# Laboratório de Administração de Sistemas Operacionais de Redes


*Prof. Me. Wallace Rodrigues de Santana*

*www.neutronica.com.br*




# Atribuição-NãoComercial-CompartilhaIgual 3.0 Brasil (CC BY-NC-SA 3.0)

## Você tem a liberdade de:

**Compartilhar** — copiar, distribuir e transmitir a obra.

**Remixar** — criar obras derivadas.

## Sob as seguintes condições:

**Atribuição** — Você deve creditar a obra da forma especificada pelo autor ou licenciante (mas não de maneira que sugira que estes concedem qualquer aval a você ou ao seu uso da obra).

**Uso não comercial** — Você não pode usar esta obra para fins comerciais.

**Compartilhamento pela mesma licença** — Se você alterar, transformar ou criar em cima desta obra, você poderá distribuir a obra resultante apenas sob a mesma licença, ou sob uma licença similar à presente.

## Ficando claro que:

**Renúncia** — Qualquer das condições acima pode ser **renunciada** se você obtiver permissão do titular dos direitos autorais.

**Domínio Público** — Onde a obra ou qualquer de seus elementos estiver em **domínio público** sob o direito aplicável, esta condição não é, de maneira alguma, afetada pela licença.

**Outros Direitos** — Os seguintes direitos não são, de maneira alguma, afetados pela licença:

- Limitações e exceções aos direitos autorais ou quaisquer **usos livres** aplicáveis;
- Os **direitos morais** do autor;
- Direitos que outras pessoas podem ter sobre a obra ou sobre a utilização da obra, tais como **direitos de imagem** ou privacidade.

**Aviso** — Para qualquer reutilização ou distribuição, você deve deixar claro a terceiros os termos da licença a que se encontra submetida esta obra. A melhor maneira de fazer isso é com um link para esta página.

# Diversidade e inclusão

Este material foi escrito visando promover a diversidade e a inclusão, respeitando e valorizando as relações humanas de modo a propiciar uma cultura mais inclusiva e que impacte positivamente a sociedade.

Ao adotar uma linguagem inclusiva, este material busca repensar os termos usados na literatura técnica para reduzir as barreiras à equidade e promover o respeito, buscando estar livre de linguagem ofensiva ou sugestiva.

A indústria de Tecnologia da Informação tem trabalhado arduamente para mudar estes termos para alternativas mais apropriadas, mas sistemas legados ainda poderão contê-los.

# Quem é Wallace Santana?

**Formação Acadêmica:**

- Tecnólogo em Mecânica de Precisão pela FATEC-SP [2001]
- Tecnólogo em Informática pela FATEC Mauá [2005]
- Mestre em Engenharia da Informação pela UFABC [2010]
- Especialista em Gestão Pública pela UNIFESP [2019]

**Experiência Profissional**

- Analista de Sistemas na CEAGESP [2005-2008]
- Analista de Tecnologia da Informação e Comunicação na PRODAM [2008-2010]
- Consultor Técnico Legislativo da Câmara Municipal de São Paulo [desde 2010]

**Docência**

- Faculdade de Mauá [2011-2015]
- FATEC São Caetano do Sul [2016-2017]
- Faculdade Drummond [desde 2018]

# Módulo Zero

Apresentação da disciplina

# Objetivo

Capacitar o aluno para a administração de sistemas operacionais de redes utilizando-se de boas práticas e ferramentas amplamente adotadas na área.

# Módulos

1. Console e interfaces gráficas
2. Comandos básicos de console
3. Utilitários de console
4. Variáveis de ambiente e arquivos de lote
5. Virtualização
6. Instalação do Windows Server
7. Configuração de Segurança do Windows Server
8. Domain Name System
9. Serviço de diretório
10. Controladores de domínio
11. Windows Powershell
12. Auditoria (módulo opcional)

# Ementa

Abordagem prática em laboratório dos processos de administração de sistemas operacionais de redes, dando ênfase a tecnologias amplamente adotadas na área e complementando os estudos desenvolvidos em “Administração de Sistemas Operacionais de Redes”.

# Referências


**BÁSICAS**

LIMONCELLI, Thomas A.; HOGAN, Christina J.; CHALUP, Strata R. **The Practice of System and Network Administration**, Second Edition. Addison-Wesley Professional, 2007.

SNYDER, Gary; NEMETH, Evi; HEIN, Trent. **Manual completo do Linux: guia do administrador**. 2.ed. São Paulo: Prentice Hall Brasil, 2007.

STANEK, William R. **Windows Server 2008: guia completo**. Porto Alegre: Bookman Companhia Editora, 2009.

**COMPLEMENTARES**

BURGESS, Mark. **Princípios de Administração de Redes e Sistemas**. 2.ed. Rio de Janeiro: LTC, 2006.

FORD JR., Jerry Lee. **Microsoft WSH and VBScript Programming**. 3.ed. Florence: Course Technology PTR, 2008.

JARGAS, Aurélio Marinho. **Shell Script Profissional**. São Paulo: Novatec, 2008.

# Módulo 1

Console e interfaces gráficas

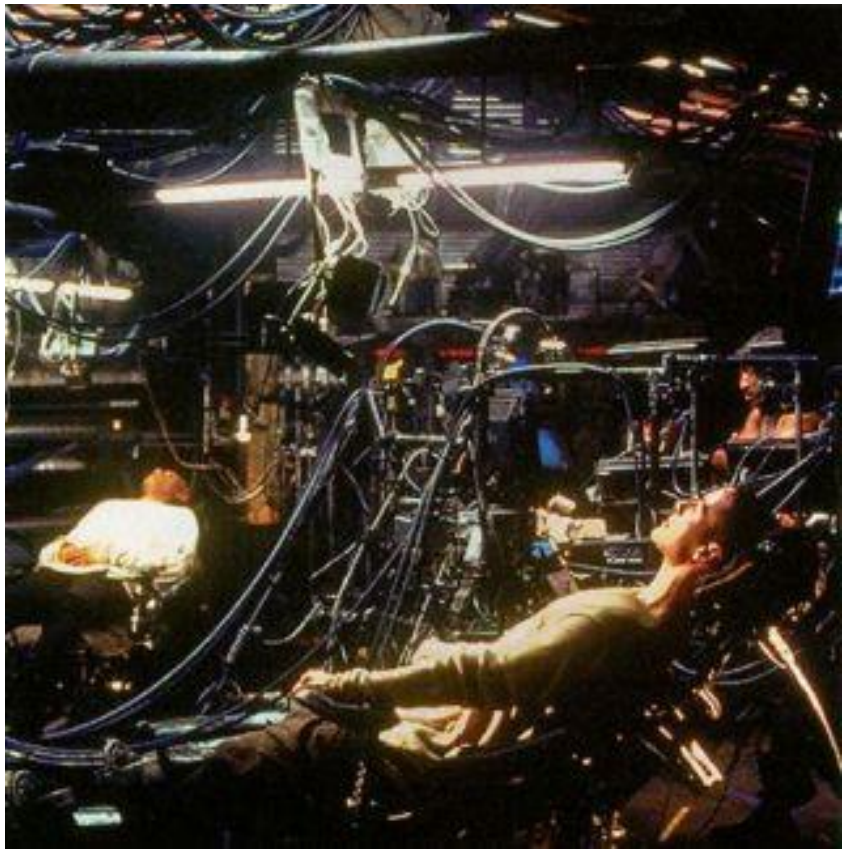
# Introdução

Uma **interface** é uma fronteira compartilhada através da qual dois ou mais componentes separados de um sistema de computador podem trocar informações, permitindo assim alguma forma de interação.

A troca pode ser realizada entre software, hardware de computador, dispositivos periféricos, humanos e combinações destes.

Alguns dispositivos de hardware de computador, como uma tela sensível ao toque, podem enviar e receber dados por meio da interface, enquanto outros, como um mouse ou microfone, podem fornecer apenas uma interface para enviar dados a um determinado sistema.

Fonte: wikipedia.org



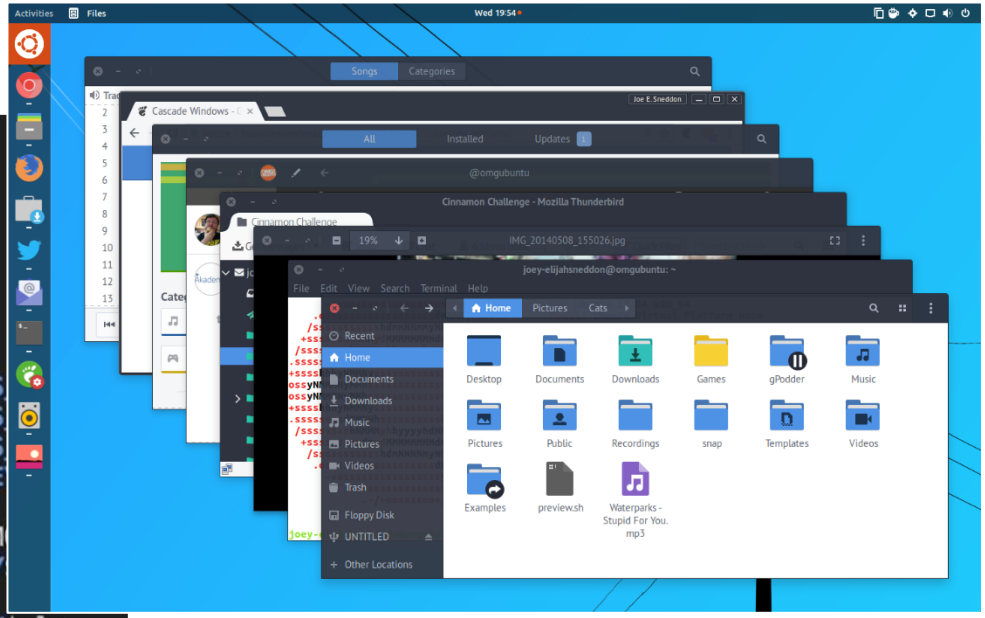
***Cena do filme The Matrix (1999)***

# Introdução

As formas mais simples de interação com um sistema de computador é por meio de interfaces do tipo texto, também conhecidas como Command Line Interface (CLI), ou por meio de interfaces gráficas, também conhecidas como Graphical User Interface (GUI).

***Command Line Interface***

```
crio-user@ajay-criodo:~$ pwd
/home/crio-user
crio-user@ajay-criodo:~$ ls
workspace
crio-user@ajay-criodo:~$ cd workspace
crio-user@ajay-criodo:~/workspace$ pwd
/home/crio-user/workspace
crio-user@ajay-criodo:~/workspace$ ls
QBox                              ajay-criodo-ME_QEATS
ajay-criodo-ME_JAVA_WARMUP_V2     ajay-criodo-ME_QEATS
ajay-criodo-ME_QBOX               ajay-criodo-ME_QEATS
ajay-criodo-ME_QEATS_REVIEW_MP    ajay-criodo-ME_QMONE
ajay-criodo-ME_QEATS_REVIEW_MP-b2
crio-user@ajay-criodo:~/workspace$ cd ajay-criodo-ME_QM
crio-user@ajay-criodo:~/workspace/ajay-criodo-ME_QMONEY
/home/crio-user/workspace/ajay-criodo-ME_QMONEY
crio-user@ajay-criodo:~/workspace/ajay-criodo-ME_QMONEY$ ls
__CRIO__  build.gradle  gradle  gradle.properties  gradlew  qmo
crio-user@ajay-criodo:~/workspace/ajay-criodo-ME_QMONEY$
```



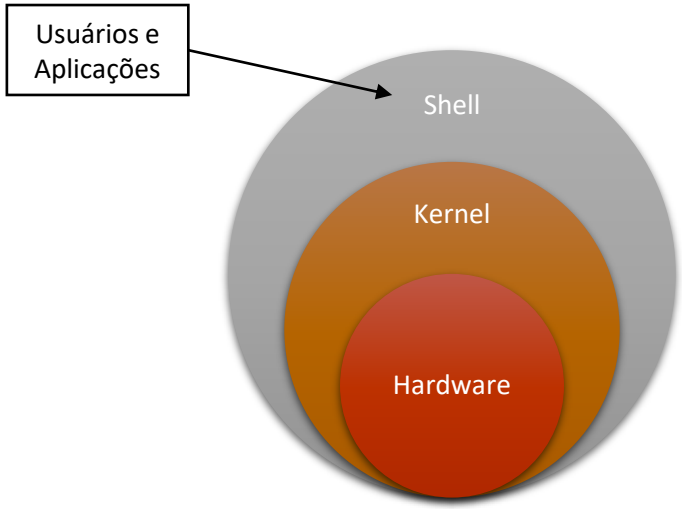

***Graphical User Interface***

# Command Line Interface

Uma Interface de Linha de Comando ou Command Line Interface (CLI) processa comandos para um programa de computador na forma de linhas de texto.

O programa que lida com a interface é chamado de interpretador de linha de comando ou processador de linha de comando.

Os sistemas operacionais implementam uma interface de linha de comando em um *shell* para acesso interativo às funções ou serviços do sistema operacional.




Fonte: wikipedia.org

# Command Line Interface

Esse acesso foi fornecido principalmente aos usuários por meio de terminais (ou consoles) de computador a partir de meados da década de 1960 e continuou a ser usado ao longo das décadas de 1970 e 1980 em sistemas VAX/VMS, Unix e sistemas de computador pessoal, incluindo DOS, CP/M e Apple DOS.

O acesso de console utiliza apenas elementos alfanuméricos para interação com o sistema, ao passo que consoles gráficas do tipo GUI (Graphical User Interface) utilizam elementos gráficos.

Fonte: wikipedia.org

# Command Line Interface

A interface de linha de comando evoluiu de uma forma de diálogo conduzida por humanos em máquinas de teletipo (TTY), em que operadores humanos trocavam informações remotamente, geralmente uma linha de texto por vez.

Os primeiros sistemas de computador frequentemente usavam máquinas de teletipo como meio de interação com um operador humano.

A interface de linha de comando em uma tela de computador pode ser entendida como uma emulação das máquinas de teletipo mecânicas.

Fonte: wikipedia.org

# Command Line Interface – tipos

**Interfaces de linha de comando do sistema operacional**

As interfaces de linha de comando do sistema operacional geralmente são programas distintos fornecidos com o sistema operacional e são frequentemente chamados de interpretador de linha de comando, processador de comando ou *shell*.

Exemplos de interpretadores de linha de comando incluem DEC's DIGITAL Command Language (DCL) no OpenVMS e RSX-11, os vários *shells* Unix (sh, ksh, csh, tcsh, zsh, Bash, etc.), CP/M's CCP, DOS 'COMMAND .COM, bem como os programas OS/2 e Windows CMD.EXE, os últimos grupos sendo fortemente baseados nos CLIs RSX-11 e RSTS do DEC.

Na maioria dos sistemas operacionais, é possível substituir o programa *shell* padrão por alternativas. Os exemplos incluem 4DOS para DOS, 4OS2 para OS/2 e 4NT/Take Command para Windows.

Fonte: wikipedia.org

# Command Line Interface – tipos

**Interfaces de linha de comando do sistema operacional - continuação**

Embora o termo *shell* seja frequentemente usado para descrever um interpretador de linha de comando, estritamente falando, um *shell* pode ser qualquer programa que constitui a interface do usuário, incluindo aqueles totalmente orientados graficamente.

Por exemplo, a GUI padrão do Windows é um programa de *shell* denominado EXPLORER.EXE, conforme definido na linha SHELL = EXPLORER.EXE no arquivo de configuração WIN.INI. Esses programas são *shells*, mas não CLIs.

Fonte: wikipedia.org

# Command Line Interface – tipos

**Interfaces de linha de comando do aplicativo**

Os programas de aplicativos (em oposição aos sistemas operacionais) também podem ter interfaces de linha de comando, e podem suportar nenhum, qualquer ou todos estes três tipos principais de mecanismos de interface de linha de comando:

- **Parâmetros:** a maioria dos sistemas operacionais oferece suporte a um meio de passar informações adicionais a um programa quando ele é iniciado. Quando um programa é iniciado a partir de um *shell* de linha de comando do sistema operacional, o texto adicional fornecido junto com o nome do programa é passado para o programa iniciado.
- **Sessões interativas de linha de comando:** após o lançamento, um programa pode fornecer a um operador um meio independente para inserir comandos na forma de texto.
- **Comunicação entre processos:** a maioria dos sistemas operacionais oferece suporte a meios de comunicação entre processos (por exemplo, fluxos padrão ou canais nomeados). As linhas de comando dos processos do cliente podem ser redirecionadas para um programa CLI por um desses métodos.

Fonte: wikipedia.org

# Command Line Interface – tipos

**Interfaces de linha de comando do aplicativo - continuação**

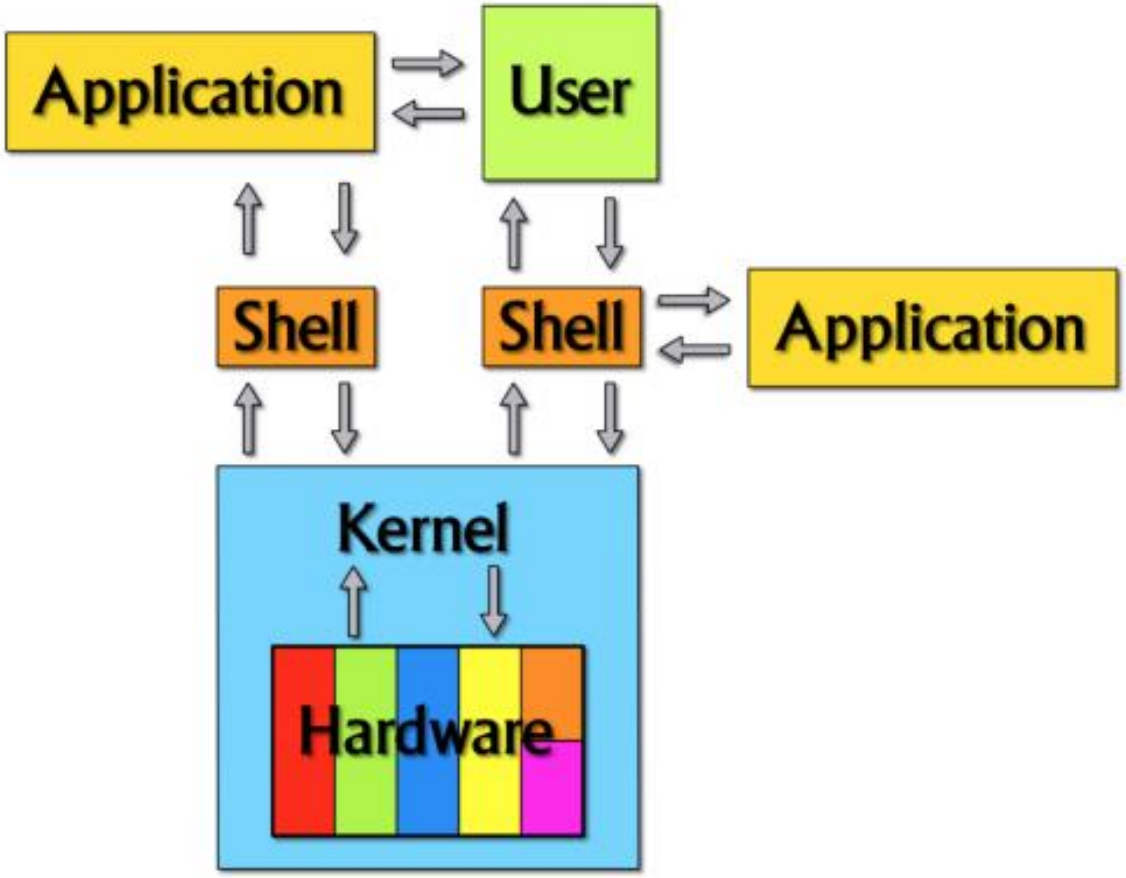
Alguns aplicativos suportam apenas um CLI, apresentando um prompt CLI ao usuário e agindo de acordo com as linhas de comando à medida que são inseridas.

Outros programas suportam CLI e GUI. Em alguns casos, uma GUI é simplesmente um invólucro em torno de um arquivo executável CLI separado. Em outros casos, um programa pode fornecer uma CLI como uma alternativa opcional à sua GUI.

CLIs e GUIs geralmente oferecem suporte a funcionalidades diferentes. Por exemplo, todos os recursos do MATLAB, um programa de computador de análise numérica, estão disponíveis por meio da CLI, enquanto a GUI do MATLAB expõe apenas um subconjunto de recursos.

Fonte: wikipedia.org

# Command Line Interface – resumo




Fonte: THONG, Jimmy. What (really) happens when you type ls -l in the shell. Disponível em <https://medium.com>, 2016.

# Graphical User Interface

A Interface Gráfica do Usuário ou Graphical User Interface (GUI) é uma forma de interface do usuário que permite aos usuários interagir com dispositivos eletrônicos por meio de ícones gráficos e indicadores de áudio, como notação primária, em vez de interfaces de usuário baseadas em texto, rótulos de comandos digitados ou navegação de texto.

As GUIs foram introduzidos em reação à curva de aprendizagem acentuada percebida de interfaces de linha de comando (CLIs), que requerem que os comandos sejam digitados em um teclado de computador.

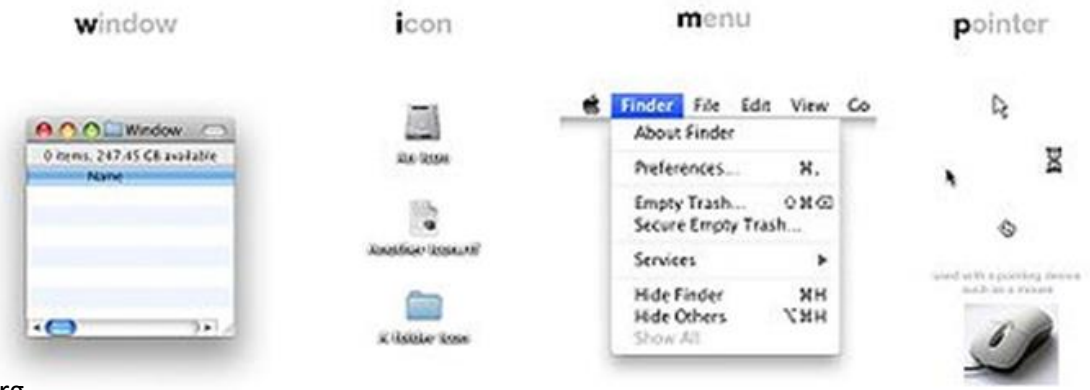
Fonte: wikipedia.org

# Graphical User Interface

A GUI usa uma combinação de tecnologias e dispositivos para fornecer uma plataforma com a qual os usuários possam interagir e realizar as tarefas de coleta e produção de informações.

Uma série de elementos que conformam uma linguagem visual evoluiu para representar informações armazenadas em computadores para tornar mais fácil para pessoas leigas trabalharem e usar software de computador.

A combinação mais comum de tais elementos em GUIs é o paradigma de janelas, ícones, menus e ponteiro, ou *"windows, icons, menus and pointer"* (WIMP), especialmente em computadores pessoais.




Fonte: wikipedia.org

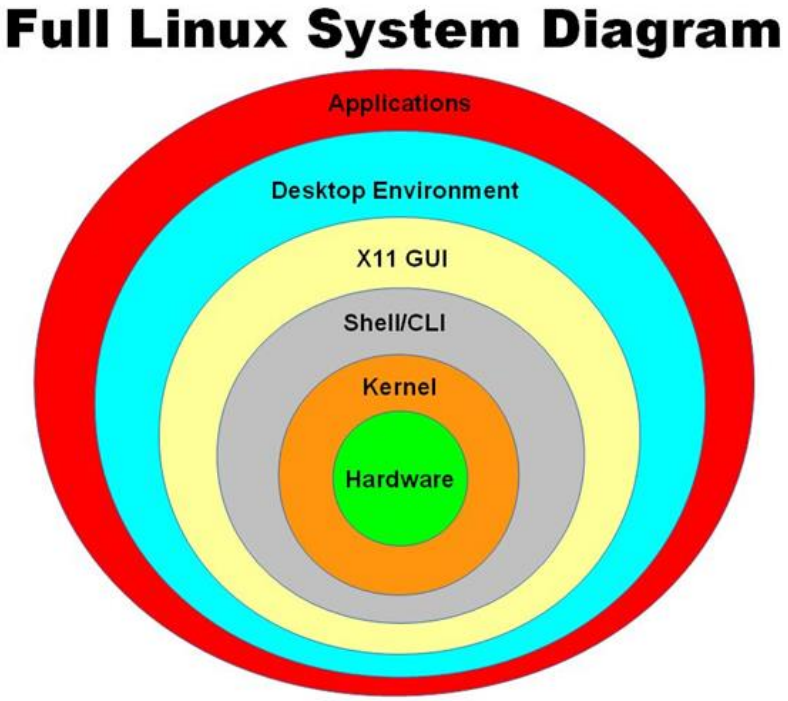
# Graphical User Interface

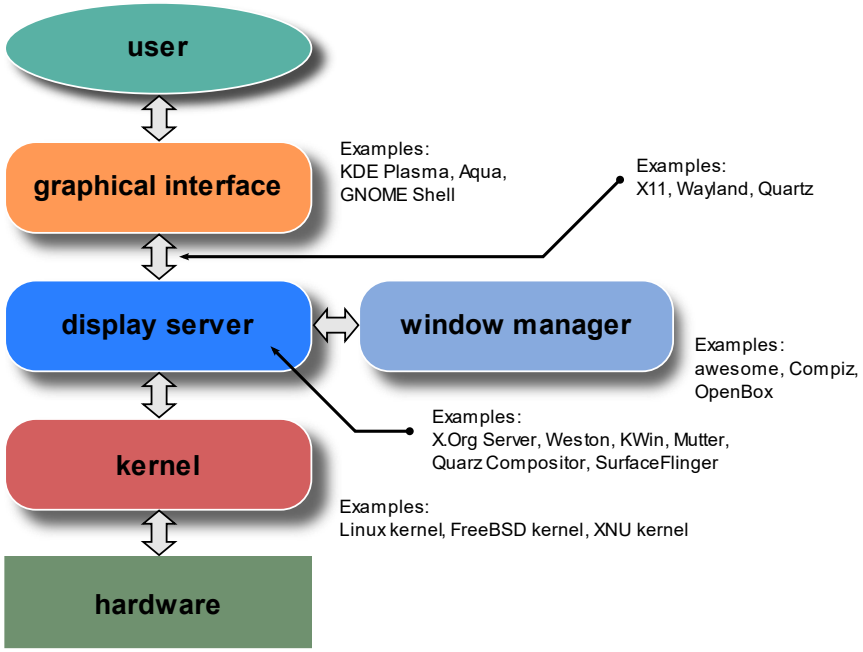
A partir de 2011, alguns sistemas operacionais baseados em *touchscreen*, como o iOS da Apple e o Android da Google, começaram a usar uma classe de GUIs denominadas pós-WIMP.

Eles suportam estilos de interação usando mais de um dedo em contato com uma tela sensível, o que permite ações como aproximar e afastar (pinch), girar (rotate) e deslizar (swipe), em adição a ação de selecionar (select), e que não são suportadas por um ponteiro ou mouse.

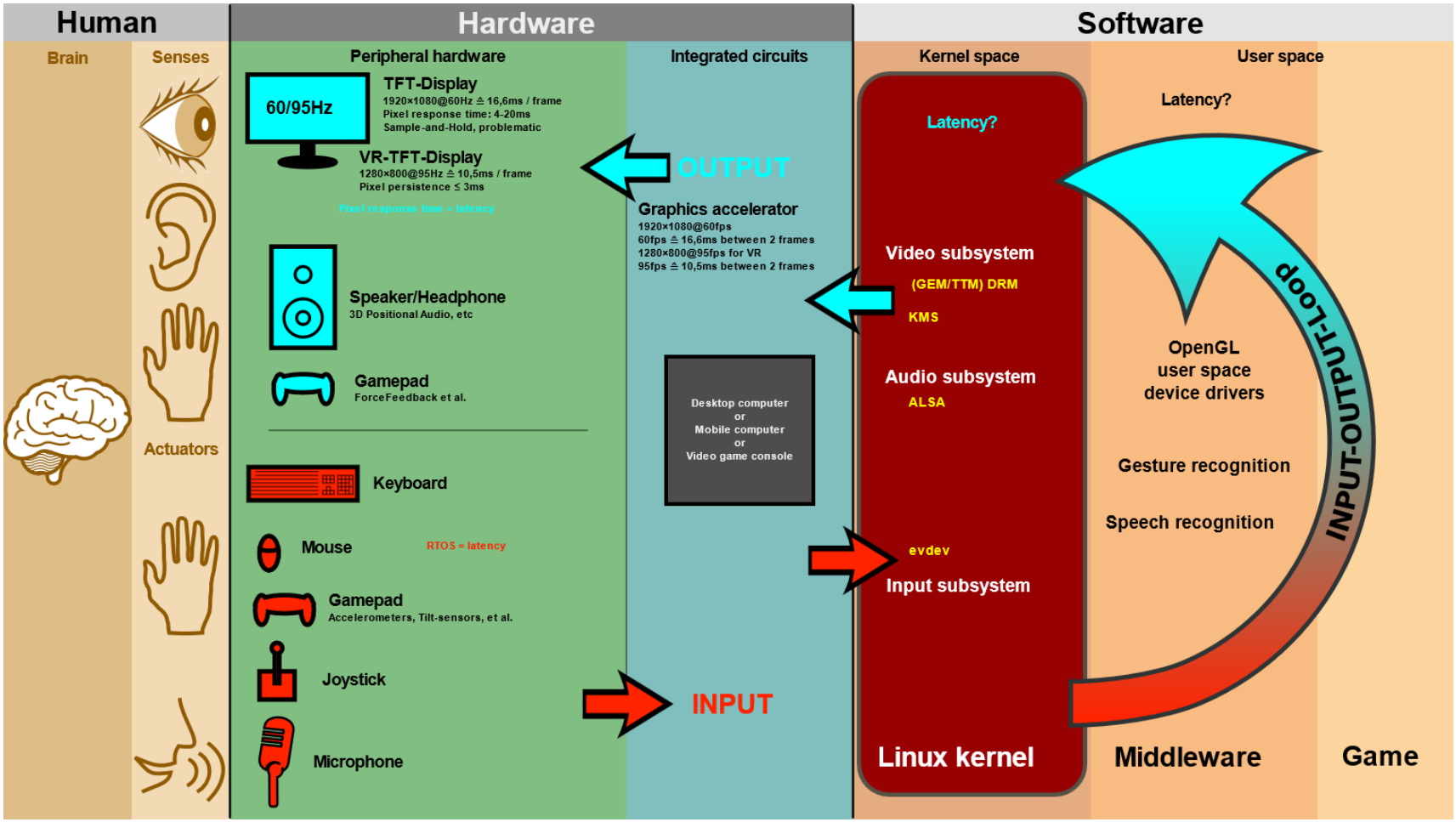
Fonte: wikipedia.org

# Graphical User Interface – resumo



# Graphical User Interface – resumo – cont.




Fonte: wikipedia.org

# Para saber mais...

… leia o documento xxxxxxxxxxx

# Módulo 2

Comandos básicos de console

# MS-DOS

MS-DOS é um acrônimo para Microsoft Disk Operating System, que é um sistema operacional para computadores pessoais baseados na arquitetura de processadores x86.

De forma geral, o MS-DOS, o IBM PC DOS e outros sistemas operacionais compatíveis são chamados simplesmente de “DOS”, que também é a sigla genérica para sistema operacional de disco.

O MS-DOS foi o principal sistema operacional para computadores pessoais compatíveis com IBM PC durante a década de 1980, a partir do qual foi gradualmente substituído por sistemas operacionais que ofereciam uma interface gráfica de usuário (GUI), tais como o Microsoft Windows.


Fonte: wikipedia.org

# COMMAND.COM

O COMMAND.COM é o interpretador de linha de comando padrão para MS-DOS, Windows 95-98, Windows 98SE e Windows Me.

Ele é o primeiro programa a ser executado após o processo de inicialização (processo init) e serve também como a interface de usuário padrão.

***MS-DOS Command Line Interface***

```
C:\>COMMAND.COM


Microsoft(R) MS-DOS(R) Version 6.22
            (C)Copyright Microsoft Corp 1981-1994.

C:\>_
```


***Cena do filme RoboCop (1987)***

Fonte: wikipedia.org

# COMMAND.COM – modos de operação

Como um *shell*, o **COMMAND.COM** tem dois modos distintos de operação:

- **Modo interativo:** onde o usuário digita comandos que são executados imediatamente;
- **Modo em lote:** onde o interpretador de comandos executa uma sequência predefinida de comandos armazenados como um arquivo de texto com a extensão .BAT.

O interpretador de linha de comando do Windows é o **CMD.EXE**.

O comprimento da linha de comando no modo interativo do MS-DOS é limitado a 126 caracteres.

Fonte: wikipedia.org

# Tipos de comandos

O MS-DOS suporta dois tipos de comandos:

- **Comandos internos:** são comandos armazenados diretamente no binário do arquivo COMMAND.COM. Assim, estes comandos estão sempre disponíveis, mas só podem ser executados diretamente a partir do interpretador de comandos;
- **Comandos externos:** são comandos armazenados em arquivos próprios, geralmente com as extensões .COM ou .EXE, e servem para adicionar funcionalidades extras ao sistema operacional. Para serem executados, devem ser invocados a partir do diretório onde estão gravados, ou então constar em um caminho de pesquisa para que possam ser encontrados.

Ao digitar **COMMAND.COM** (ou simplesmente **COMMAND**) seguido de <ENTER> na console, uma nova sessão do interpretador de comandos é inicializada.

Para encerrar a nova sessão, basta digitar o comando **EXIT** seguido de <ENTER>.

Fonte: wikipedia.org

# Comandos – obter informações do sistema

- VER - versão do interpretador de linha de comando
- VOL - mostra o nome de volume de um disco e o número de série
- DATE - mostra a data e permite alterá-la
- TIME - mostra a hora e permite alterá-la
- HELP - ajuda do MS-DOS

HELP é um comando externo.

Fonte: Ajuda do MS-DOS versão 6.22

# Comandos – manipular arquivos

- DIR - mostra a lista de arquivos e diretórios
- COPY - copia um ou mais arquivos para outra localização
- RENAME ou REN - renomeia arquivos
- ERASE ou DEL - apaga arquivos
- COPY CON - extensão do comando COPY que permite criar um arquivo

Versões antigas do DOS usam o esquema 8.3 para nomes de arquivo, ou seja, até oito caracteres para o nome do arquivo e até três caracteres para a extensão do arquivo. Versões posteriores permitem o uso de até 256 caracteres para a combinação de nome e extensão do arquivo.

A localização de um arquivo depende do diretório onde ele se encontra. Quando o arquivo é referenciado junto com o diretório onde se encontra até a raiz, chamamos isso de **endereço absoluto**.

Fonte: Ajuda do MS-DOS versão 6.22

# Comandos – manipular arquivos e diretórios

- TREE - mostra a lista de diretórios no formato hierárquico ou de árvore
- MKDIR ou MD - cria um diretório
- CHDIR ou CD - muda de diretório
- RMDIR ou RD - remove um diretório
- MOVE - move arquivos e diretórios e/ou renomeia arquivos e diretórios
- XCOPY - copia arquivos e diretórios para outra localização
- DELTREE - apaga uma árvore de diretórios

Alguns comandos podem ser usados tanto para arquivos quanto para diretórios.

TREE, MOVE, XCOPY e DELTREE são comandos externos.

Fonte: Ajuda do MS-DOS versão 6.22

# Comandos – manipular arquivos e diretórios

Ao mudar de um diretório para outro, o símbolo (\) representa o diretório raiz; o símbolo (.) representa o diretório corrente e o símbolo (..) representa o diretório acima ou anterior.

Fonte: Ajuda do MS-DOS versão 6.22

# Comandos – visualização e ordenação

- CLS - limpa a tela
- TYPE - mostra o conteúdo de um arquivo
- MORE - mostra a saída da tela com paginação
- SORT - a partir de uma entrada, organiza dados para a saída na tela, um arquivo ou outro dispositivo
- COLOR - muda a cor do texto e do fundo de tela

MORE e SORT são comandos externos, e devem sers usados em conjunto com outros comandos, sendo necessário o uso de um condutor (pipe), representado pela barra vertical (|).

COLOR está disponível a partir do Windows 2000.

Fonte: Ajuda do MS-DOS versão 6.22

# Máscaras e curingas

Para manipular um grupo de arquivos ou diretórios com nomes idênticos, é possível lançar mão de símbolos que substituem um ou mais caracteres de um nome de arquivo.

O **asterisco** (*) corresponde a qualquer sequência de caracteres, e substitui os caracteres à direita de si mesmo e encontra todas as instâncias dos critérios especificados.

Já o ponto de **interrogação** (?) corresponde a qualquer caractere único, e pode representar apenas um caractere por vez para cada ponto de interrogação especificado.

Fonte: Ajuda do MS-DOS versão 6.22

# Redirecionamento de saída

A saída de um comando é direcionada por padrão para o monitor, mas pode ser redirecionada para um arquivo, para a impressora ou para qualquer outro dispositivo suportado.

O símbolo utilizado é o sinal de maior (>), que pode ser usado nas seguintes combinações:

- **Sinal de maior (>) seguido do dispositivo de saída, como impressora (PRN ou LPT1-4), console (CON), porta serial (COM1-4) ou saída auxiliar (AUX):** redireciona o resultado do comando para o dispositivo especificado;
- **Sinal de maior (>) seguido de um nome de arquivo:** redireciona o resultado do comando para um arquivo. Se o arquivo não existir, ele será criado. Mas se o arquivo já existir, ele será sobrescrito;
- **Sinal de maior duplo (>>) seguido de um nome de arquivo:** redireciona o resultado do comando para um arquivo. Se o arquivo não existir, ele será criado. Mas se o arquivo já existir, o novo conteúdo será adicionado ao já existente.

Fonte: Ajuda do MS-DOS versão 6.22

# Para saber mais...

… verifique a ajuda do MS-DOS

# Módulo 3

Utilitários de console

# Introdução

**Utilitários de console** ou comandos externos são programas contidos no seu próprio arquivo binário, e geralmente possuem as extensões .COM ou .EXE.

Estes programas servem para adicionar funcionalidades extras ao sistema operacional.

Para que um utilitário de console possa ser executado, uma das seguintes regras deve ser atendida:

- Ser invocado a partir do diretório onde está gravado;
- Ser invocado a partir de qualquer diretório usando o seu endereço absoluto;
- Ser invocado a partir de qualquer diretório desde que sua localização conste de um caminho de pesquisa ativo.

# Comandos – informações sobre arquivos

- COMP - compara o conteúdo de dois ou mais arquivos
- FC - compara o conteúdo de dois ou mais arquivos e mostra suas diferenças
- FIND - busca por uma sequência de texto em um ou mais arquivos
- ATTRIB - exibe os atributos de um arquivo e permite alterá-los

FC substituiu o COMP, que ainda é encontrado em versões do Windows.

Fonte: Ajuda do MS-DOS versão 6.22 e do Microsoft Windows

# Comandos – informações sobre o sistema

- SYSTEMINFO - exibe informações de configuração do sistema operacional
- TASKLIST - exibe a lista dos processos em execução na máquina local
- SHUTDOWN - permite desligar uma máquina de maneira controlada

SYSTEMINFO, TASKLIST e SHUTDOWN são comandos externos.

SHUTDOWN está disponível a partir do Windows XP.

Para verificar se um comando do Windows é externo, utilizar o comando WHERE seguido do comando que se quer verificar. Se o comando for externo, a saída retornará a localização do arquivo executável.

Fonte: Ajuda do Microsoft Windows

# Comandos – informações de rede

- IPCONFIG - exibe as configurações de rede e permite reiniciar alguns aspectos de conectividade, como endereço IP (Internet Protocol) e cache do DNS (Domain Name System)
- PING - verifica a conectividade entre *hosts* usando mensagens ICMP (Internet Control Message Protocol)
- NSLOOKUP - exibe informações que permitem diagnosticar a infraestrutura do DNS

IPCONFIG, PING e NSLOOKUP são comandos externos e estão disponíveis apenas no Windows.

Fonte: Ajuda do Microsoft Windows

# Para saber mais...

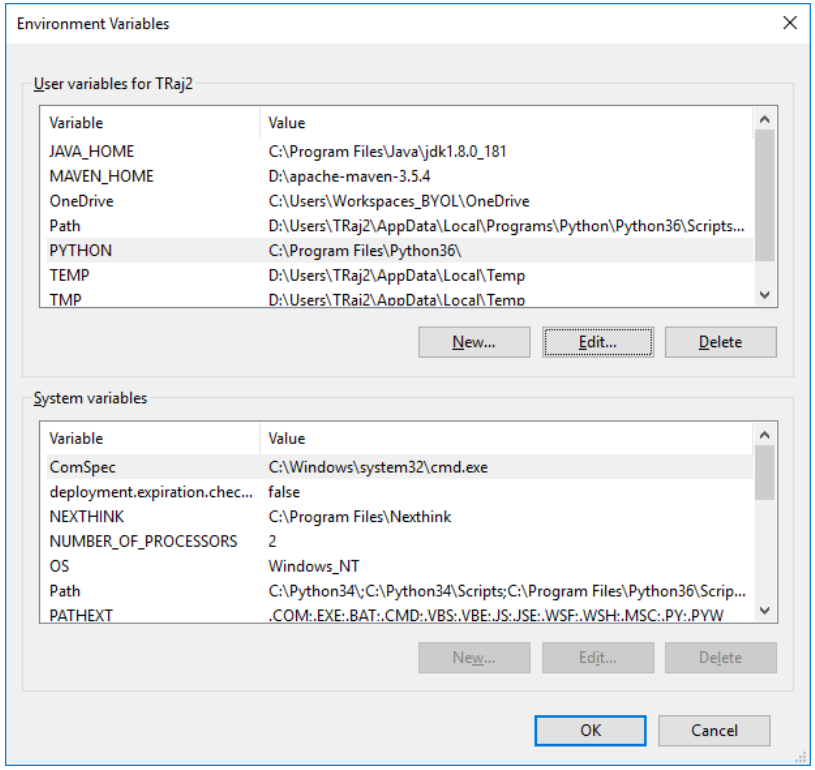
… verifique a ajuda do MS-DOS

# Módulo 4

Variáveis de ambiente e arquivos de lote

# Variáveis de ambiente

Variáveis de ambiente são sequencias de texto armazenadas em memória que podem auxiliar os processos em execução.




Fonte: Ajuda do MS-DOS versão 6.22 e do Microsoft Windows

# Variáveis de ambiente – comandos

- PROMPT - altera a aparência  do campo de entrada (prompt de comando)
- PATH - indica o diretório onde o sistema operacional irá procurar por arquivos executáveis
- SET - exibe, configura ou remove variáveis de ambiente

Fonte: Ajuda do MS-DOS versão 6.22 e do Microsoft Windows

# Arquivos de lote

Um arquivo de lote (batch file) ou programa em lote (batch program) é um arquivo de texto de extensão .BAT que contem um ou mais comandos.

Quanto o nome do arquivo é invocado, os comandos dentro do arquivo são executados sequencialmente.


Fonte: Ajuda do MS-DOS versão 6.22 e do Microsoft Windows

# Arquivos de lote – comandos

- ECHO - controla a exibição de mensagens em arquivos de lote (batch file)
- REM - insere comentários em arquivos de lote
- IF - executa um comando com base no resultado de uma condição
- CHOICE - permite que o usuário escolha opções em um arquivo de lote
- GOTO - redireciona o fluxo de execução para a linha marcada por uma etiqueta (label)
- CALL - invoca um arquivo de lote a partir de um outro sem finalizar o original

CHOICE é um comando externo. Sua sintaxe varia entre o DOS e o Windows.

Fonte: Ajuda do MS-DOS versão 6.22 e do Microsoft Windows

# Arquivos de lote – AUTOEXEC

No MS-DOS existe um arquivo de lote especial, o **AUTOEXEC.BAT**, que é executado automaticamente toda vez que o sistema operacional é executado.

