Desafio Onboarding Lenovo
Fase I – Workshop:
Windows Server

Charles Neves Epifanio de Oliveira charles.oliveira@facens.br
Leonardo dos Reis Souza leonardo.souza@facens.br

Agenda

01

Servidores

Contextualização
Conceito

02

Windows Server

Contextualização
Licenças

03

Instalação

Instalação e configurações iniciais

04

Active Directory

Conceito e aplicação

05

Configuração AD DS

Configurações relevantes

06

DNS

Configurando DNS

Agenda

07

DHCP

Controle e distribuição de IPs

08

GPMC

Aplicando políticas

09

Segurança

CVEs

10

Conclusão

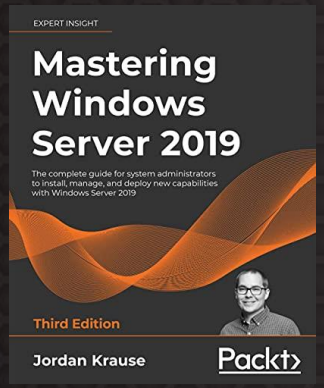
01

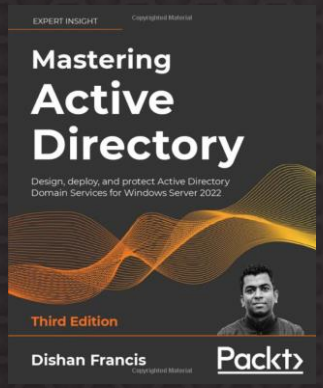
Vamos estabelecer alguns conceitos....

02

Fazer algumas práticas

Princinpais Referências





NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Microsoft Learn

ONDA

MSFT WEBCAST

01 Servidores

O que são servidores?
Mercado de SO’s de servidores
Conceito

O que são servidores?

Servidores têm diferentes aplicações e funcionalidades!

- Aplicação
- Impressoras
- Computação
- Catálogos
- Web
- Base de dados
- Comunicação
- Jogos
- Arquivos
- Fax
- Mail
- Etc.

Fonte: Geeks for Geeks. Disponível em: https://www.geeksforgeeks.org/servers-in-computer-network/

O que são servidores?

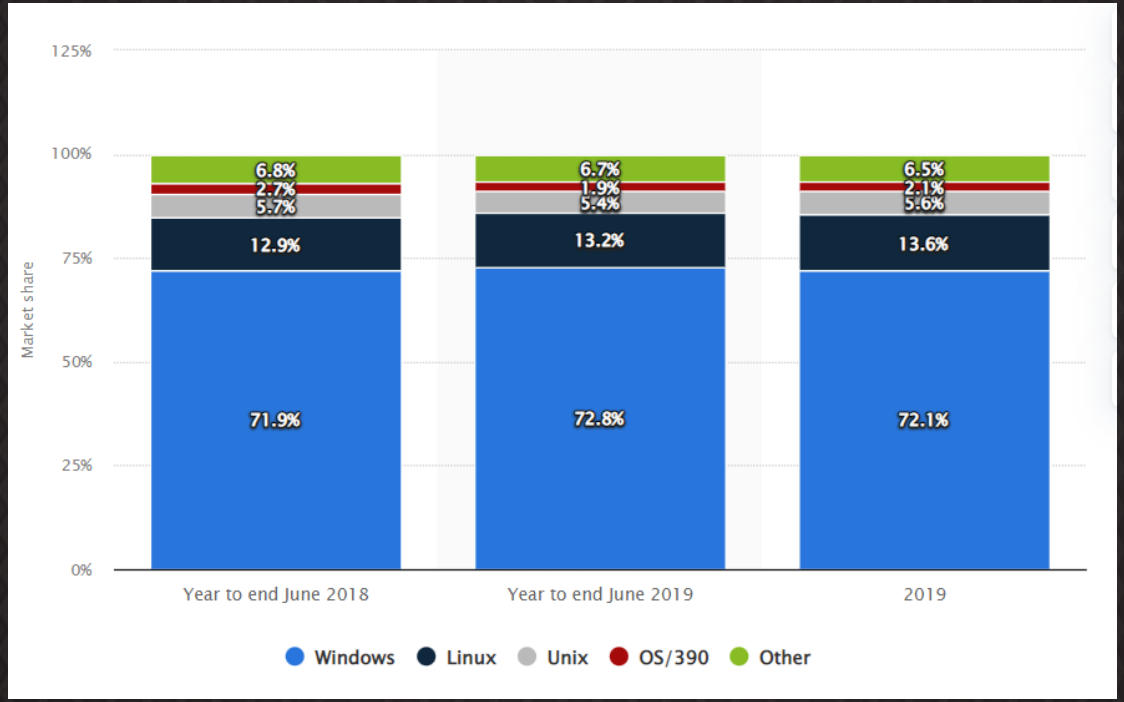
Alta disponiblidade;
Muito poder de processamento;
Alto custo.

