BCD contém qualquer código adicional necessário para iniciar o computador, juntamente com uma indicação de se o computador está saindo da hibernação ou se este é um arranque a frio. Se o computador estiver saindo da hibernação, o processo de inicialização continuará com **Winresume.exe**. Isso permite que o computador leia o arquivo **Hiberfil.sys** que contém o estado do computador quando ele foi colocado em hibernação.

Se o computador estiver sendo inicializado a partir de um início a frio, o arquivo **Winload.exe** será carregado. O arquivo **Winload.exe** cria um registro da configuração de hardware no registro. O registro é um registro de todas as configurações, opções, hardware e software do computador. O registro será explorado em profundidade mais adiante neste capítulo. **Winload.exe** também usa o Kernel Mode Code Signing (KMCS) para garantir que todos os drivers sejam assinados digitalmente. Isso garante que os drivers são seguros para carregar à medida que o computador é iniciado.

Depois que os drivers foram examinados, **Winload.exe** é executado **Ntoskrnl.exe** que inicia o kernel do Windows e configura o HAL. Finalmente, o Subsistema do Gestor de Sessões (SMSS) lê o registo para criar o ambiente do utilizador, iniciar o serviço Winlogon e preparar a área de trabalho de cada utilizador à medida que inicia sessão.

3.2.6

## Inicialização do Windows

Há dois itens de registro importantes que são usados para iniciar automaticamente aplicativos e serviços:

* **HKEY\ \_LOCAL\ \_MACHINE** - Vários aspectos da configuração do Windows são armazenados nesta chave, incluindo informações sobre serviços que começam com cada inicialização.
* **HKEY\ \_CURRENT\ \_USER** - Vários aspectos relacionados ao usuário conectado são armazenados nesta chave, incluindo informações sobre serviços que iniciam somente quando o usuário faz logon no computador.

O registro será discutido mais adiante neste tópico.

Entradas diferentes nesses locais de registro definem quais serviços e aplicativos serão iniciados, conforme indicado pelo tipo de entrada. Esses tipos incluem Run, RunOnce, RunServices, RunServicesOnce e Userinit. Essas entradas podem ser inseridas manualmente no registro, mas é muito mais seguro usar a ferramenta **Msconfig.exe** Esta ferramenta é usada para exibir e alterar todas as opções de inicialização do computador. Use a caixa de pesquisa para localizar e abrir a ferramenta Msconfig.

A ferramenta Msconfig abre a janela Configuração do sistema. Existem cinco guias que contêm as opções de configuração.

Geral

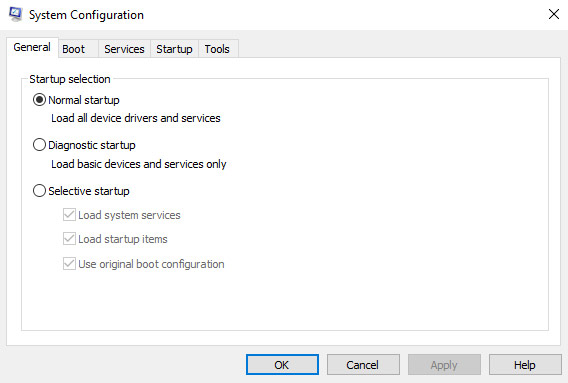
Inicialização do Sistema

Serviços

Startup

Ferramentas

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.



3.2.7

## Desligamento do Windows

É sempre melhor executar um desligamento adequado para desligar o computador. Arquivos que são deixados abertos, serviços que são fechados fora de ordem e aplicativos que travam podem ser danificados se a energia for desligada sem primeiro informar o sistema operacional. 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. Se um processo de modo de usuário não responder dentro de um determinado período de tempo, o sistema operacional exibirá a notificação e permitirá que o usuário aguarde a aplicação responder ou encerre o processo forçosamente. Se um processo de modo kernel não responder, o desligamento parecerá travar e poderá ser necessário desligar o computador com o botão liga/desliga.

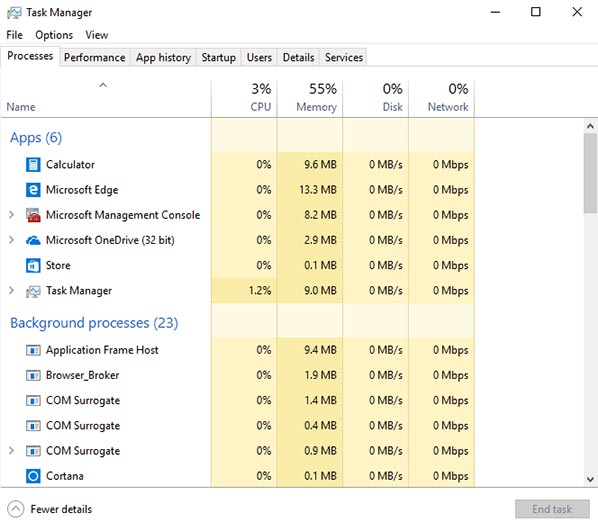
Existem várias maneiras de desligar um computador Windows: Opções de energia do menu Iniciar, o comando da linha de comando **shutdown** e usando **Ctrl+Alt+Delete** e clicando no ícone de energia. Existem três opções diferentes para escolher ao desligar o computador:

* **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.

3.2.8

## Processos, Threads e Serviços

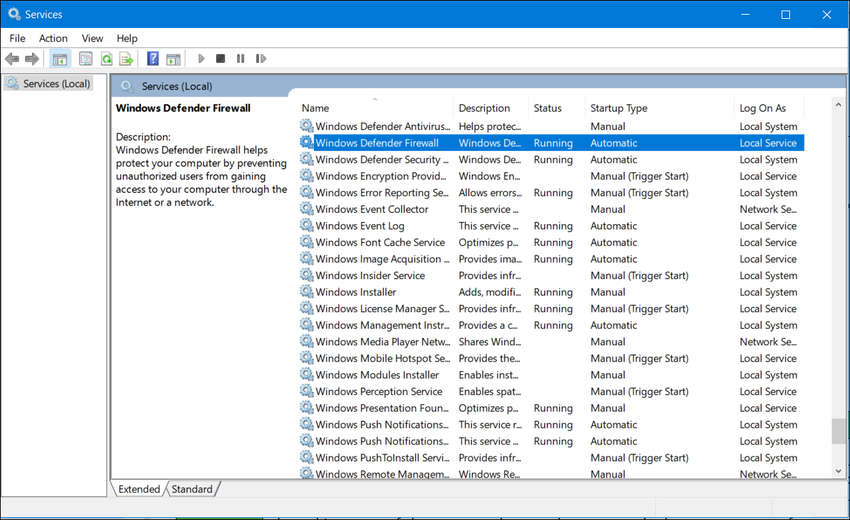
Um aplicativo do Windows é composto de processos. O aplicativo pode ter um ou muitos processos dedicados a ele. Um processo é qualquer programa em execução no momento. Cada processo que é executado é composto de pelo menos uma thread. Uma thread é uma parte do processo que pode ser executado. O processador executa cálculos na thread. 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 no mesmo espaço de endereço. Isso significa que esses threads podem não acessar o espaço de endereço de qualquer outro processo. Isso evita a corrupção de outros processos. Como Windows é multitarefas, vários threads podem ser executados ao mesmo tempo. A quantidade de threads que podem ser executados ao mesmo tempo depende do número de processadores do computador.

Alguns dos processos executados pelo Windows são serviços. Estes são programas que são executados em segundo plano para suportar o sistema operacional e as aplicações. Eles podem ser configurados para iniciar automaticamente quando o Windows for inicializado ou podem ser iniciados manualmente. Eles também podem ser interrompidos, reiniciados ou desativados.

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. Alguns programas dependem de um ou mais serviços para funcionar corretamente. Encerrar um serviço pode afetar negativamente aplicativos ou outros serviços.