Para ter o mesmo comportamento no Windows 10, por exemplo, basta criar um arquivo de lote com qualquer nome em uma das seguintes pastas:

- Válido para todos os usuários do computador:

```
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp
```

- Válido apenas para o usuário corrente:

```
C:\Users\[User Name]\AppData\Roaming\Microsoft\Windows\Start
                    Menu\Programs\Startup
```

Fonte: Ajuda do MS-DOS versão 6.22 e do Microsoft Windows

# Para saber mais...

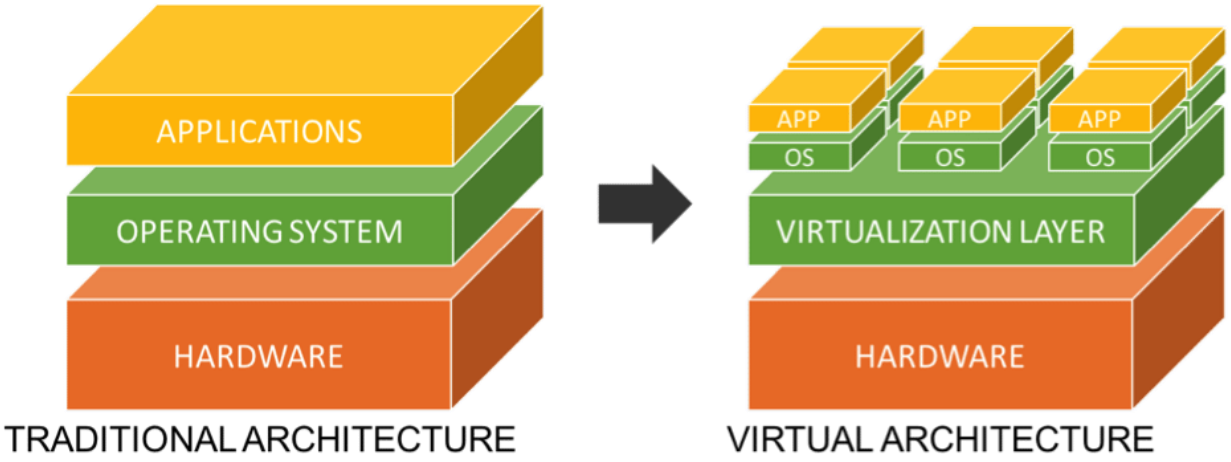
… verifique a ajuda do MS-DOS

# Módulo 5

Virtualização

# Introdução

A virtualização pode ser definida como uma metodologia de divisão de recursos de hardware de um computador em múltiplos ambientes de execução, por meio da aplicação de um ou mais conceitos ou tecnologias como particionamento de hardware e software, compartilhamento de tempo de máquina, simulação completa ou parcial, emulação, qualidade de serviço, e muitos outros.



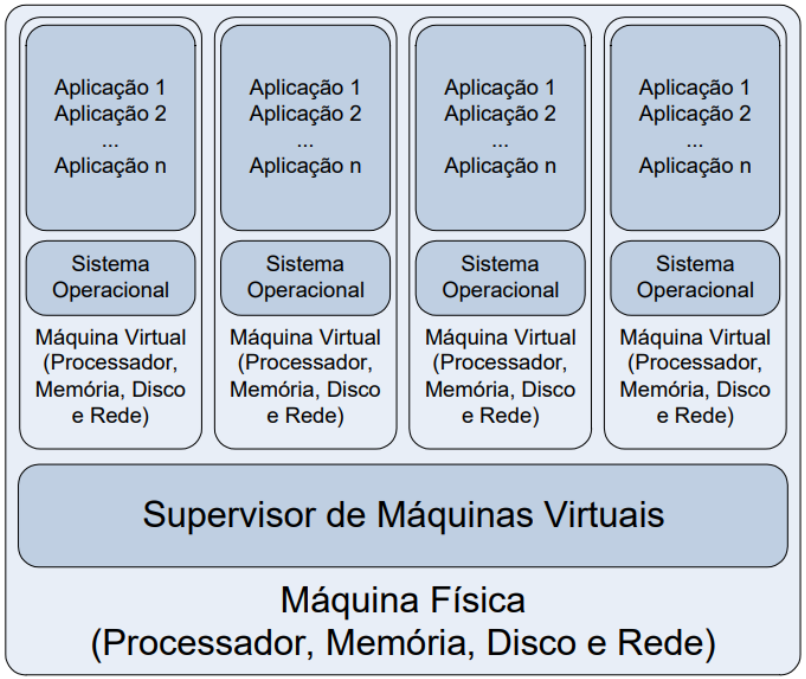

Fonte: WILLIAMS, David E.; GARCIA, Juan. Virtualization with Xen(tm): Including Xenenterprise, Xenserver, and Xenexpress. Syngress Publishing, Inc. Burlington, 2007

# Introdução

A tecnologia de virtualização consiste em fazer com que um único servidor físico seja particionado em vários servidores virtuais.

É o software de virtualização, também conhecido como Supervisor de Máquinas Virtuais, quem controla o acesso das máquinas virtuais a estes recursos.

Ao invés de se instalar um sistema operacional comum na máquina física, instala-se um sistema operacional modificado que inclui um Supervisor de Máquinas Virtuais.

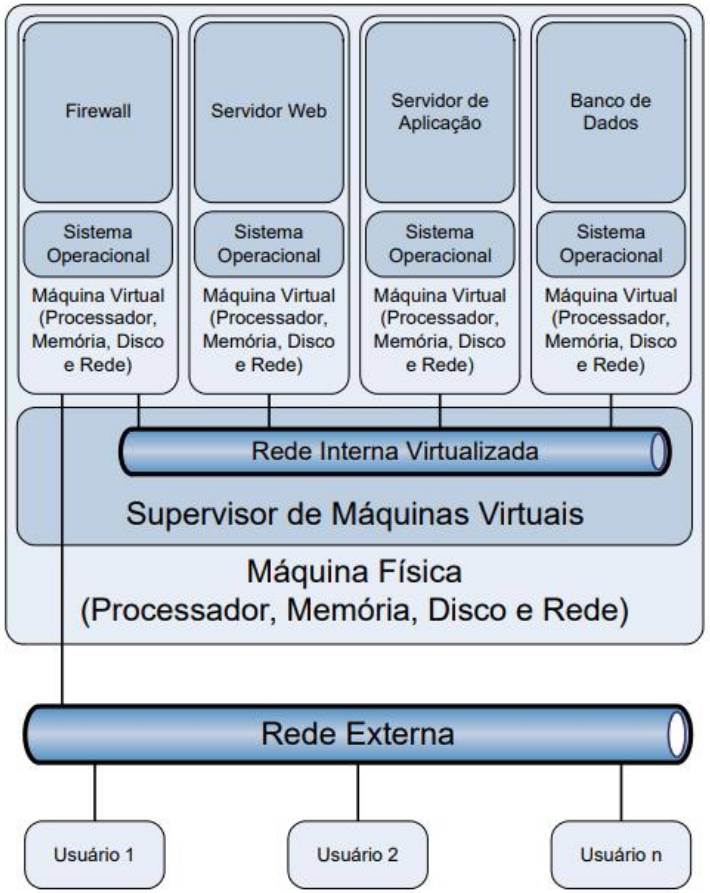



Fonte: SANTANA, W. R. Vantagens de se Executar Serviços de Rede Multicamadas em Ambientes Virtualizados com Xen. FaSCi-Tech, v. 1, p. 178-191, 2010

# Introdução

No exemplo ao lado, uma única máquina física está particionada em quatro máquinas virtuais.

O firewall possui duas interfaces de rede: uma para comunicar-se com a rede externa e outra com a rede interna, sendo que a primeira interface é compartilhada com a placa de rede física do servidor e a segunda interface é uma placa de rede lógica conectada numa rede virtualizada, em que estão conectados os outros servidores..

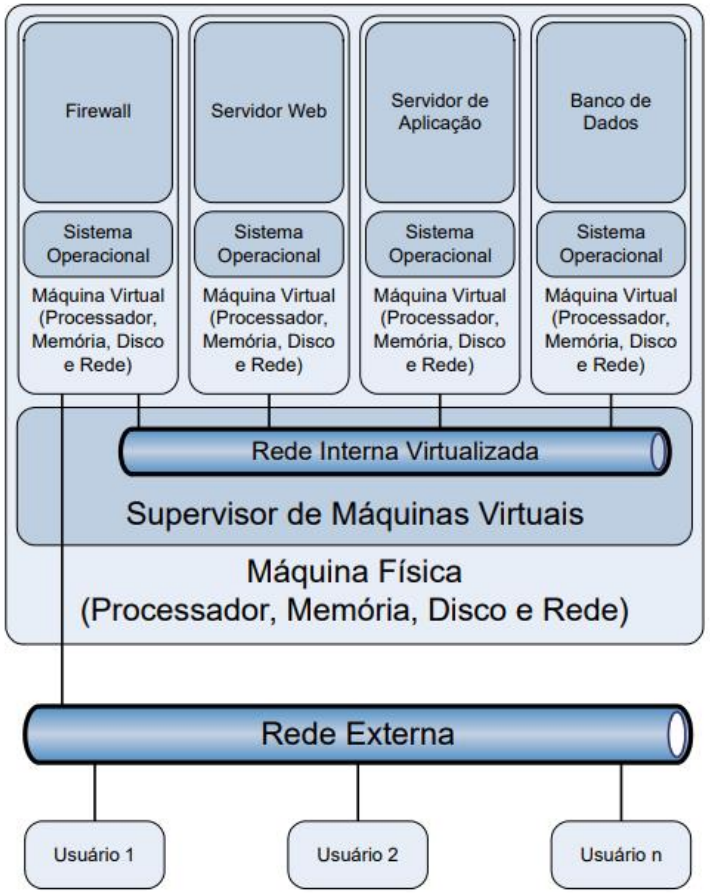



Fonte: SANTANA, W. R. Vantagens de se Executar Serviços de Rede Multicamadas em Ambientes Virtualizados com Xen. FaSCi-Tech, v. 1, p. 178-191, 2010

# Introdução

Para implementar os processadores virtuais, cada máquina virtual usará uma fatia de tempo do processador físico, ou se a máquina física tiver mais de um processador, eles podem ser alocados individualmente para cada máquina virtual.

De forma análoga se dará a alocação de memória, ou seja, cada máquina virtual irá usar uma fatia da memória física.

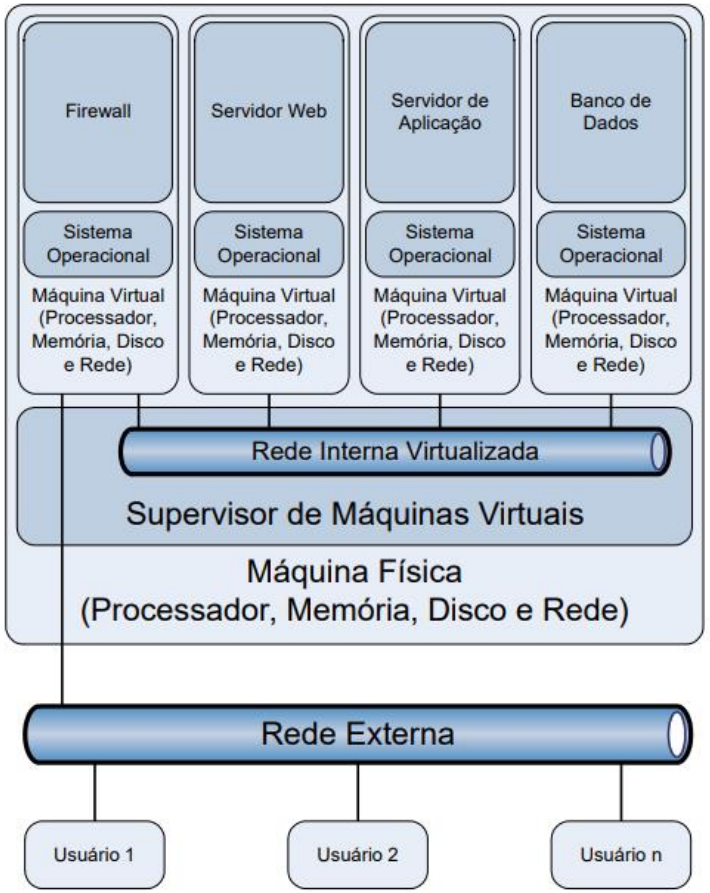



Fonte: SANTANA, W. R. Vantagens de se Executar Serviços de Rede Multicamadas em Ambientes Virtualizados com Xen. FaSCi-Tech, v. 1, p. 178-191, 2010

# Introdução

E para disponibilizar os discos virtuais, cada máquina virtual alocará uma fatia do disco rígido da máquina física.

Como o servidor de banco de dados tem por característica executar operações que exigem uma alta taxa de escrita e gravação, se a máquina física possuir mais de um disco rígido, este pode ser alocado exclusivamente para o servidor de banco de dados, de modo a aumentar o desempenho.




Fonte: SANTANA, W. R. Vantagens de se Executar Serviços de Rede Multicamadas em Ambientes Virtualizados com Xen. FaSCi-Tech, v. 1, p. 178-191, 2010

# Para saber mais...

… leia o artigo Vantagens de se Executar Serviços de Rede Multicamadas em Ambientes Virtualizados com Xen, de Wallace Rodrigues de Santana, publicado na FaSCi-Tech, v. 1, p. 178-191, 2010

# Módulo 6

Instalação Windows Server

# Windows Server

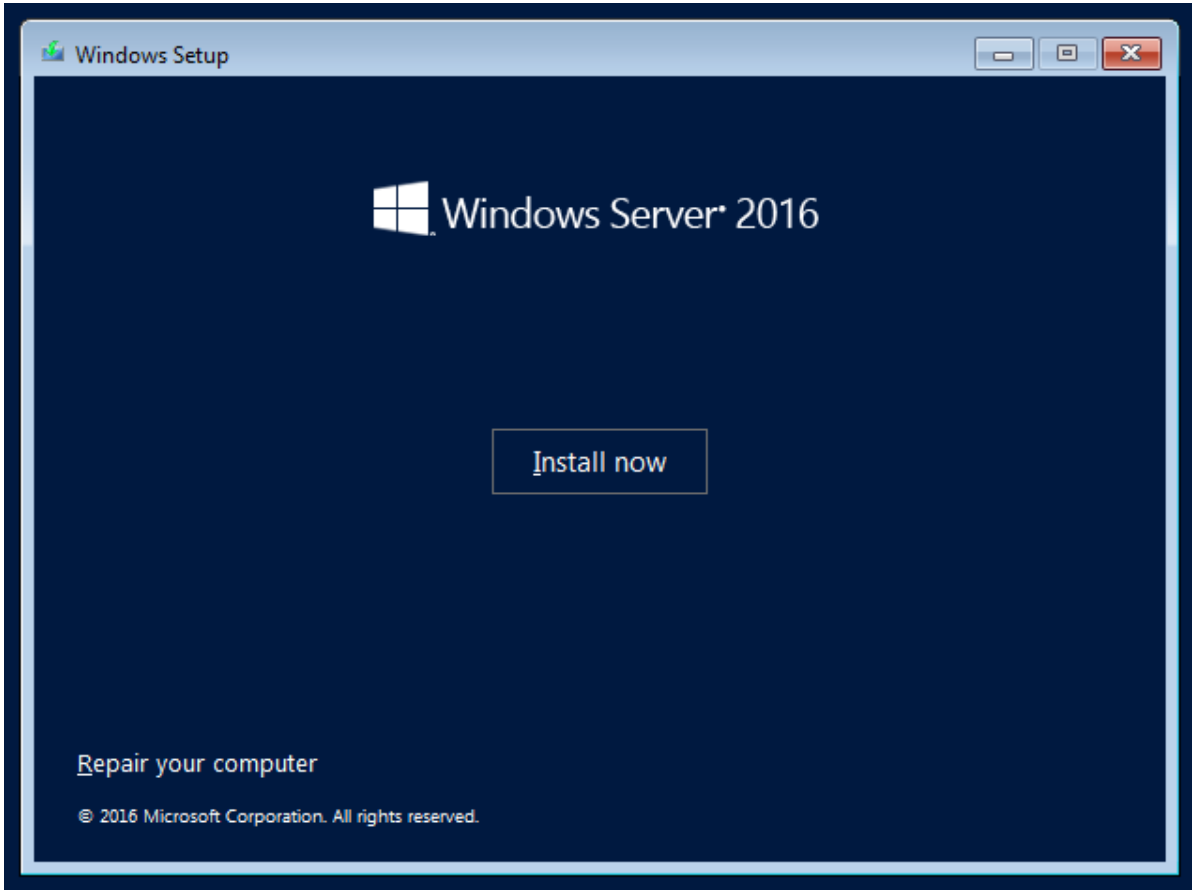
O Windows Server é uma plataforma que permite construir uma infraestrutura de aplicativos, redes e serviços da Web conectados, do grupo de trabalho ao data center.

Disponível nas versões Standard e Datacenter, com opção de instalação com e sem ambiente gráfico.

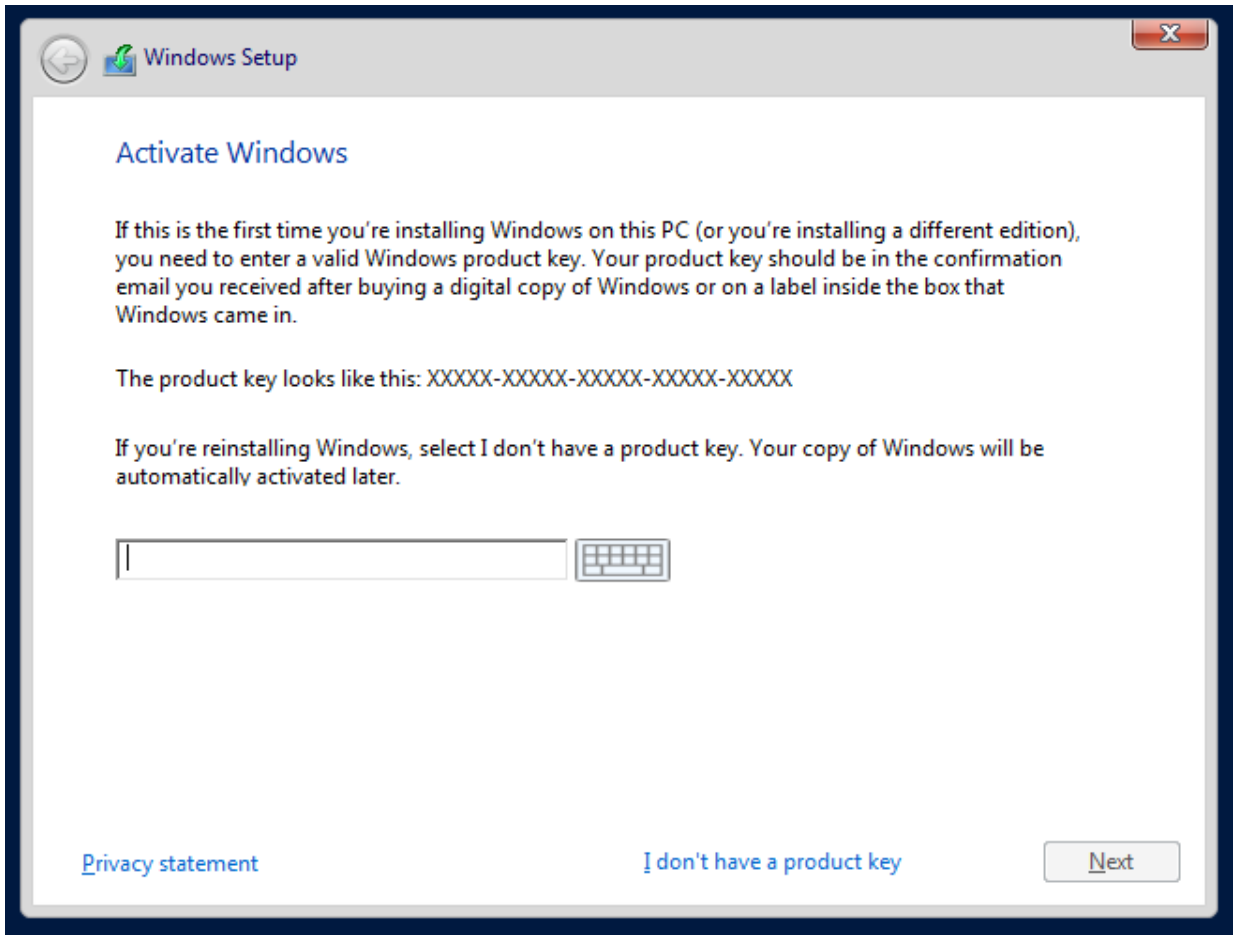

Fonte: microsoft.com

# Windows Server – instalação

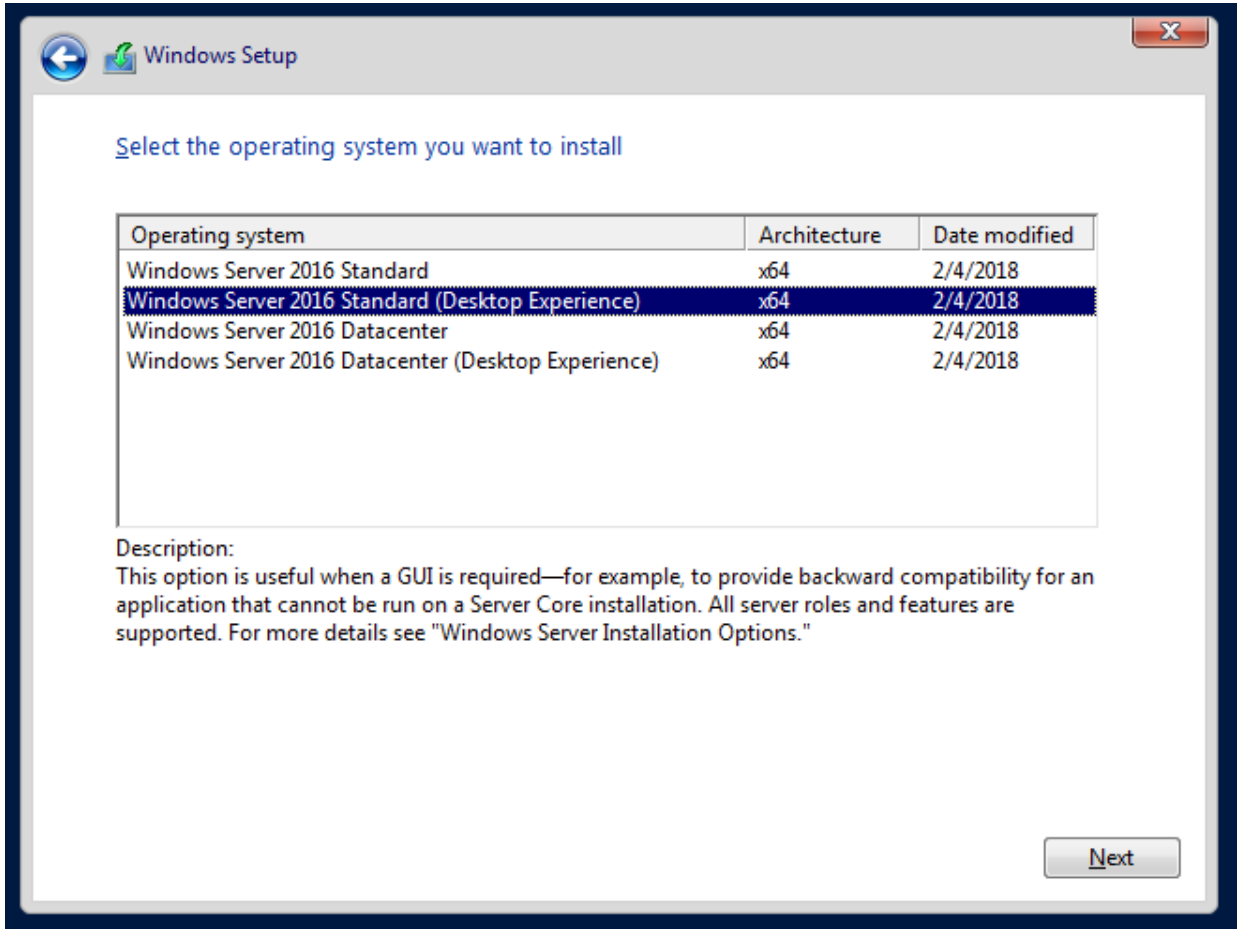
# Windows Server – instalação



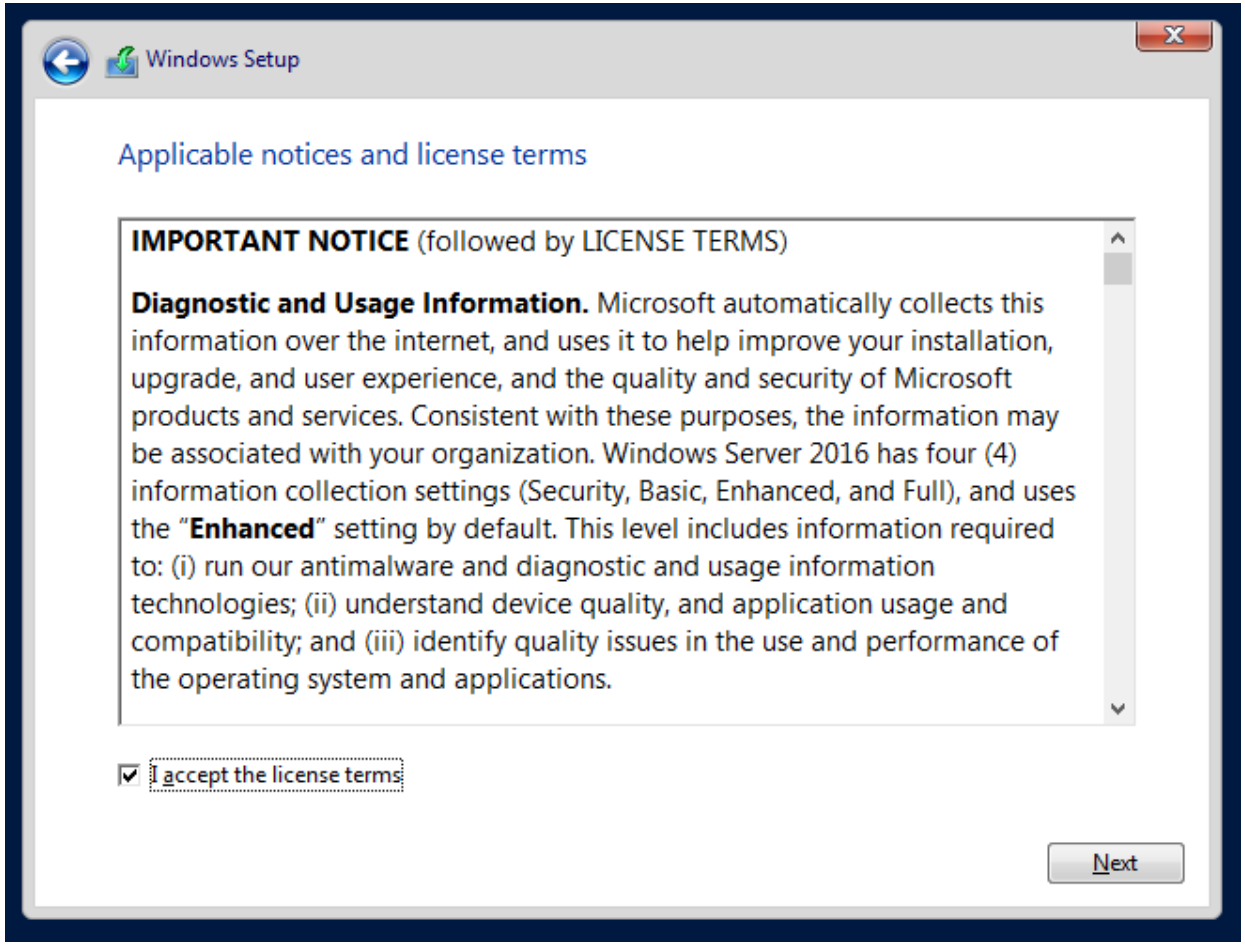
# Windows Server – instalação



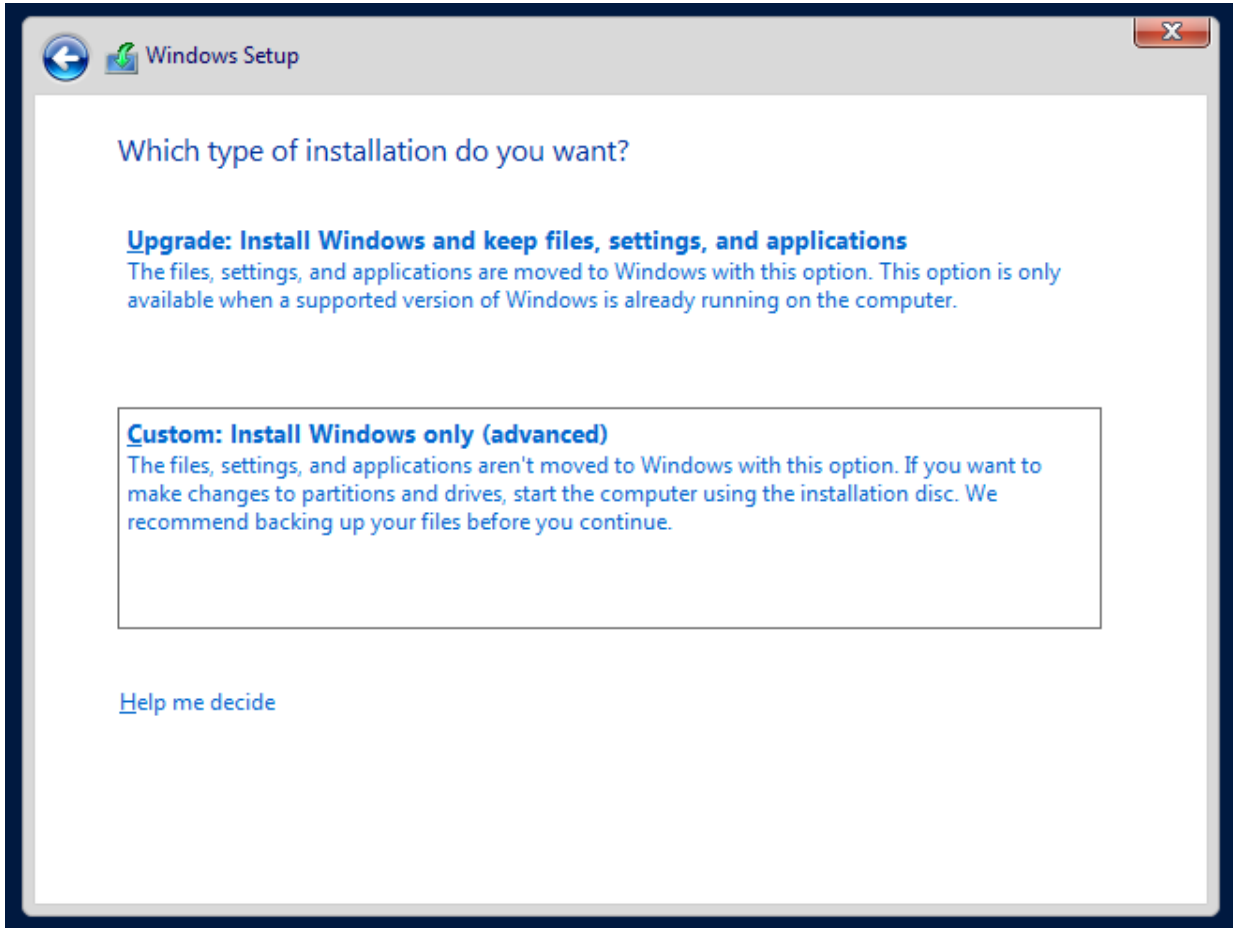
# Windows Server – instalação



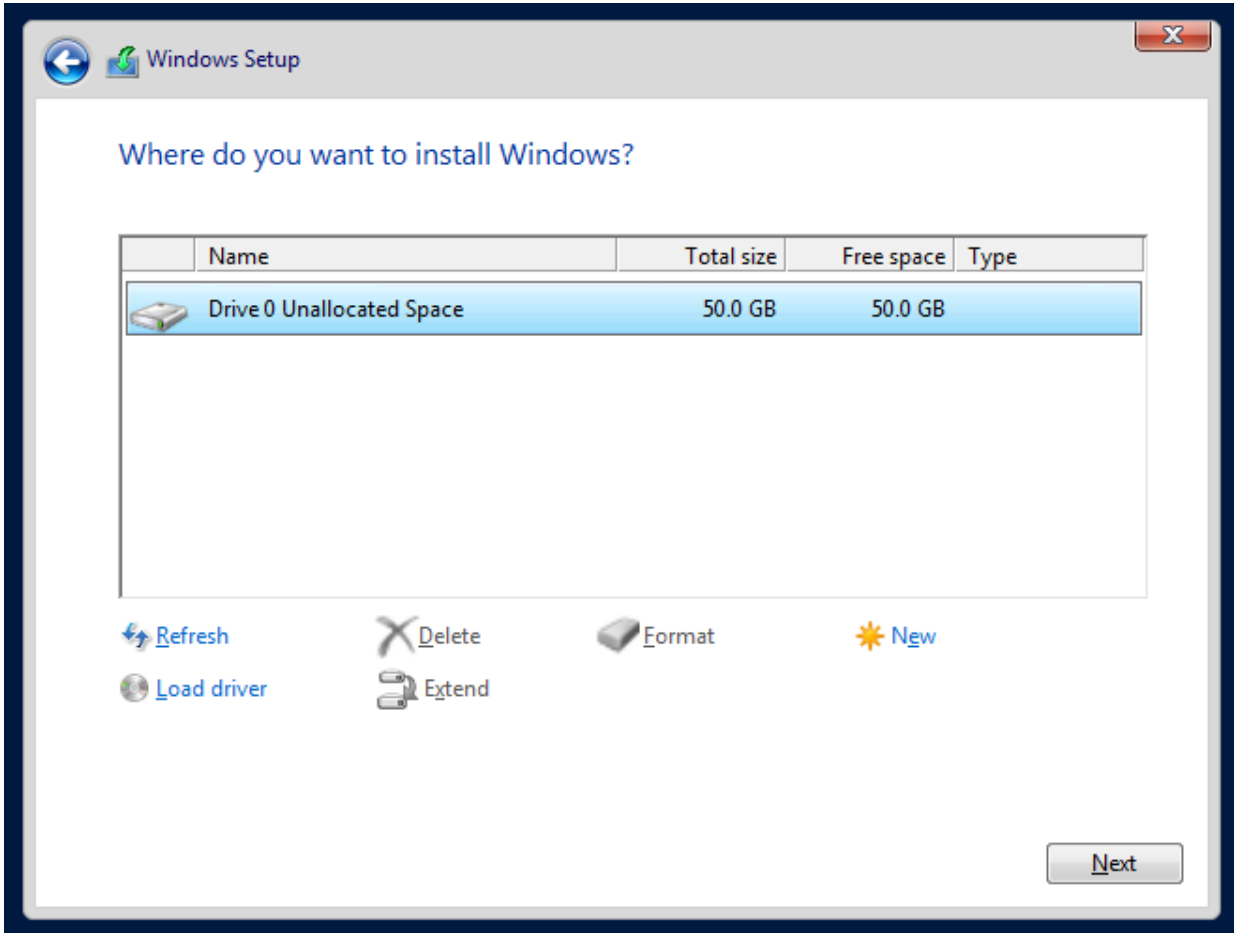
# Windows Server – instalação



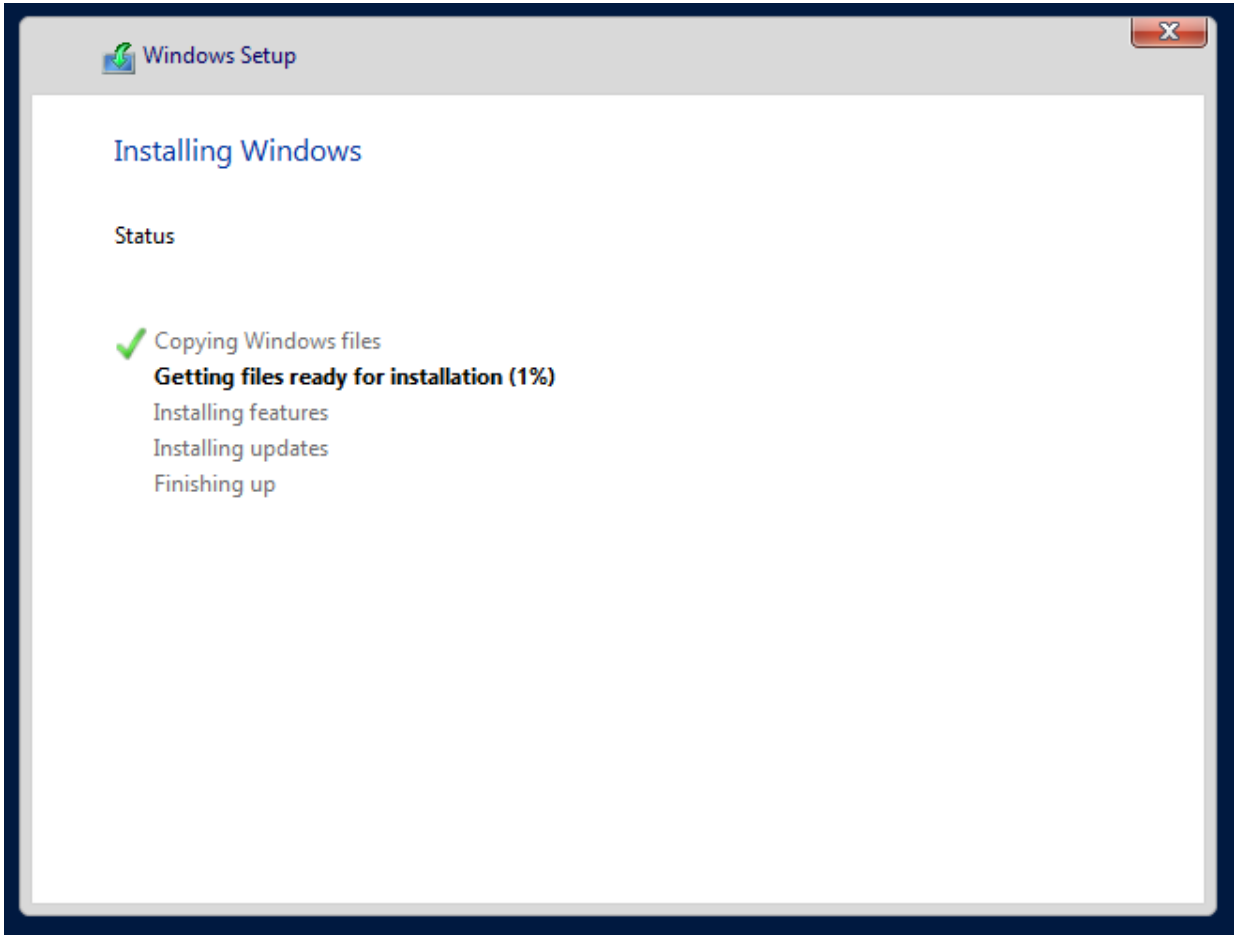
# Windows Server – instalação



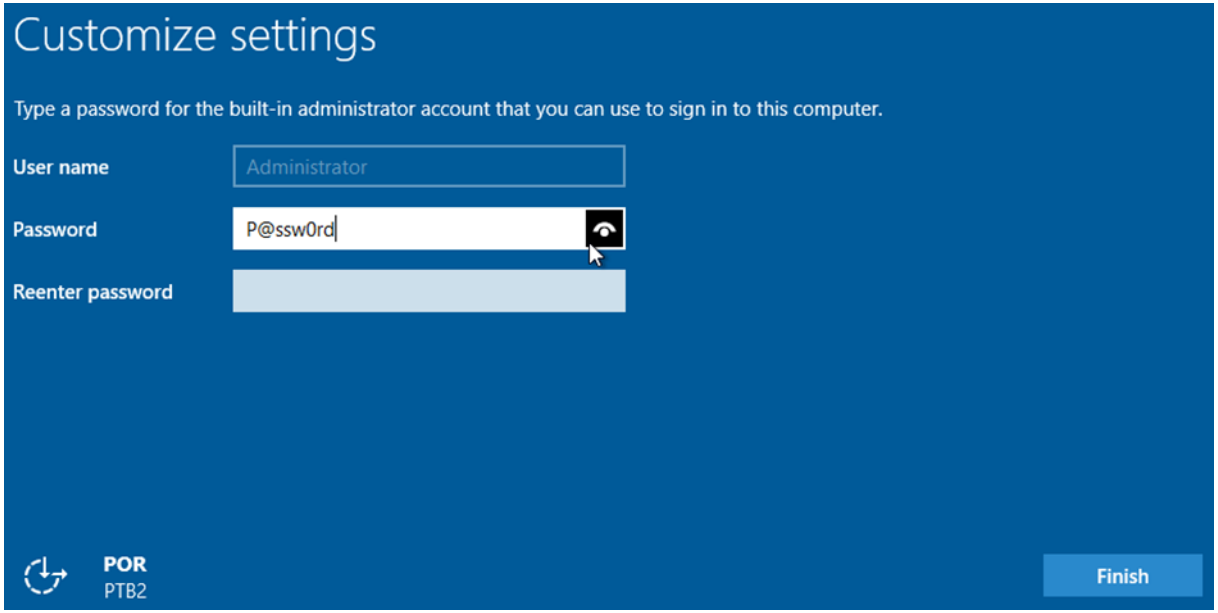
# Windows Server – instalação



# Windows Server – instalação



# Windows Server – instalação




Nos laboratórios da disciplina, a senha a ser utilizada será “P@ssw0rd”.

Nunca utilizá-la em ambientes de produção, pois apesar de possuir características de senha forte, ela é facilmente encontrada em dicionários de quebra de senha.

# Hardening

Hardening (endurecimento) é o processo de proteger um sistema reduzindo sua superfície de vulnerabilidade (ou superfície de ataque).

A redução das formas de ataque disponíveis geralmente inclui a alteração de senhas padrão, a remoção de software desnecessário, nomes de usuário ou logins desnecessários e a desativação ou remoção de serviços desnecessários.


Fonte: wikipedia.org

# Hardening – políticas de conta

Políticas de conta são um conjunto de regras especificadas para um domínio que determina as restrições colocadas nas senhas dos usuários.

| 1.1 | Account Policies | Setting |
|---|---|---|
| 1.1.1 | Enforce password | 24 remembered; not required to set for local accounts |
| 1.1.2 | Maximum password age | 90 days (maximum) |
| 1.1.3 | Minimum password age | 1 day or more |
| 1.1.4 | Minimum password length | 8 characters |
| 1.1.5 | Password must meet complexity requirements | Enabled |
| 1.1.6 | Store passwords using reversible encryption | Disabled |
| 1.1.7 | Account lockout duration | 15 minutes (minimum) |
| 1.1.8 | Account lockout threshold | 10 attempts |

...

Fonte: security.uconn.edu e networkencyclopedia.com

# Hardening – políticas de auditoria

Políticas de auditoria permitem rastrear e monitorar ações realizadas nos servidores.

| 1.2 | Audit Policy | Setting |
|---|---|---|
| 1.2.1 | Audit Account Logon Events | Success and Failure |
| 1.2.2 | Audit Account Management | Success and Failure |
| 1.2.3 | Audit Directory Service Access | No Auditing |
| 1.2.4 | Audit Logon Events | Success and Failure |
| 1.2.5 | Audit Object Access | Failure (minimum) |
| 1.2.6 | Audit Policy Change | Success (minimum) |
| 1.2.7 | Audit Privilege Use | Failure (minimum) |
| 1.2.8 | Audit Process Tracking | No Audit |

...

Fonte: security.uconn.edu e networkencyclopedia.com

# Hardening – registro de eventos

O registro de eventos coleta e armazena informações sobre eventos gerados pelo sistema operacionais, pela auditoria e por aplicações, entre outros.

| 1.4 | Event Log | Setting |
|---|---|---|
| 1.4.1 | Application: Maximum Log Size (KB) | 32768 KB or greater |
| 1.4.2 | Application: Retain old events | Disabled |
| 1.4.3 | Security: Maximum Log Size (KB) | 81920 KB or greater |
| 1.4.4 | Security: Retain old events | Disabled |
| 1.4.5 | System: Maximum Log Size (KB) | 32768 KB or greater |
| 1.4.6 | System: Retain old events | Disabled |

Fonte: security.uconn.edu e networkencyclopedia.com

# Hardening – firewall

O firewall permite bloquear ou liberar protocolos, processos ou aplicativos específicos de interagir com o sistema operacional através da rede.

| 1.5 | Windows Firewall | Setting |
|---|---|---|
| 1.5.1 | Windows Firewall: Allow ICMP exceptions (Domain) | Disabled |
| 1.5.2 | Windows Firewall: Allow ICMP exceptions (Standard) | Disabled |
| 1.5.3 | Windows Firewall: Apply local connection security rules (Domain) | For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Configured.<br>For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is No. |

...