U$D92,74 B

Mercado de Sistemas Operacionais de Servidores em 2021, bilhões de dólares

Fonte disponível em: https://www.fortunebusinessinsights.com/server-operating-system-market-106601

Market Share Global de Sistemas Operacionais de Servidores por sistemas, 2019



Fonte: Statistica. Disponível em: https://www.statista.com/statistics/915085/global-server-share-by-os/

Um servidor é o elemento de uma rede que fornece funcionalidades a clientes

02 Windows Server

Tipos de Licenças
Versões e upgrades
Um produto Microsoft
Instalação em máquina virtual

Tipos de Licenças

Essentials

Standard

Datacenter

SAC

LTSC

Desktop Experience

Server Core

Nano Server

Versões e upgrades

1993
Windows NT

1994
Windows NT Server

1996
Windows NT 4.0 Server

1997
Windows NT Server Enterprise

1998
Windows NT Server TSE

2000
NT 5.0 (Windows 2000)

2003
NT 5.2 (Windows Server 2003)

2008
Windows Server 2008

2012
Windows 2012

2016
Windows Server 2016

2019
Windows Server 2019

2022
Windows Server 2022

Versões e upgrades

Quando é necessário fazer o upgrade de versões, duas principais estratégias podem ser adotadas:

Migração

- Quando é optado por instalar em um ambiente separado a nova versão de Windows e os serviços do servidor antigo são migrados já em novas versões compatíveis para o novo ambiente;

- Menor risco;
- Maior custo;

Atualização *in-loco*

- Quando é optado por atualizar a versão do Windows para a nova versão;

- Alto risco;
- Menor custo;

Versões e upgrade

Existem algumas ferramentas relevantes para o upgrade:

Map Toolkit

- Analisa estoque da infraestrutura do servidor;
- *Verifica se os serviços, softwares e hardwares utilizados são compatíveis com a nova versão de Windows.*