3.2.9

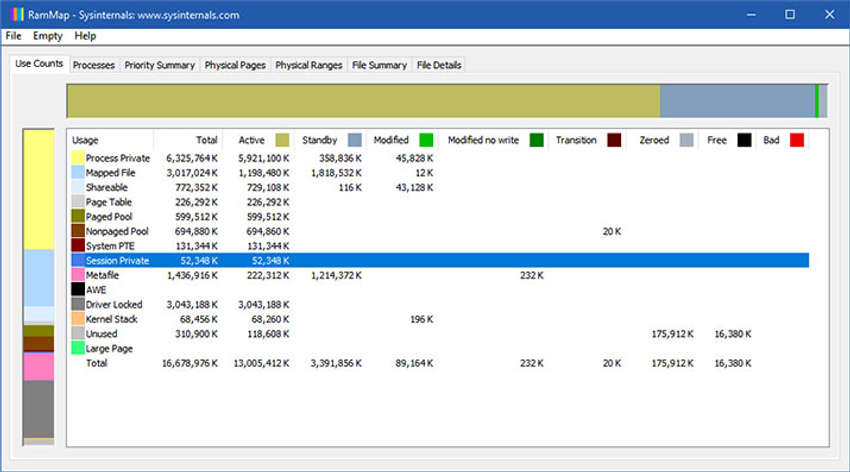
## Alocação e identificadores de memória

Um computador funciona armazenando instruções na RAM até que a CPU os processe. 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. Isso ocorre porque 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.

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 uma riqueza de informações sobre como o Windows alocou memória do sistema para o kernel, processos, drivers e aplicativos.



3.2.10

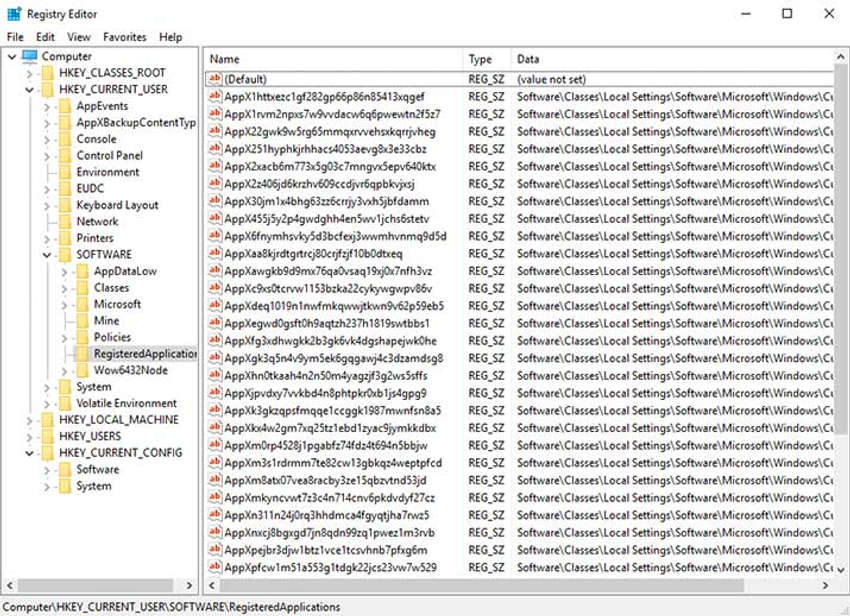
## O Registro do Windows

O Windows armazena todas as informações sobre hardware, aplicativos, usuários e configurações do sistema em um banco de dados grande conhecido como o Registro. As formas como esses objetos interagem também são registradas, como quais arquivos um aplicativo abre e todos os detalhes de propriedade de pastas e aplicativos. O registro é um banco de dados hierárquico onde o nível mais alto é conhecido como um ramo, abaixo 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 lista os cinco ramos do registro do Windows.

| **Seção (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). OLE permite que os usuários incorporem objetos de outros aplicativos (como uma planilha) em um único documento (como um documento do Word). |
| **HKEY\_LOCAL\_MACHINE (HKLM)** | Contém informações relacionadas ao sistema. |
| **HKEY\_CURRENT\_CONFIG (HKCC)** | Contém informações sobre o perfil de hardware atual. |

Novas seções (hives) 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.



A navegação no registro é muito semelhante ao explorador de arquivos do Windows. Use o painel esquerdo para navegar nas seções (hives) e na estrutura abaixo dele e use o painel direito para ver o conteúdo do item realçado no painel esquerdo. Com tantas chaves e subchaves, o caminho da chave pode se tornar muito longo. O caminho é exibido na parte inferior da janela para referência. Como cada chave e subchave é essencialmente um contêiner, o caminho é representado muito parecido com uma pasta em um sistema de arquivos. A barra invertida (\) é usada para diferenciar a hierarquia do banco de dados.

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 cadeia

Como o registro contém quase toda infomação do sistema operacional e do usuário, é essencial garantir que ele não seja comprometido. Aplicativos potencialmente mal-intencionados podem adicionar chaves do Registro para que elas sejam iniciadas quando o computador for iniciado. Durante uma inicialização normal, o usuário não verá o programa iniciar porque a entrada está no registro e o aplicativo não exibe janelas ou indicação de início quando o computador for inicializado. Um keylogger, por exemplo, seria devastador para a segurança de um computador se ele fosse iniciado na inicialização sem o conhecimento ou consentimento do usuário. Ao executar auditorias de segurança normais ou corrigir um sistema infectado, revise os locais de inicialização do aplicativo no registro para garantir que cada item seja conhecido e seguro para ser executado.

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. Outras informações, como quais documentos um usuário e um programa abriram, onde eles estão localizados e quando foram acessados, são armazenadas no registro. Isso tudo é uma informação muito útil quando uma investigação forense precisa ser realizada.

3.2.11

## Laboratório - Explorando Processos, Threads, Handles e Registro do Windows

Neste laboratório, você explorará os processos, threads e handles usando o Process Explorer no Sysinternals Suite. Você também usará o Registro do Windows para alterar uma configuração.

 Explorando Processos, Threads, Handles e Registro do Windows

3.2.12

## Verifique sua compreensão - Identifique a seção do Registro do Windows

Verifique seu entendimento e identifique a seção de registro do Windows escolhendo a MELHOR resposta para as seguintes perguntas.

1.. Qual seção de registro do Windows armazena informações sobre registros OLE (vinculação e incorporação de objetos)?

HKEY\_CLASSES\_ROOT (HKCR)

HKEY\_CURRENT\_CONFIG (HKCC)

HKEY\_CURRENT\_USER (HKCU)

HKEY\_LOCAL\_MACHINE (HKLM)

HKEY\_USERS (HKU)

2. Qual seção de registro do Windows armazena informações sobre o perfil de hardware atual?

HKEY\_CLASSES\_ROOT (HKCR)

HKEY\_CURRENT\_CONFIG (HKCC)

HKEY\_CURRENT\_USER (HKCU)

HKEY\_LOCAL\_MACHINE (HKLM)

HKEY\_USERS (HKU)

3. Qual seção de registro do Windows armazena informações sobre todas as contas de usuário no host?

HKEY\_CLASSES\_ROOT (HKCR)

HKEY\_CURRENT\_CONFIG (HKCC)

HKEY\_CURRENT\_USER (HKCU)

HKEY\_LOCAL\_MACHINE (HKLM)

HKEY\_USERS (HKU)

4. Qual seção de registro do Windows armazena informações sobre o usuário conectado no momento?

HKEY\_CLASSES\_ROOT (HKCR)

HKEY\_CURRENT\_CONFIG (HKCC)

HKEY\_CURRENT\_USER (HKCU)

HKEY\_LOCAL\_MACHINE (HKLM)

HKEY\_USERS (HKU)

5. Qual seção de registro do Windows armazena informações relacionadas ao sistema?

HKEY\_CLASSES\_ROOT (HKCR)

HKEY\_CURRENT\_CONFIG (HKCC)

HKEY\_CURRENT\_USER (HKCU)

HKEY\_LOCAL\_MACHINE (HKLM)

HKEY\_USERS (HKU)

Você identificou com sucesso as respostas corretas.

O ramo de registo HKEY\ \_CLASSES\ \_ROOT (HKCR) do Windows armazena informações sobre registos de ligação e incorporação de objectos (OLE).

O ramo de registo HKEY\ \_CURRENT\ \_CONFIG (HKCC) do Windows armazena informações sobre o perfil de hardware atual.

O ramo de registo HKEY\ \_USERS (HKU) Windows armazena informações relativas a todas as contas de utilizador no host.

O ramo de registo HKEY\ \_CURRENT\ \_USER (HKCU) do Windows armazena informações relativas ao utilizador actualmente registado.

O ramo de registo HKEY\ \_LOCAL\ \_MACHINE (HKLM) do Windows armazena informações relacionadas com o sistema.