Fonte: security.uconn.edu e networkencyclopedia.com

# Hardening – Windows Update

O Windows Update permite manter o sistema operacional atualizado.

| 1.6 | Windows Update | Setting |
|---|---|---|
| 1.6.1 | Configure Automatic Updates | Enabled: 3 - Auto download and notify for install |
| 1.6.2 | Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box | Disabled |
| 1.6.3 | Reschedule Automatic Updates scheduled installations | Enabled |

Fonte: security.uconn.edu e networkencyclopedia.com

# Hardening – direitos de usuário

Direitos de usuário são as permissões do que um usuário ou grupo de usuários podem fazer no domínio.

| 1.8 | User Rights | Setting |
|---|---|---|
| 1.8.1 | Access this computer from the network | For the Enterprise Member Server and SSLF Member Server profile(s), the recommended value is Administrators, Authenticated Users.<br>For the Enterprise Domain Controller and SSLF Domain Controller profile(s), the recommended value is Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS. |
| 1.8.2 | Act as part of the operating system | No one |
| ... | | |

Fonte: security.uconn.edu e networkencyclopedia.com

# Hardening – serviços de terminal

Os serviços de terminal permitem configurar o acesso remoto a um servidor.

| 1.10 | Terminal Services | Setting |
|---|---|---|
| 1.10.1 | Always prompt client for password upon connection | Enabled |
| 1.10.2 | Set client connection encryption level | Enabled: High Level |
| 1.10.3 | Do not allow drive redirection | For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Configured.<br>For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Enabled. |
| 1.10.4 | Do not allow passwords to be saved | Enabled |

Fonte: security.uconn.edu e networkencyclopedia.com

# Hardening – comunicações de Internet

As comunicações de Internet definem se e como o servidor irá se comunicar com o mundo externo por meio da rede.

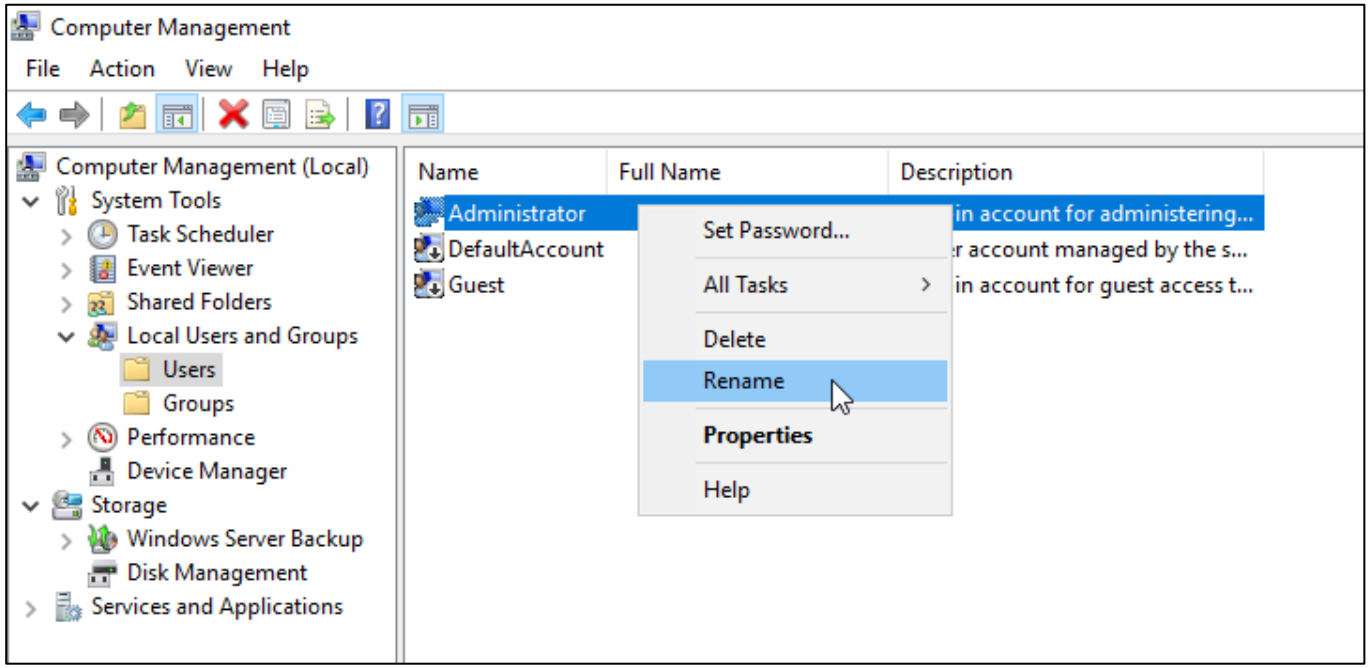
| 1.11 | Internet Communication | Setting |
|---|---|---|
| 1.11.1 | Turn off downloading of print drivers over HTTP | Enabled |
| 1.11.2 | Turn off the "Publish to Web" task for files and folders | Enabled |
| 1.11.3 | Turn off Internet download for Web publishing and online ordering wizards | Enabled |
| 1.11.4 | Turn off printing over HTTP | Enabled |
| 1.11.5 | Turn off Search Companion content file updates | Enabled |
| 1.11.6 | Turn off the Windows Messenger Customer Experience Improvement Program | Enabled |

...

Fonte: security.uconn.edu e networkencyclopedia.com

# Hardening – exemplo

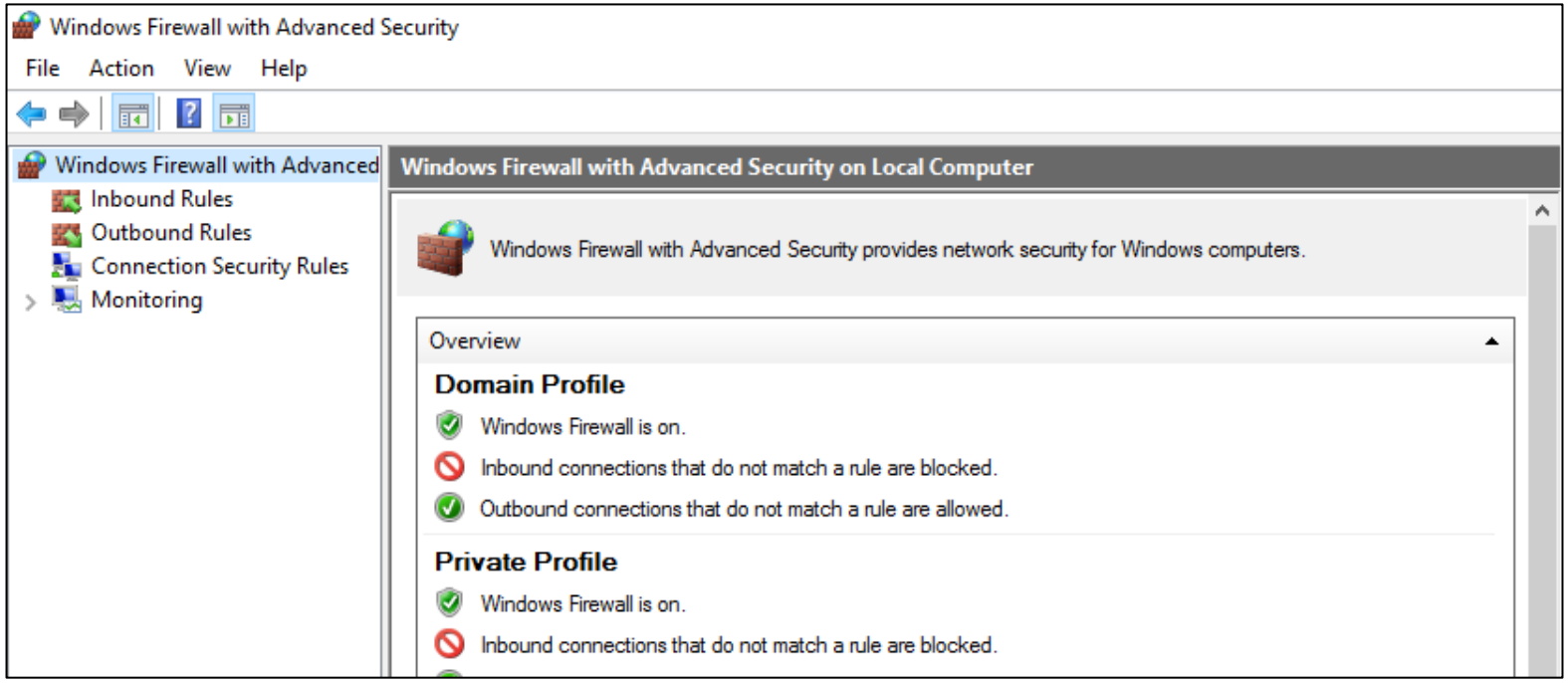
## Renomear usuário Administrator




⚠ ⊞ ⇨ **Computer Management**

# Hardening – exemplo

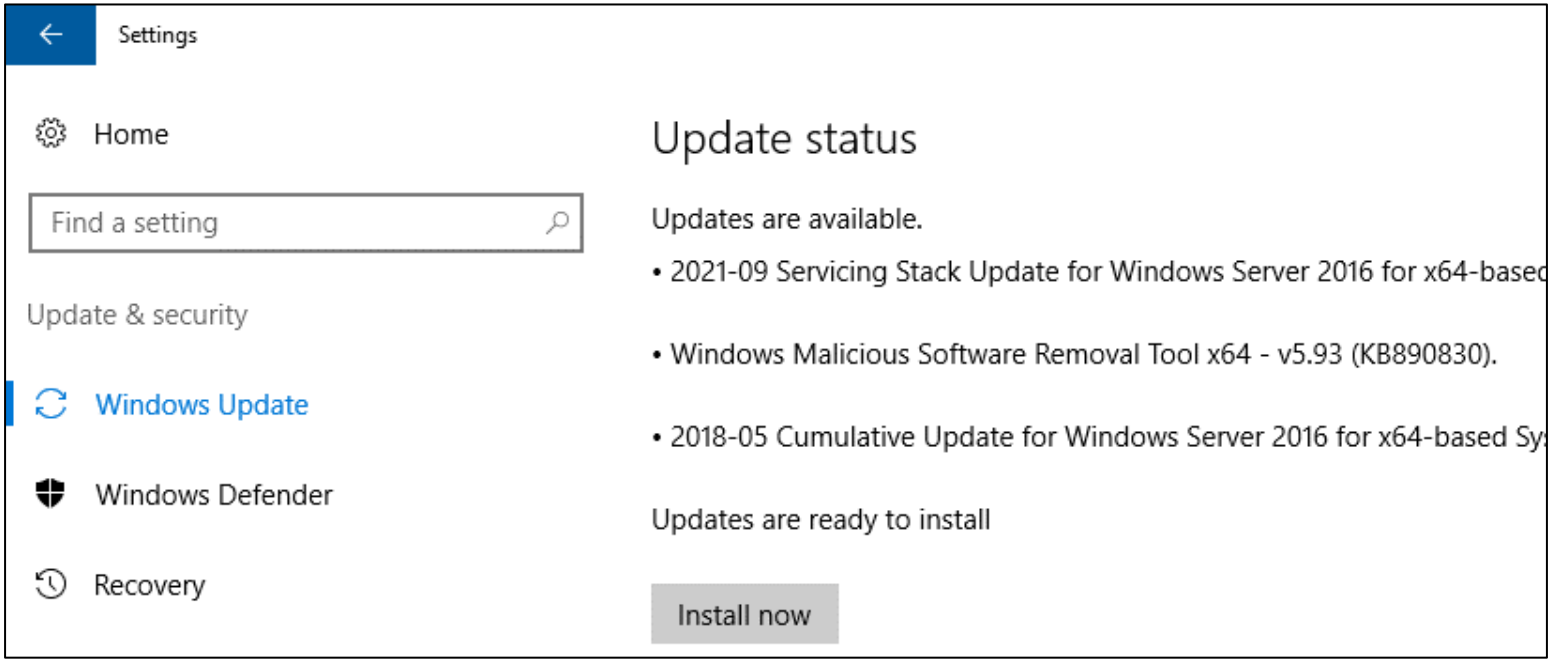
## Configurar Firewall




⇨ **Windows Firewall with Advanced Security**

# Hardening – exemplo

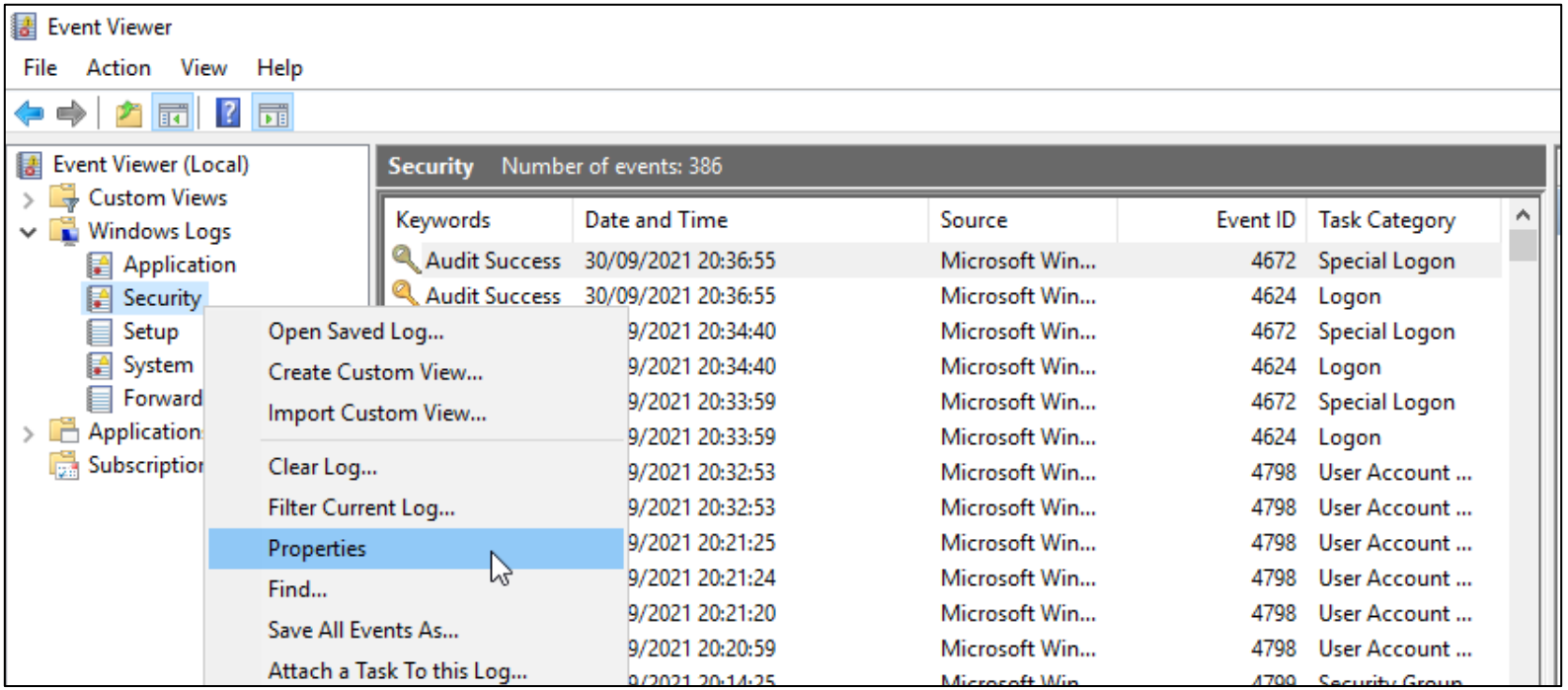
## Configurar e instalar atualizações




⚠ **Windows Update settings**

# Hardening – exemplo

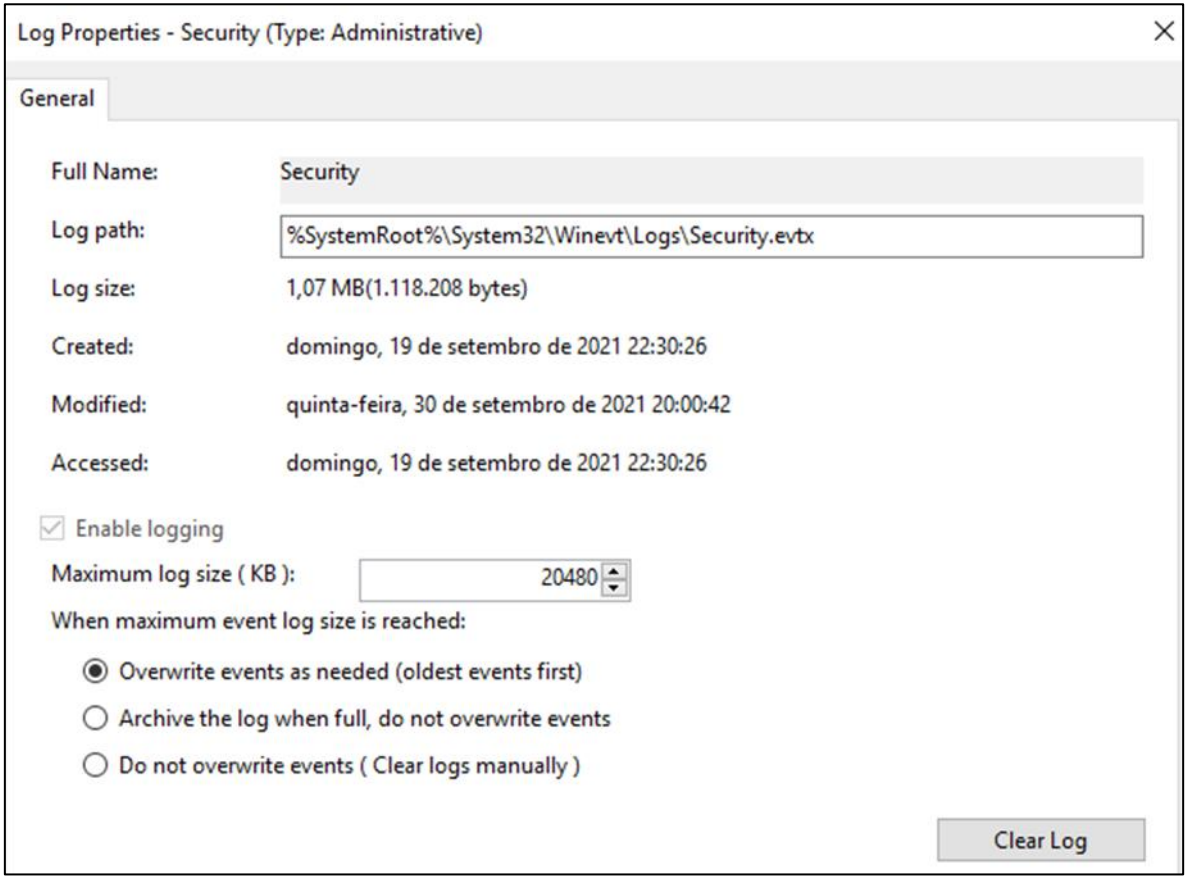
## Configurar o registro de eventos




⚠ ⇨ **Event Viewer**

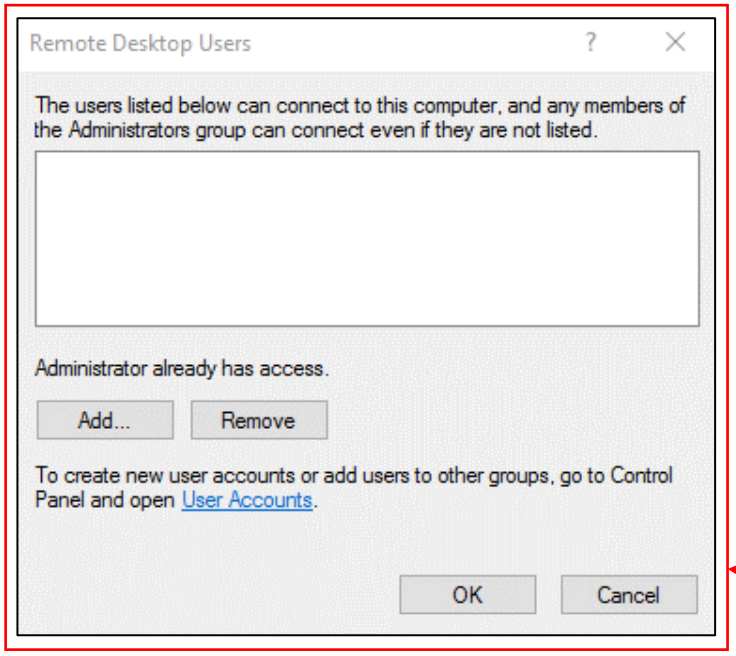
# Hardening – exemplo

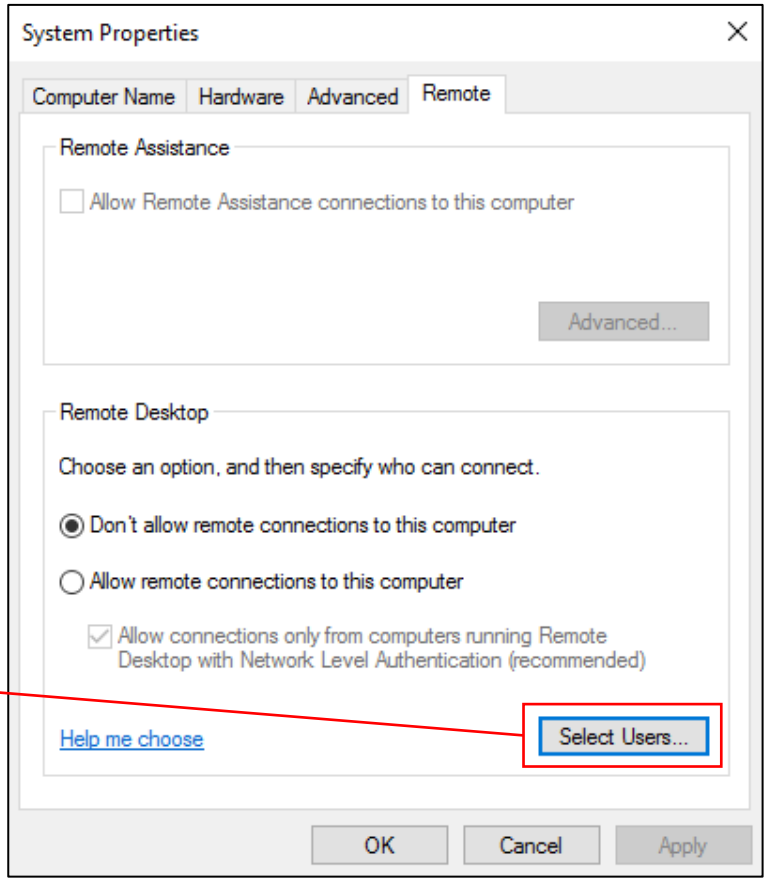
**Configurar o registro de eventos - continuação...**



# Hardening – exemplo

**Configurar serviços de assistência remota**




⇨ **Allow remote access to your computer**

# Hardening – exemplo

**Configurar o relógio usando NTP (Network Time Protocol)**

- Mostrar o fuso horário (timezone):

```
C:\>w32tm /tz
Time zone: Current:TIME_ZONE_ID_STANDARD Bias: 180min
(UTC=LocalTime+Bias)
  [Standard Name:"E. South America Standard Time"
Bias:0min Date:(M:2 D:3 DoW:6)]
  [Daylight Name:"E. South America Daylight Time" Bias:-
60min Date:(M:10 D:3 DoW:6)]
```

**⇨ Command Prompt ⇨ w32tm.exe**

# Hardening – exemplo

**Configurar o relógio usando NTP (Network Time Protocol) – continuação**

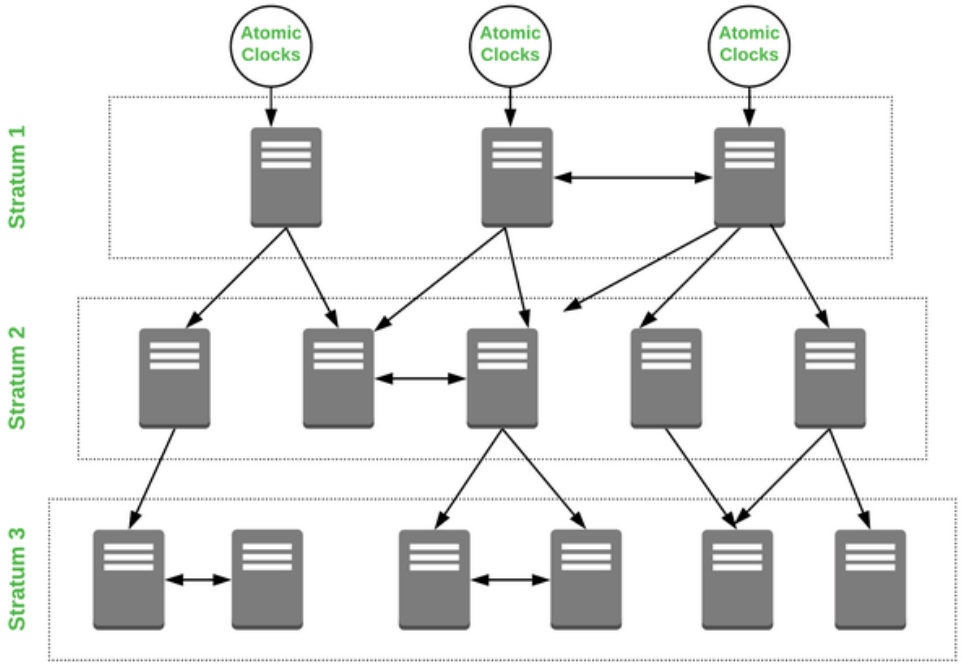
- Mostrar a fonte de tempo configurada:

```
C:\>w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 4 (secondary reference - syncd by (S)NTP)
Precision: -6 (15.625ms per tick)
Root Delay: 0.1936052s
Root Dispersion: 0.9871670s
ReferenceId: 0x287706E4 (source IP:  40.119.6.228)
Last Successful Sync Time: 30/09/2021 21:26:43
Source: time.windows.com,0x8
Poll Interval: 7 (128s)
```

# Hardening – exemplo

**Configurar o relógio usando NTP (Network Time Protocol) – continuação**

Stratum representa a distância da referência primária de tempo (stratum 0).



# Hardening – exemplo

**Configurar o relógio usando NTP (Network Time Protocol) – continuação**

- Configurar uma fonte de tempo alternativa:

```
C:\>w32tm /config /manualpeerlist:pool.ntp.org /update
The command completed successfully.
```

Onde pool.ntp.org é uma fonte de tempo.

No Brasil, é possível utilizar a fonte de tempo pool.ntp.br, entre outras.

# Hardening – exemplo

**Configurar o relógio usando NTP (Network Time Protocol) – continuação**

- Ressincronizar o relógio:

```
C:\>w32tm /resync
Sending resync command to local computer
The command completed successfully.
```

# Hardening – exemplo

**Configurar o relógio usando NTP (Network Time Protocol) – continuação**

- Iniciar o serviço:

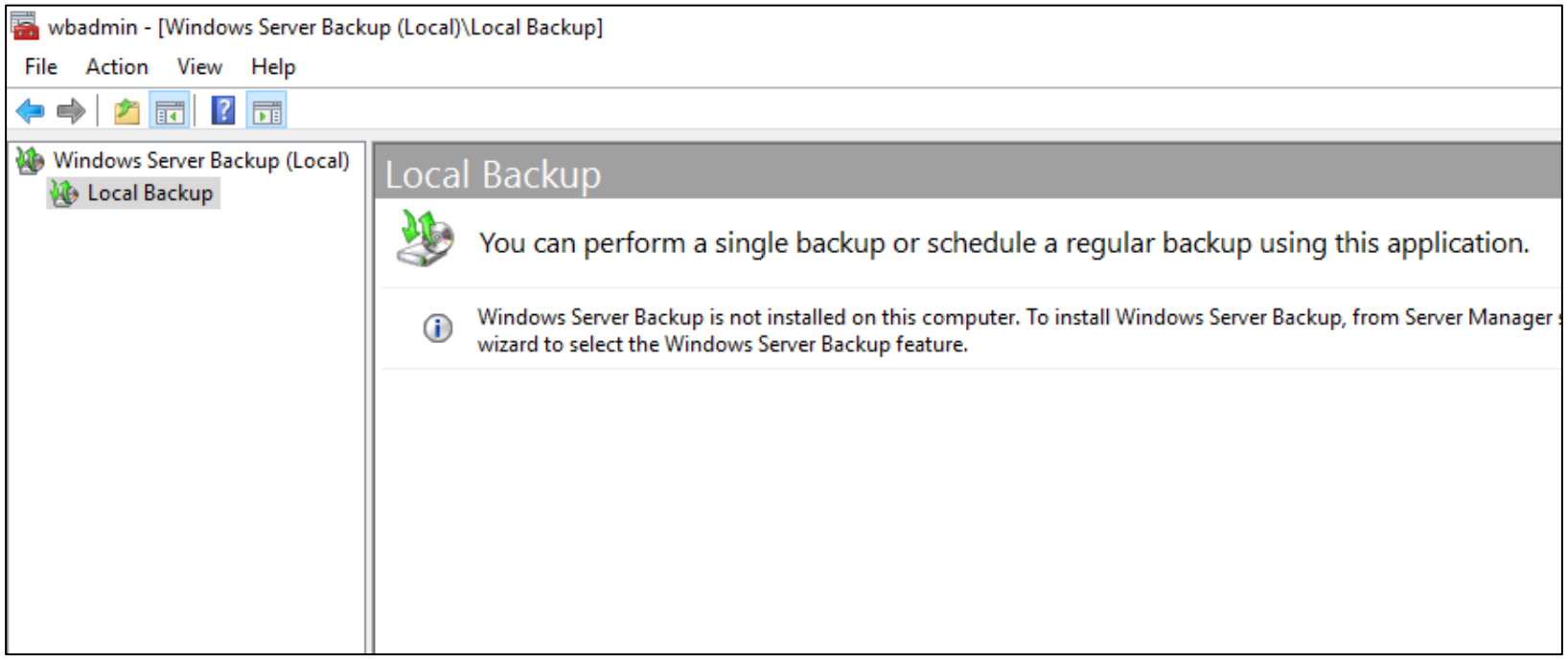
```
C:\>net start w32time
The Windows Time service is starting.
The Windows Time service was started successfully.
```

- Parar o serviço:

```
C:\>net stop w32time
The Windows Time service is stopping.
The Windows Time service was stopped successfully.
```

# Hardening – exemplo

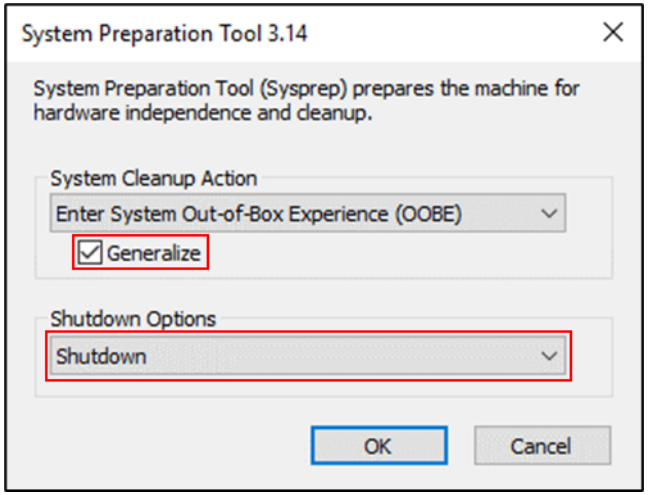
## Configurar o backup




⚠ ⇨ **Windows Server Backup**

# Hardening – exemplo

**Generalizar o sistema para criação de imagem (opcional)**




**C:\Windows\System32\Sysprep**

# Para saber mais...

… consulte o documento Server Hardening Standard (Windows), disponível em https://security.uconn.edu/server-hardening-standard-windows/

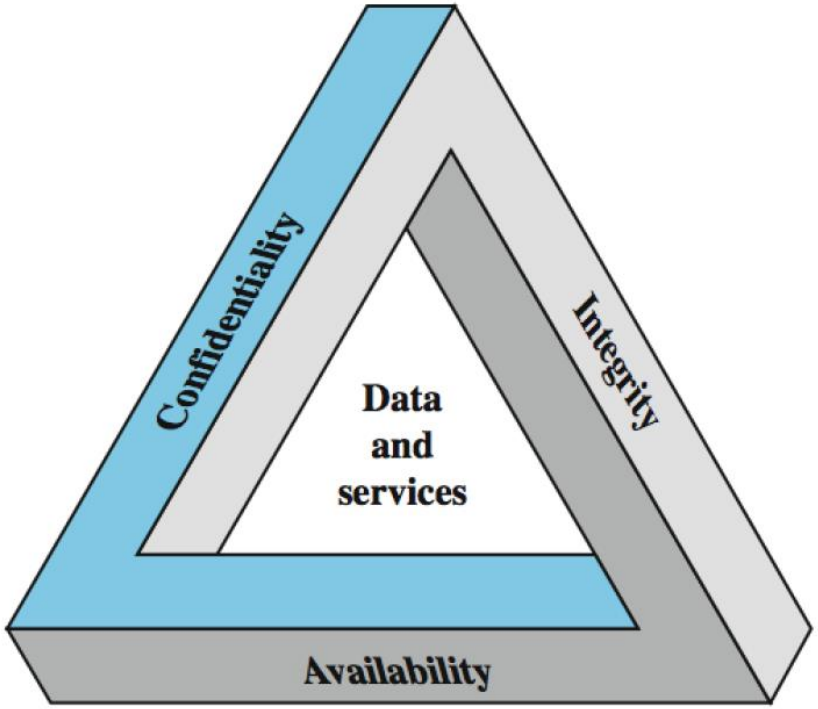
... consulte o recurso Microsoft Security Compliance Toolkit 1.0, disponível em https://www.microsoft.com/en-us/download/details.aspx?id=55319

# Módulo 7

Configuração de Segurança do Windows Server

# Introdução

De acordo com Stallings, o NIST (*National Institute of Standards and Technology*) define segurança da computação como uma tríade formada pela confidencialidade, integridade e disponibilidade, também conhecida como **Tríade da Segurança**.



# Introdução

**CONFIDENCIALIDADE**

Garantir o acesso às informações somente a indivíduos, entidades ou processos autorizados.

**INTEGRIDADE**

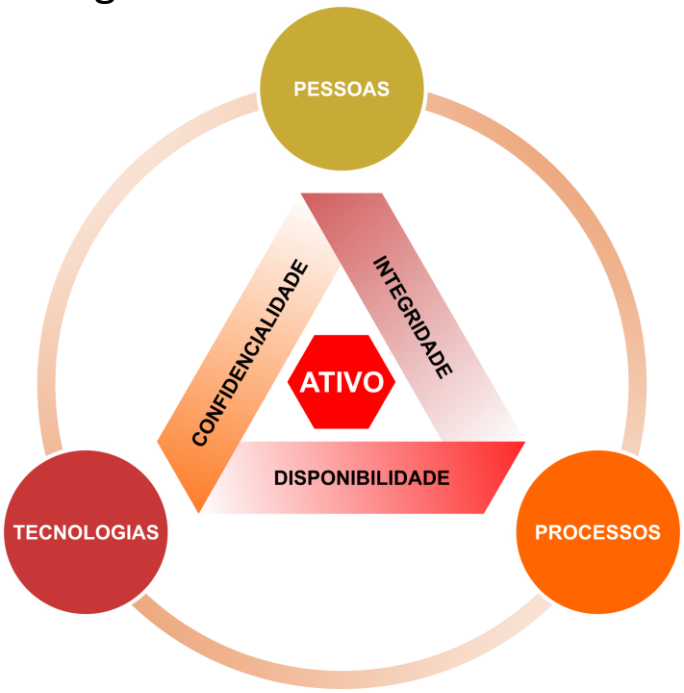
Proteger contra modificação ou destruição inadequada das informações.

**DISPONIBILIDADE**

Garantir o acesso oportuno e confiável e o uso das informações.

# Introdução

A Tríade de Segurança visa proteger um **ativo**, e para tal deve lançar mão de pessoas, processos e tecnologias.




Fonte: SANTANA, W. R. *et al*. Aplicação da norma NBR ISO/IEC 27002 para atendimento do Marco Civil da Internet e da LGPD. CONTECSI USP – 17th International Conference on Information Systems and Technology Management, São Paulo, p. 1419-1439, Setembro 2020

# Segurança do Windows Server

Para atender aos requisitos da Tríade de Segurança e garantir a segurança de um servidor com sistema operacional Windows Server, pode-se adotar a seguinte abordagem:

- Configurar o compartilhamento e as permissões de pastas e arquivos para garantir a **confidencialidade**;
- Configurar a criptografia para garantir a **integridade***; e
- Configurar RAID (Redundant Array of Independent Disks) ou *cluster* para garantir a **disponibilidade**.

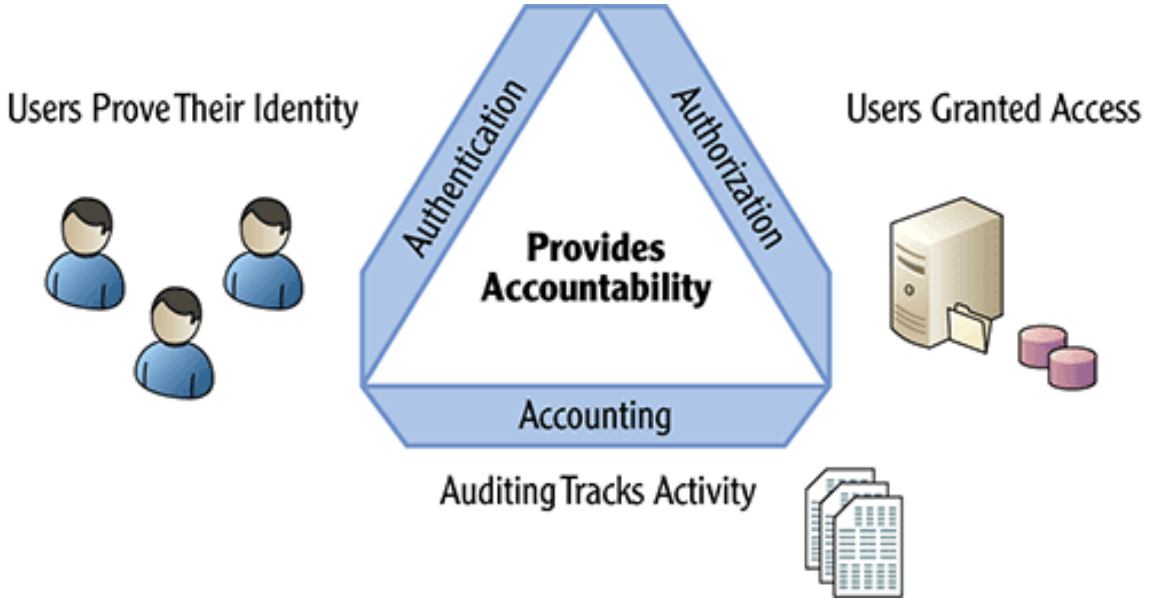
*A criptografia usada em servidores com sistema operacional Windows Server podem ser úteis também para garantir a confidencialidade.

Neste curso será abordado apenas a configuração de compartilhamentos e permissões de pastas e arquivos.

# Authentication, Authorization & Accountability

Um sistema operacional seguro precisa ser capaz de identificar usuários individuais, conceder acesso com base em suas identidades e rastrear suas ações.

Isso pode ser alcançado com a implementação de práticas que refletem os acrônimo AAA, de **Authentication**, **Authorization** e **Accountability** (Autenticação, Autorização e Auditoria/Contabilidade).




Fonte: Microsoft Windows Security Essentials, de Darril Gibson

# Authentication, Authorization & Accountability

## AUTENTICAÇÃO

Quando um usuário tenta acessar um sistema, a primeira etapa é garantir que ele prove quem é ao se autenticar. Nesta etapa obtêm-se a identificação do usuário.

## AUTORIZAÇÃO

Após a autenticação é realizada a verificação das permissões do usuário que fornecem autorização para acessar diferentes recursos. Nesta etapa é verificado se as permissões do usuário (token) coincidem com a ACL (Access Control List) do recurso.

## AUDITORIA/CONTABILIDADE

Sempre que o usuário acessa um recurso que ele tem ou não permissão de acesso, pode ser necessário rastrear suas atividades para fins de auditoria ou contabilidade. Nesta etapa, que geralmente é opcional, são verificados os acessos dos usuários aos recursos.

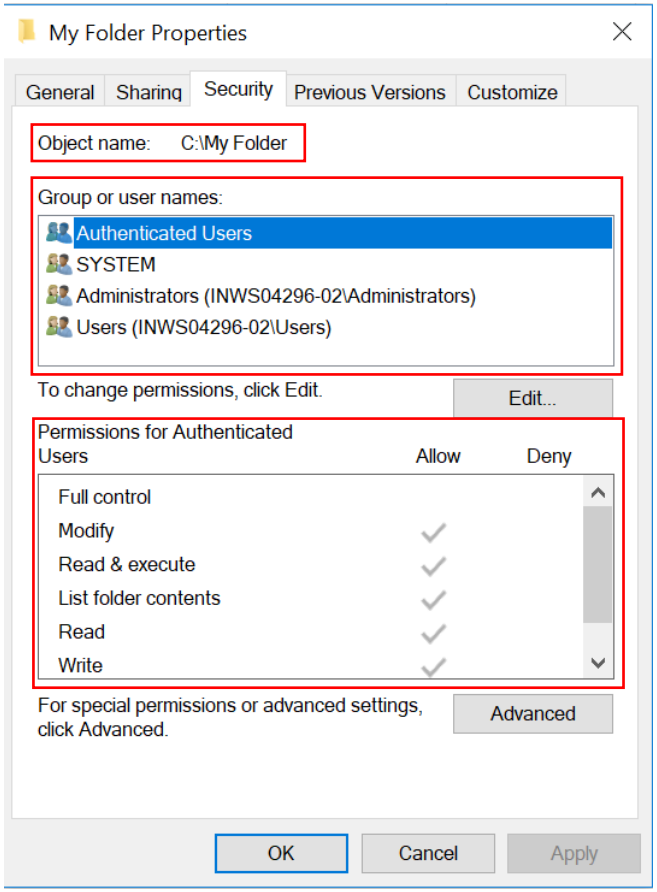
# Permissões de pastas e arquivos

As permissões são o principal método para restringir o acesso aos recursos em um servidor ou domínio do Windows Server.

É possível atribuir permissões a unidades de disco usando NTFS (New Technology File System), pastas, compartilhamentos, arquivos, objetos do Active Directory e o Registro do Windows.

Muitos dos conceitos de permissão são os mesmos para diferentes tipos de recursos, onde cada recurso pode ser configurado como Permitir ou Negar e, se a permissão Negar for atribuída, esta sempre terá precedência.

Além disso, todas as permissões podem ser atribuídas a um recurso ou objeto pai e serem herdadas por todos os recursos ou objetos filhos.