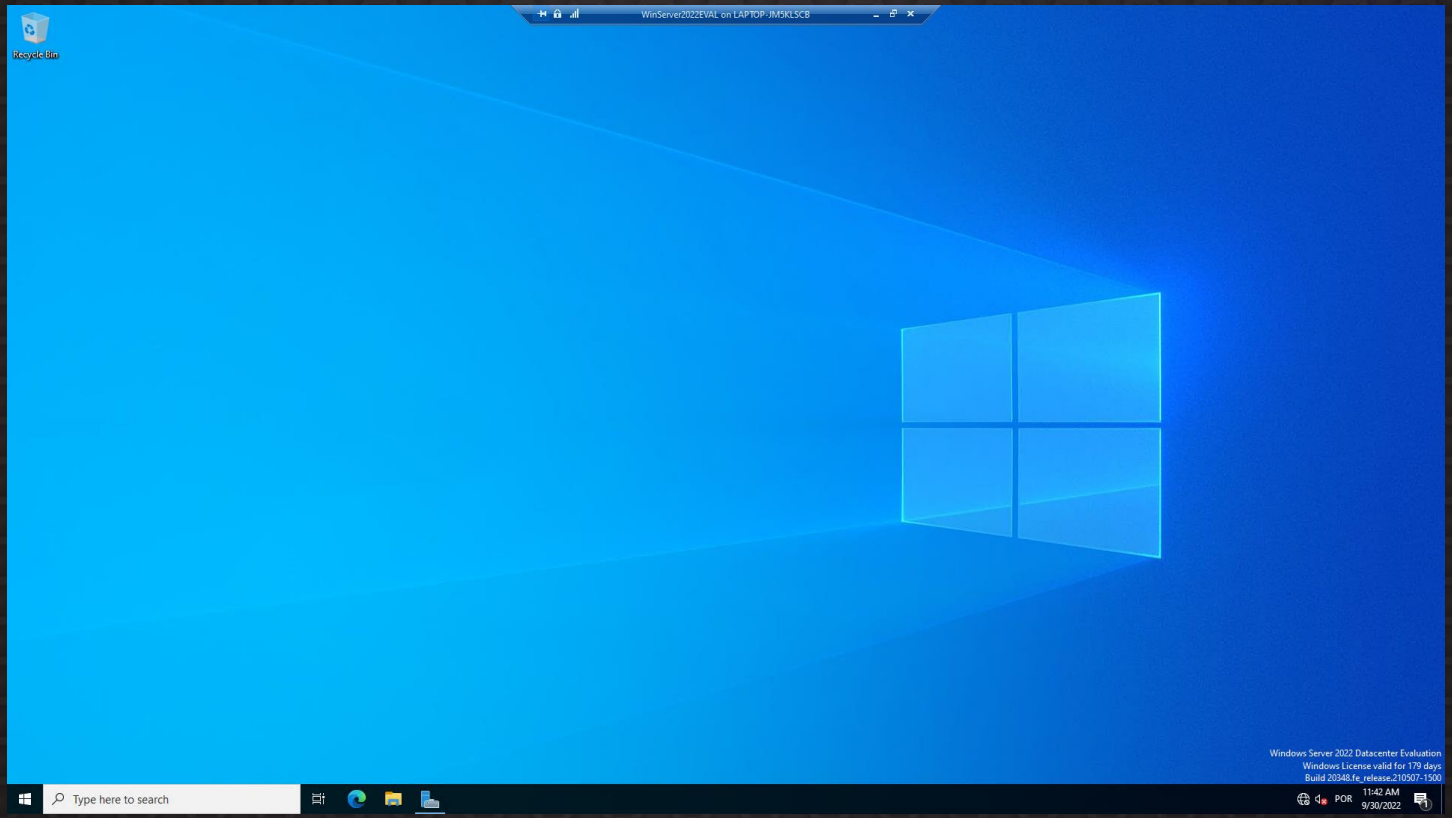
MDT *Microsoft Deployment Toolkit*

- Fornece ferramentas que auxiliam durante uma migração, automatizando algumas tarefas.