# **Configuração e monitoramento do Windows**

3.3.1

## Executar como Administrador

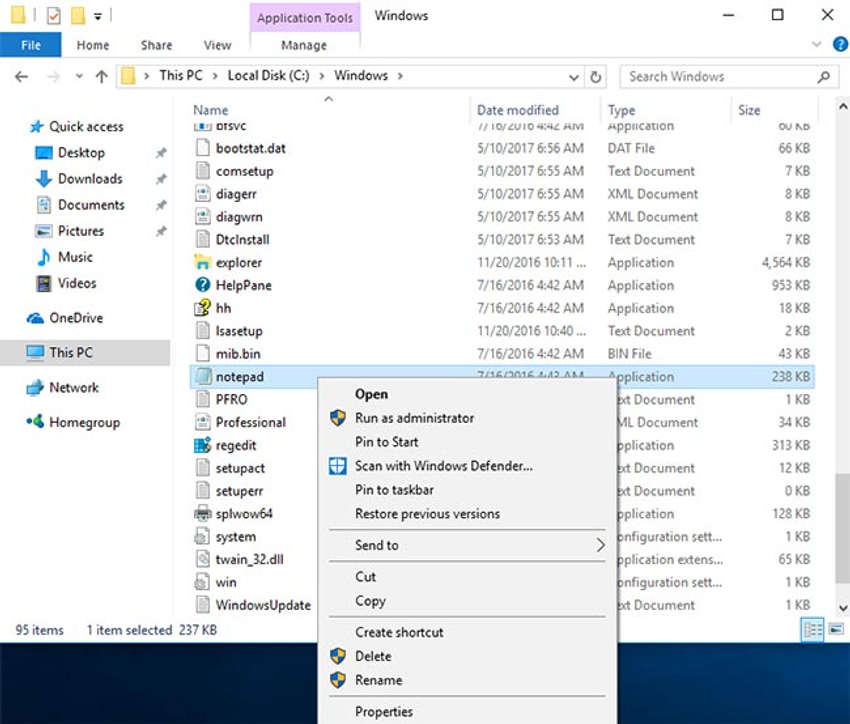
Como prática recomendada de segurança, não é aconselhável fazer logon no Windows usando a conta de Administrador ou uma conta com privilégios administrativos. Isso ocorre porque qualquer programa que é executado enquanto conectado com esses privilégios herdará privilégios administrativos. O malware que tem privilégios administrativos tem acesso total a todos os arquivos e pastas no computador.

Às vezes, é necessário executar ou instalar software que requer os privilégios do Administrador. Para conseguir isso, existem duas maneiras diferentes de instalá-lo.

Administrador

Prompt de comando do administrador

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



3.3.2

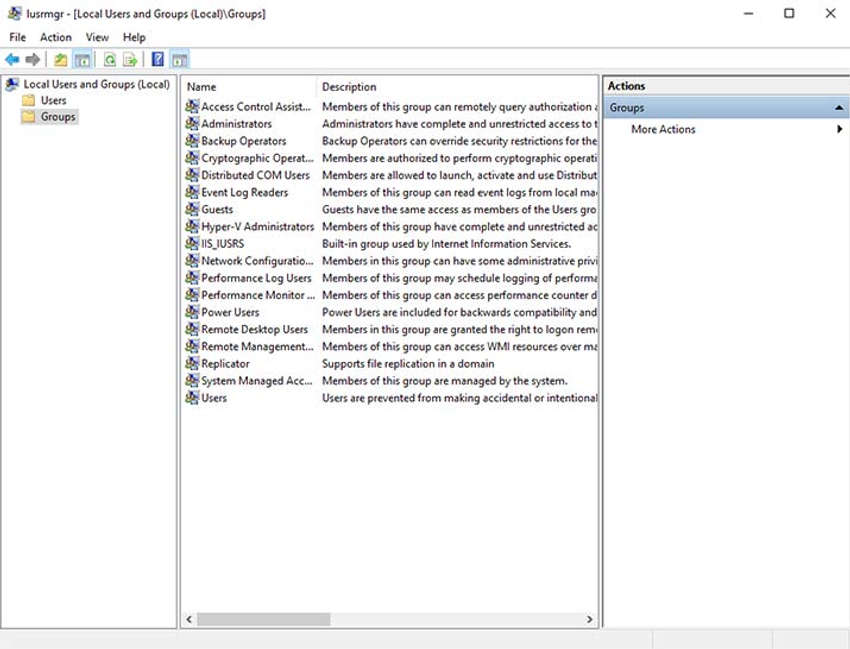
## Usuários e Domínios Locais

Quando inicia um novo computador pela primeira vez ou instala o Windows, será pedido para criar uma conta de usuário. Isso é conhecido como um usuário local. Essa conta conterá todas as configurações de personalização, permissões de acesso, locais de arquivos e muitos outros dados específicos do usuário. Há também duas outras contas presentes, o convidado e o administrador. Ambas as contas são desabilitadas por padrão.

Como prática recomendada de segurança, não habilite a conta Administrador e não conceda privilégios administrativos aos usuários padrão. Se um usuário precisar executar qualquer função que exija privilégios administrativos, o sistema solicitará a senha de Administrador e permitirá que somente essa tarefa seja executada como administrador. Exigir a senha de administrador protege o computador impedindo que qualquer software não autorizado instale, execute ou acesse arquivos.

A conta Convidados não deve ser ativada. A conta de convidado não tem uma senha associada a ela porque é criada quando um computador vai ser usado por muitas pessoas diferentes que não têm contas no computador. Cada vez que a conta de convidado faz logon, um ambiente padrão é fornecido a eles com privilégios limitados.

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. Por exemplo, o grupo Usuários do Log de Desempenho permite que os membros agendem o log de contadores de desempenho e coletem logs localmente ou remotamente. Os usuários e grupos locais são gerenciados com o miniaplicativo do **lusrmgr.msc** painel de controle, conforme mostrado na figura.



Além dos grupos, o Windows também pode usar 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. Este banco de dados é armazenado em computadores especiais ou grupos de computadores chamados controladores de domínio (DCs). Cada utilizador e computador no domínio tem de autenticar contra o controlador de domínio para iniciar sessão e acessar os recursos de rede. As configurações de segurança para cada usuário e cada computador são definidas pelo controlador de domínio para cada sessão. Qualquer configuração fornecida pelo controlador de domínio padrão para o computador local ou configuração de conta de usuário.

3.3.3

## 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. Além disso, arquivos chamados de batch podem ser criados para executar vários comandos sucessivamente, assim como um script básico.

Para abrir a CLI do Windows, procure **cmd.exe** e clique no programa. Lembre-se que clicar com o botão direito do mouse no programa oferece a opção de Executar como administrador, dando muito mais poder aos comandos que serão usados.

O prompt exibe o local atual dentro do sistema de arquivos. 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. A letra da unidade é seguida por dois pontos e barra invertida (). Isso indica a raiz, ou nível mais alto, do dispositivo. A hierarquia de pastas e arquivos no dispositivo é indicada separando-os com uma barra invertida. Por exemplo, o caminho C: \ Users \ Jim \ Desktop \ file.txt se refere a um arquivo chamado file.txt que está na pasta Desktop dentro da pasta Jim dentro da pasta Usuários na raiz da unidade C:.
* Comandos que têm opções opcionais usam a barra (/) para delinear entre o comando e a opção.
* 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**.

Mesmo que a CLI tenha muitos comandos e recursos, ela não pode funcionar em conjunto com o núcleo do Windows ou a GUI. 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 e pode ser aberto pesquisando por “powershell” e clicando no programa. 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.

Para ver mais informações sobre o Windows PowerShell e começar a usá-lo, digite **help** no PowerShell, conforme mostrado na saída do comando.

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=108518.