Fonte: Microsoft Windows Security Essentials, de Darril Gibson

# Permissões de pastas e arquivos

As permissões NTFS básicas são as listadas no quadro abaixo:

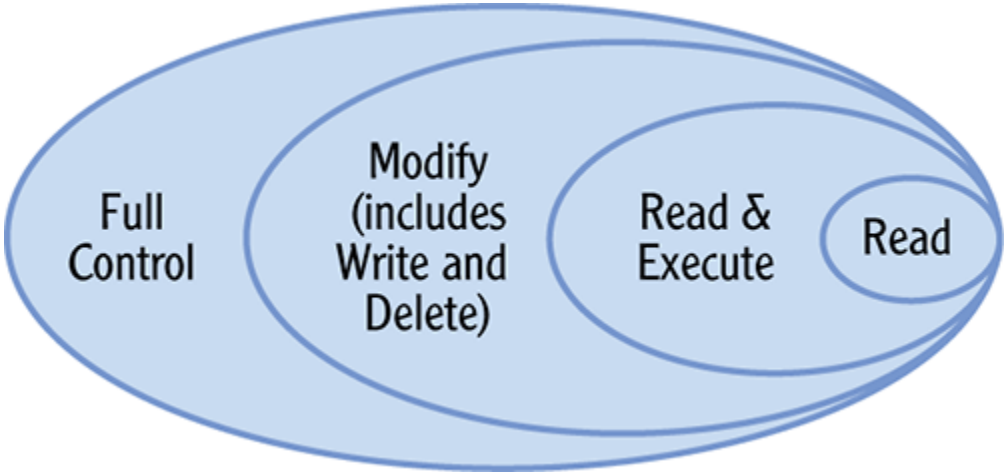
| PERMISSÃO | DESCRIÇÃO |
|---|---|
| **Read** | Um usuário pode ler o conteúdo de um arquivo ou pasta. |
| **Read & Execute** | Um usuário pode ler o conteúdo de um arquivo ou pasta e, se for um programa, o usuário pode iniciá-lo (executá-lo). |
| **List Folder Contents** | Isso se aplica apenas a pastas e concede ao usuário permissão para listar itens na pasta e nas pastas filhas. |
| **Write** | Isso concede ao usuário permissão para fazer alterações no arquivo e salvá-las. Quando concedido a uma pasta, dá ao usuário permissão para adicionar arquivos a uma pasta. Um usuário não pode excluir arquivos com permissão de gravação. |
| **Modify** | Os usuários recebem todas as permissões de leitura (Read & Execute e List Folder Contents) e permissão de gravação (Write). Além disso, eles podem excluir arquivos e pastas com essa permissão. |
| **Full Control** | Isso inclui todas as permissões, incluindo as permissões avançadas, entre elas a de Take Ownership (assumir a propriedade). |

Fonte: Microsoft Windows Security Essentials, de Darril Gibson

# Permissões de pastas e arquivos

Várias dessas permissões básicas incluem outras permissões, conforme mostrado na figura abaixo.

Por exemplo, se um usuário tiver permissão de Full Control sobre um arquivo ou pasta, ele terá todas as permissões. Da mesma forma, a permissão Modify inclui a capacidade de gravar e excluir, mas também inclui Read & Execute e Read.




Fonte: Microsoft Windows Security Essentials, de Darril Gibson

# Permissões de pastas e arquivos

As permissões NTFS avançadas são as listadas no quadro abaixo:

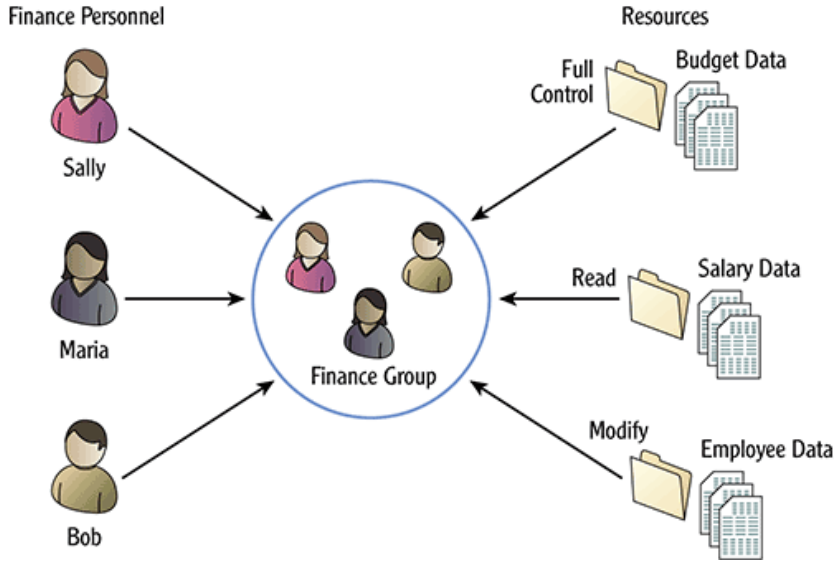
| PERMISSÃO | DESCRIÇÃO |
|---|---|
| **Read** | List Folder / Read Data, Read Attributes, Read Extended Attributes, e Read Permissions. Quando atribuído a uma pasta, inclui também a permissão List Folder. |
| **Read & Execute** | List Folder / Read Data, Read Attributes, Read Extended Attributes, Read Permissions, e Traverse Folder / Execute File. |
| **List Folder Contents** | List Folder / Read Data, Read Attributes, Read Extended Attributes, and Traverse Folder / Execute File. A permissão List Folder Contents está disponível apenas para pastas, e não para arquivos. |
| **Write** | Create Files / Write Data, Create Folders / Append Data, Write Attributes, e Write Extended Attributes. |
| **Modify** | List Folder / Read Data, Read Attributes, Read Extended Attributes, Read Permissions, Traverse Folder / Execute File, Create Files / Write Data, Create Folders / Append Data, Write Attributes, Write Extended Attributes, e Delete. |
| **Full Control** | Isso inclui todas as 13 permissões avançadas. |

Fonte: Microsoft Windows Security Essentials, de Darril Gibson

# Permissões de pastas e arquivos

Para facilitar a administração da segurança de acesso aos recursos, os usuários são associados a grupos cujas permissões serão configuradas.

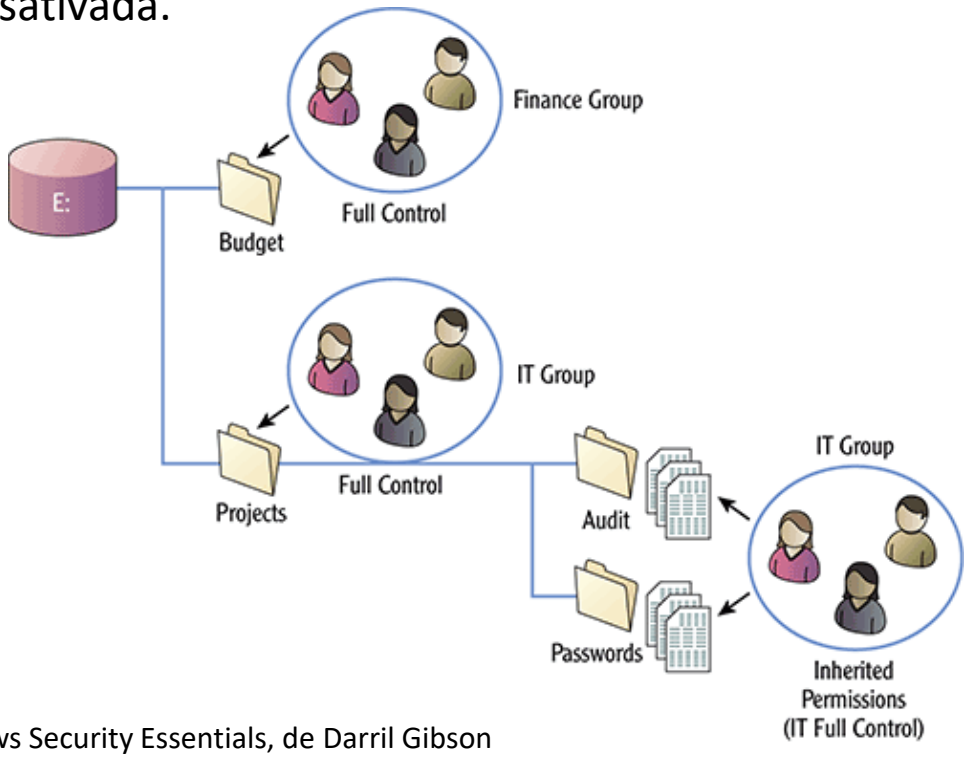
Se um usuário for membro de diferentes grupos aos quais são atribuídas diferentes permissões, o usuário receberá o total cumulativo de todas as permissões.




Fonte: Microsoft Windows Security Essentials, de Darril Gibson

# Permissões de pastas e arquivos

Outra forma de facilitar a administração de recursos é utilizando o recurso de herança (inheritance), onde as permissões podem ser herdadas de pastas para arquivos e por subpastas dentro de uma pasta. A herança é habilitada por padrão, mas pode ser desativada.

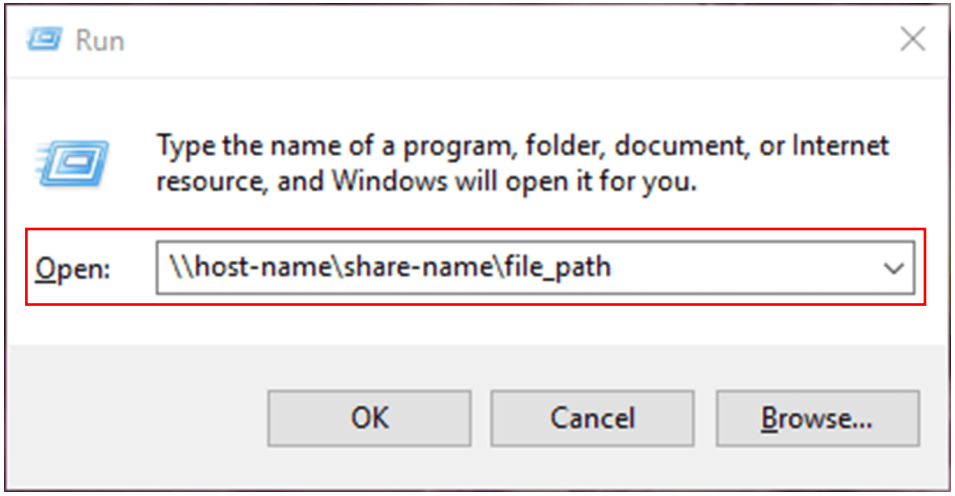



Fonte: Microsoft Windows Security Essentials, de Darril Gibson

# Compartilhamento de pastas

Em uma rede, é comum compartilhar pastas em um servidor ou estação de trabalho para que os usuários da rede possam acessar as pastas.

Quando uma pasta é compartilhada, os usuários podem acessar o compartilhamento por meio de unidades mapeadas ou inserindo o caminho UNC (Universal Naming Convention) ou Convenção Universal de Nomenclatura.




Fonte: Microsoft Windows Security Essentials, de Darril Gibson

# Compartilhamento de pastas

As permissões de compartilhamento são as listadas no quadro abaixo:

| PERMISSÃO | DESCRIÇÃO |
|---|---|
| **Read** | Usuários com essa permissão podem ler quaisquer arquivos ou pastas dentro do compartilhamento. |
| **Change** | Usuários com essa permissão podem ler, gravar, modificar e excluir arquivos e pastas no compartilhamento. Isso é equivalente à permissão Modify do NTFS. |
| **Full Control** | Usuários com essa permissão podem fazer qualquer coisa com arquivos e pastas no compartilhamento, incluindo alterar as permissões subjacentes. |

As permissões de compartilhamento se aplicam apenas quando um usuário o acessa através da rede, e não quando a pasta é acessada localmente.

As permissões de compartilhamento não substituem as permissões NTFS. Em vez disso, as permissões de compartilhamento interagem com as permissões NTFS.

Fonte: Microsoft Windows Security Essentials, de Darril Gibson

# Combinando permissões NTFS e de compartilhamento

Quando os usuários acessam um compartilhamento na rede, as permissões NTFS e de compartilhamento são aplicadas.

É possível determinar a permissão resultante com as três etapas a seguir:

1. Determinar as permissões NTFS cumulativas;
2. Determinar as permissões de compartilhamento cumulativas;
3. Identificar qual permissão cumulativa é mais restritiva.

Fonte: Microsoft Windows Security Essentials, de Darril Gibson

# Combinando permissões NTFS e de compartilhamento – exemplo 1

Imagine que a usuária Sally é membro do grupo de TI (IT Group) e do grupo de Finanças (Finance Group) e está acessando um compartilhamento pela rede chamado Orçamento (Budget). As permissões são as seguintes:

| | IT Group Permissions | Finance Group Permissions |
|---|---|---|
| NTFS Permission | Full Control | Read |
| Share Permissions | Change | Read |

Sally

Determinando a permissão resultante:

1. Determinar as permissões NTFS cumulativas: Full Control, porque Full Control inclui Read;
2. Determinar as permissões de compartilhamento cumulativas: Change, porque Change inclui Read;
3. Identificar qual permissão cumulativa é mais restritiva: Change, porque Change é mais restritiva do que Full Control.

Qual é a permissão desta usuária se ela acessar a pasta enquanto estiver conectada ao computador que hospeda a pasta?

Fonte: Microsoft Windows Security Essentials, de Darril Gibson

# Combinando permissões NTFS e de compartilhamento – exemplo 2

Qual é a permissão resultante se a usuária Sally acessar este mesmo compartilhamento pela rede com a nova permissão configurada? As permissões são as seguintes:

| | IT Group Permissions | Finance Group Permissions | Sally Permissions |
|---|---|---|---|
| NTFS Permission | Modify | Read | Deny Full Control |
| Share Permissions | Full Control | Change | None assigned |

Sally

Determinando a permissão resultante:

1. Determinar as permissões NTFS cumulativas: Deny Full Control, porque Deny tem precedência;
2. Determinar as permissões de compartilhamento cumulativas: Full Control, porque Full Control inclui Change;
3. Identificar qual permissão cumulativa é mais restritiva: Deny Full Control, porque Deny Full Control é mais restritiva do que conceder Full Control.

Qual é a permissão desta usuária se ele acessar a pasta enquanto estiver conectada ao computador que hospeda a pasta?

Fonte: Microsoft Windows Security Essentials, de Darril Gibson

# Combinando permissões NTFS e de compartilhamento – exemplo 3

O usuário Bob também é membro do grupo de TI (IT Group) e do grupo de Finanças (Finance Group). Qual é a permissão resultante se ele acessar este mesmo compartilhamento pela rede? As permissões são as seguintes:

| | IT Group Permissions | Finance Group Permissions | Sally Permissions |
|---|---|---|---|
| NTFS Permission | Modify | Read | Deny Full Control |
| Share Permissions | Full Control | Change | None assigned |


Determinando a permissão resultante:

1. Determinar as permissões NTFS cumulativas: Modify, porque Modify inclui Read;
2. Determinar as permissões de compartilhamento cumulativas: Full Control, porque Full Control inclui Change;
3. Identificar qual permissão cumulativa é mais restritiva: Modify, porque Modify é mais restritivo do que Full Control.

Qual é a permissão deste usuário se ele acessar a pasta enquanto estiver conectado ao computador que hospeda a pasta?

Fonte: Microsoft Windows Security Essentials, de Darril Gibson

# Para saber mais...

… leia o documento xxxxxxxxxxx

# Módulo 8

Domain Name System

# DNS

O Domain Name System é um banco de dados hierárquico que oferece o serviço de resolução de nomes URL (Uniform Resource Locator) usados para identificar um domínio.

Toda comunicação na Internet é feita por meio dos endereços IP, mas é muito mais fácil memorizar URL´s do que endereços IP.

Assim, o que o serviço de DNS faz é converter as URL´s em endereços IP:

**www.brasil.gov.br → 170.246.252.242**

**www.tj.sp.gov.br → 200.142.86.230**

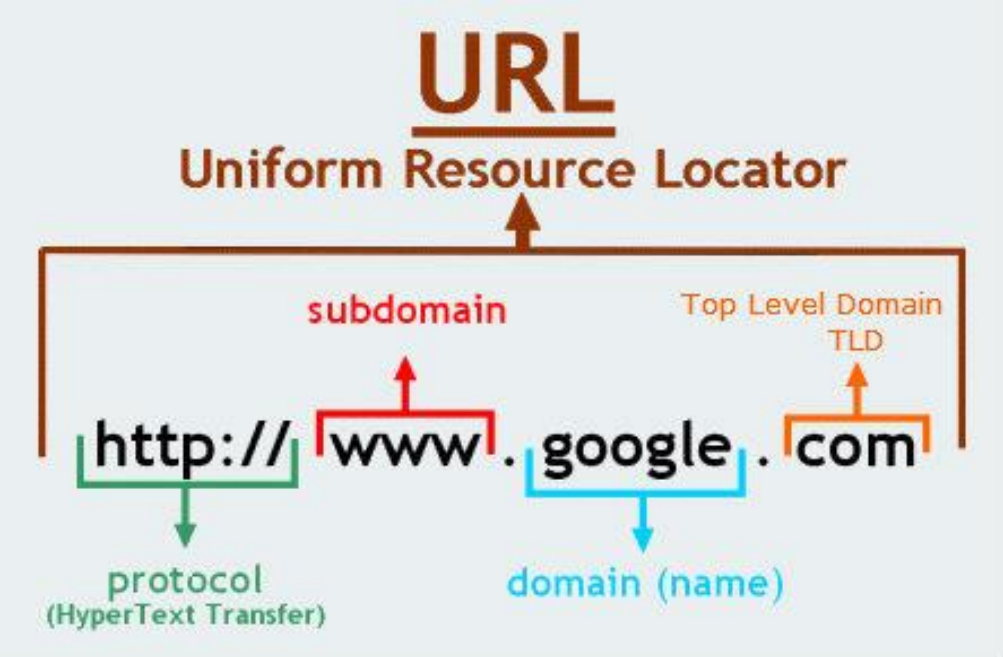
**www.google.com → 172.217.172.132**

**www.bb.com.br → 170.66.11.10**

# URL – Uniform Resource Locator

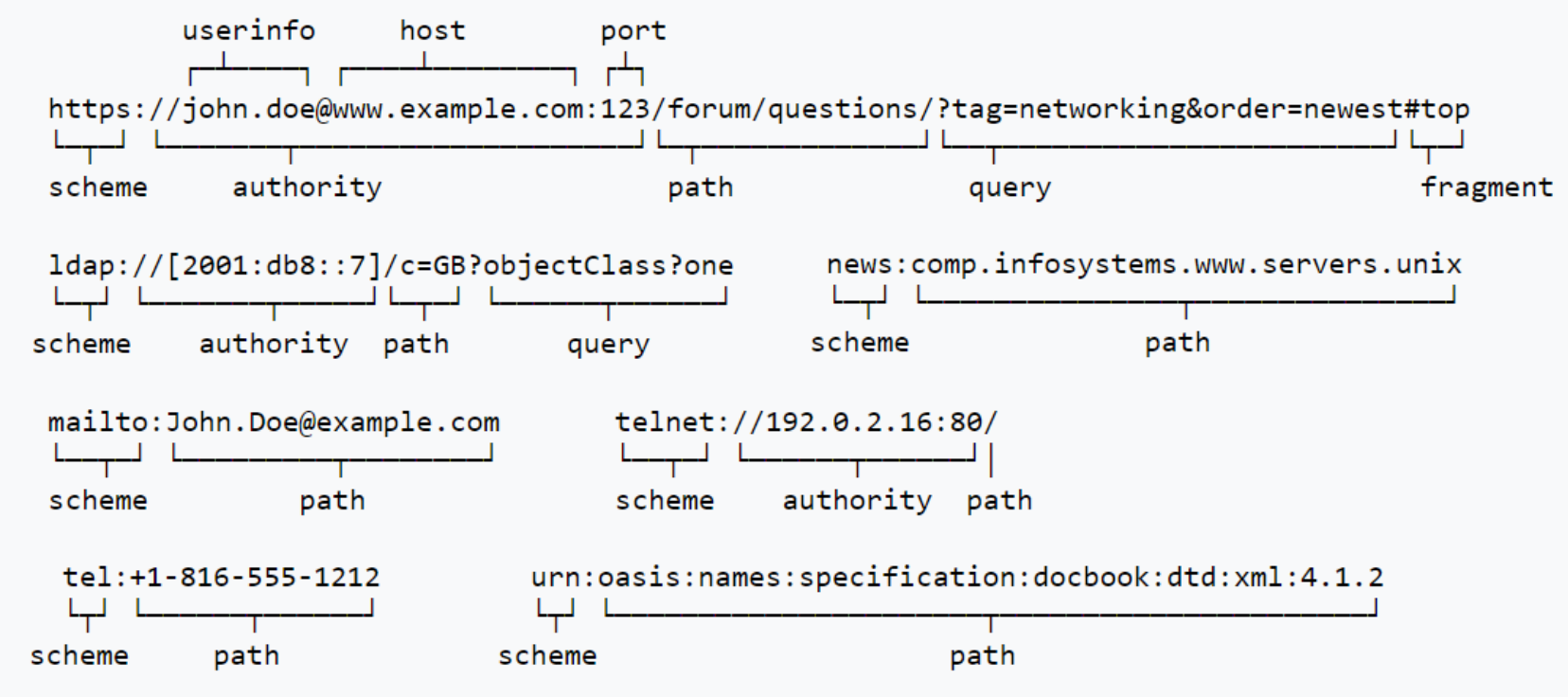
Um URL (Uniform Resource Locator), é uma referência a um recurso da web que especifica sua localização em uma rede de computadores e um mecanismo para recuperá-lo.

Um URL é um tipo específico de URI (Uniform Resource Identifier).



# URI – Uniform Resource Identifier

Um URI (Uniform Resource Identifier) é uma cadeia de caracteres que identifica inequivocamente um recurso específico.



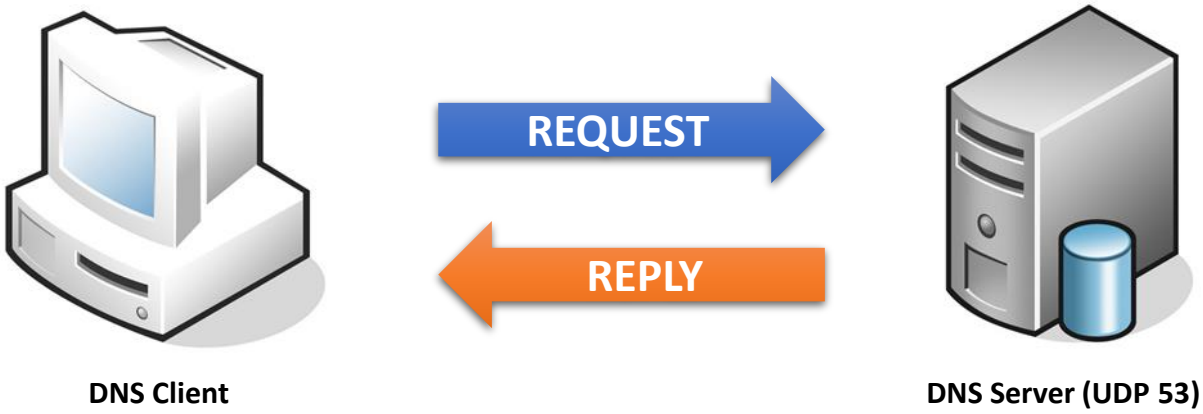

Fonte: wikipedia.org

# DNS

Um cliente DNS é todo aquele que requisita respostas a uma determina consulta feita a um servidor DNS.

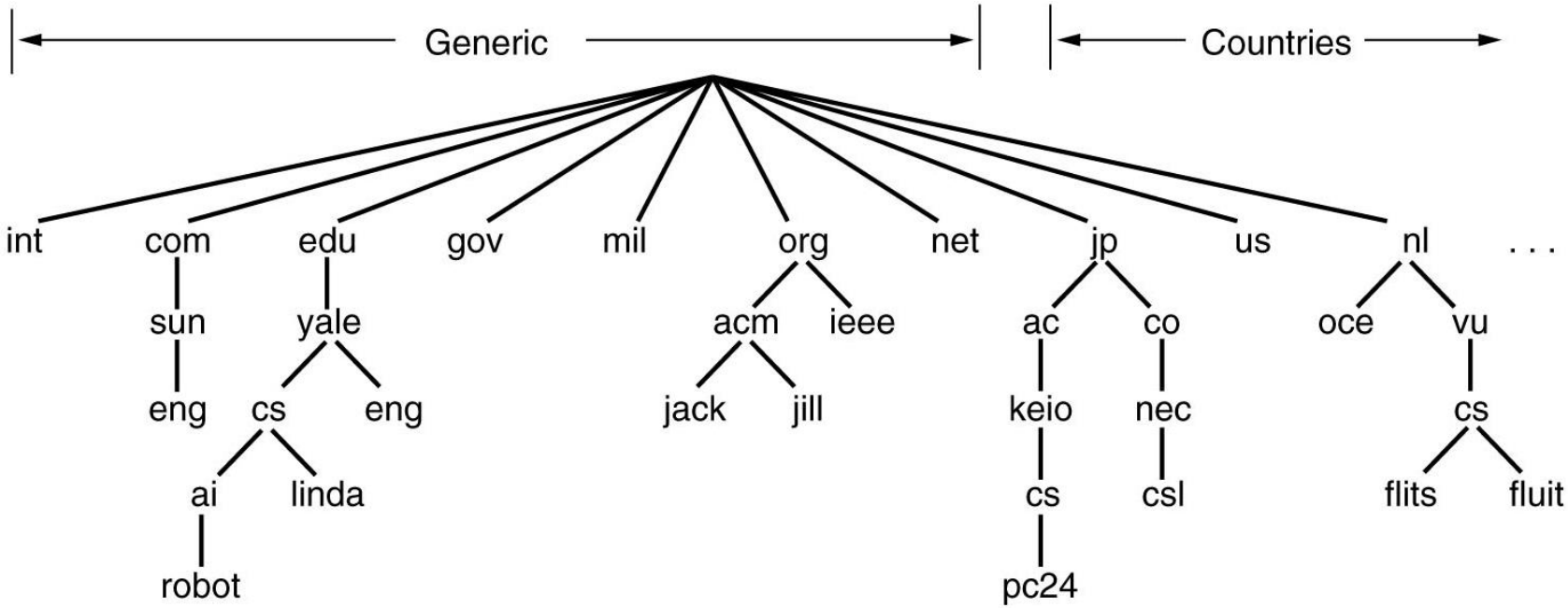
Um servidor DNS é todo aquele que responde às consultas feitas por um cliente.

O servidor DNS opera na porta UDP 53.



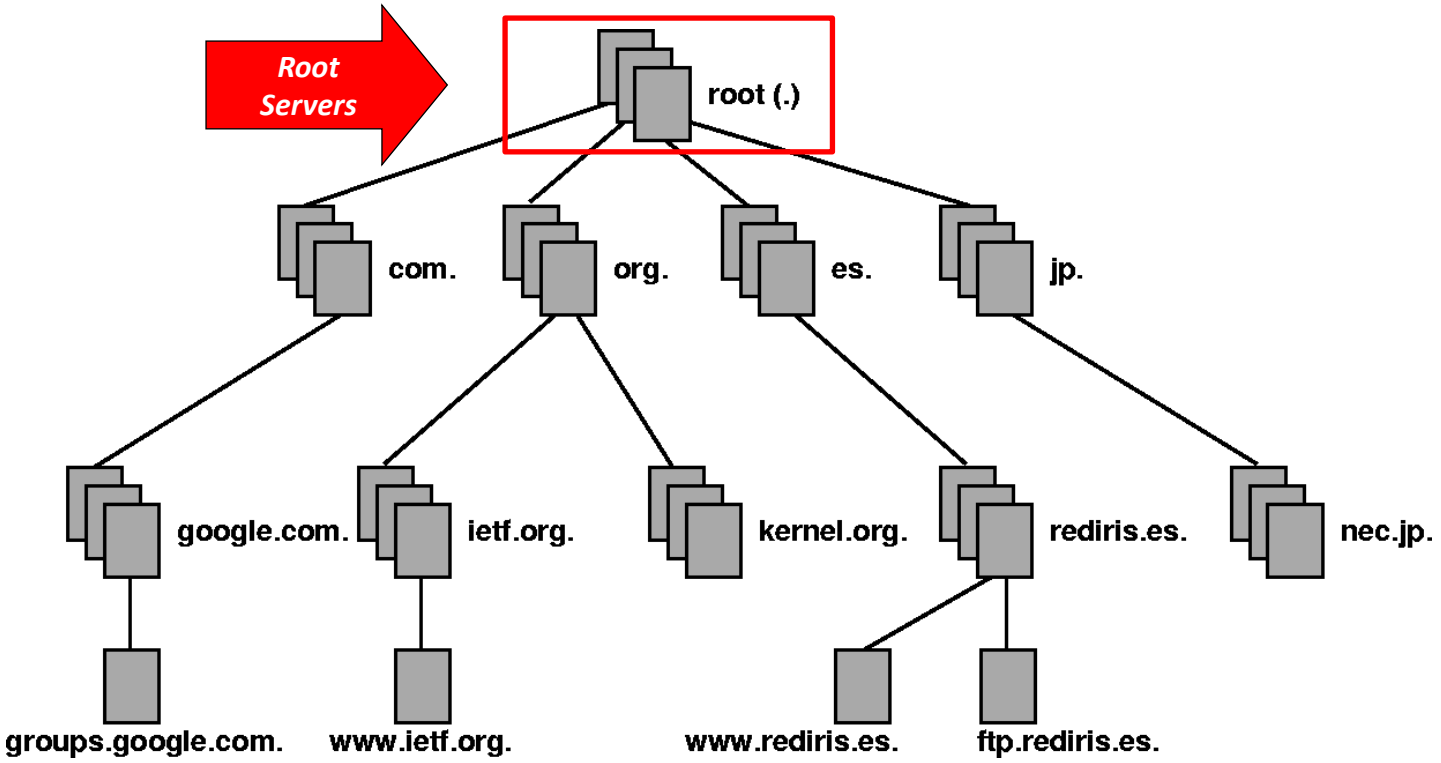
# DNS

Os nomes de domínio servem para identificar uma rede ou grupo de computadores. Estão dispostos de forma hierárquica e geralmente possuem um ou mais servidores DNS responsáveis por mapear todos os nomes abaixo daquele domínio (ou subdomínio) em endereços IP.



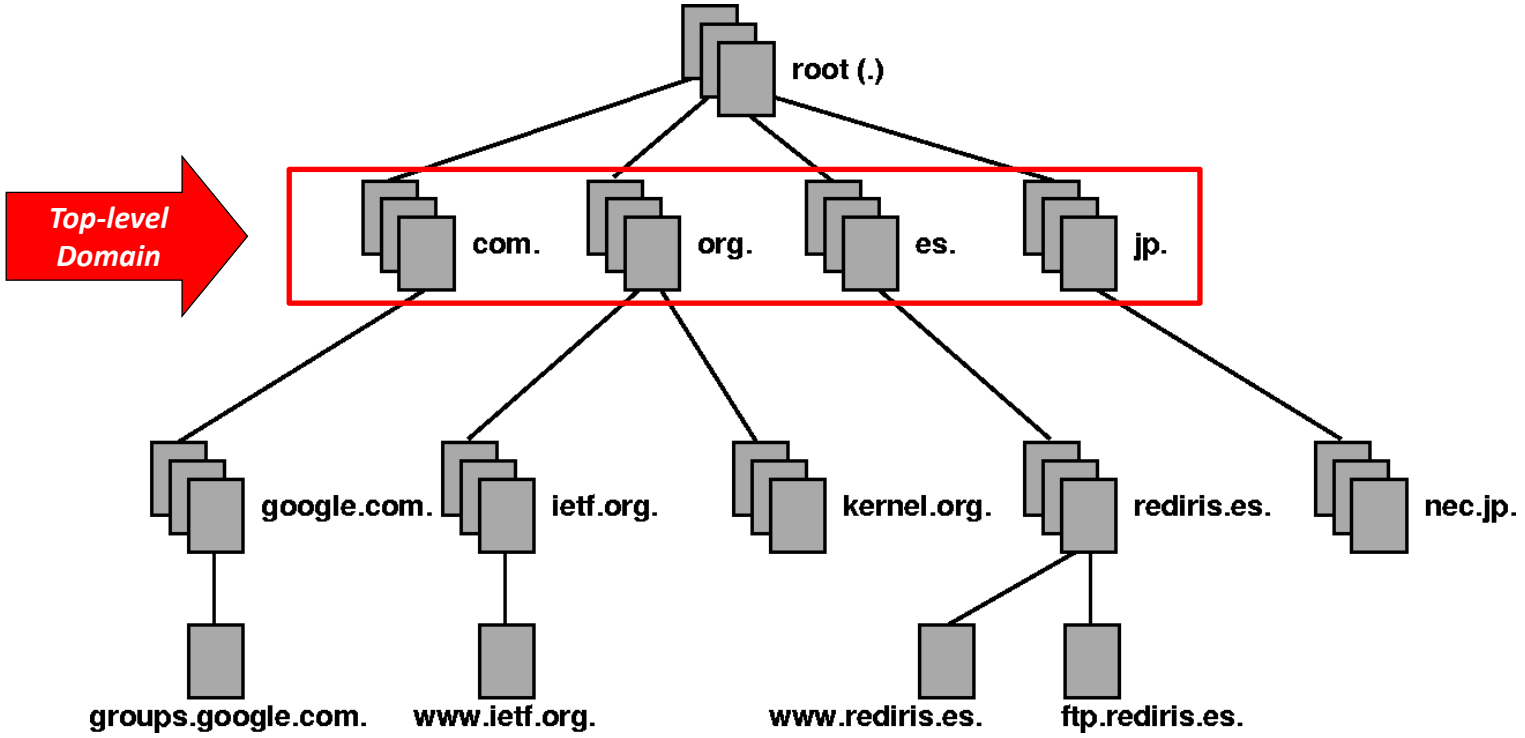
# DNS

O ponto mais alto da cadeia é denominado *root*. O servidor DNS responsável por este ponto é o *root server*. Este servidor possui todas as entradas para os servidores imediatamente abaixo dele.



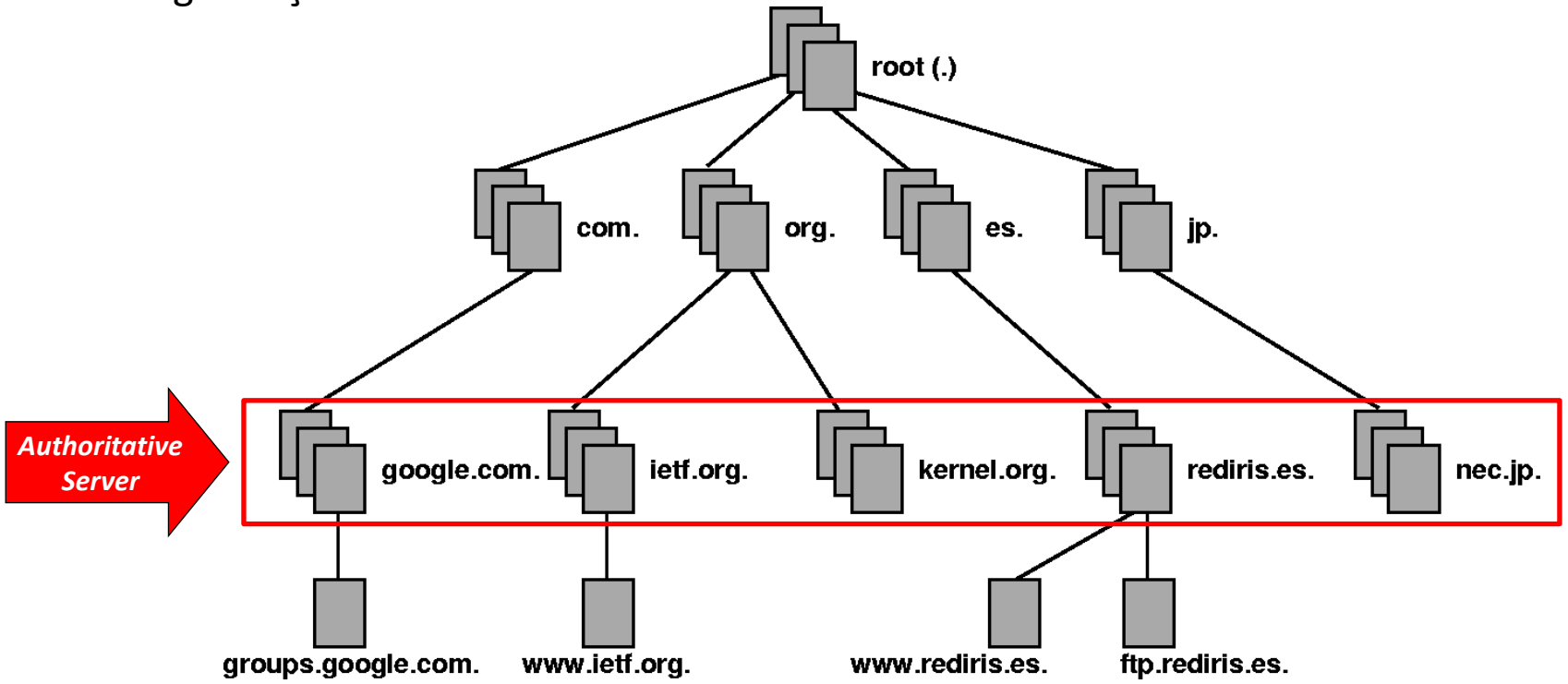
# DNS

Os *Top-level Domain* identificam domínios genéricos, como .com ou .gov, e domínios de países, como .br, .jp, .it, etc. O servidor DNS responsável por este ponto é o *TLD server*. Este servidor possui todas as entradas para os servidores imediatamente abaixo dele.

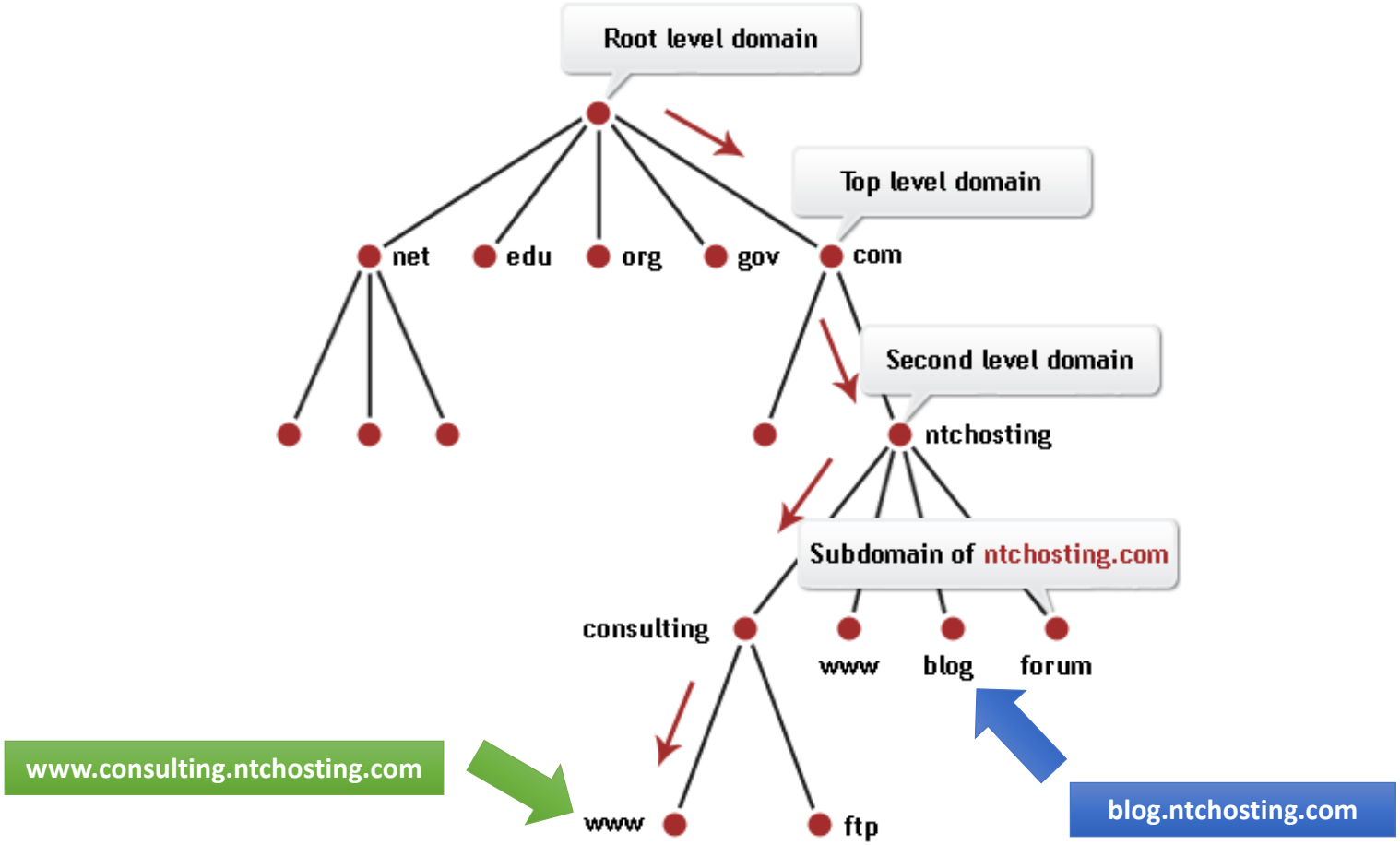


# DNS

Os servidores autoritativos são responsáveis pelas empresas ou organizações que representam. O servidor DNS responsável por este ponto é o *authoritative server*. Este servidor possui todas as entradas para os servidores e demais *hosts* dentro da organização.



# DNS – exemplo


Root level domain
Top level domain
net
edu
org
gov
com
Second level domain
ntchosting
Subdomain of ntchosting.com
consulting
www
blog
forum
www
ftp
www.consulting.ntchosting.com
blog.ntchosting.com

# DNS – Root servers

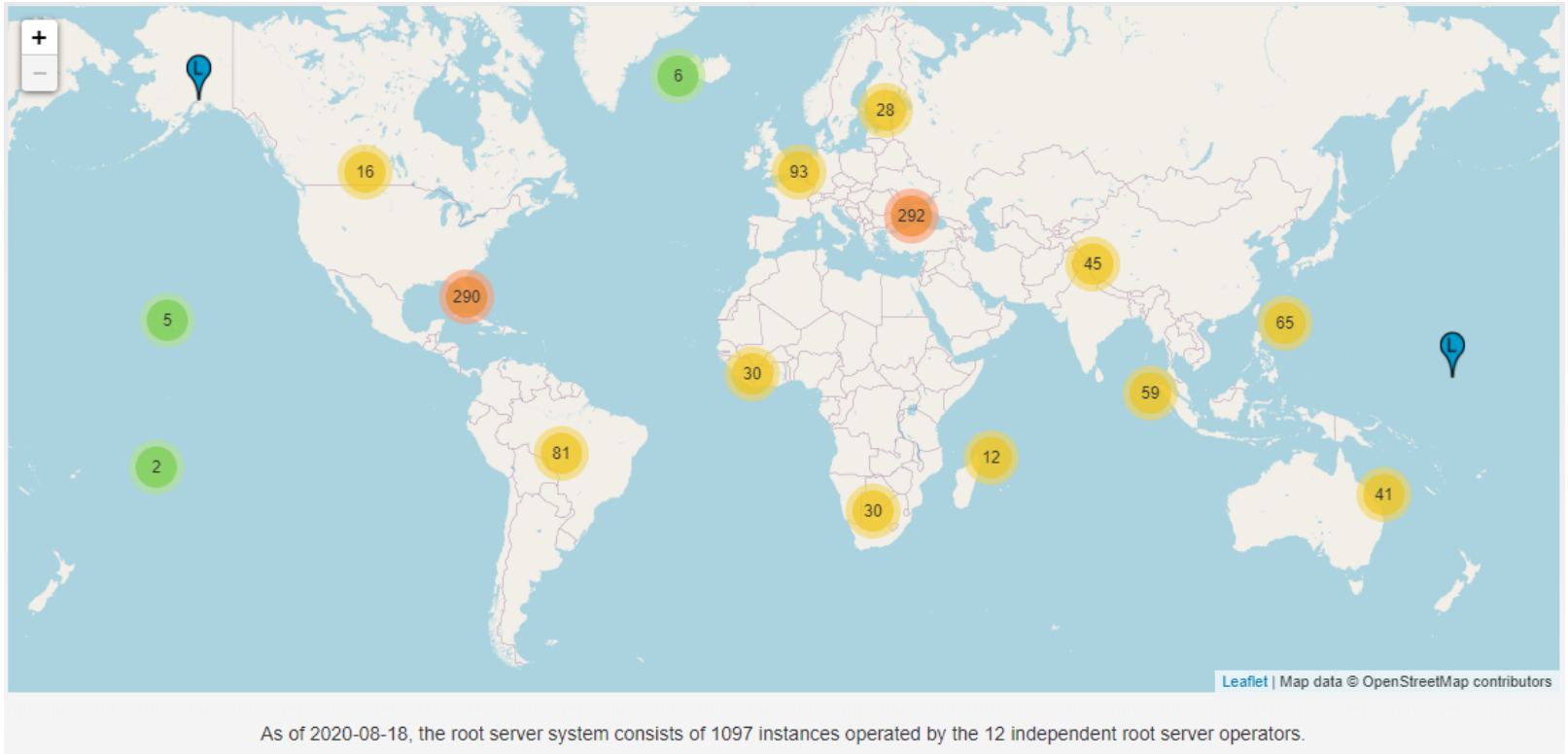
Os *root servers* são servidores DNS que possuem informações sobre os servidores *top-level domain* e são os primeiros a serem consultados. Ao todo são treze.

| NOME | IP | OPERADOR |
|---|---|---|
| a.root-servers.net | 198.41.0.4 | Verisign, Inc. |
| b.root-servers.net | 199.9.14.201 | USC-ISI |
| c.root-servers.net | 192.33.4.12 | Cogent Communications |
| d.root-servers.net | 199.7.91.13 | University of Maryland |
| e.root-servers.net | 192.203.230.10 | NASA |
| f.root-servers.net | 192.5.5.241 | Internet Systems Consortium, Inc. |
| g.root-servers.net | 192.112.36.4 | US Department of Defense |
| h.root-servers.net | 198.97.190.53 | US Army Research Lab |
| i.root-servers.net | 192.36.148.17 | Netnod |
| j.root-servers.net | 192.58.128.30 | Verisign, Inc. |
| k.root-servers.net | 193.0.14.129 | RIPE NCC |
| l.root-servers.net | 199.7.83.42 | ICANN |
| m.root-servers.net | 202.12.27.33 | WIDE Project |

Fonte: www.iana.org/domains/root/servers

# DNS – Root servers

Os *root servers* são formados por 1097 instâncias mantidas por doze operadores diferentes, distribuídas geograficamente conforme o mapa.