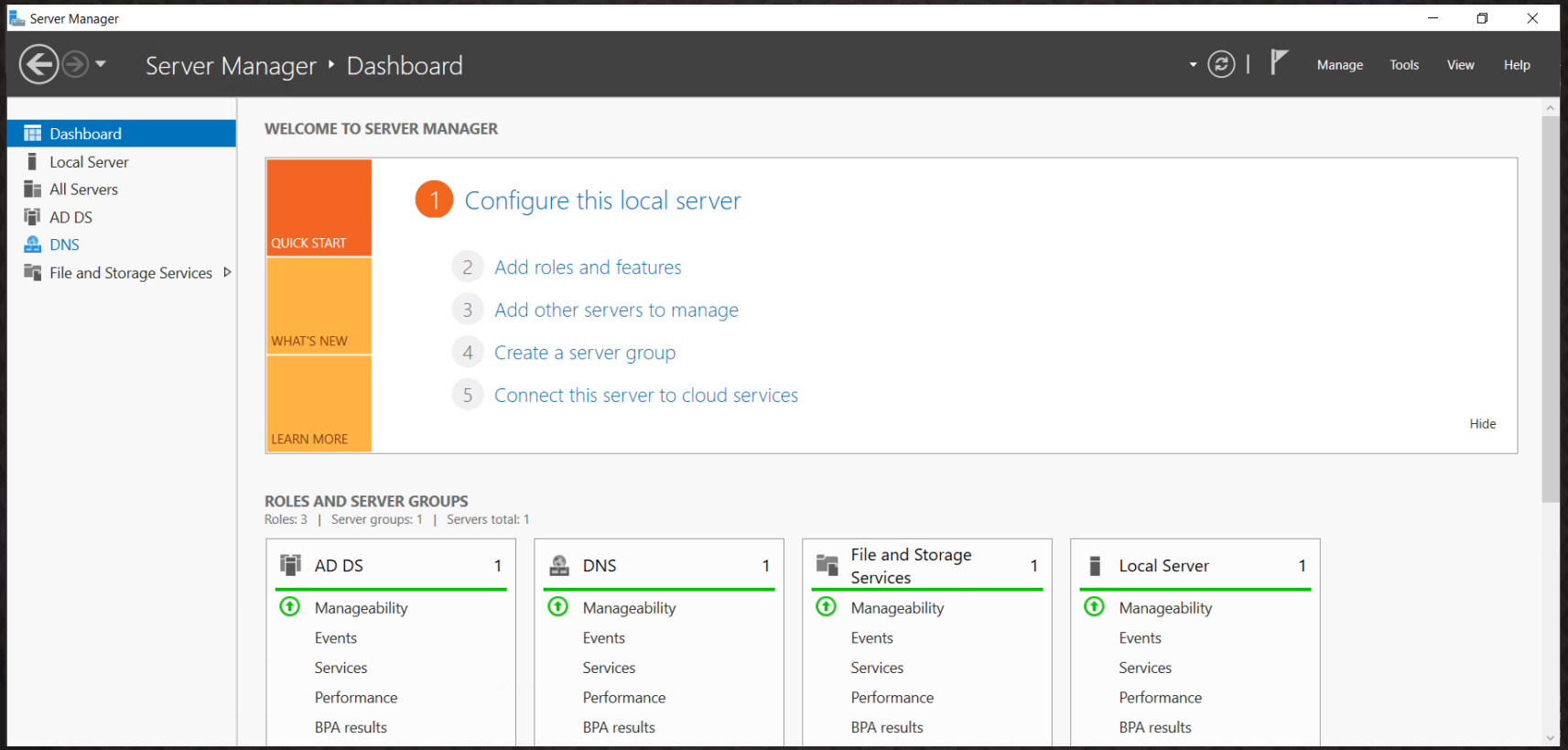
Um produto Microsoft

Atualmente o Windows Server (desde a versão 2019) adotou o modelo de atualização LTSC igual ao Windows 10 e 11, no qual há atualizações e serão reduzidas as mudanças de versões (exemplo versão 21H2 – *2021 segundo semestre*).