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 &quot;Run as administrator&quot; 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 --

Há quatro níveis de ajuda no Windows PowerShell:

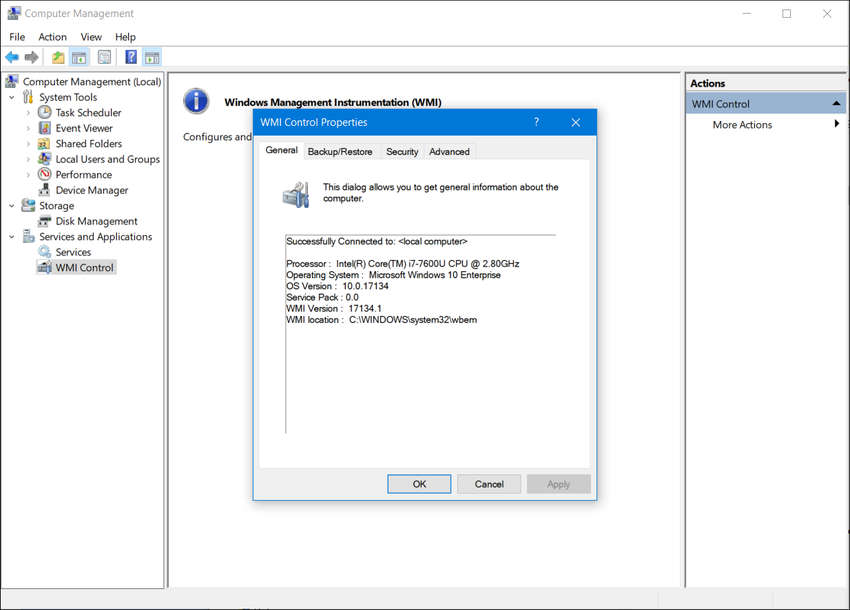
* **get-help** PS command - Exibe a ajuda básica para um comando
* **get-help** PS command\ [\ -examples] - Exibe a ajuda básica para um comando com exemplos
* **get-help** PS command\ [\ -detailed] - Exibe ajuda detalhada para um comando com exemplos
* **get-help** PS command\ [\ -full] - Exibe todas as informações de ajuda de um comando com exemplos em maior profundidade

3.3.4

## 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**.

A janela Propriedades de Controle WMI é mostrada na figura.



Estas são as quatro guias na janela Propriedades de Controle WMI:

* **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

Alguns ataques hoje usam o WMI para se conectar a sistemas remotos, modificar o registro e executar comandos. O WMI ajuda-os a evitar a detecção porque é tráfego comum, na maioria das vezes confiável pelos dispositivos de segurança de rede e os comandos WMI remotos geralmente não deixam evidências no host remoto. Devido a isso, o acesso WMI deve ser estritamente limitado.

3.3.5

## O comando net

O Windows tem muitos comandos que podem ser inseridos na linha de comando. Um comando importante é o comando **net**, que é usado na administração e manutenção do sistema operacional. O comando **net** suporta muitos subcomandos que seguem o comando **net** e podem ser combinados com opões para focar na saída específica.

Para ver uma lista de muitos comandos **net**, escreva **net help** na linha de comandos. 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**, conforme mostrado abaixo.

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:\>

A tabela lista alguns comandos **net** comuns.

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

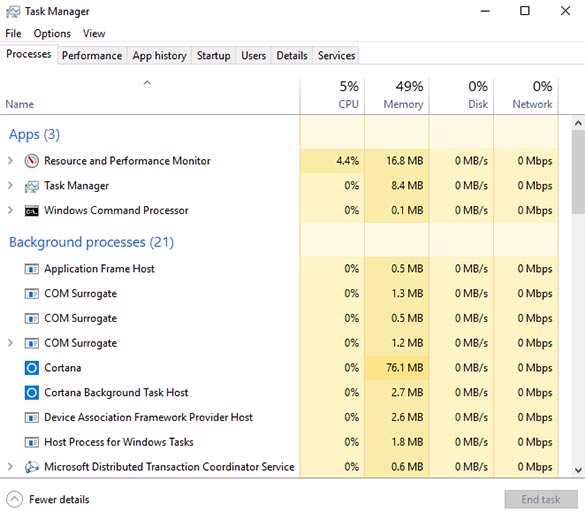
3.3.6

## Gerenciador de tarefas e Monitor de recursos

Existem duas ferramentas muito importantes e úteis para ajudar um administrador a compreender os vários aplicativos, serviços e processos diferentes que estão sendo executados em um computador Windows. Essas ferramentas também fornecem informações sobre o desempenho do computador, como CPU, memória e uso da rede. Essas ferramentas são especialmente úteis ao investigar um problema em que o malware é suspeito. Quando um componente não está executando da maneira que deveria ser, essas ferramentas podem ser usadas para determinar qual o problema pode ser.

**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.

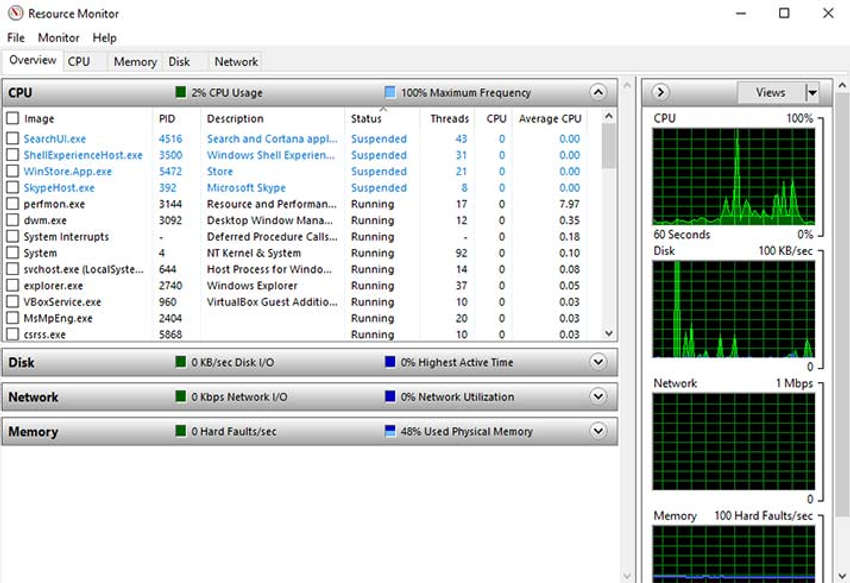


A tabela descreve as sete guias no Gerenciador de Tarefas.

| **Guias do gerenciador de tarefas** | **Descrição** |
| --- | --- |
| **Processos** | * Lista todos os programas e processos que estão em execução no momento. * Exibe a utilização da CPU, da memória, do disco e da rede de cada processo. * As propriedades de um processo podem ser examinadas ou encerradas se ele não estiver se comportando corretamente ou tiver parado. |
| **Desempenho** | * Uma exibição de todas as estatísticas de desempenho fornece uma visão geral útil do desempenho da CPU, memória, disco e rede. * Clicar em cada item no painel esquerdo irá mostrar estatísticas detalhadas desse item no painel direito. |
| **Histórico de aplicativos** | * O uso de recursos por aplicativo ao longo do tempo fornece informações sobre aplicativos que estão consumindo mais recursos do que deveriam. * Clique em **Opções** e **Mostrar histórico de todos os processos** para ver o histórico de todos os processos executados desde que o computador foi iniciado. |
| **Inicializar** | * Todos os aplicativos e serviços que iniciam quando o computador é inicializado são mostrados nesta guia. * Para desativar o início de um programa na inicialização, **clique com** o botão direito do mouse no item e escolha **Desativar**. |
| **Usuários** | * Todos os usuários que estão conectados ao computador são mostrados nesta guia. * Também são mostrados todos os recursos que os aplicativos e processos de cada usuário estão usando. * Nesta guia, um administrador pode desconectar um usuário do computador. |
| **Detalhes** | * Semelhante à guia Processos, essa guia fornece opções de gerenciamento adicionais para processos, como definir uma prioridade para que o processador dedique mais ou menos tempo a um processo. * A afinidade da CPU também pode ser definida, o que determina qual núcleo ou CPU um programa usará. * Além disso, 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. |
| **Serviços** | * Todos os serviços que são carregados são mostrados nesta guia. * O ID do processo (PID) e uma breve descrição também são mostrados juntamente com o status de Executando ou Parado. * Na parte inferior, há um botão para abrir o console Serviços que fornece gerenciamento adicional de serviços. |

**Monitor de recursos**

Quando forem necessárias informações mais detalhadas sobre o uso de recursos, você poderá usar o Monitor de Recursos, conforme mostrado na figura.



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.

A tabela descreve as cinco guias do Monitor de Recursos.