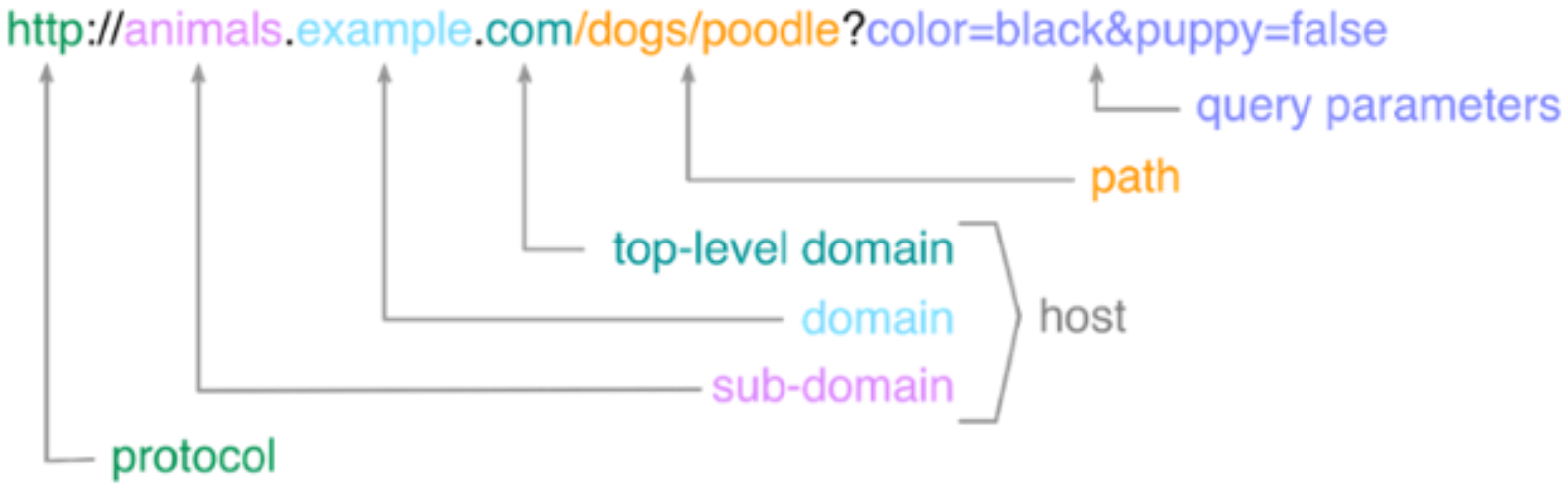



Fonte: root-servers.org

# DNS – Top-level domain

Um Top-level domain (TLD) é um dos domínios no nível mais alto da hierarquia de nomes de domínio da Internet. Os top-level domain são instalados a partir dos root server.

Para todos os domínios em níveis inferiores, é a última parte do nome do domínio, ou seja, o último rótulo de um nome de domínio totalmente qualificado, também conhecido como FQDN (Fully Qualified Domain Name).




Fonte: wikipedia.org

# DNS – Authoritative server

Um Authoritative server é um servidor que fornece respostas a perguntas sobre nomes em uma zona. Um authoritative server somente retorna respostas para consultas sobre nomes de domínio que foram especificamente configurados pelo administrador. Os servidores de nomes também podem ser configurados para fornecer respostas autoritativas a consultas em algumas zonas, enquanto atuam como um servidor de nomes em cache para todas as outras zonas.

Um authoritative server pode ser do tipo principal ou primário ou um servidor secundário. Um servidor primário para uma zona é o servidor que armazena as versões definitivas de todos os registros nessa zona.

Um authoritative server primário é identificado pelo registro SOA (Start of Authority). Um servidor secundário para uma zona usa um mecanismo de atualização automática para manter uma cópia idêntica do banco de dados do servidor primário para uma zona.

Fonte: wikipedia.org

# DNS – Authoritative server
# Start of authority

Um registro SOA (Start of Authority) é um tipo de registro de recurso no Sistema de Nomes de Domínio (DNS) que contém informações administrativas sobre a zona, especialmente no que se refere a transferências de zona.

O formato de registro SOA é especificado no RFC 1035.


Fonte: wikipedia.org

# DNS – Authoritative server
# Start of authority

**IN:** Tipo de zona a que se refere o SOA. Geralmente usa-se IN para Internet;

**SOA:** Abreviação de Start of Authority;

**MNAME:** Nome do servidor principal da zona. Neste exemplo, master.example.com;

**RNAME:** E-mail do administrador responsável pela zona. Neste exemplo, hostmaster@example.com. Note que o símbolo “@” foi trocado por “.”;

**SERIAL:** Número de série para esta zona. Se um servidor de nomes secundário perceber que este número aumentou, ele irá assumir que os dados foram atualizados e iniciará uma transferência de zona;

Fonte: wikipedia.org

# DNS – Authoritative server
# Start of authority

**REFRESH:** Número de segundos após o qual os servidores de nomes secundários devem consultar o mestre para detectar alterações de zona;

**RETRY:** Número de segundos após o qual os servidores de nomes secundários devem tentar novamente contatar o servidor primário, caso o mesmo não responda. Este valor tem de ser menor que REFRESH;

**EXPIRE:** Número de segundos após o qual os servidores de nome secundários devem parar de responder à solicitação para esta zona se o mestre não responder. Este valor deve ser maior que a soma de REFRESH e RETRY;

**TTL:** Tempo de vida para fins de armazenamento em cache negativo. Originalmente, esse campo tinha o significado de um valor TTL mínimo para registros de recursos nessa zona; foi alterado para o seu significado atual pelo RFC 2308.

Fonte: wikipedia.org

# DNS – Authoritative server
# Registros de recurso

Registros de recursos DNS ou “resource records” ou simplesmente “RRs” são o conteúdo do arquivo de zona DNS. O arquivo de zona contém mapeamentos entre nomes de domínio e endereços IP na forma de registros de texto.

Existem muitos tipos de registros de recursos*. Os mais comuns são:

- SOA – start of authority;
- TXT – text;
- NS – name server;
- A – address;
- PTR – pointer;
- CNAME – canonical name;
- MX – mail exchange;
- SRV – server.

*Uma lista completa pode ser consultada em en.wikipedia.org/wiki/List_of_DNS_record_types

# DNS – Authoritative server
# Registros de recurso

**SOA:** Cada arquivo de zona terá um registro SOA e ele estará presente no início. Esse tipo de registro contém informações sobre a própria zona e sobre outros registros. Cada zona terá apenas um registro SOA.

```
IN   SOA      nameserver.place.dom.  postmaster.place.dom.
```

**TXT:** Este registro serve para adicionar comentários ou informações adicionais.

```
example.com   IN  TXT   "This domain name is an example"
```

Fonte: interserver.net

# DNS – Authoritative server
# Registros de recurso

**NS:** Este registro serve para mostrar quais são os servidores autoritativos da zona. Eles indicam servidores primários e secundários para a zona especificada no registro SOA. As zonas podem conter muitos registros NS, mas devem conter pelo menos um registro NS para uma zona DNS.

Por exemplo, quando o administrador do domínio abc.com delega autoridade para que noamdc1.noam.abc.com. administre o subdomínio noam.abc.com., a seguinte linha deve ser adicionada à zona abc.com e noam.abc.com:

```
noam.abc.com. IN NS noamdc1.noam.abc.com.
```

Ou seja, o servidor “noamdc1.noam.abc.com” passa a ser autoritativo para o domínio “noam.abc.com”.

Fonte: interserver.net

# DNS – Authoritative server
# Registros de recurso

**A:** Este registro mapeia um nome de domínio para um endereço IP. No exemplo abaixo, o seguinte registro de recurso, localizado na zona abc.com, mapeia o FQDN do servidor para seu endereço IP:

```
abc.com IN A 172.16.48.1
```

Para mapear o FQDN de endereços IPv6, usa-se o registro AAAA ao invés de A.

**PTR:** Este registro é um ponteiro que funciona como um reverso ao registro A. Ele mapeia um nome de domínio para um endereço IP de modo a se obter o DNS reverso, como no exemplo abaixo:

```
1.48.16.172.in-addr.arpa. IN PTR abc.com.
```

Fonte: interserver.net

# DNS – Authoritative server
# Registros de recurso

**CNAME:** Este registro serve para criar um alias para o nome do domínio. Um exemplo do registro CNAME é dado abaixo.

```
ftp.abc.com. IN CNAME ftp1.abc.com.
```

Depois que um cliente DNS consulta o registro de recurso para ftp.abc.com, o servidor DNS localiza o registro de recurso CNAME. Em seguida, ele resolve a consulta do registro de recurso A para ftp1.abc.com e retorna os registros de recurso A e CNAME para o cliente.

Fonte: interserver.net

# DNS – Authoritative server
# Registros de recurso

**MX:** Esse registro representa o servidor responsável por processar ou encaminhar mensagens de correio eletrônico em um domínio DNS.

Processar uma mensagem significa entregá-la ao destinatário ou passá-lo para um tipo diferente de transporte de correio. Encaminhar uma mensagem significa enviá-lo para seu servidor de destino final, ou seja, ele será o SMTP (Simple Mail Transfer Protocol) para outro servidor de troca de mensagens que esteja mais próximo do destino final ou o enfileire por um período de tempo especificado.

Somente servidores de troca de mensagens usam registros MX. O exemplo a seguir mostra registros de recursos MX para os servidores de e-mail para o domínio noam.abc.com.:

```
*. noam.abc.com. IN MX 0 mailserver1.noam.abc.com.
*. noam.abc.com. IN MX 10 mailserver2.noam.abc.com.
*. noam.abc.com. IN MX 10 mailserver3.noam.abc.com.
```

O número após IN MX indica a prioridade do servidor de mensagens.

Fonte: interserver.net

# DNS – Authoritative server
# Registros de recurso

**SRV:** Esse registro permite que sejam especificados servidores para os quais devem ser direcionados o tráfego de serviços específicos.

Abaixo segue o formato deste registro:

```
_serv._prot.example.com SRV 10 0 5060 serv.example.com
```

Onde:

- Service: o nome do serviço, que deve ser precedido de "_";
- Protocol: o nome do protocolo, que deve ser precedido de "_";
- Domain: o nome do domínio que receberá o tráfego original desse serviço;
- Priority: o primeiro número (10) indica a prioridade do servidor alvo;
- Weight: se dois registros tiverem a mesma prioridade, o peso (0) será usado;
- Port: a porta TCP ou UDP que será usada pelo serviço (5060);
- Target: o domínio ou subdomínio alvo, que deve ter um registro A ou AAAA para resolver para o endereço IP.

Fonte: interserver.net

# DNS – Authoritative server
# Registros de recurso

Exemplo de uso do registro SRV:

```
_ldap._tcp.example.com. IN SRV 10 50 389 ds1.example.com.
```

Onde:

- Service: LDAP;
- Protocol: TCP;
- Domain: example.com;
- Priority: 10;
- Weight: 50;
- Port: 389 (TCP);
- Target: ds1.example.com.

Fonte: interserver.net

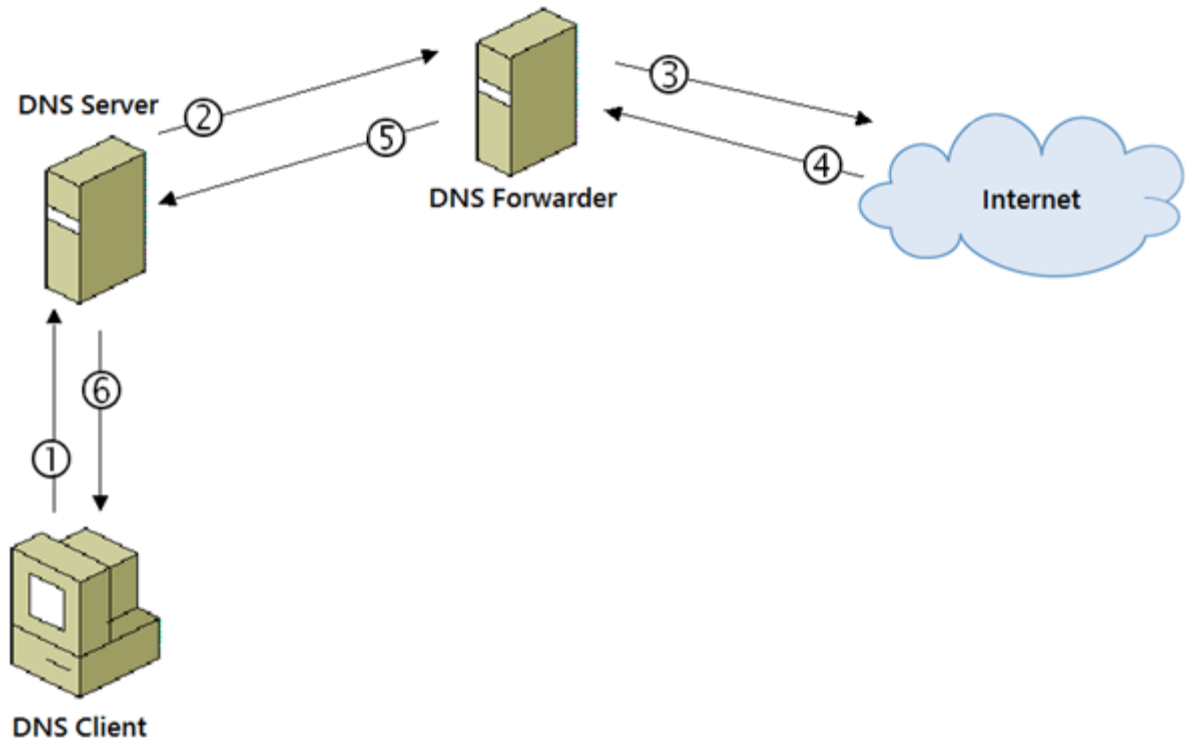
# DNS – Authoritative server Exemplo

```
$ORIGIN example.com.     ; start of the zone file
$TTL 30m                 ; default cache expiration time for resource records
example.com. IN SOA ns.example.com. root.example.com. (
1999120701               ; serial number of this zone file
1d                       ; frequency to refresh secondary DNS (d=day)
1d                       ; frequency to refresh secondary DNS in case of problem
4w                       ; secondary DNS expiration time (w=week)
1h                       ; minimum caching time if resolution failed
)
example.com. NS dns1.dnsprovider.com.    ; name server
example.com. NS dns2.dnsprovider.com.    ; another name server
example.com. MX 10 mx1.dnsprovider.com   ; mail server
example.com. MX 10 mx2.dnsprovider.com   ; another mail server
example.com. A 192.168.100.1             ; IP address for root domain
www          A 192.168.100.1             ; IP address for www subdomain
```

Fonte: ns1.com

# DNS - Forwarder

Um DNS forwarder ou encaminhador é um servidor DNS que encaminha consultas DNS para outros servidores e armazena localmente um cache de pesquisas já realizadas.



# Arquivo hosts

O arquivo *hosts.txt* é um arquivo texto que nos primórdios da Internet era mantido manualmente e disponibilizado via compartilhamento de arquivos pelo Stanford Research Institute para a associação ARPANET, contendo os nomes de host e seus endereços.

Nos sistemas operacionais modernos, este arquivo permanece como um mecanismo de resolução de nome alternativo.

No GNU/Linux, este arquivo se encontra em:

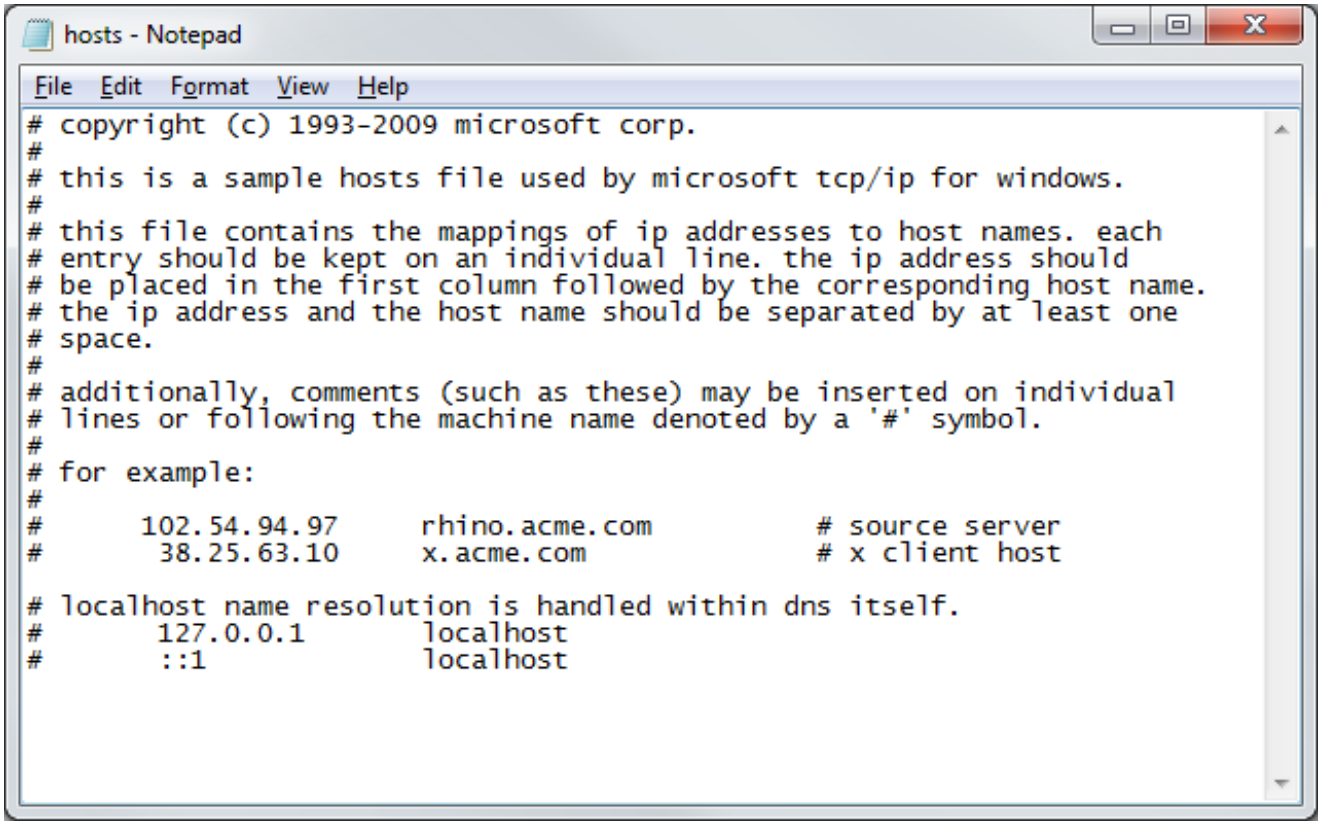
**\etc\hosts**

No Windows, este arquivo se encontra em:

**c:\windows\system32\drivers\etc\hosts.txt**

# Arquivo hosts

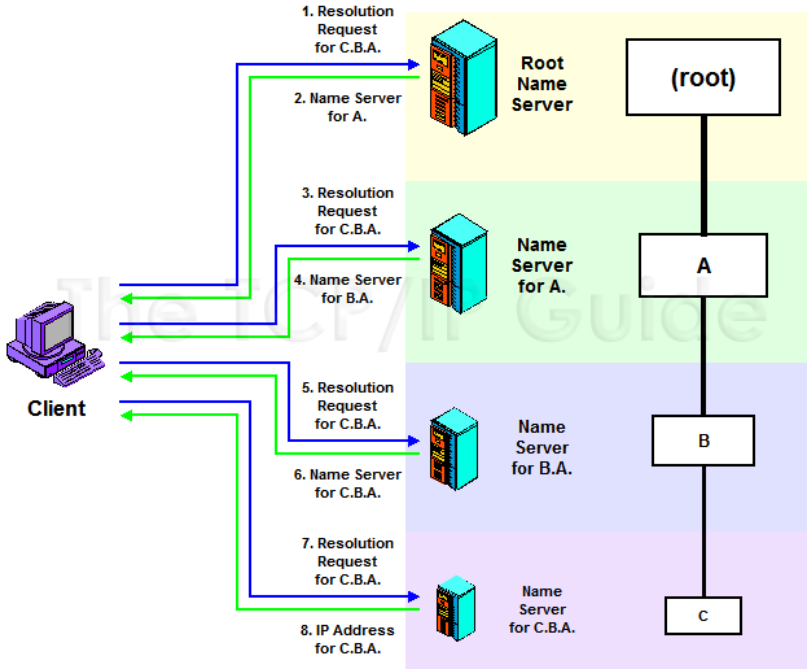
Arquivo *hosts.txt* no Windows:



# DNS – resolução de nomes
# Técnica iterativa

Quando um cliente envia uma solicitação iterativa para um servidor DNS, o servidor responde com a resposta à solicitação, ou seja, o endereço IP correspondente, ou então com o nome de outro servidor que tenha as informações.

O cliente original deve então iterar com o novo servidor, enviando uma nova solicitação para este possa responder ou fornecer outro nome de servidor.

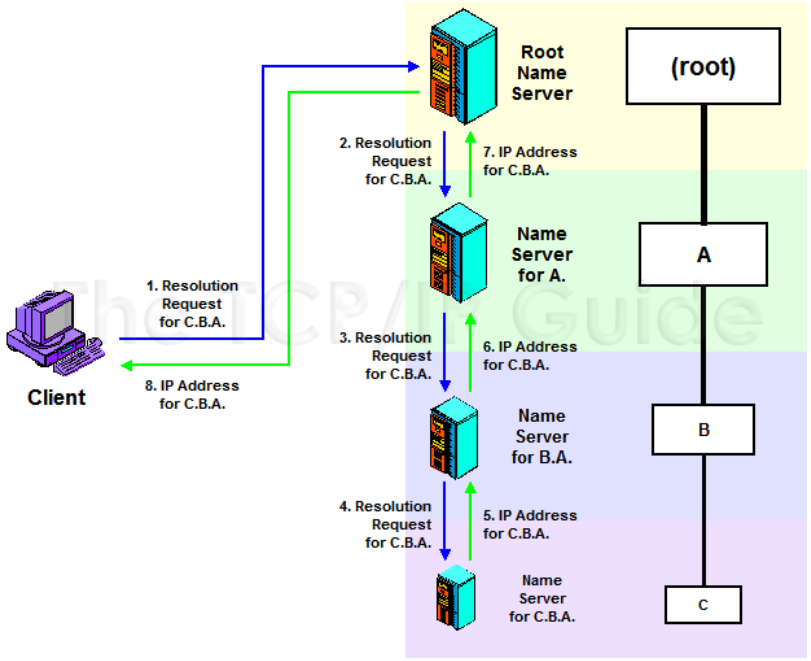



Fonte: tcpipguide.com

# DNS – resolução de nomes
# Técnica recursiva

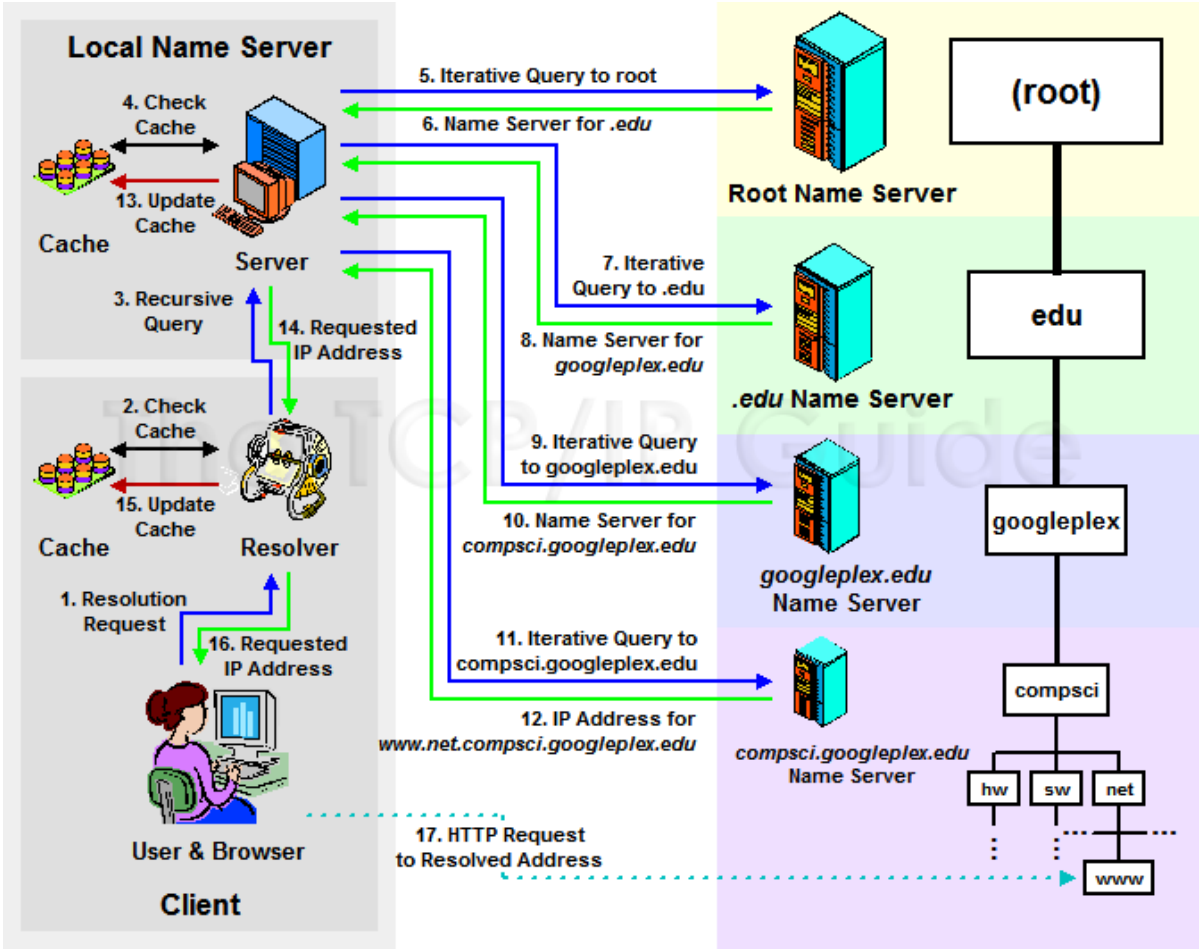
Quando um cliente envia uma solicitação recursiva para um servidor DNS, o servidor responde com a resposta se tiver a informação solicitada. Caso contrário, o servidor assumirá a responsabilidade de encontrar a resposta, tornando-se um cliente em nome do cliente original e enviando novas solicitações para outros servidores.

O cliente original envia apenas uma solicitação e, eventualmente, obtém as informações desejadas (ou uma mensagem de erro, se não estiver disponível).




Fonte: tcpipguide.com

# DNS – resolução de nomes
# Resumo



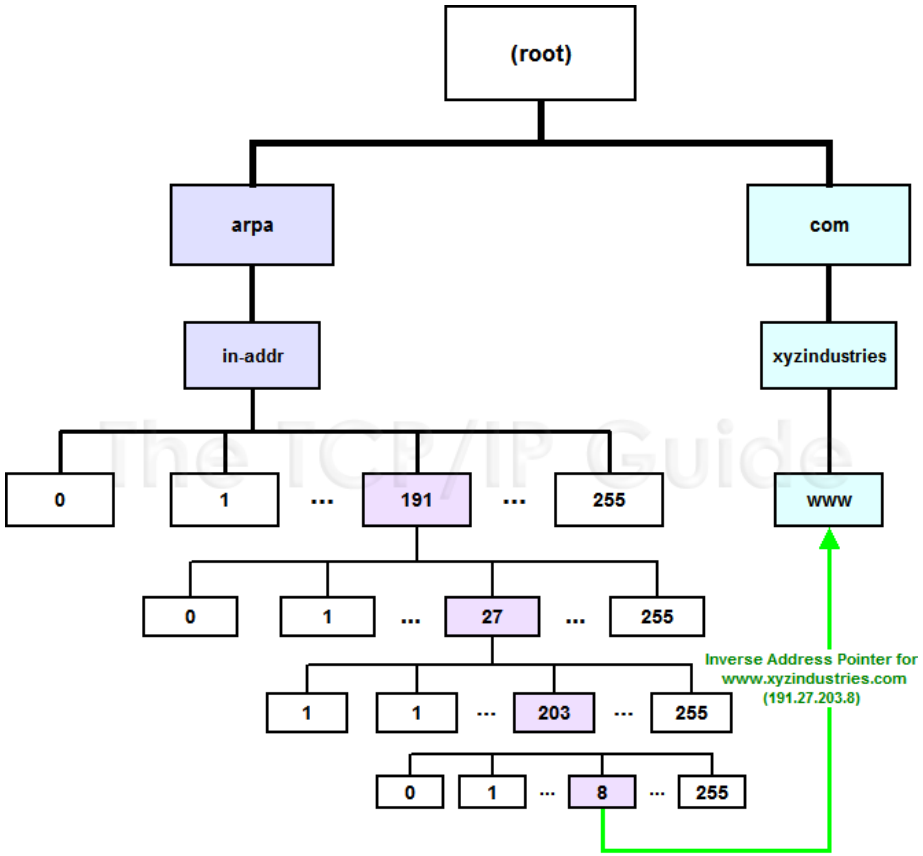

Fonte: tcpipguide.com

# DNS – resolução de nomes
# Pesquisa reversa

A hierarquia especial "IN-ADDR.ARPA" foi criada para permitir pesquisas reversas fáceis de nomes DNS.

"IN-ADDR.ARPA" contém 256 subdomínios numerados de 0 a 255, cada um dos quais tem 256 subdomínios numerados de 0 a 255 e assim por diante, abaixo de quatro níveis. Assim, cada endereço IP é representado na hierarquia.

No diagrama ao lado, o nome de domínio DNS “www.xyzindustries.com” tem um registro de recurso convencional apontando para seu endereço IP 191.27.203.8, bem como um registro de resolução reversa em 8.203.27.191.IN-ADDR.ARPA, apontando para o nome de domínio “www.xyzindustries.com”.




Fonte: tcpipguide.com

# DNS – Ferramentas

NSLOOKUP é uma ferramenta disponível em ambiente Linux e Windows que permite pesquisar informações sobre registros de DNS de um determinado servidor DNS.

# DNS – NSLOOKUP

Exemplo de pesquisa recursiva sem especificar o servidor DNS:

```
C:\>nslookup www.brasil.gov.br
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    www.brasil.gov.br
Address:  170.246.255.242
```

# DNS – NSLOOKUP

Exemplo de pesquisa recursiva especificando o servidor DNS:

```
C:\>nslookup www.brasil.gov.br dns.google
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    www.brasil.gov.br
Address:  170.246.255.242
```

# DNS – NSLOOKUP

Exemplo de pesquisa do registro SOA:

```
C:\>nslookup -type=soa www.brasil.gov.br dns.google
Server:  dns.google
Address:  8.8.4.4

brasil.gov.br
        primary name server = alpha.planalto.gov.br
        responsible mail addr = postmaster.planalto.gov.br
        serial  = 2020080810
        refresh = 300 (5 mins)
        retry   = 300 (5 mins)
        expire  = 604800 (7 days)
        default TTL = 300 (5 mins)
```

# DNS – NSLOOKUP

Exemplo de pesquisa recursiva especificando o servidor DNS autoritativo do domínio:

```
C:\>nslookup www.brasil.gov.br alpha.planalto.gov.br
Server:  alpha.planalto.gov.br
Address:  170.246.255.10

Name:    www.brasil.gov.br
Address:  170.246.255.242
```

# DNS – NSLOOKUP

Exemplo de pesquisa não recursiva para “br”:

```
C:\>nslookup -norecurse -type=ns br a.root-servers.net
(…)
Server:  UnKnown
Address:  198.41.0.4

br      nameserver = a.dns.br
br      nameserver = b.dns.br
(…)
a.dns.br        internet address = 200.219.148.10
b.dns.br        internet address = 200.189.41.10
(…)
```

# DNS – NSLOOKUP

Exemplo de pesquisa não recursiva para “gov.br”:

```
C:\>nslookup -norecurse -type=ns gov.br a.dns.br
Server:  a.dns.br
Address:  200.219.148.10

gov.br  nameserver = a.dns.br
gov.br  nameserver = b.dns.br
gov.br  nameserver = c.dns.br
gov.br  nameserver = d.dns.br
gov.br  nameserver = e.dns.br
gov.br  nameserver = f.dns.br
```

# DNS – NSLOOKUP

Exemplo de pesquisa não recursiva para “brasil.gov.br”:

```
C:\>nslookup -norecurse -type=ns brasil.gov.br a.dns.br
Server:  a.dns.br
Address:  200.219.148.10

brasil.gov.br   nameserver = alpha.planalto.gov.br
brasil.gov.br   nameserver = alpha2.planalto.gov.br
alpha.planalto.gov.br   internet address =
170.246.255.10
alpha2.planalto.gov.br  internet address =
170.246.255.11
```

# DNS – NSLOOKUP

Exemplo de pesquisa não recursiva para “www.brasil.gov.br”:

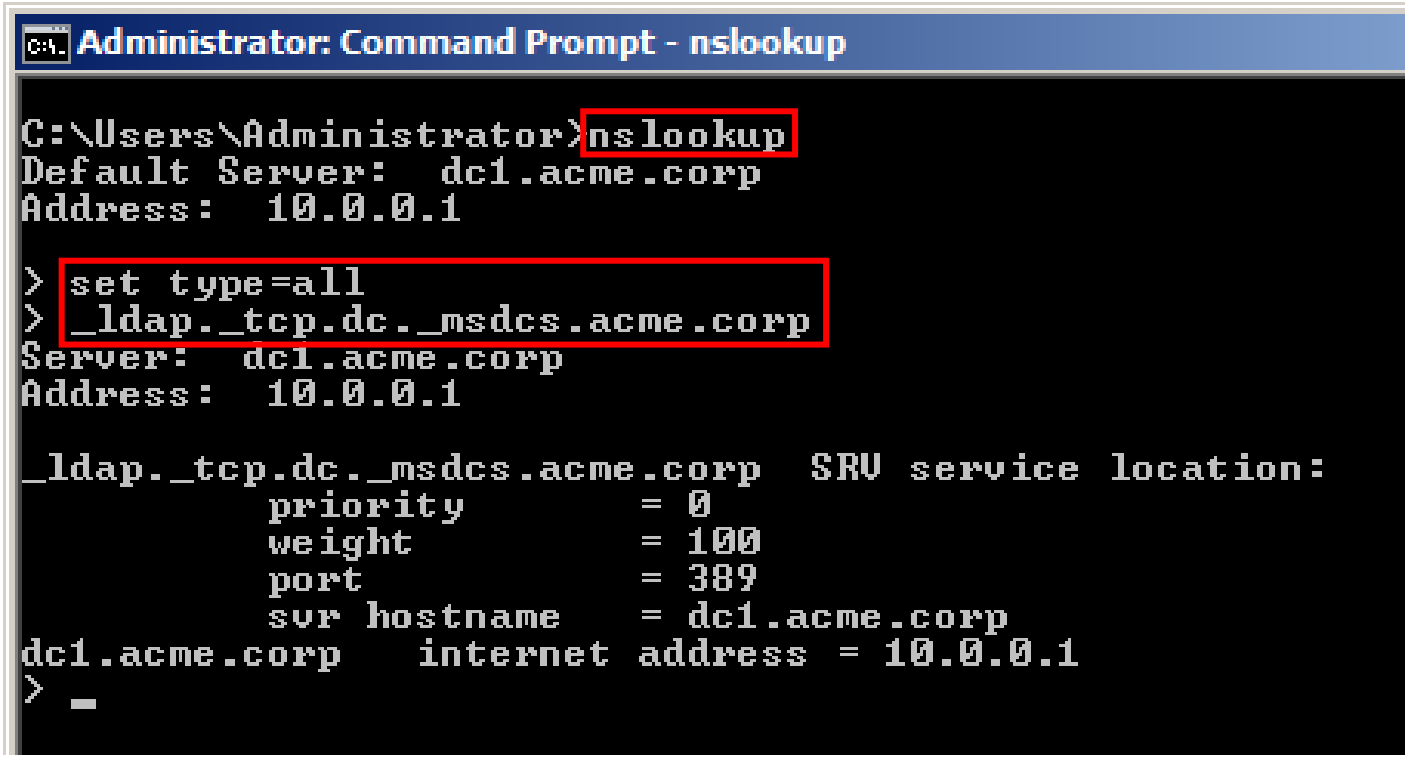
```
C:\>nslookup -norecurse -type=a www.brasil.gov.br
alpha.planalto.gov.br

Server:  alpha.planalto.gov.br
Address:  170.246.255.10

Name:    www.brasil.gov.br
Address:  170.246.255.242
```

# DNS – NSLOOKUP

Exemplo de pesquisa para o controlador de domínio que atende uma determinada rede, neste exemplo a rede ACME.CORP:



# Para saber mais...

… leia o material online sobre Domain Name System, de Júlio Battisti.

... leia a apostila Domain Name Service Configuração e Administração, de Rubens Queiroz de Almeida.

… veja a animação online do funcionamento do protocolo DNS, da RAD University.

… leia o tutorial DNS apresentado no 3º PTT Fórum, do registro.br.

… veja a lista de Top-Level Domains, da Internet Assigned Numbers Authority (IANA).

… veja a lista de Domínios de Segundo Nível do Brasil, do registro.br.

# Módulo 9

Serviço de diretório

# Introdução

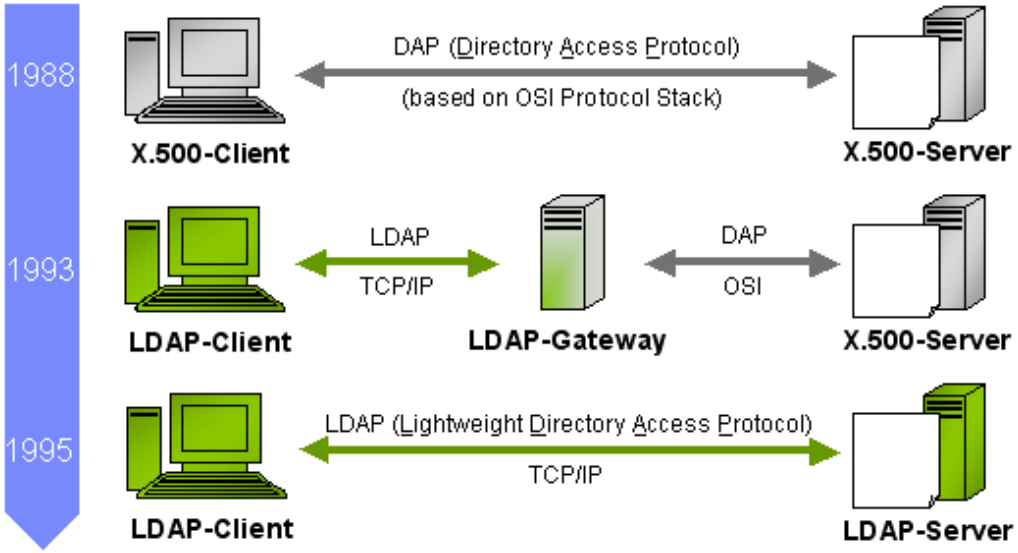
Serviço de diretório é um sistema que armazena e organiza informações sobre usuários, computadores e recursos compartilhados em uma rede de computadores.

Um serviço de diretório é útil para administrar e gerenciar usuários e recursos em uma rede de forma organizada e centralizada.

# LDAP

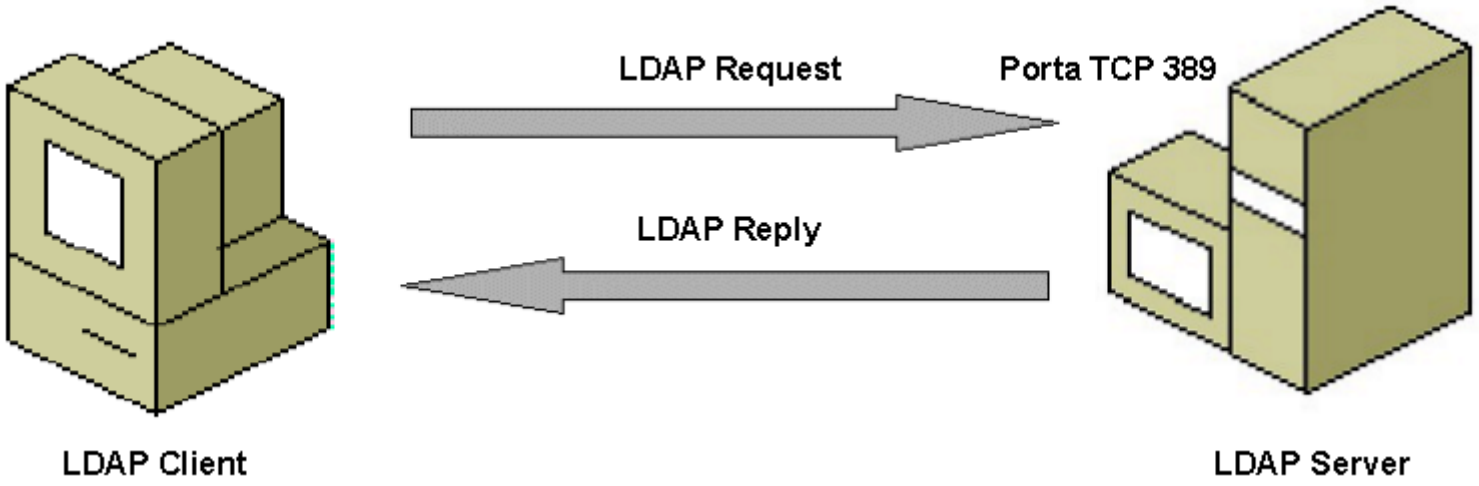
LDAP (Lightweight Directory Access Protocol) ou Protocolo Leve de Acesso à Diretórios tem a função de definir como as informações sobre usuários, computadores e recursos são armazenadas no banco de dados do repositório central do serviço de diretório.

O LDAP é um protocolo baseado no modelo cliente/servidor e foi desenvolvido como alternativa ao protocolo X.500, desenvolvido pela ITU-T e pela ISO.



# LDAP

O LDAP é um protocolo que segue o modelo cliente/servidor. O cliente LDAP conecta-se ao servidor LDAP por meio da porta TCP 389.