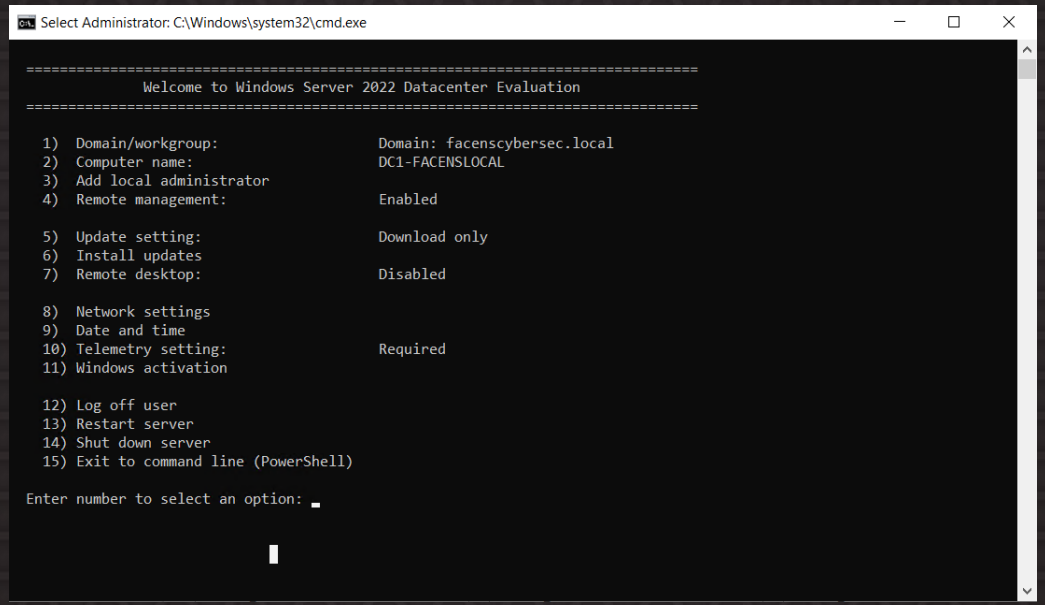
Um produto Microsoft



Um produto Microsoft



Um produto Microsoft



03 Instalação

Atividade prática

Requisitos Mínimos

64bits

Arquitetura

1,4GHz

Velocidade

512MB

RAM

*800MB Durante a Instalação

32GB

Armazenamento

Roteiro de Instalação

Criar VM

Respeitando os Requisitos Mínimos

Instalar a .ISO

Escolha sua versão em Windows Insider

Configurar

Configurações Pós-Instalação

Configuração Pós-Instalação

Renomear Computador

- SRVXX-Função

Alterar Data e Hora do Sistema

- Configurar horário local

Definir Endereço IPv4

- Mascara de SubRede
- Gatway Padrão
- Excluir IPv6

04 Active Directory

Domain
Domain Controller
Active Directory
Estrutura hierárquica (Florestas, árvores, domínios e OU's)
Functional Level

Domínio (*Domain*)

Um domínio é....

- A identificação de autonomia administrativa, autoridade ou controle dentro da internet.
- “Um domínio contém os componentes lógicos para atingir um determinado objetivo administrativo”
- “Limites de segurança para os objetos dentro dele”

Exemplos

- “facens.br”
- “microsoft.com”
- “gov.br”

Todos acima são domínios primários.

O “.com” e “.br” são top-level domains (ou, sufixos de domínios).

Domain Controller

- Servidor que armazena o Active Directory;
- Servidor que responde os pedidos de autenticação em um domínio Windows - *login*.

- Acrônimo DC;

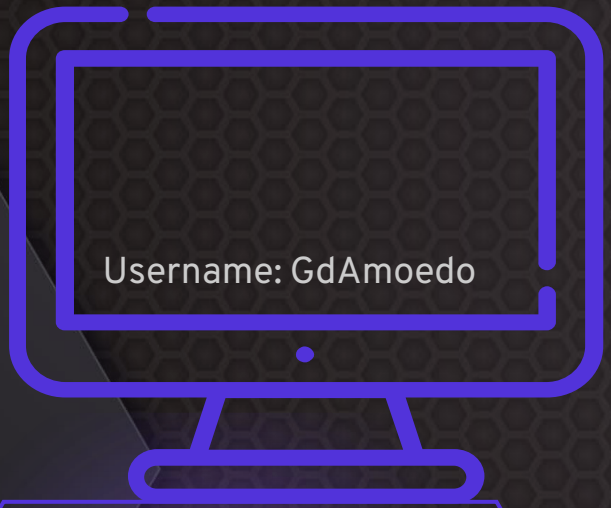
Active Directory

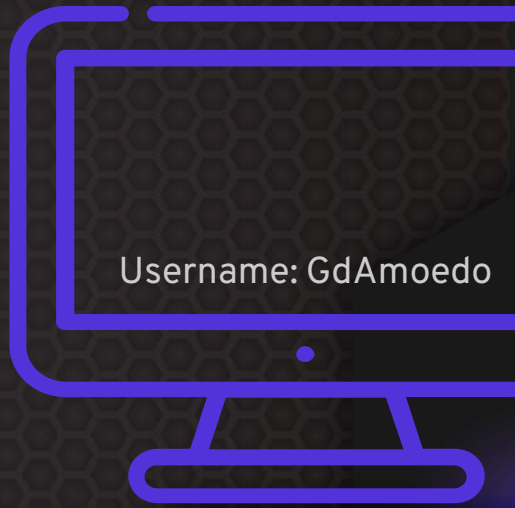
- *Plataforma onde se constrói uma estrutura hierárquica para armazenar objetos tais como nomes de usuários, senhas e contas.*
- O AD armazena uma base de dados com informações que serão utilizadas para garantir a autenticação dentro de uma rede.
- Uma vez autenticado, vários programas podem usar o mesmo token de autenticação daquele usuário.
- O Active Directory usa um armazenamento de **dados estruturado** como base para uma **organização lógica** e hierárquica de informações de diretório.