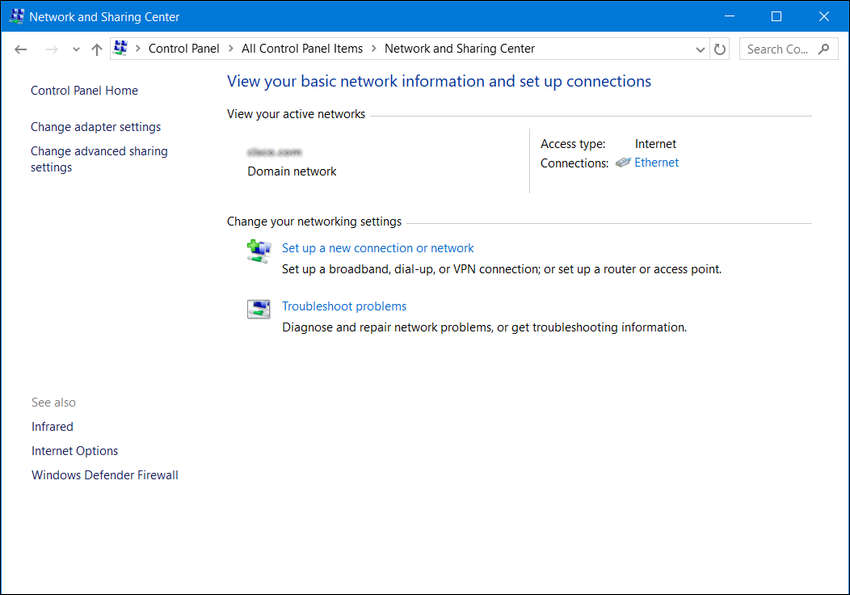
| **Guias do Monitor de Recursos** | **Descrição** |
| --- | --- |
| **Visão geral** | * A guia exibe o uso geral de cada recurso. * Se você selecionar um único processo, ele será filtrado em todas as guias para mostrar somente as estatísticas desse processo. |
| **CPU** | * O PID, o número de threads, qual CPU o processo está usando e o uso médio da CPU de cada processo é mostrado. * Informações adicionais sobre quaisquer serviços em que o processo se baseia e os identificadores e módulos associados podem ser vistas expandindo as linhas inferiores. |
| **Memória** | * Todas as informações estatísticas sobre como cada processo usa memória são mostradas nesta guia. * Além disso, 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. |
| **Rede** | * Todos os processos que estão usando a rede são mostrados nesta guia, com estatísticas de leitura/gravação. * Mais importante ainda, as conexões TCP atuais são mostradas, juntamente com todas as portas que estão escutando. * Esta guia é muito útil ao tentar determinar quais aplicativos e processos estão se comunicando pela rede. * Permite saber se um processo não autorizado está acessando a rede, ouvindo uma comunicação e o endereço com o qual está se comunicando. |

3.3.7

## Redes

Um dos recursos mais importantes de qualquer sistema operacional é a capacidade do computador se conectar a uma rede. Sem esse recurso, não há acesso aos recursos de rede ou à internet. Para configurar as propriedades de rede do Windows e testar as configurações de rede, o Centro de Rede e Compartilhamento é usado. A maneira mais fácil de executar esta ferramenta é procurá-la e clicar nela. Use o Centro de Rede e Compartilhamento para verificar ou criar conexões de rede, configurar o compartilhamento de rede e alterar as configurações do adaptador de rede.

**Centro de Rede e Compartilhamento**



A visualização inicial mostra uma visão geral da rede ativa. Essa exibição mostra se há acesso à Internet e se a rede é privada, pública ou convidada. O tipo de rede, com ou sem fio, também é mostrado. Nessa janela, você pode ver o Grupo Doméstico ao qual o computador pertence ou criar um caso ainda não faça parte de um Grupo Doméstico. Essa ferramenta também pode ser usada para alterar configurações do adaptador, alterar configurações de compartilhamento antecipado, configurar uma nova conexão ou solucionar problemas. Observe que o Grupo Doméstico foi removido do Windows 10 na versão 1803.

**Alterar as configurações do adaptador**

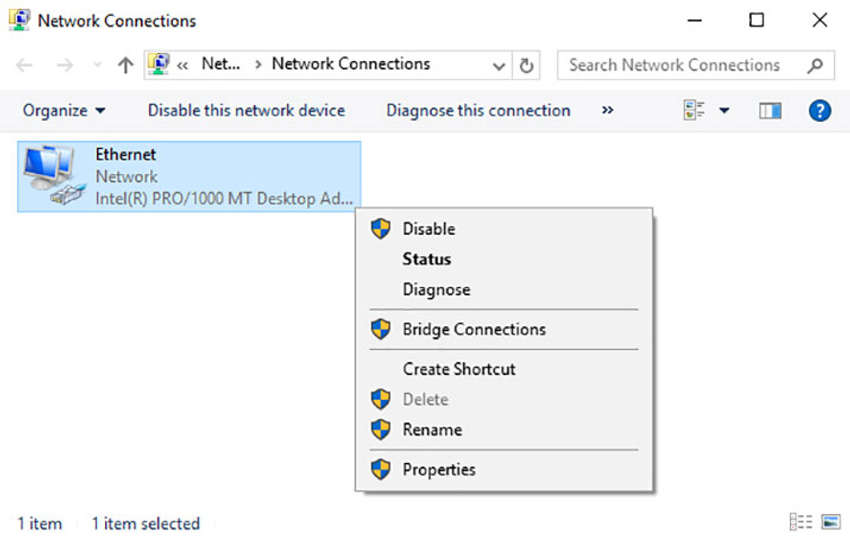
Para configurar um adaptador de rede, escolha **Alterar configurações do adaptador** no Centro de Rede e Compartilhamento para mostrar todas as conexões de rede disponíveis. Selecione o adaptador que você deseja configurar. Neste caso, alteramos um adaptador Ethernet para adquirir seu endereço IPv4 automaticamente da rede.

1. Propriedades do adaptador de acesso

2. Acessar propriedades de TCP/IPv4

3. Alterar configurações

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



**nslookup and netstat**

O Sistema de Nomes de Domínio (DNS, Domain Name System) 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. Quando o endereço é retornado, você sabe que o DNS está funcionando corretamente. Você também pode verificar quais portas estão abertas, onde elas estão conectadas e qual é seu status atual. Digite **netstat** na linha de comando para ver detalhes das conexões de rede ativas, conforme mostrado na saída do comando. O comando **netstat** será examinado mais adiante neste módulo.

C:\Users\USER >netstat

Conexões Ativas

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 ESTABELECIDO

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

3.3.8

## Acessando recursos de rede

Como outros sistemas operacionais, o Windows usa rede para muitos aplicativos diferentes, como serviços da Web, email e arquivos. Originalmente desenvolvido pela IBM, a Microsoft ajudou no desenvolvimento do protocolo SMB (Server Message Block) para compartilhar recursos de rede. O SMB é usado principalmente para acessar arquivos em hosts remotos (Ele é usado para compartilhar recursos de rede.). O formato UNC (Universal Naming Convention) é usado para se conectar a recursos, por exemplo:

**\\ nome\_do\_servidor\ nome\_do\_compartilhamento\arquivo**

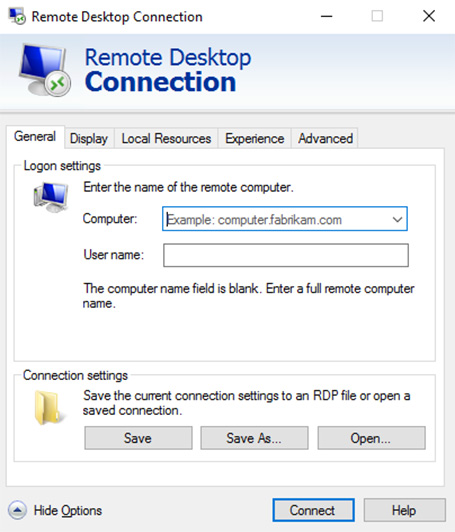
No UNC, nome\_do\_servidor é o servidor que está hospedando o recurso. Pode ser um nome DNS, um nome NetBIOS ou simplesmente um endereço IP. O nome do compartilhamento é a raiz da pasta no sistema de arquivos no host remoto, enquanto o arquivo é o recurso que o host local está tentando encontrar. O arquivo pode estar mais profundo dentro do sistema de arquivos e essa hierarquia precisará ser indicada.