# LDAP

Dentre as diversas implementações do protocolo LDAP, podemos destacar o eDirectory da Novell, o OpenLDAP da comunidade GNU/Linux e o Active Directory da Microsoft.

Novell eDirectory™

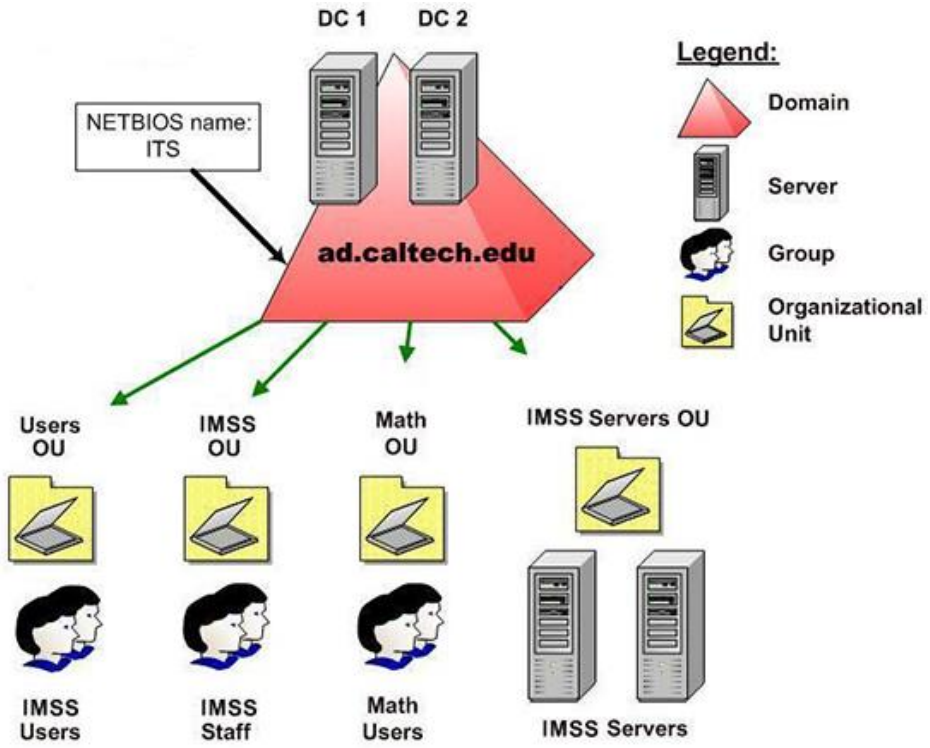

Windows Server®
Active Directory

# Active Directory

O Active Directory é a implementação da Microsoft para o serviço de diretório baseado no protocolo LDAP.

Também conhecido como AD, foi introduzido a partir do Windows Server 2000.

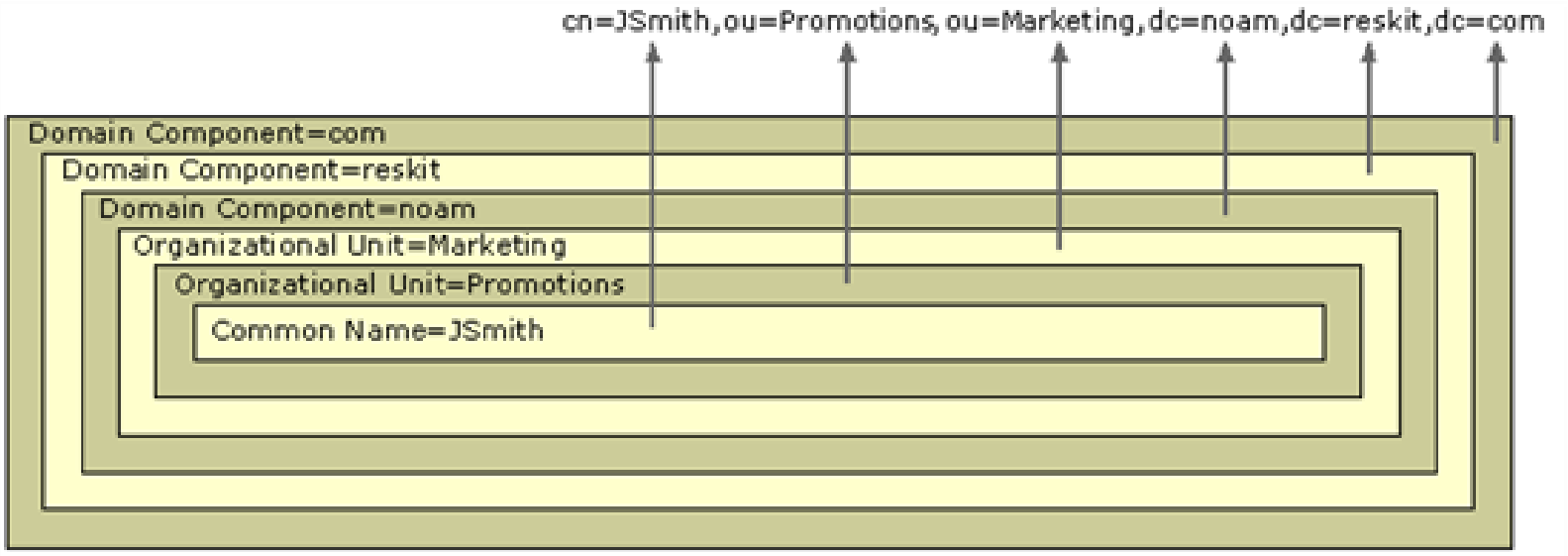
Na nomenclatura da Microsoft, uma unidade administrativa denomina-se Domínio, e é representada por um triângulo. Todo domínio deve ter, no mínimo, um controlador de domínio, também conhecido como DC, que é responsável por conter o banco de dados do serviço de diretório. Os demais servidores do domínio são conhecidos como servidores membros ou members servers.



# Active Directory – objetos

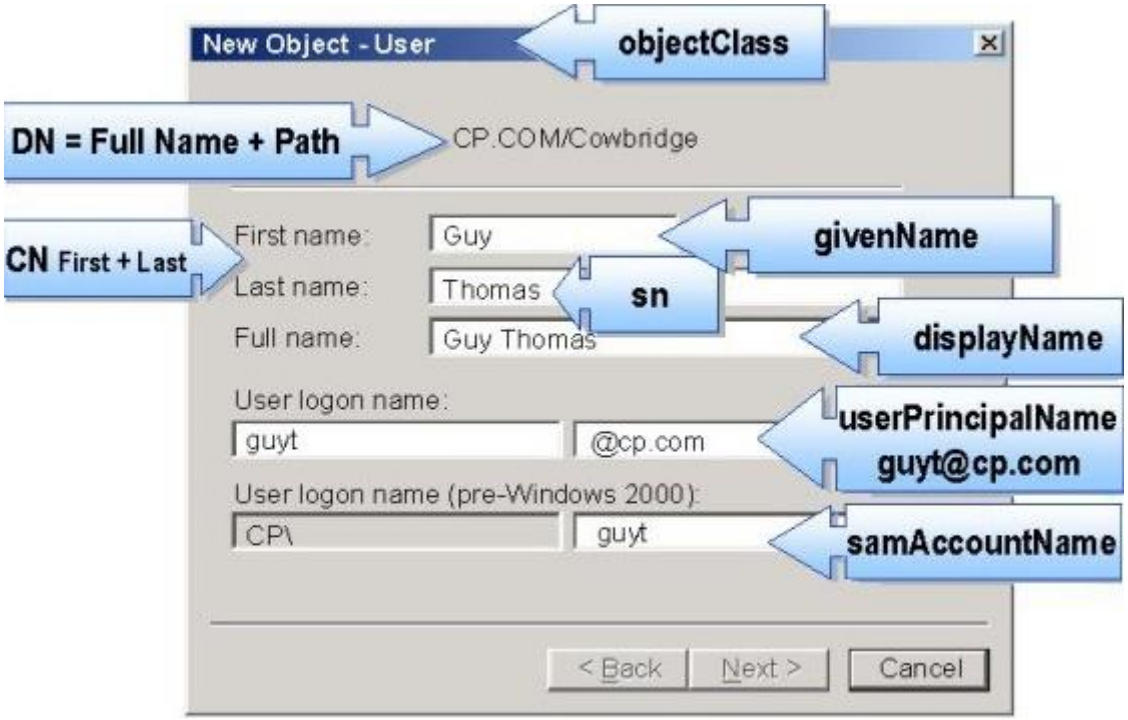
Todo objeto no Active Directory deve possuir um Distinguished Name (nome distinto), que deve ser único e exclusivo.

Isso é possível usando-se o caminho completo do objeto, incluindo o nome do objeto e todos os objetos pai para até a raiz do domínio. Desta forma o cliente LDAP consegue recuperar as informações do objeto do diretório.



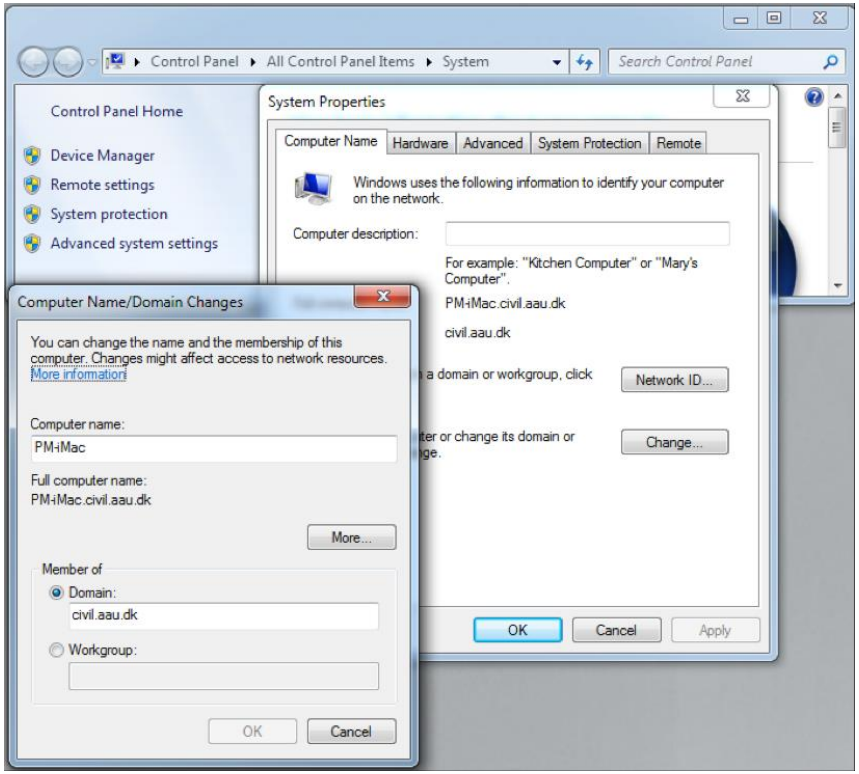
# Active Directory – atributos

Atributos são informações sobre um usuário, organização, grupo ou qualquer outro tipo de objeto. Cada atributo é associado a um tipo que fornece diversas propriedades sobre como os clientes e o servidor de diretórios devem interagir com esse atributo.



# Active Directory – logon

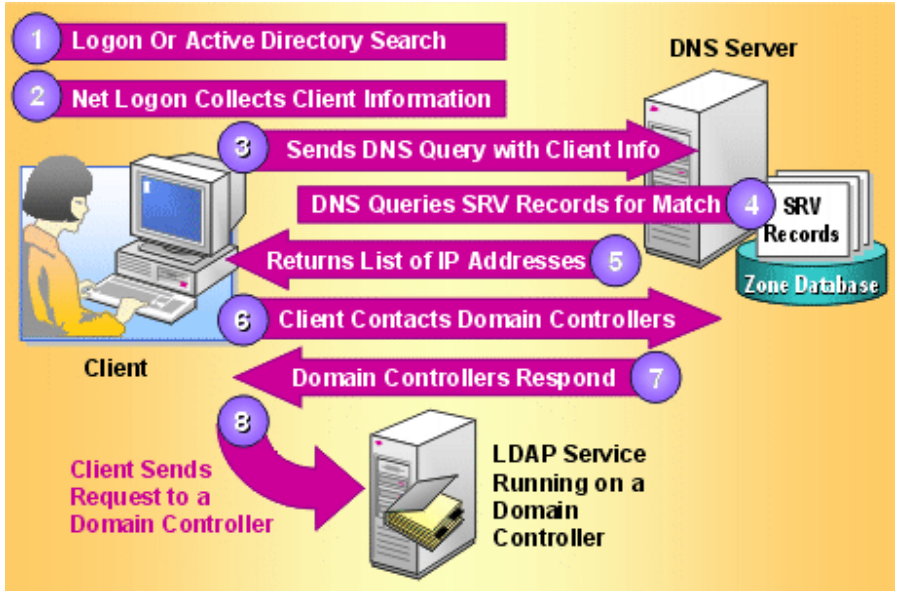
Para que os usuários possam conectar-se no domínio, as estações de trabalho devem estar registradas no domínio e os usuários devem possuir contas cadastradas no serviço de diretório.

# Active Directory – DNS

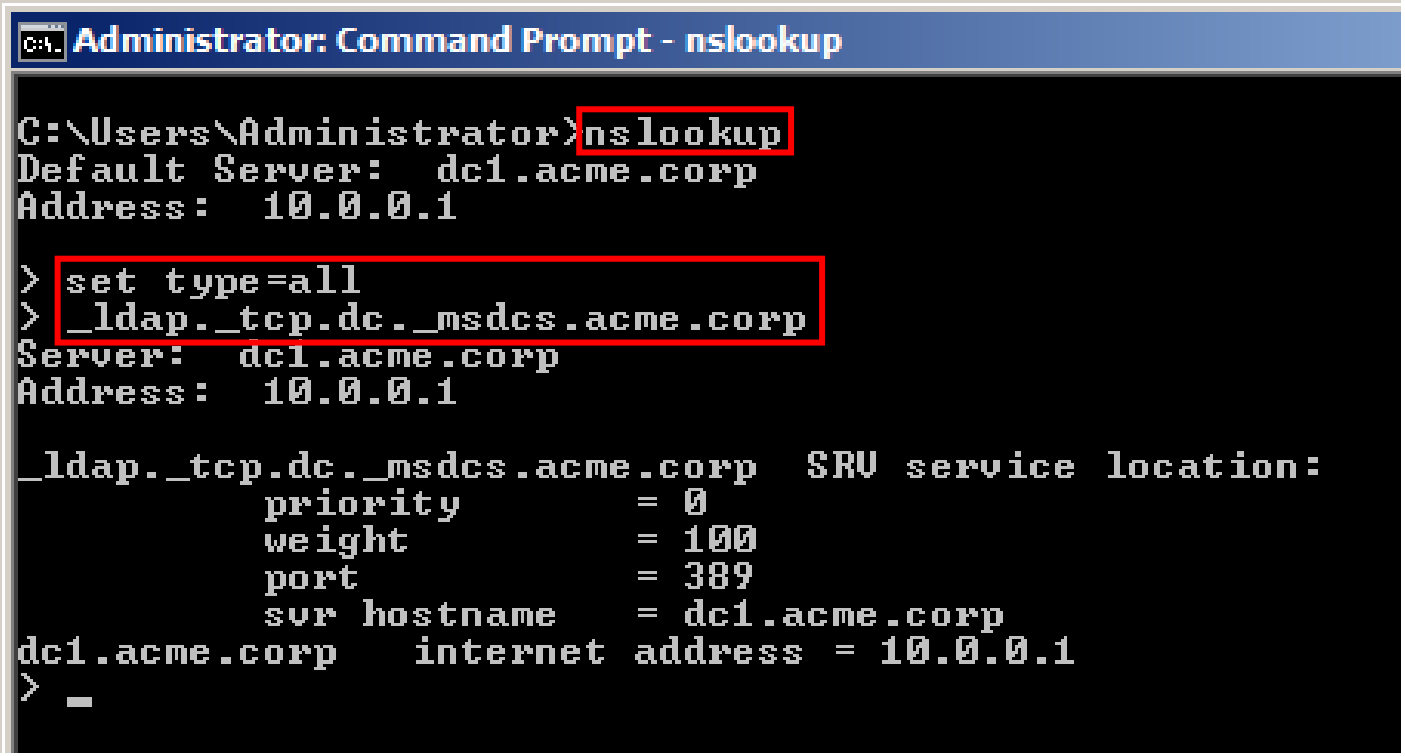
Para que a estação de trabalho possa encontrar o controlador de domínio da rede quando o usuário insere suas credencias, a estação faz uma consulta ao servidor DNS.

O Active Directory é dependente do serviço de DNS, pois sem ele a estação de trabalho não tem como encontrar o controlador de domínio responsável por autenticar aquele usuário.



# Active Directory – consulta DNS

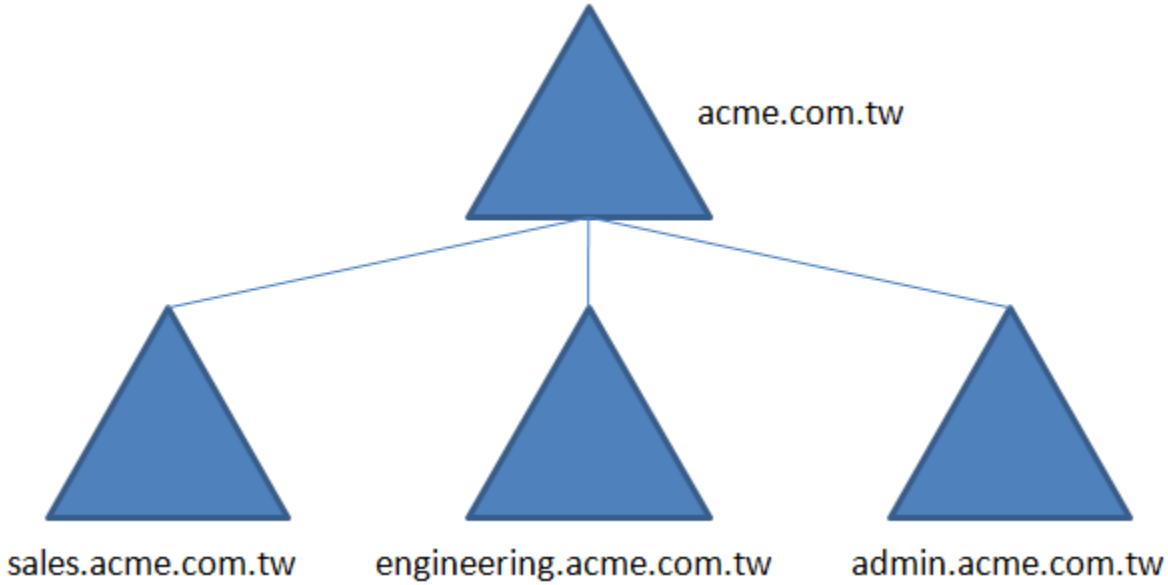
Para consultar o controlador de domínio que atende uma determinada rede, neste exemplo a rede ACME.CORP, pode-se usar o comando `nslookup`:



# Active Directory – árvore

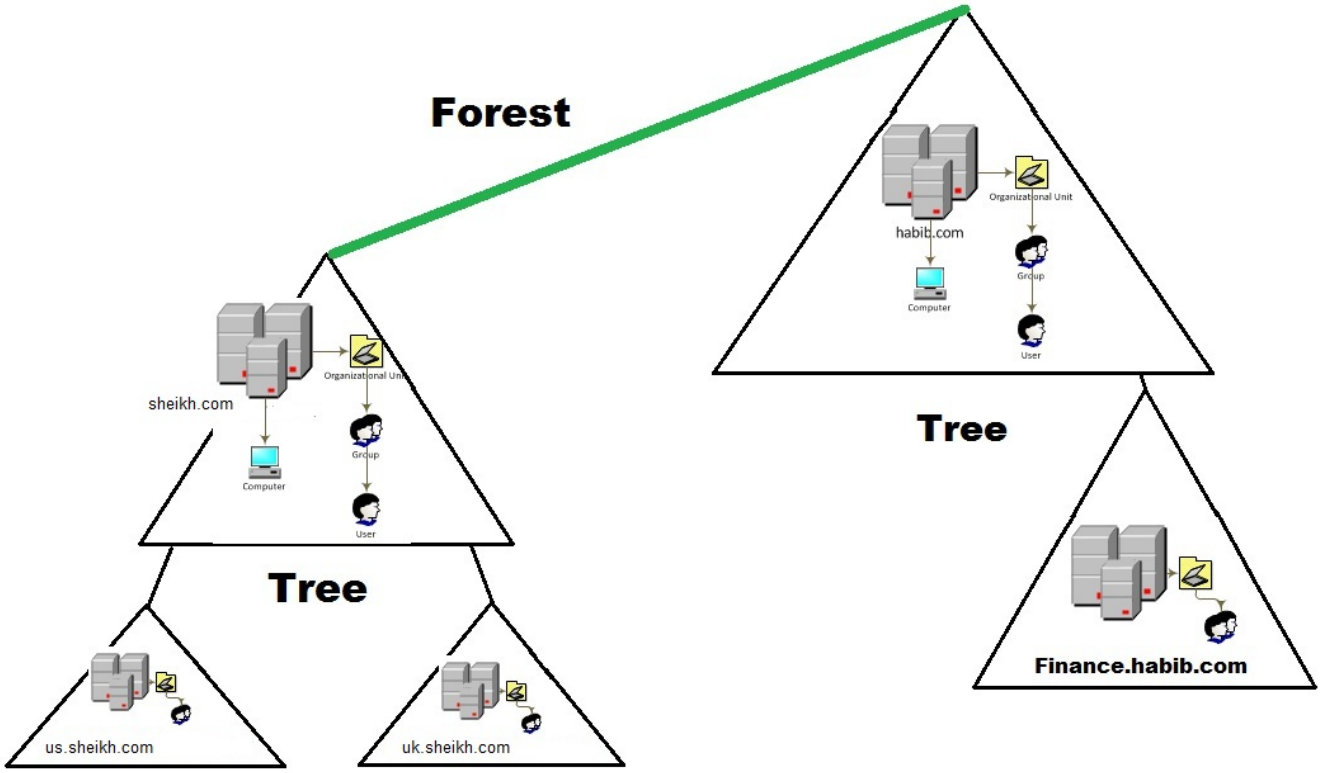
Várias unidades administrativas, ou domínios, podem ser combinados desde que compartilhem o mesmo espaço de nomes, de modo que tenhamos um domínio pai ou raiz e domínios filhos ou subdomínios. A este conjunto de domínios dá-se o nome de Árvore.

No exemplo abaixo, os domínios sales, engineering e admin são subdomínios do domínio raiz acme.com.tw.



# Active Directory – floresta

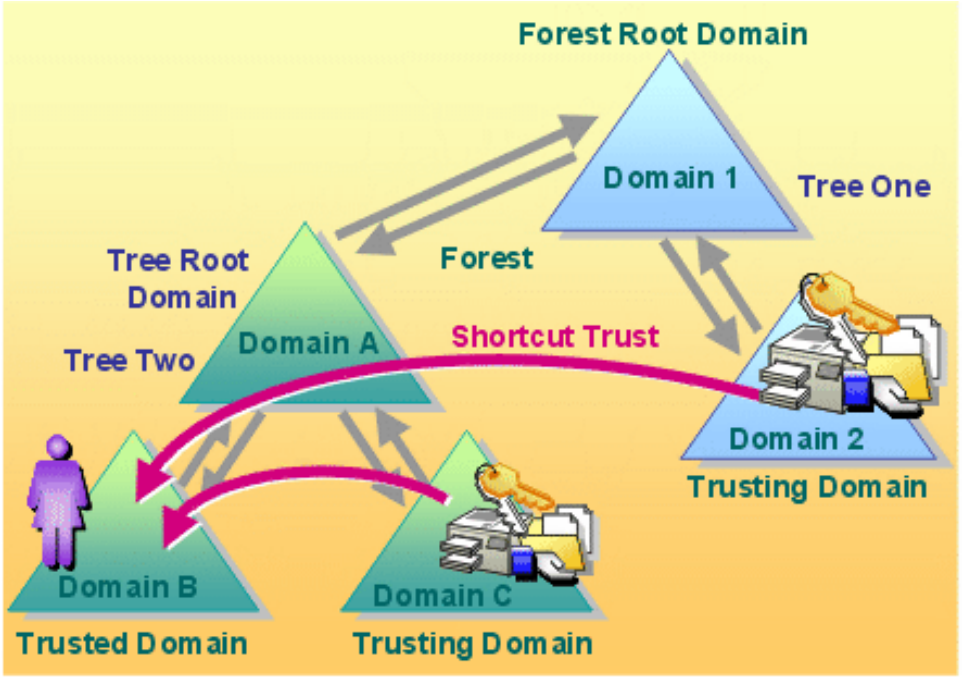
Unidades administrativas ou domínios, que não compartilham o mesmo espaço de nomes, também podem ser combinados. Neste caso teremos uma Floresta.



# Active Directory – trust

O trust ou relação de confiança é um canal de autenticação que permite que usuários de um domínio possam acessar recursos em outro domínio.

Pode ser do tipo direta, quando um domínio é subdomínio de outro; ou transitiva, quando dois domínios são subdomínios de uma mesma raiz.



# Para saber mais...

… leia o documento sobre Arquitetura do Active Directory, da Microsoft.

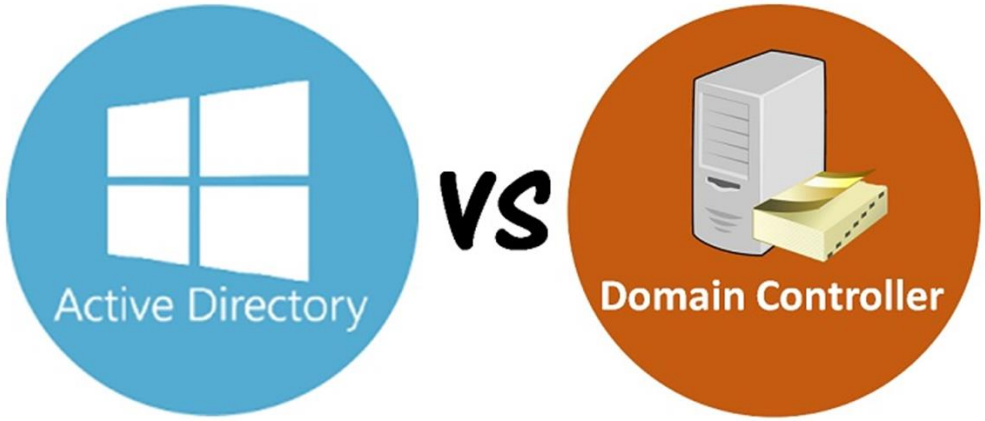
# Módulo 10

Controladores de domínio

# Controlador de Domínio vs Domínio

Um **Controlador de Domínio** é um servidor que responde às solicitações de autenticação e verifica os usuários em uma rede de computadores.

Já um **Domínio** é uma forma hierárquica de organizar usuários e computadores que trabalham juntos na mesma rede.




Em outras palavras, o Active Directory é um tipo de domínio e um controlador de domínio é um servidor com um papel importante nesse domínio, pois ele mantém todos os dados organizados e protegidos dentro desse domínio.

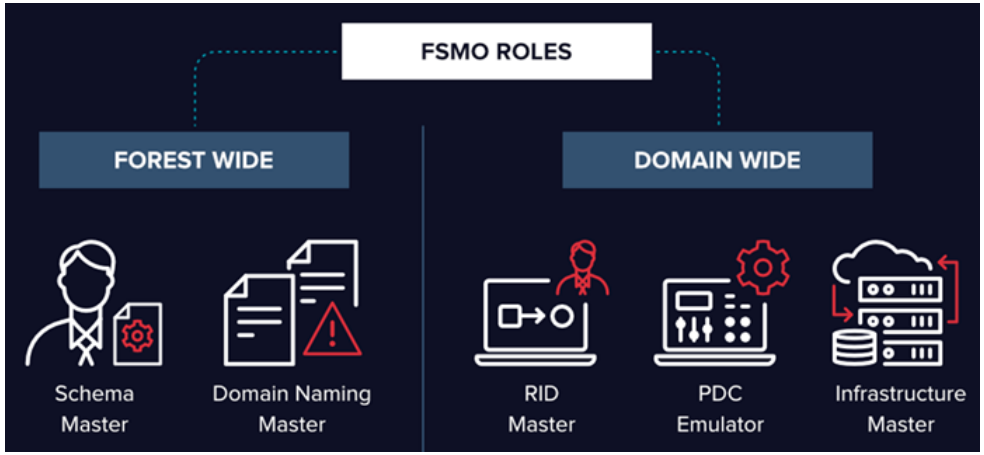
Fonte: varonis.com

# Papéis de um controlador de domínio

Os controladores de domínio que mantêm funções de mestre de operações são designados para executar tarefas específicas que tem o objetivo de garantir a consistência e eliminar registros conflitantes no banco de dados do Active Directory.

O Active Directory Domain Services (ADDS) define cinco papéis de mestre de operações, também conhecido como FSMO (Flexible Single-Master Operations):

- Schema Master;
- Domain Naming Master;
- Infrastructure Master;
- RID (Relative IDentification) Master;
- PDC (Primary Domain Controller) Emulator.




Fonte: windowstechno.com

# Papéis de um controlador de domínio

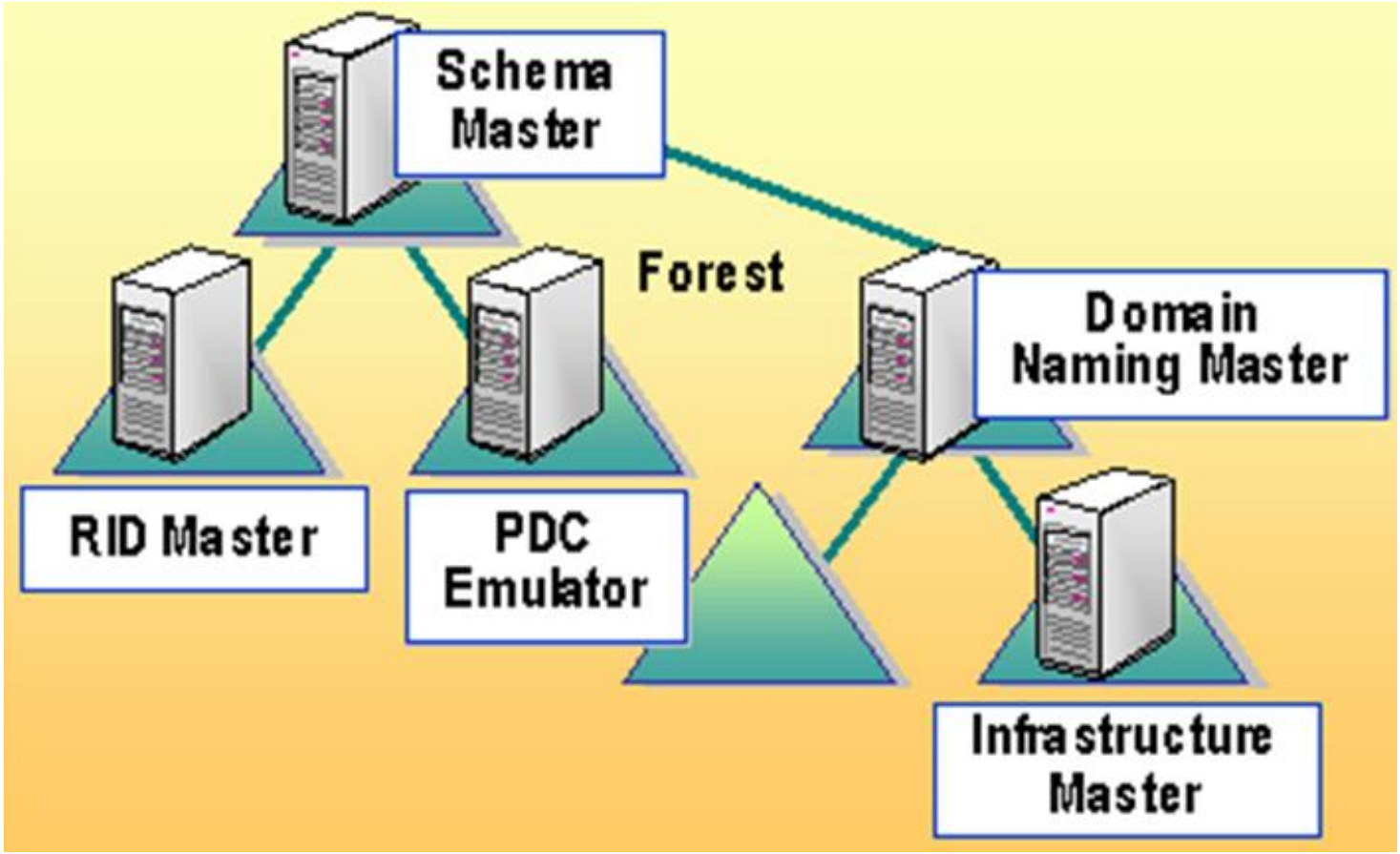
Os papéis FSMO podem ser aplicados a uma floresta ou a um domínio, e tem grupos de segurança específicos para que possam ser configurados.

A tabela abaixo mostra os papéis FSMO relacionados aos seus respectivos grupos de segurança e escopo de aplicação:

| Papel FSMO | Grupo de Segurança | Escopo |
|---|---|---|
| Schema Master | Schema Admins | Floresta |
| Domain Naming Master | Enterprise Admins | Floresta |
| Infrastructure Master | Domains Admins | Domínio |
| RID Master | Domains Admins | Domínio |
| PDC Master | Domains Admins | Domínio |

Fonte: windowstechno.com

# Papéis de um controlador de domínio




Fonte: windowstechno.com

# FSMO – Schema Master

O Schema Master controla todas as atualizações e modificações do esquema do Active Directory.

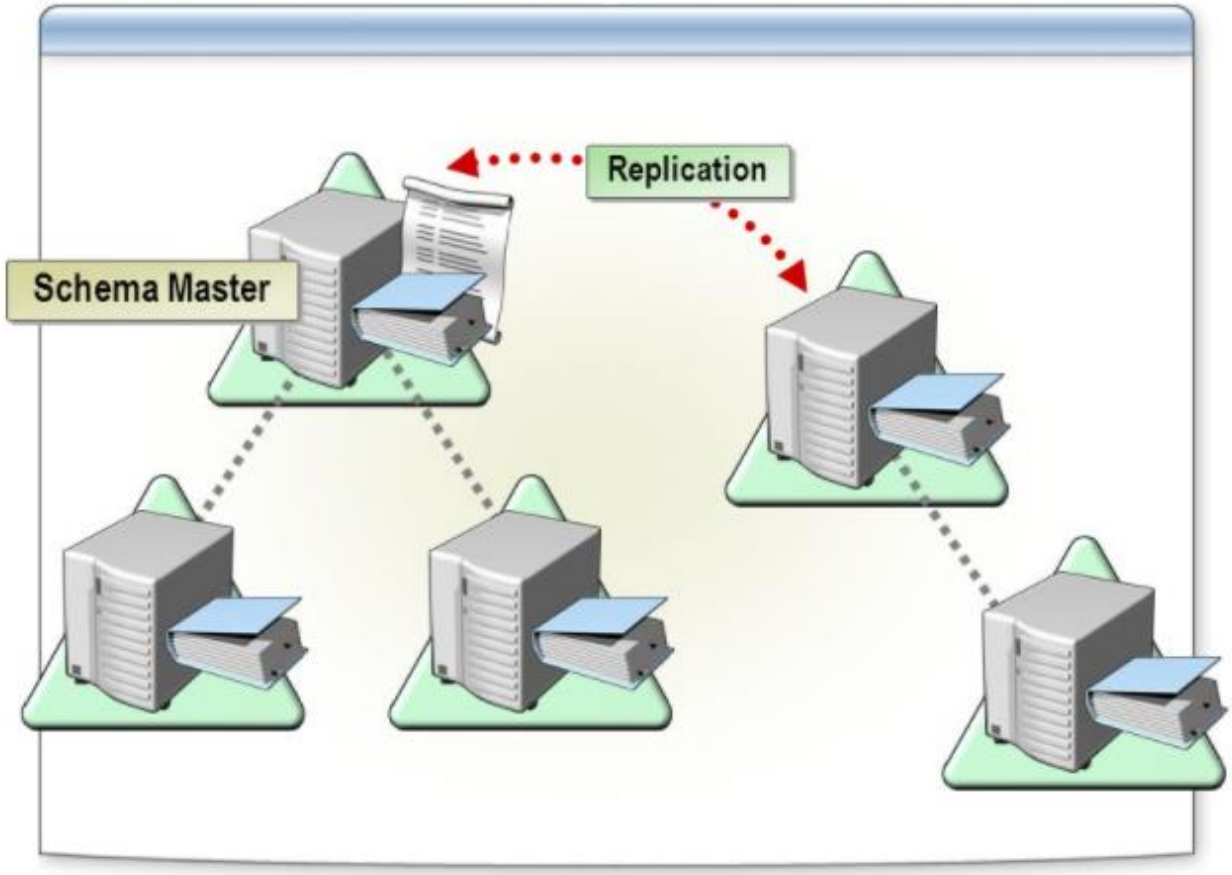
Depois que a atualização do esquema é concluída, ela é replicada do Schema Master para todos os outros controladores de domínio no domínio.

Para atualizar o esquema de uma floresta, deve-se ter acesso ao Schema Master.

Pode haver apenas um Schema Master em toda a floresta. Em caso de falha, este papel pode ser transferido para qualquer outro controlador de domínio na floresta.

Fonte: varoniz.com

# FSMO – Schema Master




Fonte: varoniz.com

# FSMO – Schema Master

**O que acontece quando o Schema Master não está disponível?**

Não há impacto direto sobre os usuários, pois eles não usam este recurso diretamente. No entanto, este papel é importante para que os administradores possam estender o esquema do Active Directory para oferecer suporte a outros produtos, como por exemplo o servidor de correio eletrônico Microsoft Exchange, entre outros.

Fonte: varoniz.com

# FSMO – Domain Naming Master

O Domain Naming Master controla a adição ou remoção de domínios na floresta.

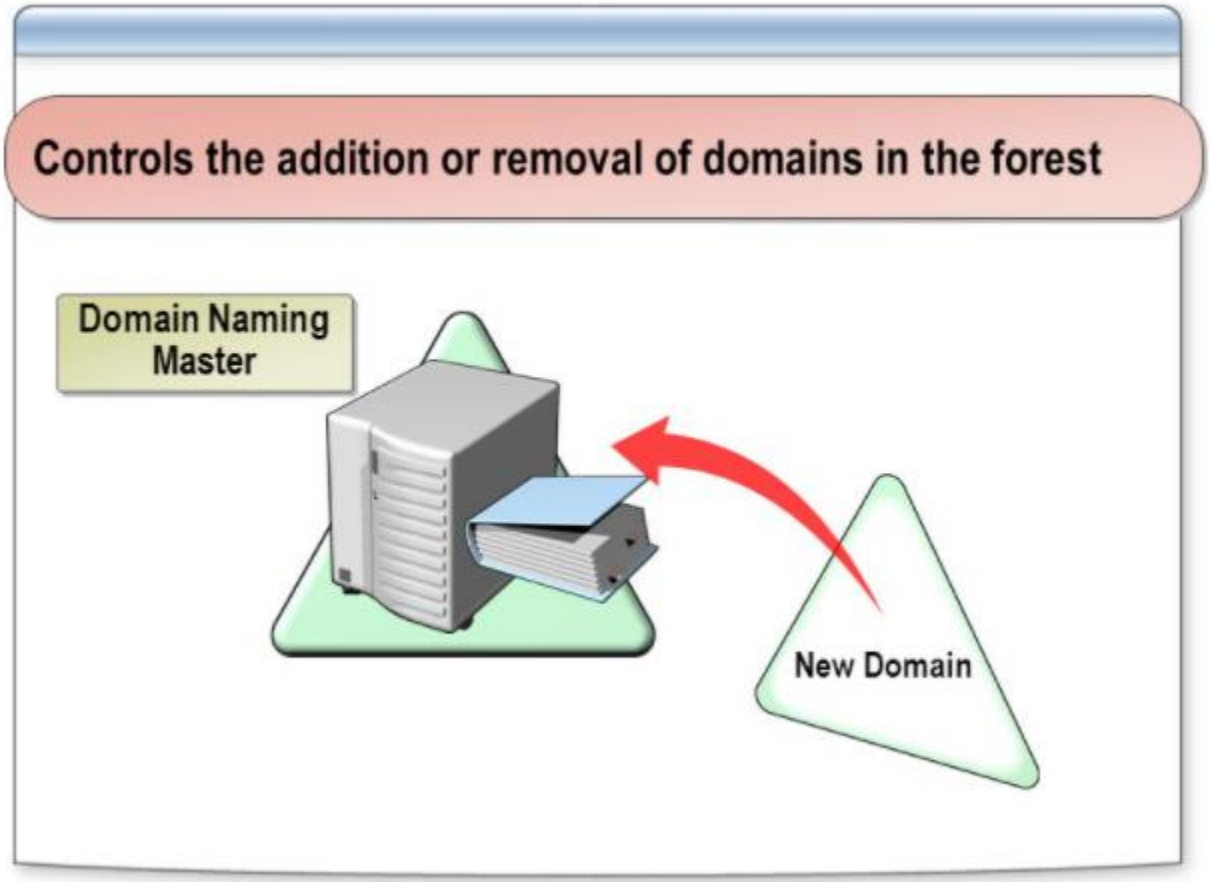
Este controlador de domínio é o único que pode adicionar ou remover um domínio no Active Directory.

Ele também pode adicionar ou remover referências cruzadas a domínios em diretórios externos.

Pode haver apenas um Domain Naming Master em toda a floresta. Em caso de falha, este papel pode ser transferido para qualquer outro controlador de domínio na floresta.

Fonte: varoniz.com

# FSMO – Domain Naming Master




Fonte: varoniz.com

# FSMO – Domain Naming Master

**O que acontece quando o Domain Naming Master não está disponível?**

O papel de Domain Naming Master só é necessário quando se adiciona ou se remove um domínio de uma floresta. Até que tais mudanças sejam necessárias para a infraestrutura do domínio, este papel pode permanecer desligado por um período indefinido de tempo. Transferir essa função para outro controlador de domínio é uma ação significativa. Depois que o papel de Domain Naming Master for transferido, o controlador de domínio que estava executando o papel não pode ser colocado online novamente.

Fonte: varoniz.com

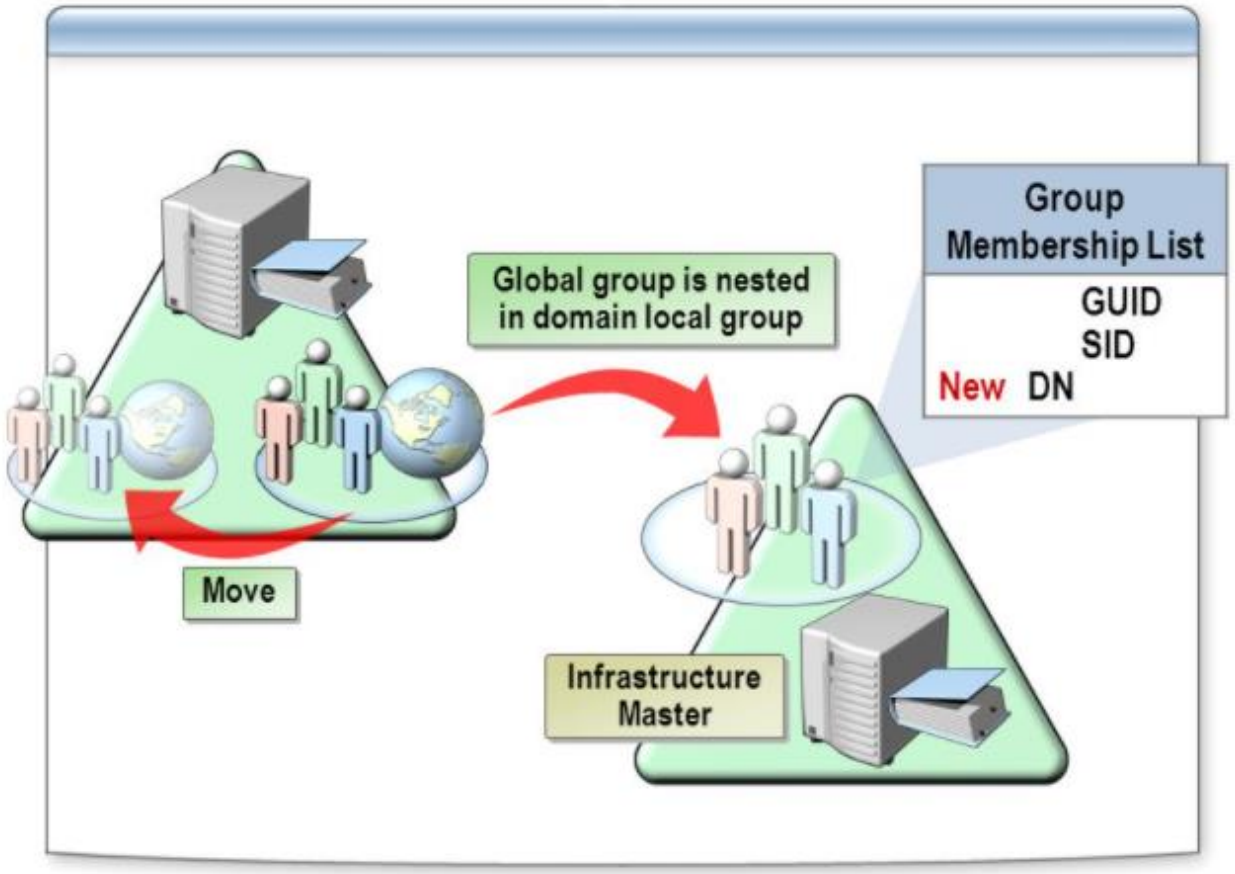
# FSMO – Infrastructure Master

Quando um objeto em um domínio é referenciado por outro objeto em outro domínio, ele representa a referência pelo GUID, o SID (para referências a entidades de segurança) e o DN do objeto que está sendo referenciado. O detentor da função FSMO de infraestrutura é o DC responsável por atualizar o SID e o nome distinto de um objeto em uma referência de objeto entre domínios. A qualquer momento, pode haver apenas um controlador de domínio atuando como mestre de infraestrutura em cada domínio.

Observação: a função de mestre de infraestrutura (IM) deve ser mantida por um controlador de domínio que não seja um servidor de catálogo global (GC). Se o mestre de infraestrutura for executado em um servidor de catálogo global, ele parará de atualizar as informações do objeto porque não contém nenhuma referência aos objetos que não contém. Isso ocorre porque um servidor de Catálogo Global mantém uma réplica parcial de cada objeto na floresta. Como resultado, as referências de objetos entre domínios nesse domínio não serão atualizadas e um aviso a esse respeito será registrado no log de eventos desse DC. Se todos os controladores de domínio em um domínio também hospedarem o catálogo global, todos os controladores de domínio terão os dados atuais e não será importante qual controlador de domínio terá a função de mestre de infraestrutura..

Fonte: varoniz.com

# FSMO – Infrastructure Master




Fonte: varoniz.com

# FSMO – Infrastructure Master

**O que acontece quando o Infrastructure Master não está disponível?**

Uma falha do mestre de infraestrutura será perceptível para os administradores, mas não para os usuários.

Como o mestre é responsável por atualizar os nomes dos membros do grupo de outros domínios, pode parecer que a associação ao grupo está incorreta, embora, conforme mencionado anteriormente nesta lição, a associação não seja realmente afetada. Você pode obter a função de mestre de infraestrutura para outro controlador de domínio e, em seguida, transferi-la de volta para o detentor da função anterior quando esse sistema ficar online.

Fonte: varoniz.com

# FSMO – RID Master

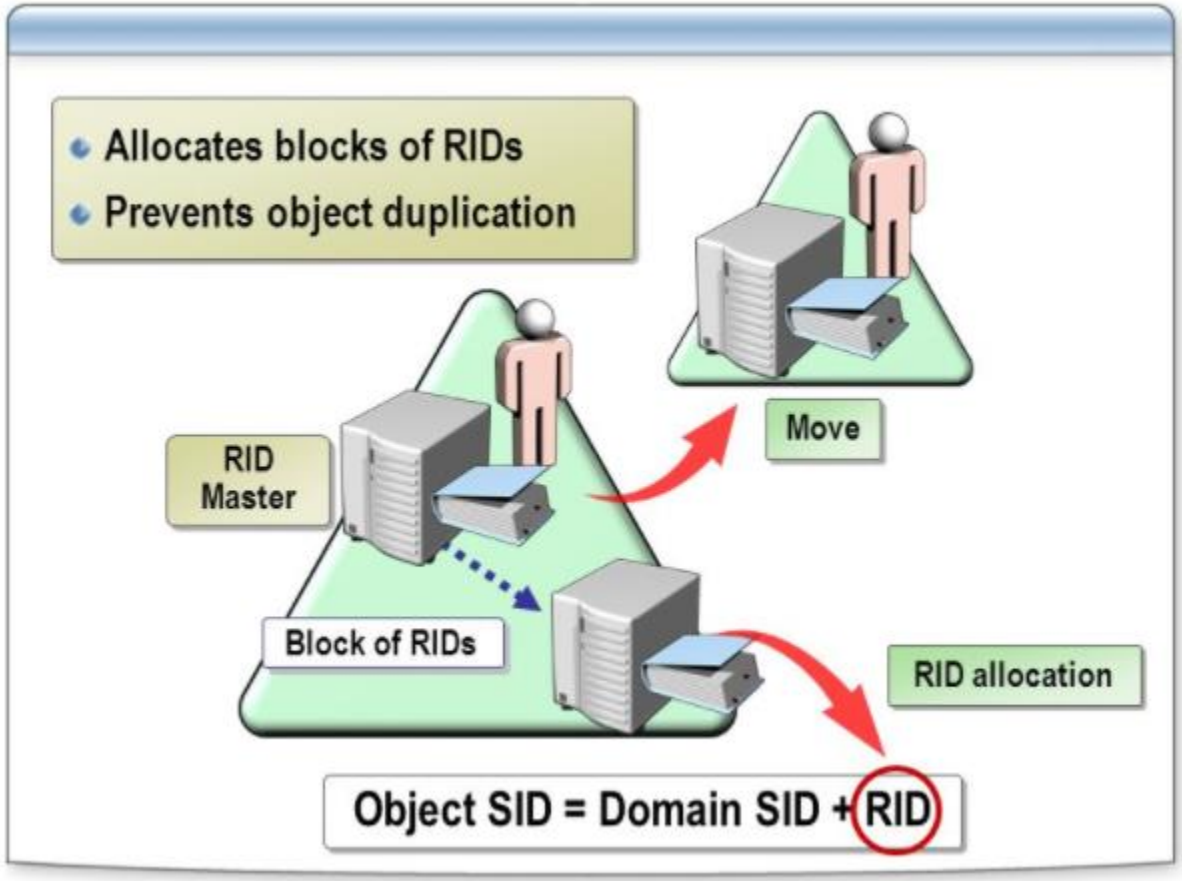
O RID Master é responsável pelo processamento de solicitações de pool RID de todos os controladores de um domínio específico.

Quando um controlador de domínio cria um objeto principal de segurança, como um usuário ou grupo, ele anexa um SID exclusivo ao objeto. Esse SID consiste em um SID de domínio (o mesmo para todos os SIDs criados em um domínio) e um RID exclusivo para cada SID principal de segurança criado em um domínio.

Cada controlador de domínio em um domínio é alocado a um pool de RIDs que pode atribuir às entidades de segurança que cria. Quando um pool RID alocado de um controlador de domínio cai abaixo de um limite, esse controlador de domínio emite uma solicitação de RIDs adicionais para o RID Master do domínio. O RID Master do domínio responde à solicitação recuperando RIDs do pool de RIDs não alocados do domínio e os atribui ao pool do controlador de domínio solicitante. A qualquer momento, pode haver apenas um controlador de domínio atuando como RID Master no domínio.

Fonte: varoniz.com

# FSMO – RID Master




Fonte: varoniz.com

# FSMO – RID Master

**O que acontece quando o RID Master não está disponível?**

Um RID Master com falha eventualmente impedirá que os controladores de domínio criem novos SIDs e, portanto, impedirá que se crie novas contas para usuários, grupos ou computadores. No entanto, os controladores de domínio recebem um pool considerável de RIDs do RID Master, portanto, a menos se você esteja gerando várias contas novas, muitas vezes pode-se ficar algum tempo sem o RID Master online enquanto ele está sendo reparado. Transferir esse papel para outro controlador de domínio é uma ação significativa. Depois que o papel de mestre RID é transferido, o controlador de domínio que estava executando o papel não pode ser colocado online novamente.

Fonte: varoniz.com

# FSMO – PDC Emulator

O PDC Emulator é necessário para sincronizar o tempo entre os dispositivos de uma rede. O objetivo do serviço de horário é garantir que o serviço de horário do Windows use uma relação hierárquica que controla a autoridade e não permite loops para garantir o uso de horário comum apropriado.

O PDC Emulator de um domínio é autoritativo para aquele domínio e deve ser configurado para obter o tempo de uma fonte externa.

Em um domínio, o controlador de domínio com o papel de PDC Emulator executa as seguintes funções:

- As alterações de senha realizadas por outros controladores de domínio são replicadas preferencialmente para o PDC Emulator;
- As falhas de autenticação que ocorrem em um determinado controlador de domínio em um domínio devido a uma senha incorreta são encaminhadas ao PDC Emulator antes que uma mensagem de falha de senha inválida seja relatada ao usuário;
- O bloqueio de conta é processado no emulador PDC.
- A edição ou criação de objetos de política de grupo (GPO) é sempre feita a partir da cópia GPO encontrada no compartilhamento SYSVOL do PDC Emulator, a menos que configurado para não fazê-lo pelo administrador.

Fonte: varoniz.com

# FSMO – PDC Emulator

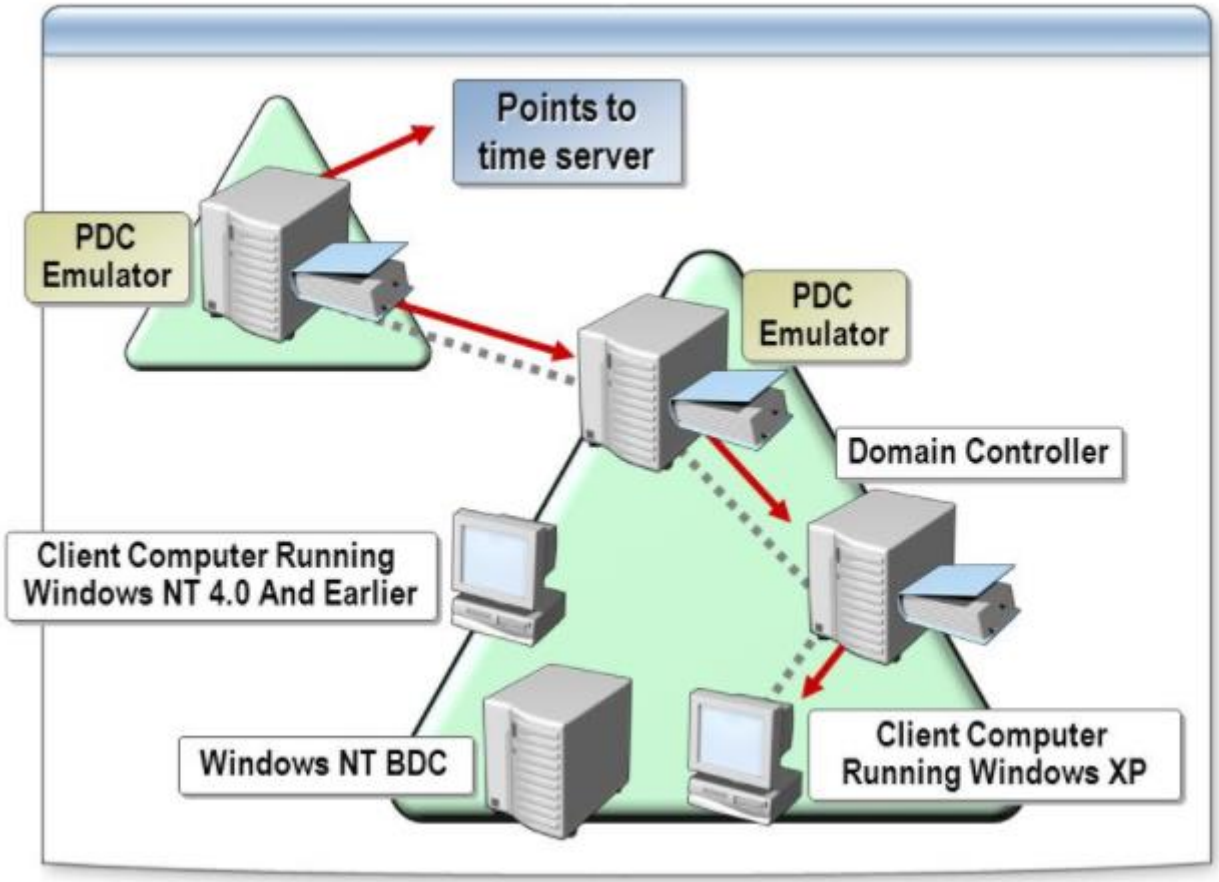
Adicionalmente, o PDC Emulator executa todas as funcionalidades que um PDC baseado no Microsoft Windows NT 4.0 Server ou PDC anterior executa para clientes baseados no Windows NT 4.0 ou anteriores.

Esta parte da função do emulador PDC torna-se desnecessária quando todas as estações de trabalho, servidores membros e controladores de domínio que executam o Windows NT 4.0 ou anterior são atualizados para o Windows 2000/2003.

A qualquer momento, pode haver apenas um controlador de domínio atuando como PDC Emulator em cada domínio da floresta.

Fonte: varoniz.com

# FSMO – PDC Emulator




Fonte: varoniz.com

# FSMO – PDC Emulator

**O que acontece quando o PDC Emulator não está disponível?**

O PDC Emulator com falha é o que que terá o impacto mais imediato nas operações normais e nos usuários se ficar indisponível. Felizmente, a função do PDC Emulator pode ser transferida para outro controlador de domínio e, em seguida, transferida de volta para o detentor do papel original quando o sistema ficar online novamente.

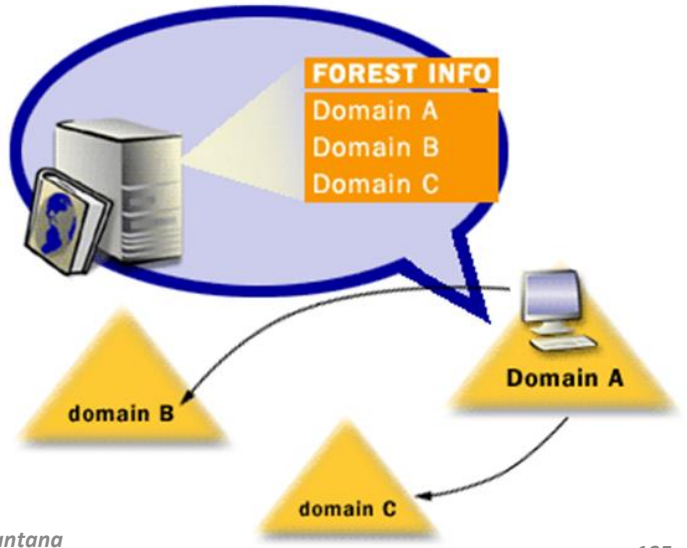
Fonte: varoniz.com

# Global Catalog

Cada controlador de domínio armazena os objetos do domínio no qual está instalado, no entanto, um controlador de domínio designado como servidor de Catálogo Global ou Global Catalog armazena os objetos de todos os domínios da floresta.

Para cada objeto que não está no domínio para o qual o servidor de catálogo global tem autoridade como controlador de domínio, um conjunto limitado de atributos é armazenado em uma réplica parcial do domínio.

Portanto, um servidor de catálogo global armazena sua própria réplica de domínio gravável completa (todos os objetos e todos os atributos), além de uma réplica parcial somente leitura de todos os outros domínios da floresta.




Fonte: varoniz.com

# Global Catalog

O catálogo global é criado e atualizado automaticamente pelo sistema de replicação do AD DS (Active Directory Domain Services).

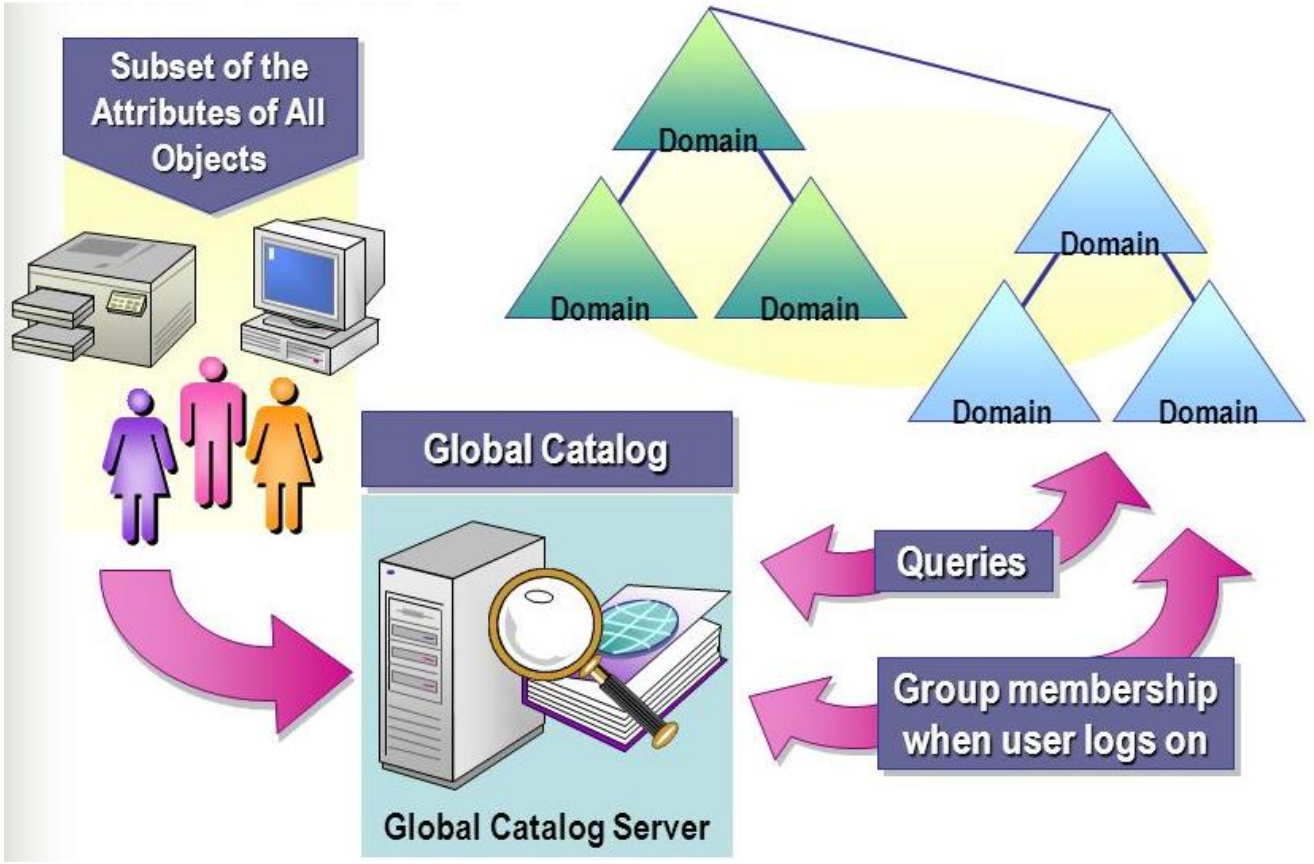
Os atributos de objeto replicados para servidores de catálogo global são os atributos com maior probabilidade de serem usados para pesquisar o objeto no AD DS.

Os atributos replicados para o catálogo global são identificados no esquema como o Conjunto de Atributos Parcial ou Partial Attribute Set (PAS) e são definidos por padrão pela Microsoft.

No entanto, para otimizar a pesquisa, é possível editar o esquema adicionando ou removendo atributos que são armazenados no catálogo global.

Fonte: varoniz.com

# Global Catalog




Fonte: varoniz.com

# Global Catalog

O catálogo global possibilita que os clientes pesquisem no AD DS sem precisar ser encaminhado de um servidor para outro até que seja encontrado um controlador de domínio que tenha a partição de diretório de domínio que armazena o objeto solicitado.

Por padrão, as pesquisas do AD DS são direcionadas aos servidores de catálogo global.

O primeiro controlador de domínio em uma floresta é criado automaticamente como um servidor de catálogo global.

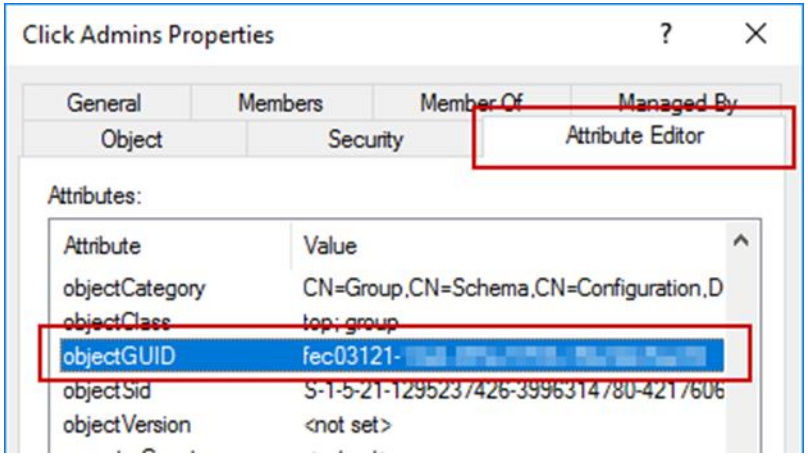
Depois disso, é pode designar outros controladores de domínio para serem servidores de catálogo global, se necessário.

Fonte: varoniz.com

# SID vs GUID

Quando um novo usuário de domínio ou conta de grupo é criado, o Active Directory armazena o SID (Security IDentifier) da conta na propriedade ObjectSID de um objeto Usuário ou Grupo. Ele também atribui ao novo objeto um GUID (Globally Unique IDentifier), que é um valor de 128 bits exclusivo não apenas na empresa, mas também em todo o mundo.

Os GUIDs são atribuídos a todos os objetos criados pelo Active Directory, não apenas aos objetos Usuário e Grupo. O GUID de cada objeto é armazenado em sua propriedade ObjectGUID.




Fonte: Microsoft

# SID vs GUID

Se um usuário muda de um domínio para outro, ele obtém um novo SID. O SID de um objeto de grupo não muda porque os grupos permanecem no domínio em que foram criados.

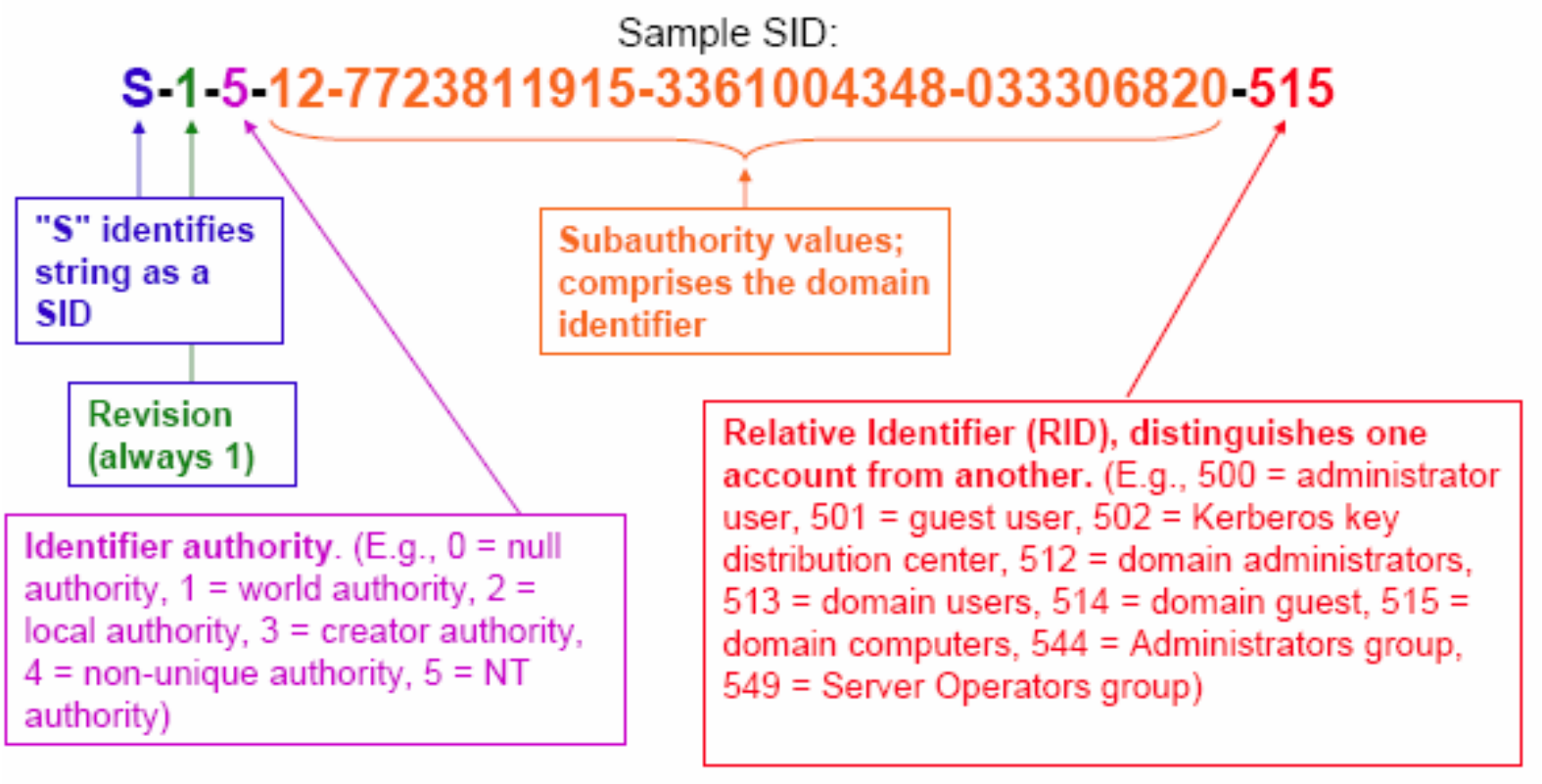
Se um funcionário se mudar da América do Norte para a Europa, por exemplo, mas permanecer na mesma empresa, um administrador do Active Directory poderá mover o objeto Usuário do funcionário de uma unidade organizacional para outra.

Quando o administrador fizer isso, o objeto Usuário da conta precisará de um novo SID. A parte do identificador de domínio de um SID emitida na América do Norte é exclusivo, de tal modo que o SID da conta do usuário na Europa tem um identificador de domínio diferente.

A parte relativa do identificador de um SID é exclusiva em relação ao domínio, portanto, se o domínio muda, o identificador relativo também muda.

Fonte: Microsoft

# SID vs GUID

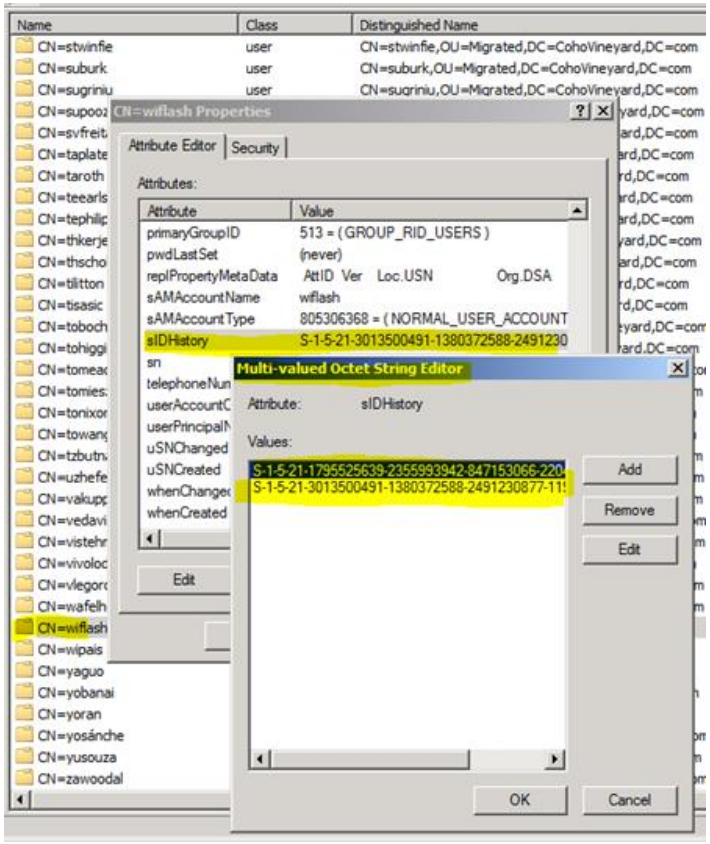



Fonte: c-jump.com

# SID vs GUID – continuação

Quando um objeto Usuário é movido de um domínio para outro, um novo SID deve ser gerado para a conta do usuário e armazenado na propriedade ObjectSID.

Antes que o novo valor seja gravado na propriedade, o valor anterior é copiado para outra propriedade de um objeto Usuário, SIDHistory. Esta propriedade pode conter vários valores. Cada vez que um objeto Usuário é movido para outro domínio, um novo SID é gerado e armazenado na propriedade ObjectSID e outro valor é adicionado à lista de SIDs antigos em SIDHistory.




Fonte: Microsoft

# SID vs GUID

Quando um usuário entra e é autenticado com êxito, o serviço de autenticação de domínio consulta o Active Directory em busca de todos os SIDs associados ao usuário, incluindo o SID atual do usuário, os SIDs antigos do usuário e os SIDs dos grupos do usuário.

Todos esses SIDs são retornados ao cliente de autenticação e são incluídos no token de acesso do usuário.

Quando o usuário tenta obter acesso a um recurso, qualquer um dos SIDs no token de acesso (incluindo um dos SIDs em SIDHistory) pode permitir ou negar o acesso do usuário.

Fonte: Microsoft

# Para saber mais...

… leia o documento xxxxxxxxxxx

# Módulo 11

Windows Powershell

# Windows PowerShell

O Windows PowerShell é uma solução de automação de tarefas multiplataforma que consiste em um shell de linha de comando, em uma linguagem de script e uma estrutura de gerenciamento de configuração.

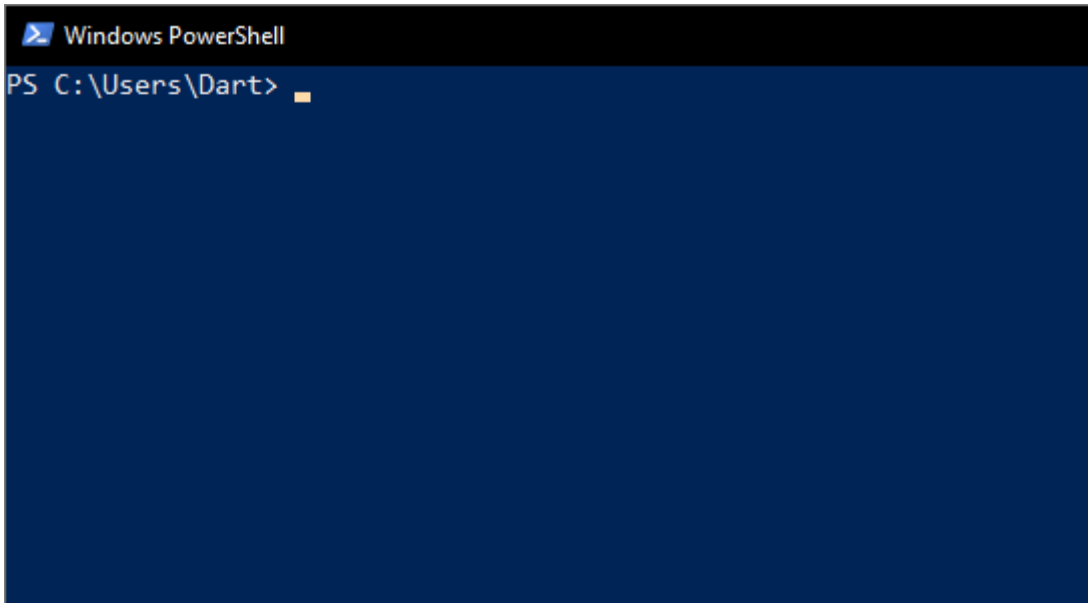
Inclui um prompt interativo e um ambiente para criação de scripts para administração do sistema e automação.

O PowerShell pode ser executado no Windows, Linux e macOS.


Fonte: microsoft.com

# Windows PowerShell

## Acessando o console PowerShell




⇨ **Windows PowerShell**

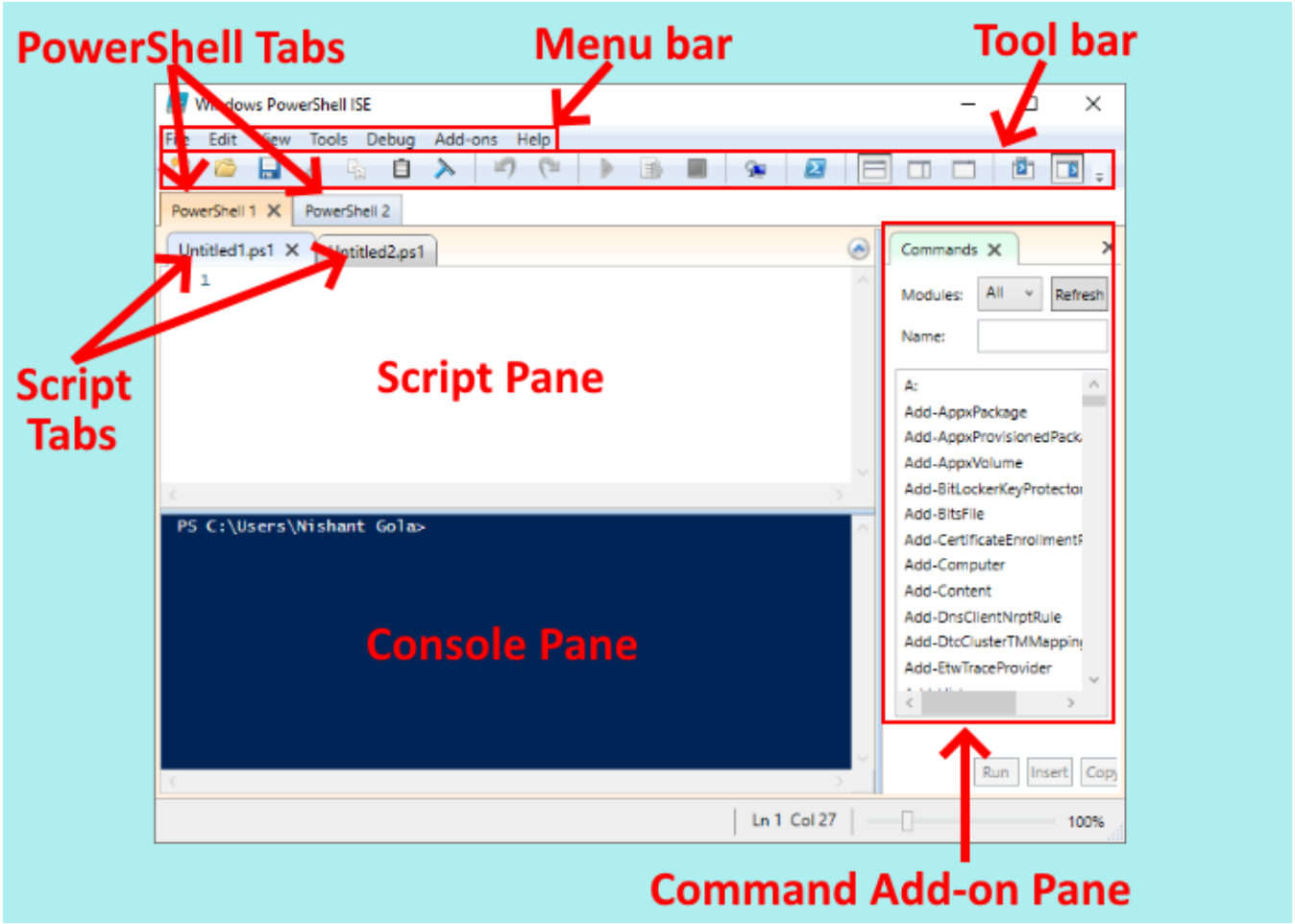
# Windows PowerShell ISE

O Windows PowerShell Integrated Scripting Environment (ISE) é um aplicativo para o Windows PowerShell.

No Windows PowerShell ISE, é possível executar comandos e escrever, testar e depurar scripts em uma única interface de usuário gráfica baseada no Windows com edição multilinha, preenchimento de tabulação, coloração de sintaxe, execução seletiva e ajuda contextual.

Fonte: tutorialspoint.com

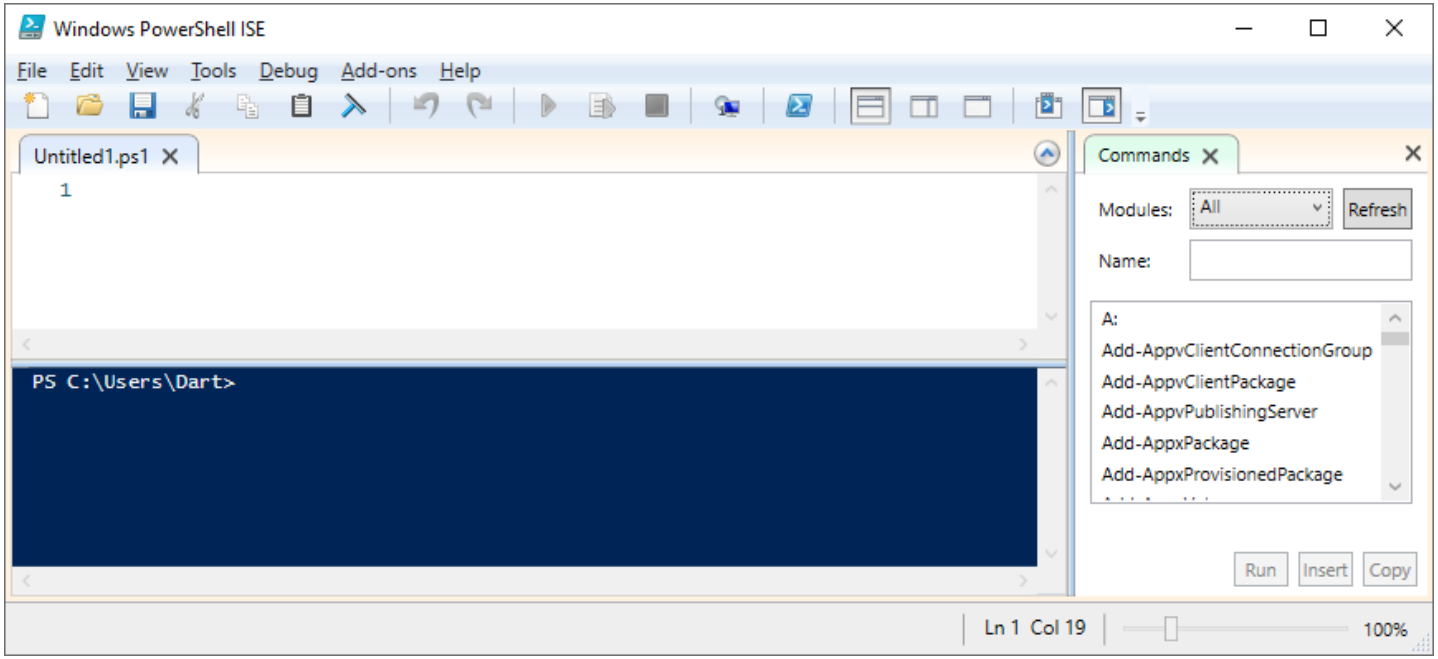
# Windows PowerShell ISE




Fonte: br.atsit.in

# Windows PowerShell

## Acessando o PowerShell ISE




⇨ **Windows PowerShell ISE**

# Obtendo informações do sistema

- $PSVersionTable - retorna a versão do shell
- $env:Path - retorna o diretório onde o sistema operacional irá procurar por arquivos executáveis

Digitar $env: seguido de <TAB> faz com que apareçam outras opções, como as exemplificadas abaixo:

- $env:COMPUTERNAME – retorna o nome do computador
- $env:USERNAME - retorna o nome do usuário conectado

Digitar o comando dir env: retorna todas as opções de uma só vez.

Comandos do Prompt de Comando (MS-DOS) também são aceitos no PowerShell.

Fonte: Ajuda do Windows

# Categorias de comandos

Existem quatro categorias de comandos do PowerShell:

- Cmdlet (Command-Lets);
- Funções PowerShell;
- Scripts PowerShell;
- Comandos nativos do Windows e do Linux.

Neste curso será abordado apenas o uso de Cmdlet.

Fonte: Ajuda do Windows

# Cmdlet (Command-Lets)

Um cmdlet ou “Command let” é um comando “leve” usado no ambiente Windows PowerShell.

O PowerShell invoca esses cmdlets no prompt de comando, que podem ser criados e invocados programaticamente por meio de APIs do Windows PowerShell.

Os cmdlets são diferentes dos comandos em outros ambientes de shell pelos seguintes motivos:

- São objetos de classe do .NET Framework, e não apenas arquivos executáveis autônomos;
- Podem ser facilmente construídos a partir de apenas algumas linhas de código;
- Análise, apresentação de erro e formatação de saída não são manipuladas por cmdlets, mas sim pelo Windows PowerShell;
- O processo de cmdlets funciona em objetos que não estão no fluxo de texto e os objetos podem ser passados como saída para condutores (pipe);
- Os cmdlets são baseados em registros, pois processam um único objeto por vez.

Fonte: tutorialspoint.com

# Cmdlet (Command-Lets) – verbos

O PowerShell usa um par verbo-substantivo para os nomes dos Cmdlets e para suas classes .NET derivadas.

A parte do verbo do nome identifica a ação que o Cmdlet executa, enquanto a parte substantiva do nome identifica a entidade na qual a ação é executada.

Por exemplo, o Cmdlet Get-Command recupera todos os comandos registrados no PowerShell.

Fonte: Ajuda do Windows

# Cmdlet (Command-Lets) – verbos

**Verbos Cmdlet:**

- Add - adiciona um recurso ou anexa um item em outro item

Exemplo: Add-Computer

Observação: assim como existe o verbo Add, também existe o Remove

- Clear - Remove um recurso

Exemplo: Clear-Content

- Close - altera o estado de um recurso.

Observação: assim como existe o verbo Close, também existe o Open

- Format - formata (arruma) objetos ou saídas em determinados layouts
- Get - ação que recupera informações, por exemplo, uma lista de objetos

Exemplo: Get-Command

Fonte: Ajuda do Windows

# Cmdlet (Command-Lets) – verbos

**Verbos Cmdlet (continuação):**

- Move - Move recursos de uma localização para outra
- New - Cria um novo recurso de um item, como uma variável ou um evento
- Show - Exibe informações relacionadas ao “substantivo”
- Start - Inicia uma instancia de um item como um serviço ou processo
- Stop - Para uma instancia de um item como um serviço ou processo

Fonte: Ajuda do Windows

# Cmdlet (Command-Lets) – exemplos

- Get-Service Spooler - mostra o estado do serviço de servidor de impressão
- Stop-Service Spooler - para a execução do serviço de servidor de impressão
- Start-Service Spooler - inicia a execução do serviço de servidor de impressão

Para ver uma lista de todos os processos em execução, usar o Cmdlet Get-Process.

Para obter ajuda sobre um determinado Cmdlet, usar Get-Help seguido do par verbo-substantivo.