Ao compartilhar recursos na rede, a área do sistema de arquivos que será compartilhada precisará ser identificada. O controle de acesso pode ser aplicado às pastas e arquivos para restringir usuários e grupos a funções específicas, como ler, gravar ou negar. Há também compartilhamentos especiais que são criados automaticamente pelo Windows. Essas ações são chamadas de ações administrativas. Um compartilhamento administrativo é identificado pelo cifrão ($) que vem após o nome do compartilhamento. Cada volume de disco tem um compartilhamento administrativo, representado pela letra do volume e o $, como C$, D$ ou E$. A pasta de instalação do Windows é compartilhada como admin$, a pasta das impressoras é compartilhada como print$ e há outros compartilhamentos administrativos que podem ser conectados. Somente usuários com privilégios administrativos podem acessar esses compartilhamentos.

A maneira mais fácil de se conectar a um compartilhamento é digitar o UNC do compartilhamento no Explorador de Arquivos do Windows, na caixa na parte superior da tela que mostra a listagem de rastreamento do local atual do sistema de arquivos. Quando o Windows tentar se conectar ao compartilhamento, você será solicitado a fornecer credenciais para acessar o recurso. Lembre-se de que, como o recurso está em um computador remoto, as credenciais precisam ser para o computador remoto, não para o computador local.

Além de acessar compartilhamentos em hosts remotos, você 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). Ao investigar incidentes de segurança, um analista de segurança usa o RDP frequentemente para acessar computadores remotos. Para iniciar o RDP e conectar-se a um computador remoto, procure área de trabalho remota e clique no aplicativo. A janela Conexão de área de trabalho remota é mostrada na figura.

Como o RDP foi projetado para permitir que usuários remotos controlem hosts individuais, ele é um alvo natural para atores de ameaças. Deve-se ter cuidado ao ativar o RDP, especialmente em versões legado sem os patches do Windows, como aquelas que ainda são encontradas em sistemas de controle industrial. Deve-se ter cuidado para limitar a exposição do RDP à internet, e abordagens de segurança e políticas de controle de acesso, como Zero Trust, devem ser usadas para limitar o acesso a hosts internos.



3.3.9

## 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 chamado 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.

**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.

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

3.3.10

## Laboratório – Criação de Contas de Usuário

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

 Criar contas de usuário

3.3.11

## Laboratório - Usando o Windows PowerShell

O objetivo do laboratório é explorar algumas das funções do PowerShell.

 Usando o Windows PowerShell

3.3.12

## Laboratório - Gerenciador de Tarefas do Windows

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

 Gerenciador de Tarefas no Windows

3.3.13

## Laboratório - Monitorar e gerenciar recursos do sistema no Windows

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

# **Segurança do Windows**

3.4.1

## O Comando netstat

Quando o malware está presente em um computador, ele geralmente abre portas de comunicação no host para enviar e receber dados. O comando **netstat** pode ser usado para procurar conexões de entrada ou saída que não estão autorizadas. Quando usado por conta própria, o comando **netstat** exibirá todas as conexões TCP ativas.

Examinando essas conexões, é possível determinar quais dos programas estão escutando conexões que não estão autorizadas. Quando um programa é suspeito de ser malware, uma pequena pesquisa pode ser realizada para determinar sua legitimidade. A partir daí, 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, você pode vincular as conexões aos processos em execução que as criaram no Gerenciador de Tarefas. Para fazer isso, abra um prompt de comando com privilégios administrativos e digite o comando **netstat -abno**, conforme mostrado na saída do comando.

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

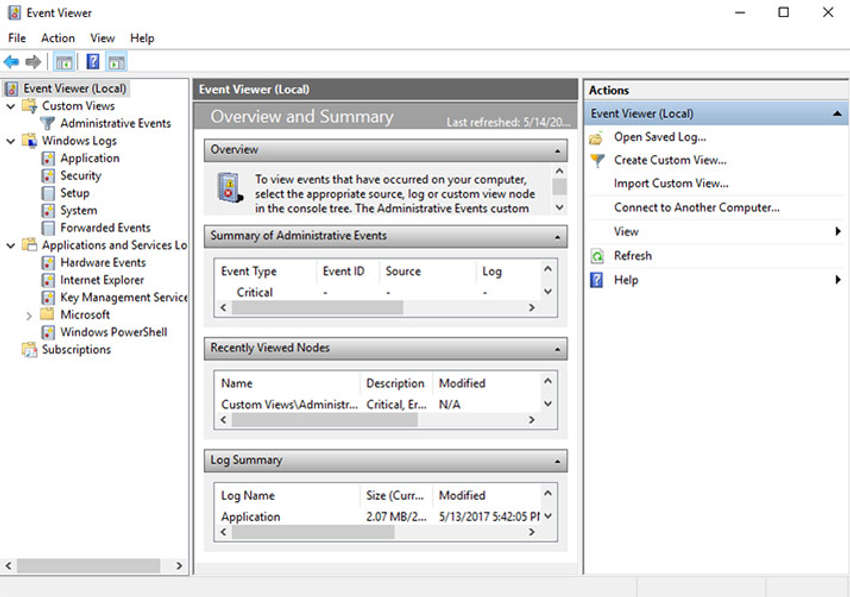
**Observação**: Se você não estiver no modo administrador, uma mensagem “A operação solicitada requer elevação” será exibida. Pesquise Prompt de Comando. Clique com o botão direito do mouse em **Prompt de comando** e escolha **Executar como administrador.**

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. Você também pode rastrear esse processo para o Gerenciador de Tarefas do Windows e cancelar o processo. Pode haver mais de um processo listado com o mesmo nome. Se este for o caso, use o PID para encontrar o processo correto. Cada processo em execução no computador tem um PID exclusivo. 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**.

3.4.2

## 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 valiosa ferramenta de solução de problemas porque fornecem informações para identificar um problema. Para abrir o Visualizador de Eventos, procure-o e clique no ícone do programa, conforme mostrado na figura.



O Windows inclui duas categorias de logs de eventos: Logs do Windows e Logs de Aplicativos e Serviços. Cada uma dessas categorias tem vários tipos de log. Os eventos exibidos nesses logs têm um nível: informações, aviso, erro ou crítico. Eles também têm a data e hora em que o evento ocorreu, juntamente com a origem do evento e um ID que se relaciona com esse tipo de evento.

Também é possível criar uma visualização personalizada. Isso é útil ao procurar certos tipos de eventos, encontrar eventos que aconteceram durante um determinado período de tempo, exibir eventos de um determinado nível e muitos outros critérios. Há uma exibição personalizada interna chamada Eventos administrativos que mostra todos os eventos críticos, de erro e de aviso de todos os logs administrativos. Esta é uma boa visão para começar ao tentar solucionar um problema.

Os logs de eventos de segurança são encontrados em Logs do Windows. Eles usam IDs de evento para identificar o tipo de evento.

3.4.3

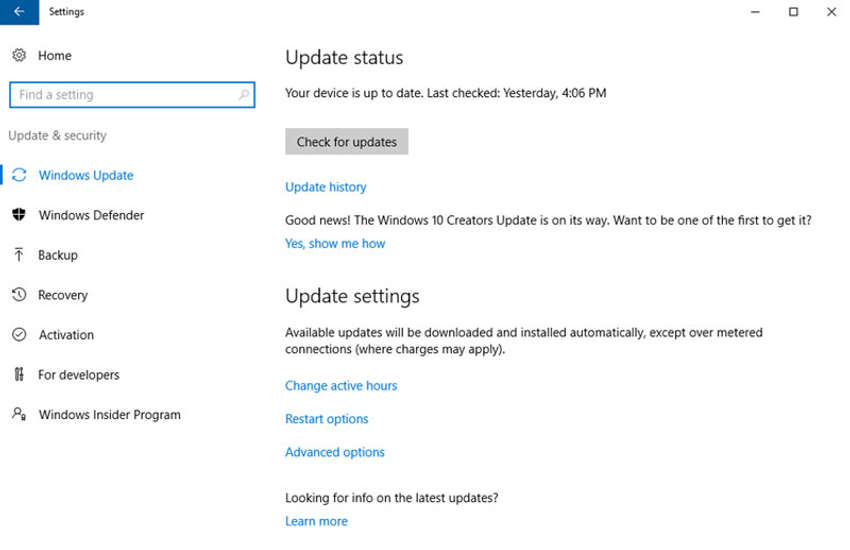
## Configurações do Windows Update

Nenhum software é perfeito e o sistema operacional Windows não é exceção. Os invasores estão constantemente criando novas maneiras de comprometer computadores e explorar códigos ruins. Alguns desses ataques vêm tão rapidamente que as defesas contra eles ainda não foram criadas e distribuídas. Estes são chamados de ataque de dia zero. Microsoft e desenvolvedores de software de segurança estão sempre tentando ficar à frente dos atacantes, mas eles nem sempre são bem-sucedidos. Para garantir o mais alto nível de proteção contra esses ataques, certifique-se sempre de que o Windows está atualizado com os service packs e patches de segurança mais recentes.