Fonte: Ajuda do Windows

# Cmdlet (Command-Lets) – formatação de saída

Para formatar a saída de um Cmdlet e facilitar a sua visualização, é possível combiner Cmdlets com o condutor pipe ( | ), representado por uma barra vertical, como nos exemplos abaixo:

- Get-Process | more
- Get-Process | Format-List
- Get-Process | Format-List | more

Fonte: Ajuda do Windows

# Cmdlet (Command-Lets) – formatação de saída

Também é possível redirecionar a saída de um Cmdlet para um Arquivo, como nos exemplos abaixo:

- Get-Process | ConvertTo-HTML | Out-File “Processos.html”
- Get-Process | Export-CSV “Processos.csv”

Uma outra forma de visualização é por meio de uma janela gráfica:

Get-Process | Out-GridView

Fonte: Ajuda do Windows

# Módulos adicionais

Dependendo das configurações da máquina onde o PowerShell está instalado, poderá haver ou não determinados módulos disponíveis que acrescentam funcionalidades adicionais ao shell.

Para verificar os módulos disponíveis no PowerShell, deve-se utilizar o seguinte Cmdlet:

- Get-Module

Fonte: Ajuda do Windows

# Módulos adicionais – exemplo

Se a máquina for um controlador de domínio em um domínio Active Directory, por exemplo, ela terá um módulo adicional do PowerShell, onde será possível executar Cmdlet como demonstrados abaixo:

- Search-ADAccount -AccountDisabled

retorna uma lista de usuários do Active Directory que estão desabilitados

- Get-ADUser -Identity <username> -properties LastLogOnDate

retorna a data e a hora da última vez que o usuário especificado conectou-se ao domínio

Fonte: Ajuda do Windows

# Para saber mais...

… consulte a ajuda do Windows PowerShell

# Módulo 12

Auditoria

# Introdução

"Exame ou verificação de uma dada matéria, tendente a analisar a conformidade da mesma com determinadas regras, normas ou objetivos, conduzido por uma pessoa idônea, tecnicamente preparada, realizado com observância de certos princípios, métodos e técnicas geralmente aceites, com vista a possibilitar ao auditor formar uma opinião e emitir um parecer sobre a matéria analisada."

*Organização das Instituições Superiores de Controle (ISC) da Comunidade dos Países de Língua Portuguesa (CPLP)*

"A auditoria é uma atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais de uma determinada entidade, com o objetivo de verificar sua conformidade com certos objetivos e políticas institucionais, orçamentos, regras, normas ou padrões."

*Abílio Bueno Neto e Davi Solonca*

# Conceitos

Alguns conceitos básicos relacionados com a auditoria são: campo, âmbito e área de verificação.

- **Campo da auditoria:** É a definição do objeto e do período a fiscalizar, bem como da natureza da auditoria a realizar (por exemplo, auditoria da legalidade e/ou regularidade de determinadas operações em determinado mês, ano ou, em alguns casos, ao período de gestão do administrador da instituição). O seu objeto pode ser uma entidade completa (organismo público, empresa ou projeto, etc.), uma parte ou uma função dessa entidade;
- **Âmbito da auditoria:** Tem por finalidade determinar a amplitude e a exaustão dos processos de auditoria preconizados, o que inclui uma limitação racional dos trabalhos a executar, de modo a tornar aceitável para o auditor o risco de serem errôneas as suas conclusões de auditoria. Em outras palavras, determina o escopo;
- **Área de verificação:** É a área determinada pelo campo da auditoria e pelo seu âmbito (escopo), quando considerados em conjunto. A área de auditoria delimita de modo muito preciso os temas da auditoria, em função, por um lado, da entidade a fiscalizar e, por outro, da natureza da auditoria preconizada.

Fonte: Organização das Instituições Superiores de Controle (ISC) da Comunidade dos Países de Língua Portuguesa (CPLP)

# Conceitos

Algumas técnicas usadas em auditorias de sistemas são comuns a outros tipos de auditoria, como:

- **Entrevista:** reunião realizada com os envolvidos com o ponto auditado, que deve ser documentada;
- **Questionário:** conjunto de perguntas que podem ser aplicadas a muitas pessoas simultaneamente, sem a presença do auditor;
- **Verificação in loco**: observação direta de instalações, atividades ou produtos auditados.

Fonte: Auditoria de Sistemas Informatizados, Abílio Bueno Neto e Davi Solonca.

# Auditoria de sistemas

Uma auditoria de sistemas de informação pode abranger desde o exame de dados registrados em sistemas informatizados, até a avaliação do próprio sistema operacional e demais aplicativos, bancos de dados, bem como incluir a avaliação do ambiente de desenvolvimento, do ambiente de operação, do ambiente de gerenciamento da rede e todos os demais elementos associados a um ou mais sistemas de informação corporativos.

A auditoria de sistemas de informação inclui também o exame detalhado das políticas de segurança da informação e dos controles adotados para mitiga-los.

Fonte: Auditoria de Sistemas Informatizados, Abílio Bueno Neto e Davi Solonca.

# Auditoria de sistemas – demonstração Cenário

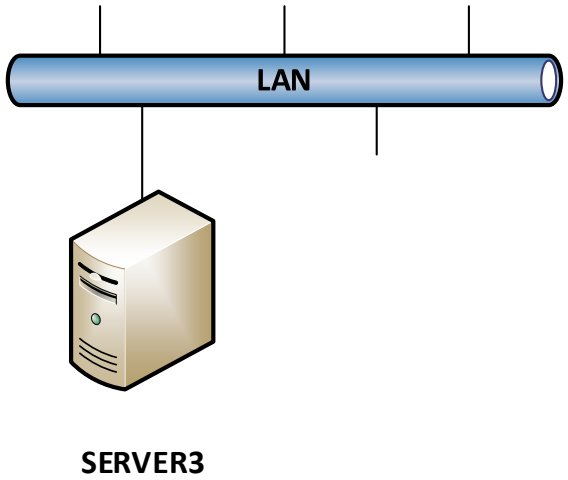
Nesta demonstração será usado um servidor Windows 2008 R2 Standard, com a seguinte configuração:

- **SERVER3**: IP 192.168.0.3, sem nenhum serviço específico.

Iremos demonstrar como auditar a criação e exclusão de arquivos em uma dada pasta.

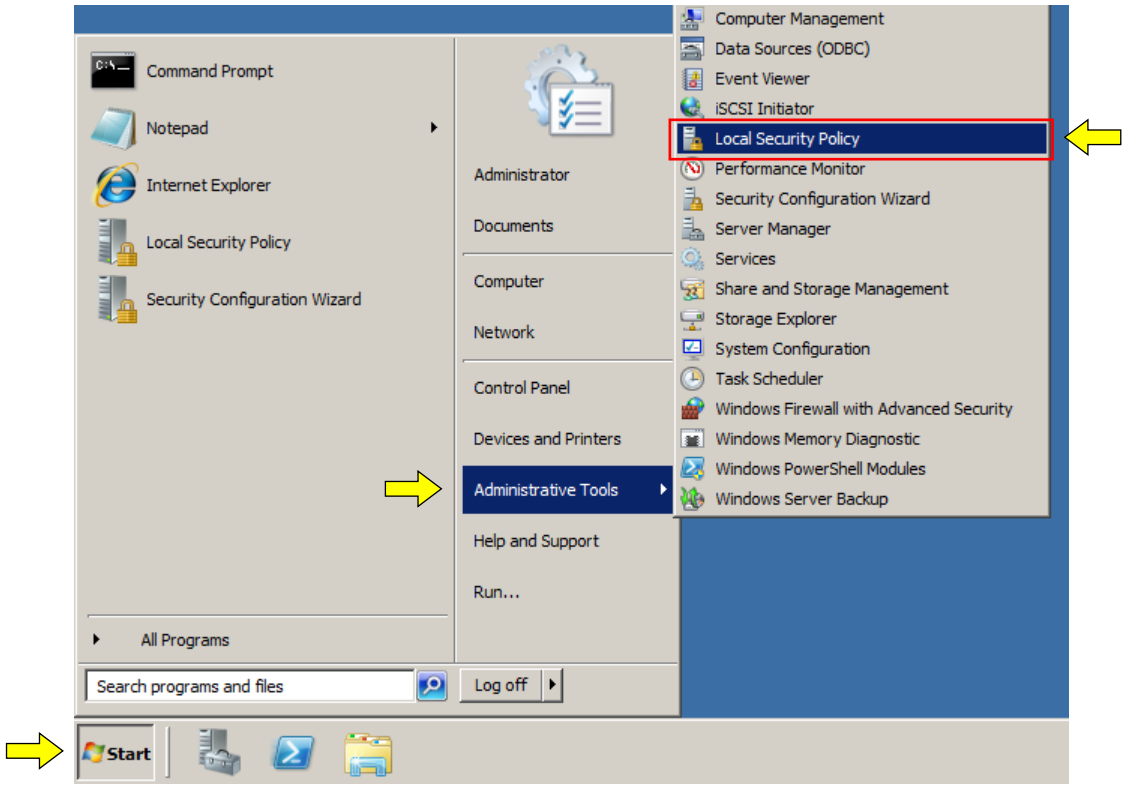
Para isso são necessários dois passos:

- Editar a política de segurança local (que também pode ser feita usando-se políticas de grupo (GPO) a serem distribuídas pelo Active Directory);
- Habilitar a auditoria na pasta desejada.



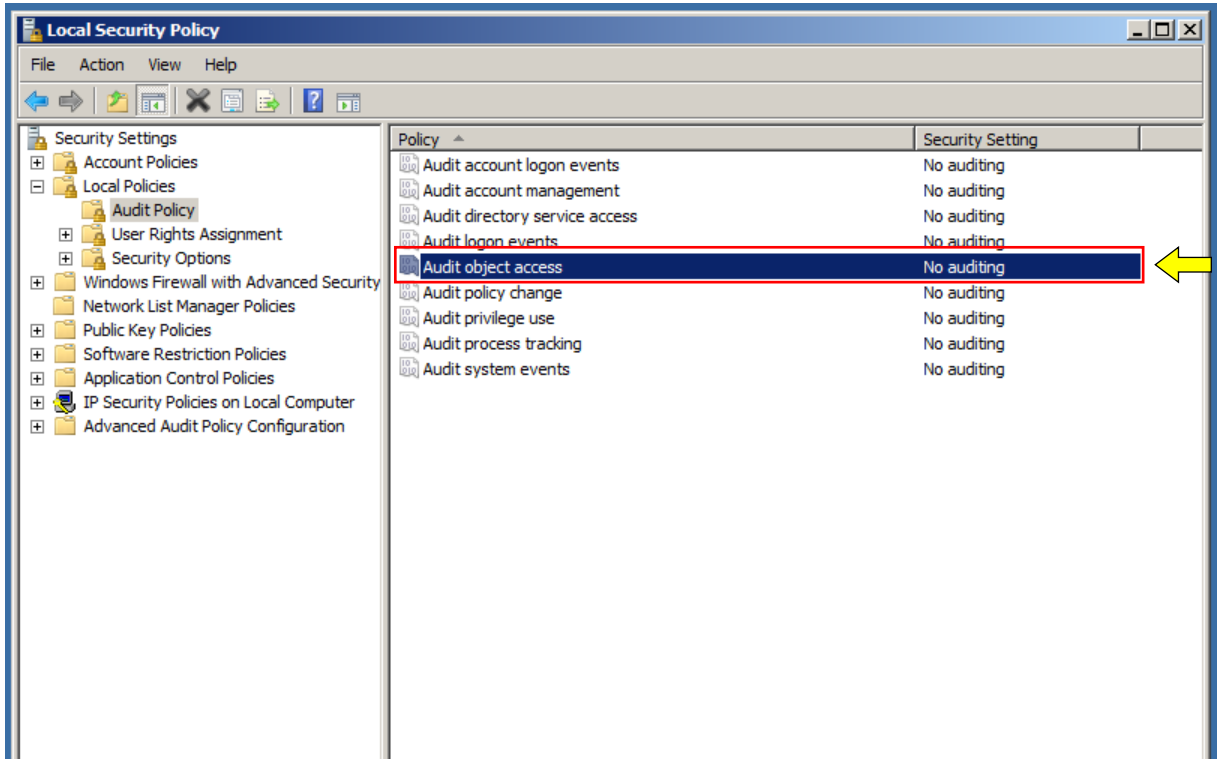
# Auditoria de sistemas – demonstração Editando a política de segurança local

No Windows a Política de Segurança Local é configurada a partir do Local Security Policy.



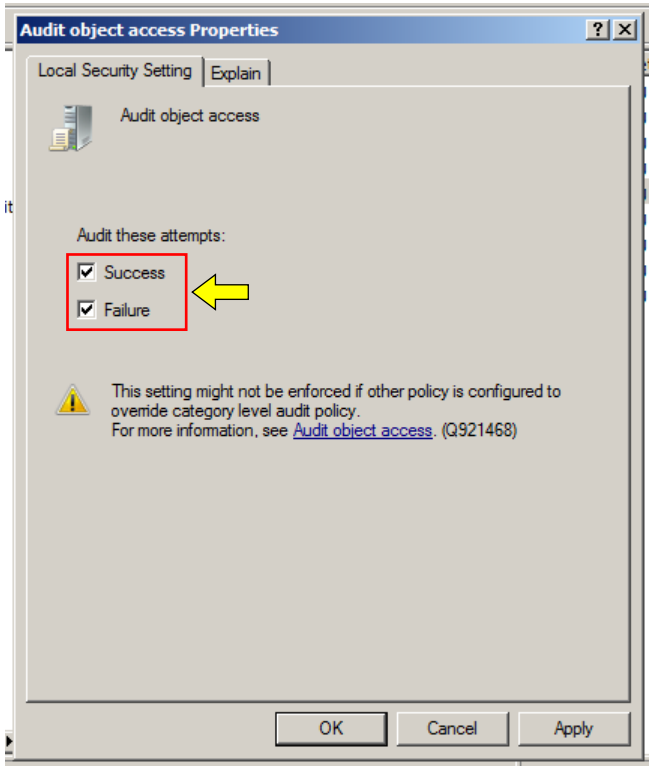
# Auditoria de sistemas – demonstração
# Editando a política de segurança local

Na console do Local Security Policy, em Security Settings, clicar em Local Policies, Audit Policy e por fim dar duplo clique em Audit object acsess.



# Auditoria de sistemas – demonstração
# Editando a política de segurança local

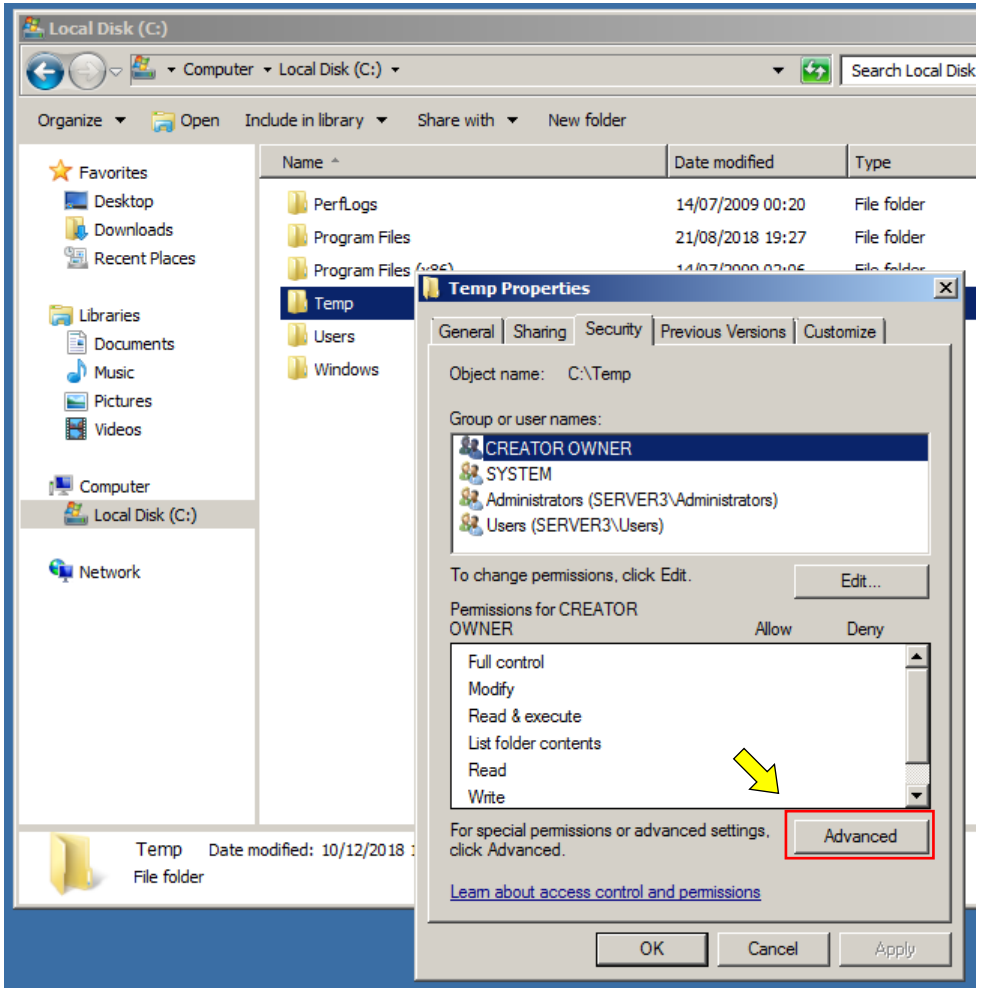
Na janela Audit object access Properties, selecionar as caixas de seleção Success e Failure.



# Auditoria de sistemas – demonstração
# Habilitando a auditoria

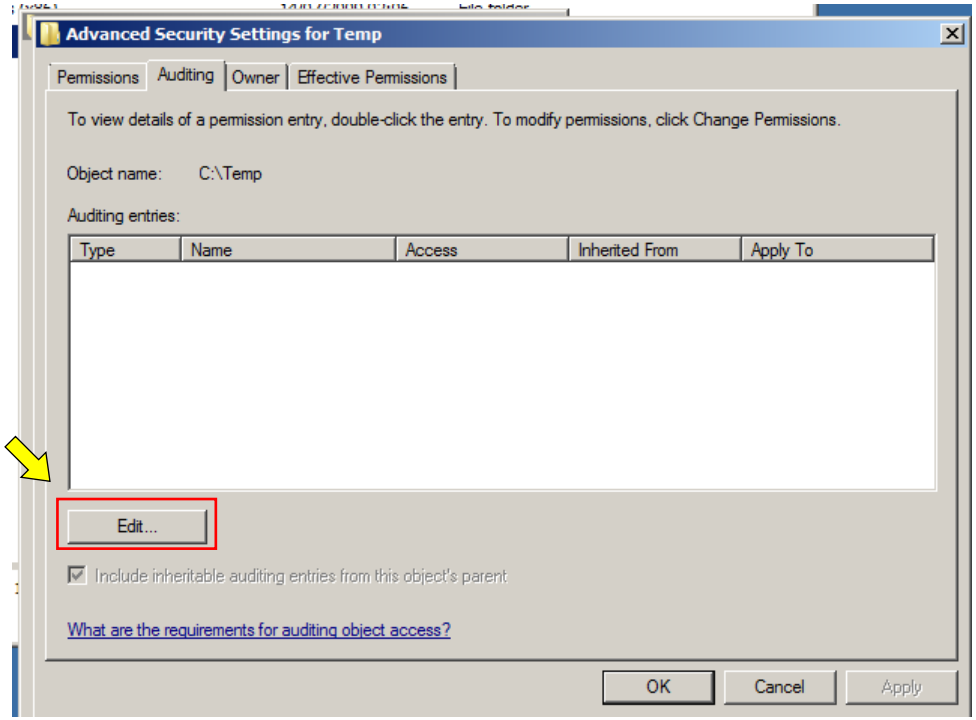
Para habilitar a auditoria, seguir os seguintes passos:

- Criar uma pasta Temp em C:;
- A partir do Windows Explorer, clicar com o botão direito na pasta criada e selecionar Properties;
- Na janela de propriedades, selecionar a aba Security e clicar em Advanced.



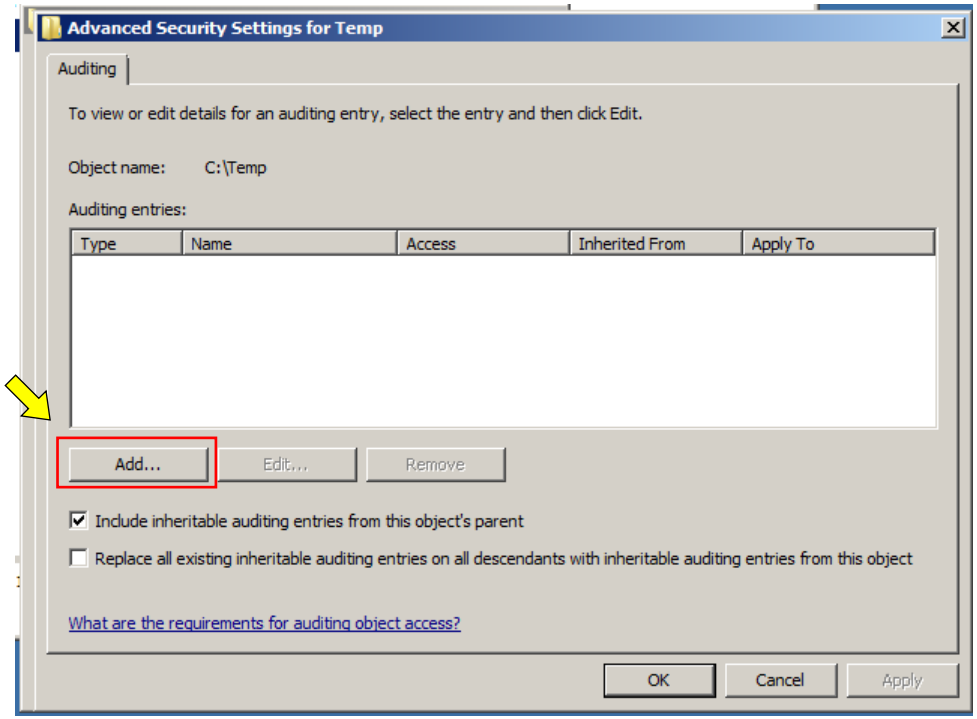
# Auditoria de sistemas – demonstração
# Habilitando a auditoria

Na janela Advanced Security Settings selecionar a aba Auditing e clicar em Edit...



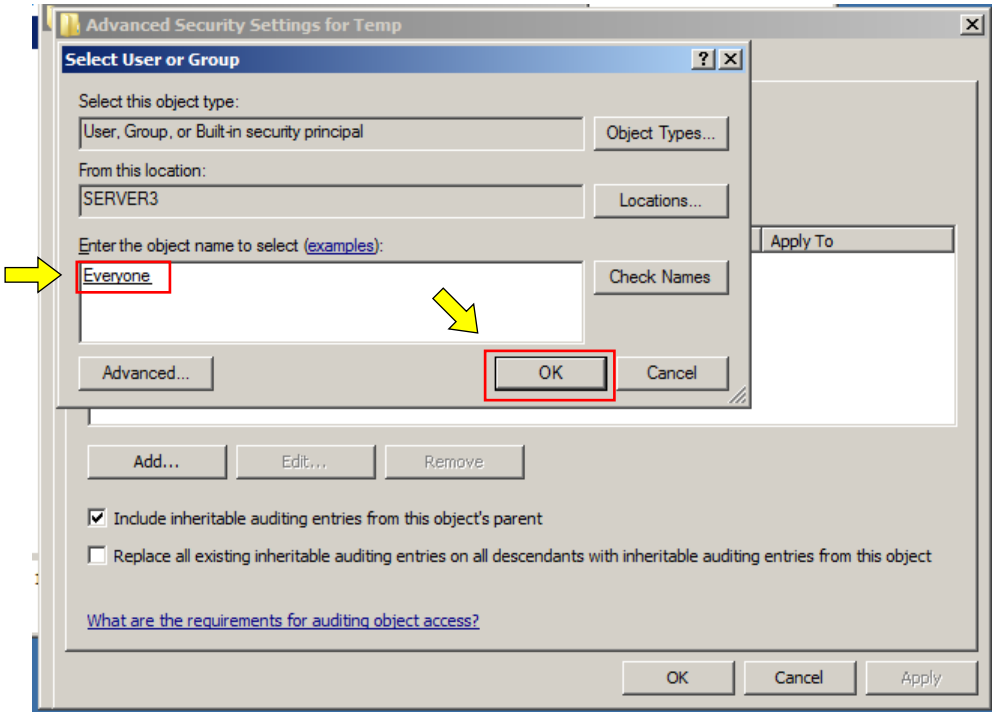
# Auditoria de sistemas – demonstração
# Habilitando a auditoria

Em Auditing,  clicar em Add...



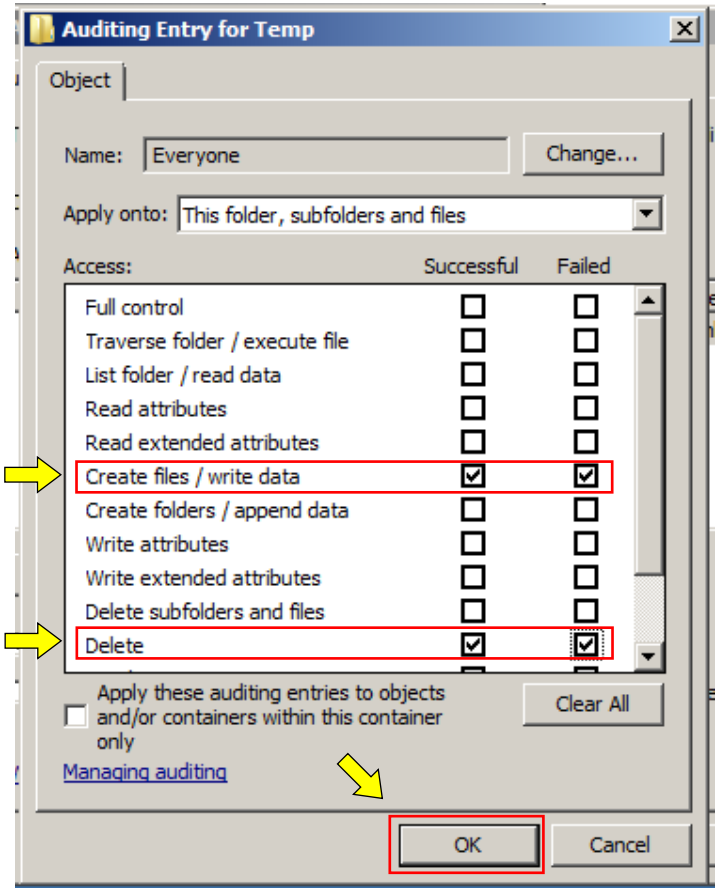
# Auditoria de sistemas – demonstração
# Habilitando a auditoria

Na janela Select User or Group, adicionar o grupo Everyone (Todos) e clicar em OK.



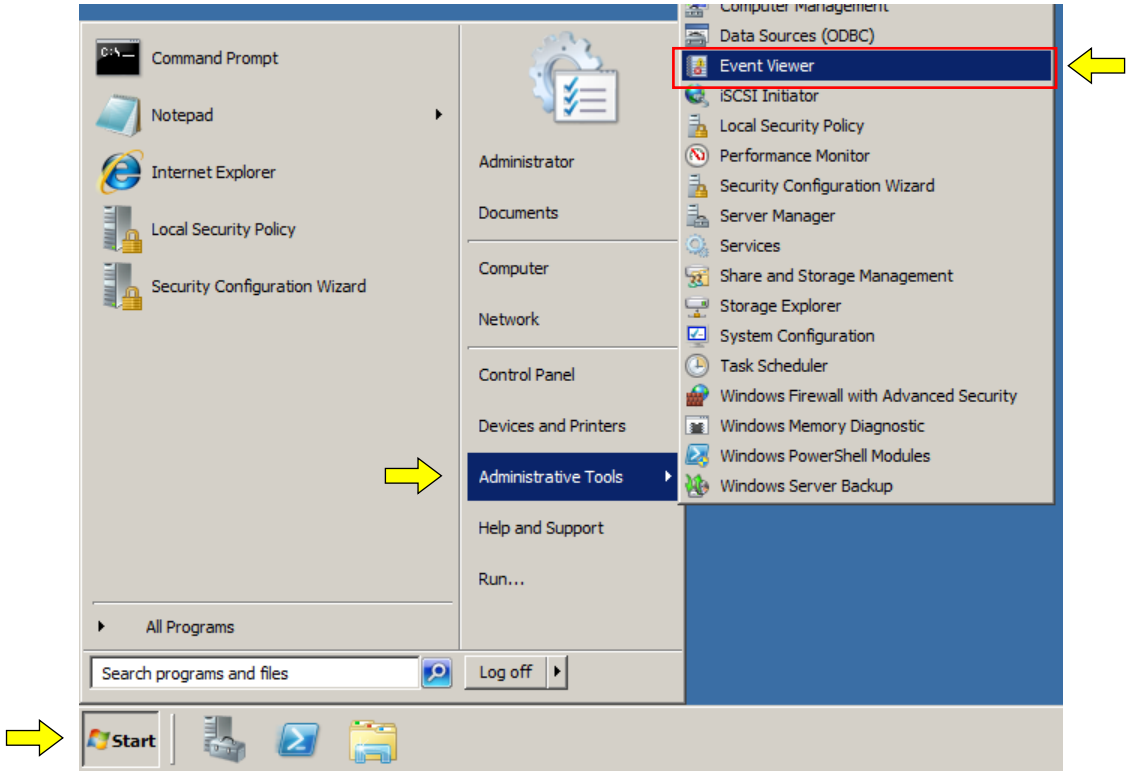
# Auditoria de sistemas – demonstração
# Habilitando a auditoria

Na janela Auditing Entry, selecionar as caixas de seleção para “Create files / write data” e “Delete”, tanto para eventos executados com sucesso (Successful) quanto para eventos executados com falha (Failed).



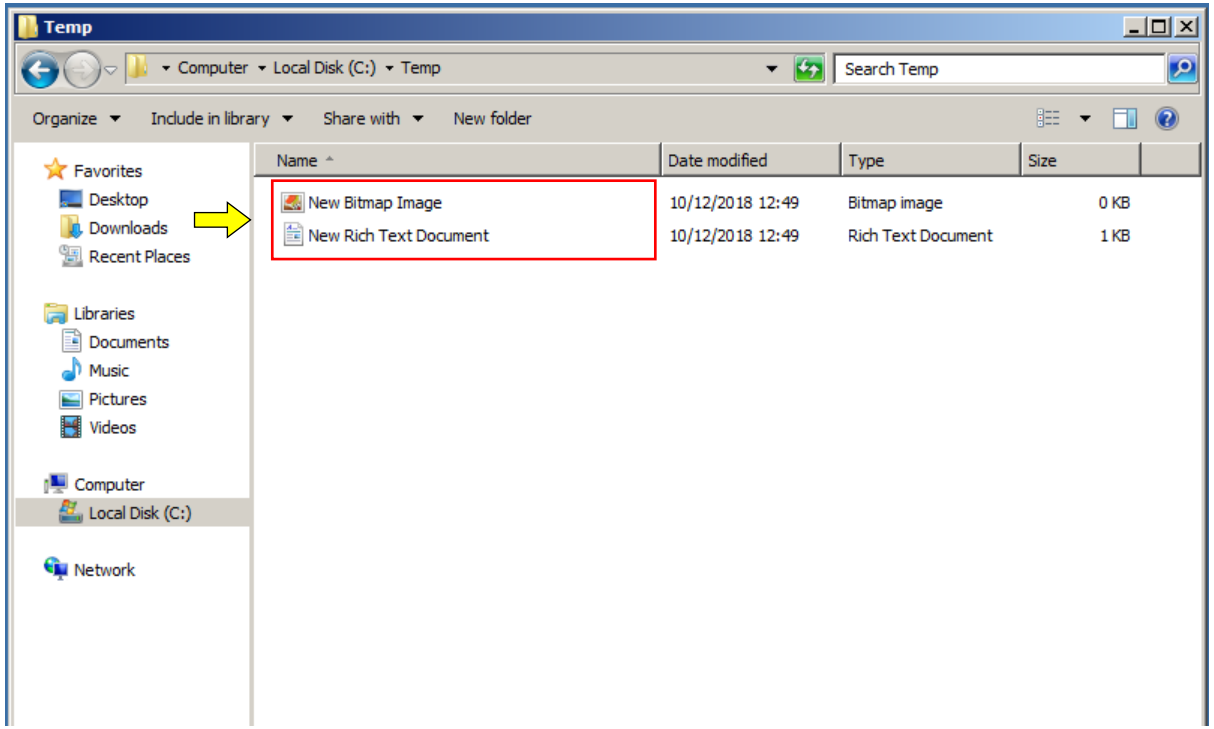
# Auditoria de sistemas – demonstração Verificando os eventos de auditoria

No Windows o Registro de Eventos é visualizado a partir do Event Viewer.



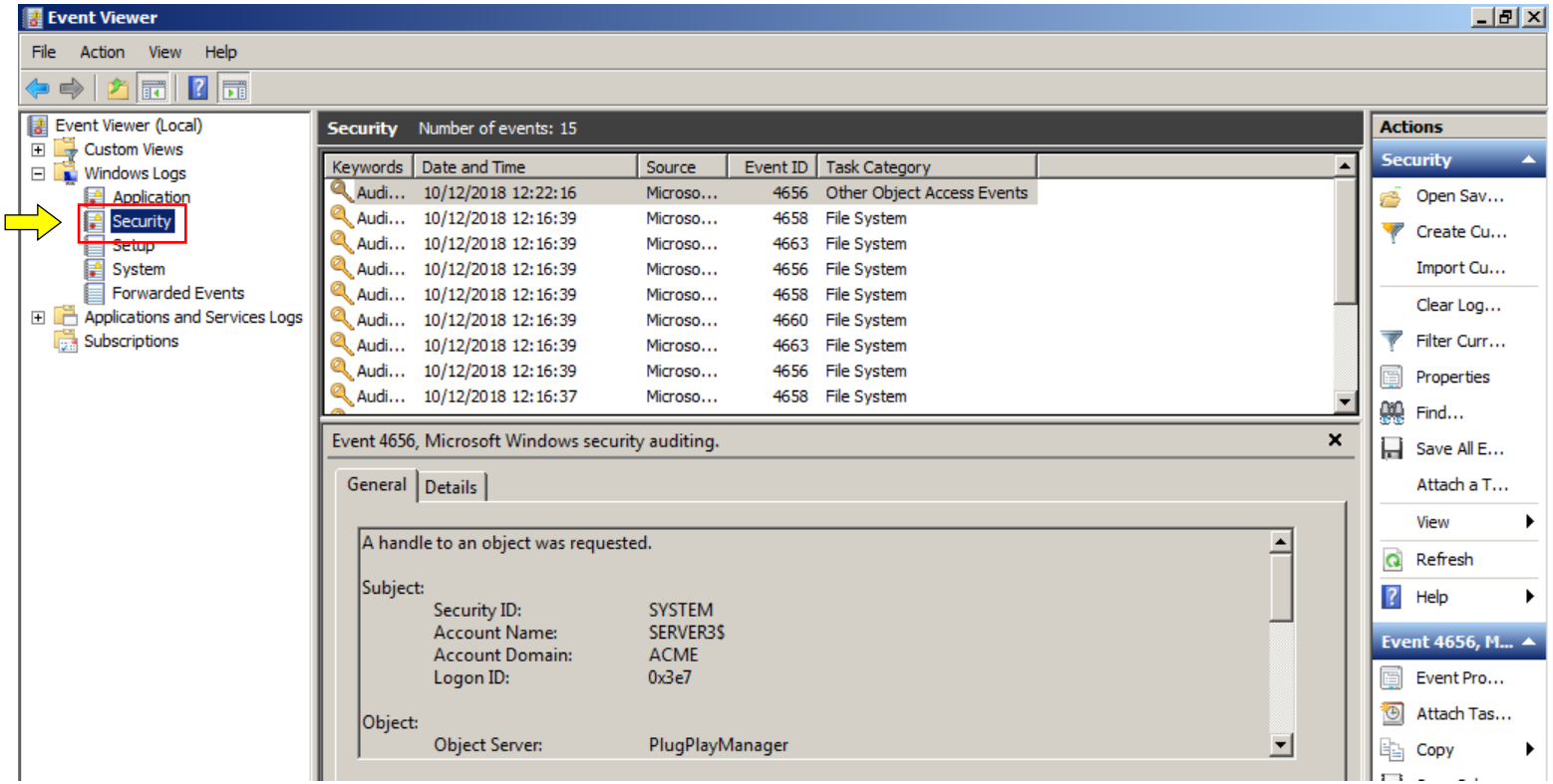
# Auditoria de sistemas – demonstração
# Testando a auditoria

Após habilitar a auditoria na pasta C:\Temp, experimente criar e apagar alguns arquivos nesta pasta, para que os eventos possam ser gerados e visualizados posteriormente.



# Auditoria de sistemas – demonstração
# Verificando os eventos de auditoria

Uma vez na console do Event Viewer, em Event Viewer (Local), clicar em Windows Logs e em seguida clicar em Security.

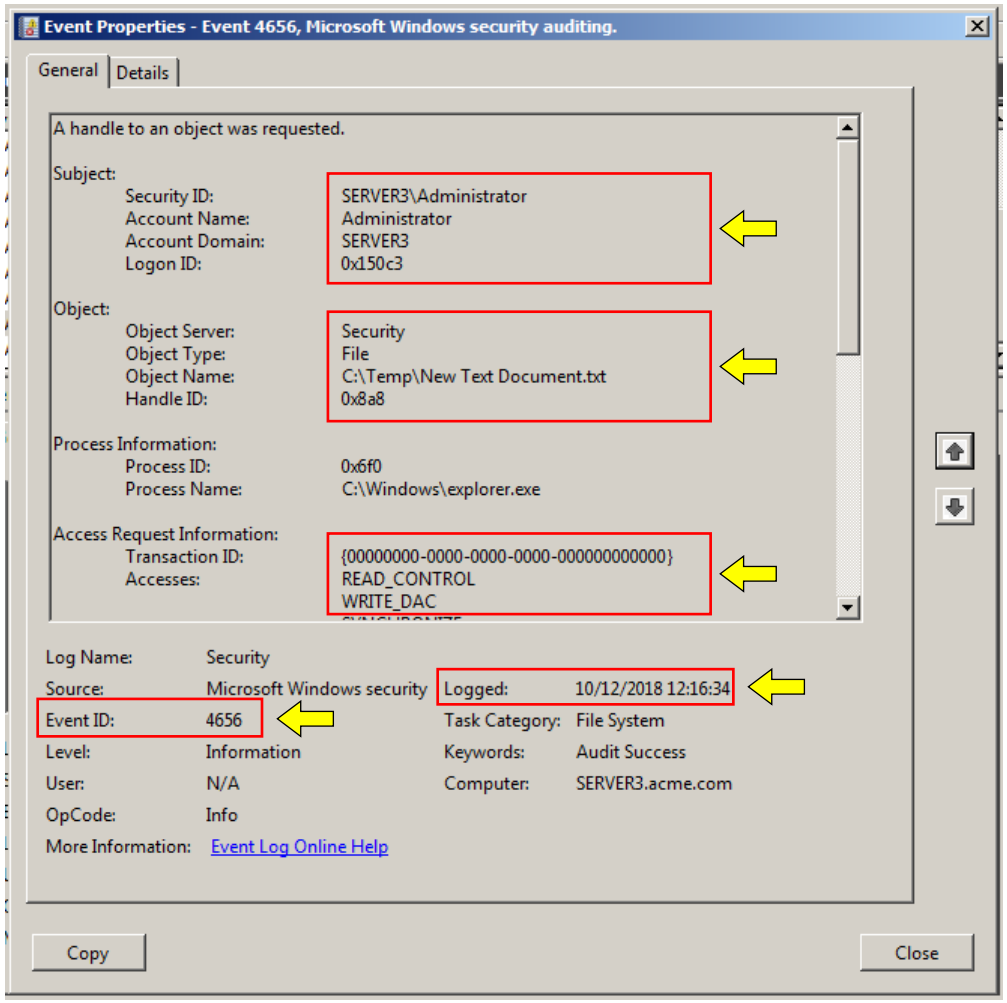


# Auditoria de sistemas – demonstração
# Verificando os eventos de auditoria

No registro de evento de auditoria, para os eventos de criação de arquivos, procurar pelo código de evento 4656.

Neste evento é possível ver quem foi o usuário; qual o nome do arquivo envolvido; e qual foi a operação.

Neste caso, o usuário Administrator criou (WRITE_DAC) o arquivo C:\Temp\New Text Document.txt, na data e hora indicados.

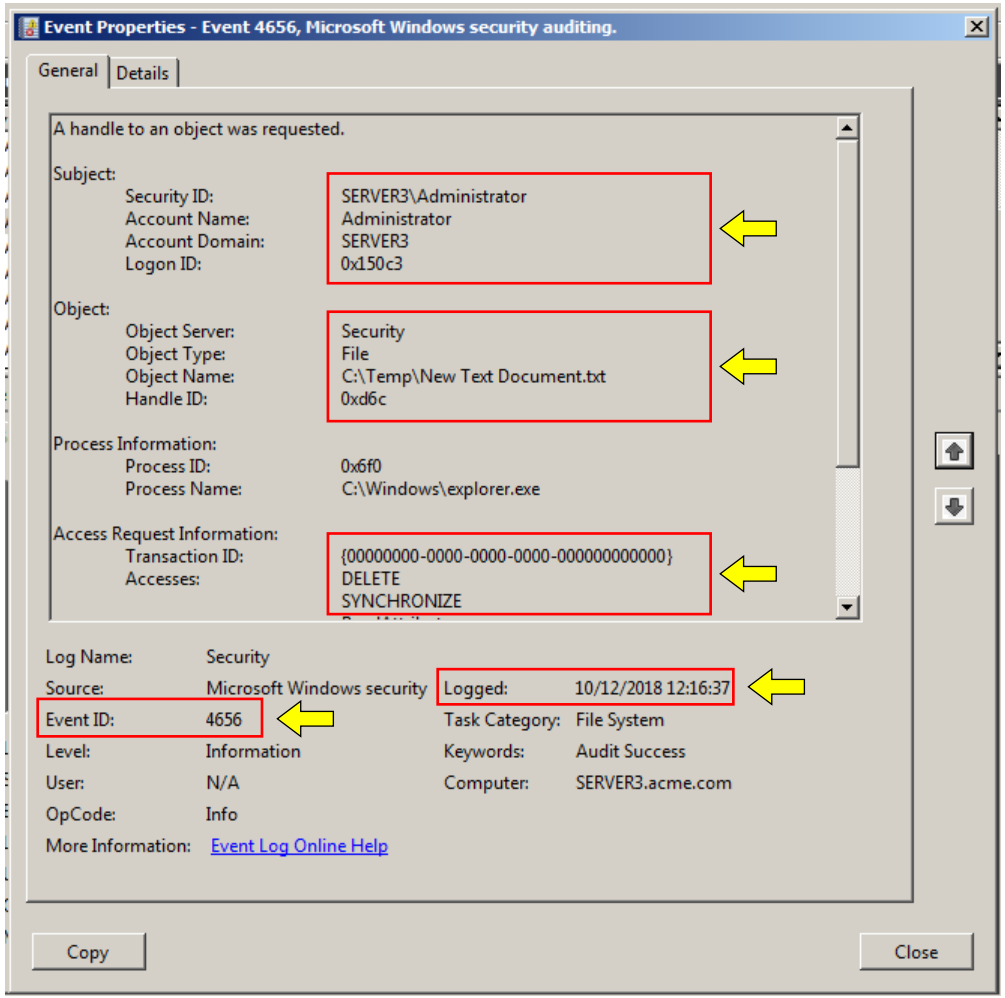


# Auditoria de sistemas – demonstração
# Verificando os eventos de auditoria

No registro de evento de auditoria, para os eventos de criação de arquivos, procurar pelo código de evento 4656.

Neste evento é possível ver quem foi o usuário; qual o nome do arquivo envolvido; e qual foi a operação.

Neste caso, o usuário Administrator apagou (DELETE) o arquivo C:\Temp\New Text Document.txt, na data e hora indicados.



# Auditoria de sistemas – cuidados

A auditoria do Windows aumenta o processamento e os arquivos de registro de eventos (log) crescem muito rápido.

Por isso, a auditoria do Windows só deve ser ligada para averiguar comportamentos pontuais no sistema ou para investigar problemas.

# Para saber mais...

… leia a apostila Auditoria de Sistemas Informatizados, de Abílio Bueno Neto e Davi Solonca

FIM