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. 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. Essas atualizações incluem atualizações de segurança, atualizações críticas e service packs. Dependendo da configuração escolhida, o Windows baixa e instala, automaticamente, todas as atualizações de alta prioridade que o computador precisar, ou notifica o usuário, conforme essas atualizações estiverem disponíveis. Para configurar as configurações da atualização do Windows, procure o Windows Update e clique no aplicativo.

O status da atualização, mostrado na figura, permite que você verifique as atualizações manualmente e veja o histórico de atualizações do computador.



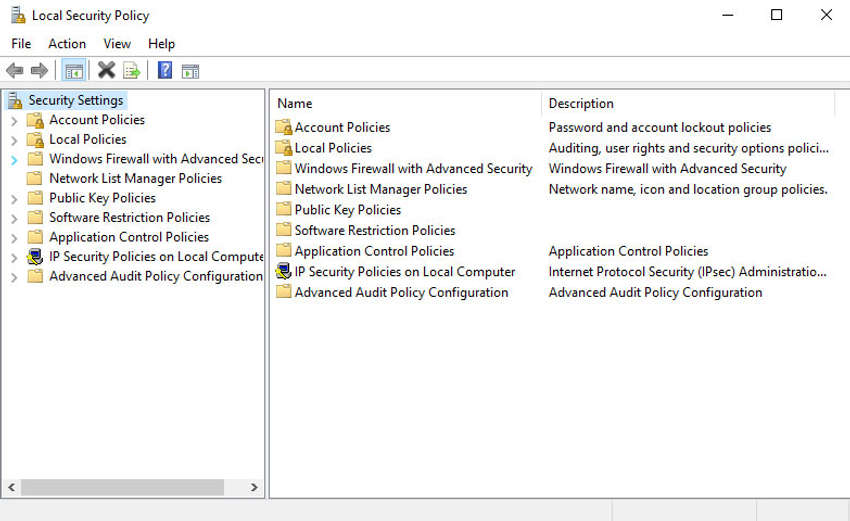
Há também configurações para as horas em que o computador não será reiniciado automaticamente, por exemplo, durante o horário comercial regular. Você também pode escolher quando reiniciar o computador após uma atualização, se necessário, com as opções Reiniciar. Opções avançadas também estão disponíveis para escolher como as atualizações são instaladas como outros produtos da Microsoft são atualizados.

3.4.4

## Ferramenta de 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. A política de segurança é um documento em constante desenvolvimento, baseado em mudanças na tecnologia, nos negócios e nas necessidades dos funcionários.

Na maioria das redes que usam computadores Windows, o Active Directory é configurado com domínios em um servidor Windows. Computadores Windows ingressam no domínio. O administrador configura uma Política de Segurança de Domínio que se aplica a todos os computadores que ingressam no domínio. As políticas de conta são definidas automaticamente quando um usuário efetua login em um computador que é membro de um domínio. A Política de Segurança Local do Windows, mostrada na figura, pode ser usada para computadores autônomos que não fazem parte de um domínio do Active Directory. Para abrir o aplicativo Política de Segurança Local, procure Política de Segurança Local e clique no programa.



As diretrizes de senha são um componente importante de uma política de segurança. Qualquer usuário que fizer logon em um computador ou se conectar a um recurso de rede deve ter uma senha. As senhas ajudam a evitar roubo de dados e atos mal-intencionados. As senhas também ajudam a confirmar se o registro de eventos é válido, garantindo que o usuário seja quem diz ser. Na Política de Segurança Local, a Política de Senha é encontrada em Políticas de Conta e define os critérios para as senhas 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. Por exemplo, você pode definir a política para permitir que o usuário insira um nome de usuário e / ou senha incorretos cinco vezes. Após cinco tentativas, a conta é bloqueada por 30 minutos. Depois de 30 minutos, o número de tentativas é redefinido para zero e o usuário pode tentar entrar novamente.

É importante garantir que os computadores estejam seguros, quando os usuários estiverem ausentes. Uma política de segurança deve conter uma regra sobre a necessidade de se bloquear um computador, quando a proteção de tela for iniciada. Isso garantirá que, depois de um curto período de tempo longe do computador, a proteção de tela será iniciada e o computador não poderá ser usado, até que o usuário faça login novamente.

Se a política de segurança local em cada computador autônomo for a mesma, use o recurso Exportar política. Salve a diretiva com um nome, como workstation.inf. Copie o arquivo de política para uma mídia externa ou unidade de rede para usar em outros computadores independentes. 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 muitas outras configurações de segurança que se aplicam especificamente ao computador local. Você pode configurar Direitos de Usuário, Regras de Firewall e até mesmo a capacidade de restringir os arquivos que os usuários ou grupos têm permissão para executar com o AppLocker.

3.4.5

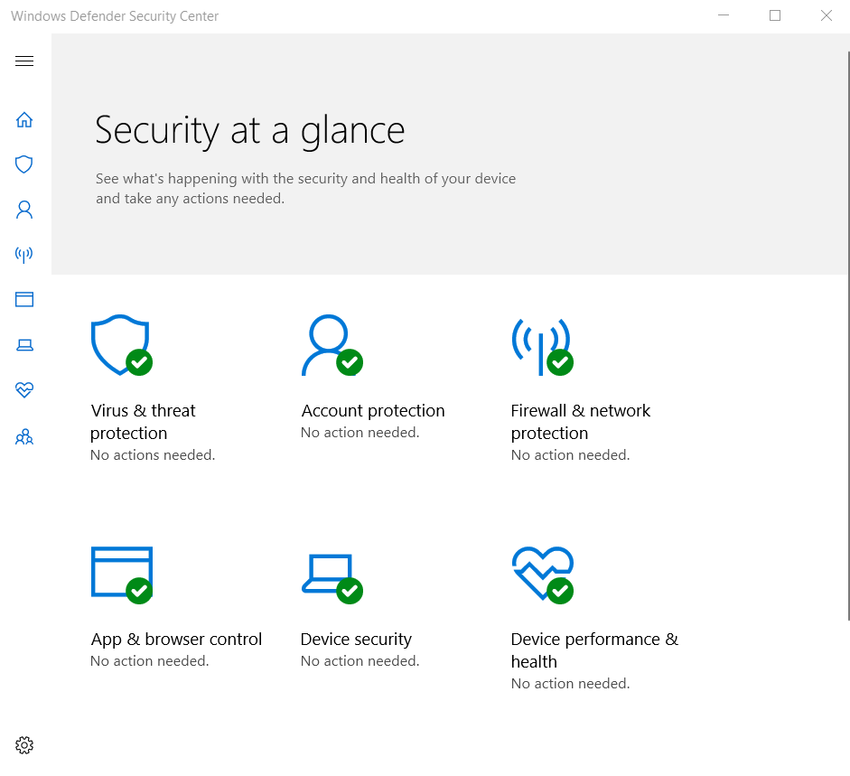
## Windows Defender

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 que você proteja os computadores e dispositivos móveis com software antimalware de qualidade. Os seguintes tipos de programas antimalware estão disponíveis:

* **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 exibem anúncios em seu 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 verifica a existência de keyloggers e outros spywares.
* **Fontes confiáveis / não confiáveis** - Este programa avisa sobre programas inseguros prestes a serem instalados ou sites inseguros antes de serem visitados.

Pode ser necessário usar vários programas diferentes e fazer várias varreduras para remover completamente todos os softwares mal-intencionados. Execute apenas um programa de proteção contra malware por vez.

Várias empresas de segurança confiáveis, como McAfee, Symantec e Kaspersky, oferecem proteção completa contra malware para computadores e dispositivos móveis. O Windows possui proteção interna contra vírus e spyware chamada Windows Defender, como mostrado na figura. O Windows Defender está ativado por padrão para fornecer proteção em tempo real contra infecções.



Para abrir o Windows Defender, procure-o e clique no programa. Embora o Windows Defender funcione em segundo plano, você pode executar varreduras manuais do computador e dispositivos de armazenamento. Você também pode atualizar manualmente as definições de vírus e spyware na guia **Atualizar**. Além disso, para ver todos os itens encontrados durante varreduras anteriores, clique na guia **Histórico**.

3.4.6

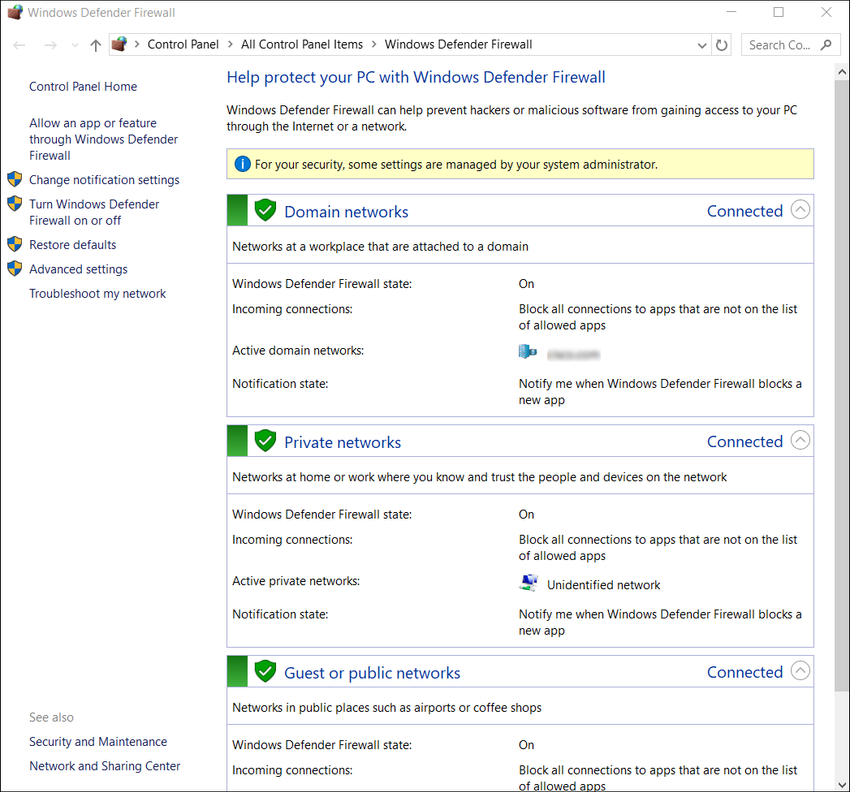
## Firewall do Windows Defender

Um firewall nega, seletivamente, o tráfego a um computador ou a um segmento de rede. Os firewalls trabalham, geralmente, abrindo e fechando as portas usadas por vários aplicativos. Ao abrir apenas as portas necessárias em um firewall, você está implementando uma política de segurança restritiva. Qualquer pacote não explicitamente permitido é negado. Ao contrário, uma política de segurança permissiva permite acesso por todas as portas, exceto aquelas explicitamente negadas. Antigamente, software e hardware eram enviados com configurações permissivas. Como os usuários negligenciavam a configuração do equipamento, as configurações permissivas padrão deixavam muitos dispositivos expostos a invasores. Agora, a maioria dos dispositivos é enviada com configurações o mais restritivas possível, mesmo que permitindo ainda uma configuração fácil.

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.

Se desejar usar um firewall por software diferente, você precisará desativar o firewall do Windows. Para desativar o Firewall do Windows, clique em **Ativar ou desativar o Firewall do Windows.**

Muitas configurações adicionais podem ser encontradas em **Configurações avançadas**. Aqui você pode criar regras de tráfego de entrada ou saída com base em critérios diferentes. Você também pode importar e exportar políticas ou monitorar diferentes aspectos do firewall.



3.4.7

Verifique sua compreensão - Identifique a ferramenta do Windows

Verifique sua compreensão e identifique o comando ou ferramenta do Windows escolhendo a MELHOR resposta para as seguintes perguntas.

# **Resumo do sistema operacional Windows**

3.5.1

## O que aprendi neste módulo?

**Histórico do Windows**

Os primeiros computadores precisaram de um sistema operacional de disco (DOS, Disk Operating System) 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 (GUI) que executava dentro do MS-DOS. No entanto, as versões modernas do Windows estão no controle direto do computador e seu hardware e suportam vários processos de usuário. Isso é muito diferente do que o MS-DOS de processo único e penas um usuário. Desde 1993, houve mais de 20 lançamentos do Windows que são baseados no sistema operacional NT. Os usuários usam uma GUI do Windows para trabalhar com arquivos de dados e software. A GUI tem uma área principal conhecida como Área de Trabalho e uma Barra de Tarefas situada abaixo da área de trabalho. A Barra de Tarefas inclui o menu Iniciar, ícones de inicialização rápida e uma área de notificação. O Windows tem muitas vulnerabilidades. Recomendações para proteger o sistema operacional Windows incluem o uso de proteção contra vírus ou malware, uso de senhas fortes, uso de firewall e uso limitado da conta de administrador, entre outras.

**Arquitetura e operações do Windows**

O Windows consiste em uma camada de abstração de hardware (HAL) que é um software que lida com toda a comunicação entre o hardware e o kernel. O kernel tem controle sobre todo o computador e lida com solicitações de entrada e saída, memória e todos os periféricos conectados ao computador. O Windows opera em dois modos diferentes. O primeiro é o modo de usuário. A maioria dos programas do Windows são executados no modo de usuário. O segundo é o modo kernel. Ele permite o acesso direto do código do sistema operacional ao hardware do computador. O Windows suporta vários sistemas de arquivos diferentes, mas o NTFS é o mais utilizado. Os volumes NTFS incluem o setor de inicialização de partição, tabela de arquivos mestre, arquivos de sistema e a área de arquivo. Quando um computador inicializa, ele primeiro acessa as informações do sistema e o código armazenados no hardware do BIOS. O código de inicialização do BIOS executa um auto-teste do sistema chamado POST, localiza e carrega o sistema operacional Windows e carrega outros programas associados para iniciar o sistema operacional. O Windows deve ser sempre desligado corretamente.

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 4 gigabytes. Cada processo num computador Windows de 64 bits suporta um espaço de endereço virtual de até 8 terabytes. 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 existem chaves, seguido por subchaves. Existem cinco seções (hives) de registo que contêm dados relativos à configuração e operação do Windows. Existem centenas de chaves e subchaves.

**Configuração e monitoramento do Windows**

Por razões de segurança, não é aconselhável iniciar sessão no Windows utilizando a conta de Administrador ou uma conta com privilégios administrativos. Não dê privilégios administrativos aos usuários padrão. Não ative a conta Convidados, a menos que o computador seja usado por muitas pessoas diferentes que não tenham contas. 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 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 Centro de Rede e Compartilhamento é utilizado para configurar as propriedades de rede do Windows e testar as definições de rede. O protocolo SMB (Server Message Block) é usado para compartilhar recursos de rede, como arquivos em hosts remotos. O formato UNC (Universal Naming Convention) é usado para se conectar a recursos. O Windows Server é uma edição do Windows que é usada principalmente em data centers. Ele fornece serviços de rede, arquivos, Web e gerenciamento para uma rede ou domínio do Windows.

**Segurança do Windows**

O malware pode abrir portas de comunicação para se comunicar e espalhar. 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. Isso permite que softwares potencialmente mal-intencionados desconhecidos sejam identificados e desativados. O Visualizador de Eventos do Windows fornece acesso a vários eventos registrados em relação à operação de um computador. O registro do Windows registra eventos de aplicativos e serviços do Windows. Os níveis de gravidade de eventos registrados variam por meio das informações, advertência, erro ou níveis críticos. É muito importante manter o Windows atualizado para se proteger contra novas ameaças à segurança. Os patches de software, as atualizações e os service packs abordam as vulnerabilidades de segurança à medida que são descobertas. O Windows deve ser configurado para baixar e instalar atualizações automaticamente à medida que elas se tornarem disponíveis. O Windows pode ser configurado para instalar e reiniciar um computador em horários especificados do dia.

Módulo 3: Questionário do sistema operacional Windows

Parte superior do formulário