Active Directory

- Autenticação
- Autorização
- Alta Disponibilidade
- SSO Single Sign-on
- Auditável
- Não repúdio

Active Directory





Nem sempre uma “identidade digital” representa uma pessoa!

Catálogo Global

Localização

O servidor localiza objetos, tais como usuários e pastas, sempre que a pesquisa é realizada pro usuários.

Autenticação

O servidor valida o nome principal do usuário, para garantir o acesso a serviços apenas a contas autorizadas.

Validação

O catálogo global é utilizado por controladores para validar as referências a objetos de outros domínios na floresta.

Fonte: Microsoft Learn. Disponível em: https://learn.microsoft.com/pt-br/windows/win32/ad/global-catalog?source=recommendations

Active Directory

- **Active Directory é uma solução Microsoft!**
- Alternativas são:
  - Oracle Directory Service
  - Red Hat Directory Service
  - Novell Directory Services

Microsoft
Active Directory

Estrutura Hierárquica

Florestas

- Instância completa de um Active Directory
- Domínio de maior nível hierárquico

- “Não se pode ter um domínio com nível hierárquico mais alto que de uma floresta”

Árvores (...*de domínios*...)

- Coleção de domínios organizados dentro de uma floresta.

- Exemplo: Escritórios regionais.

Estrutura Hierárquica

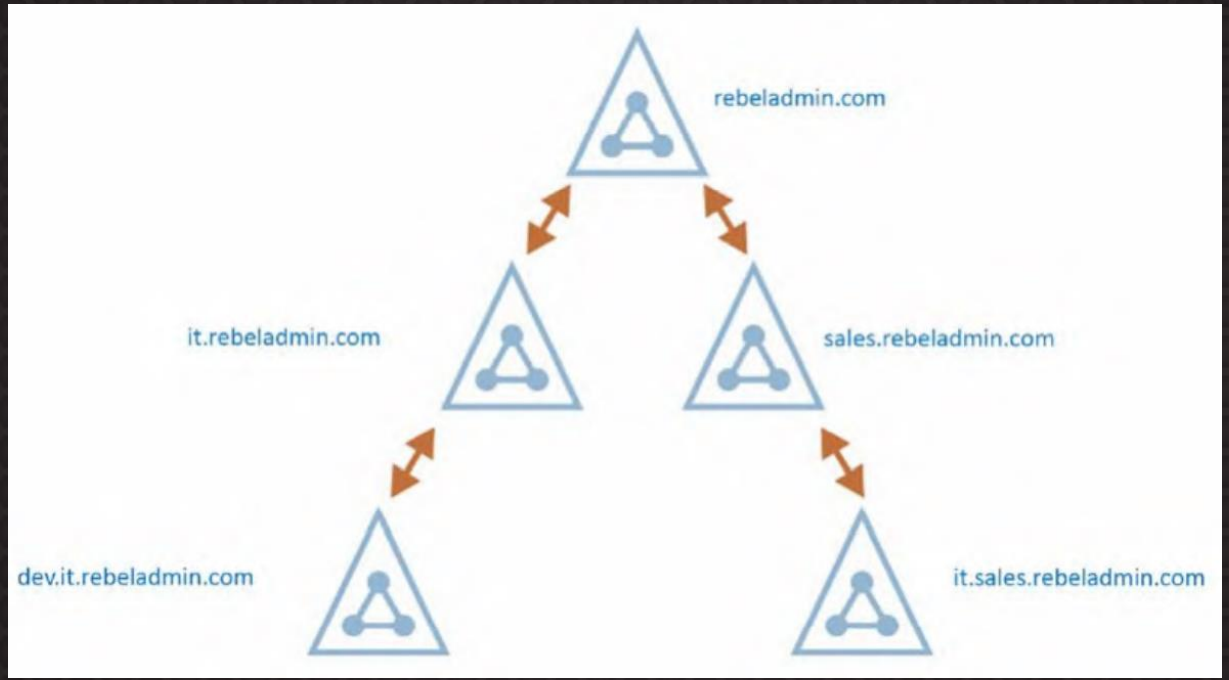
Domínios pais e filhos

- Relação de um domínio (filho) pertencente ao domínio de nível hierárquico maior (pai).
- Exemplo:
  - Pai: microsoft.com
  - Filho: docs.microsoft.com

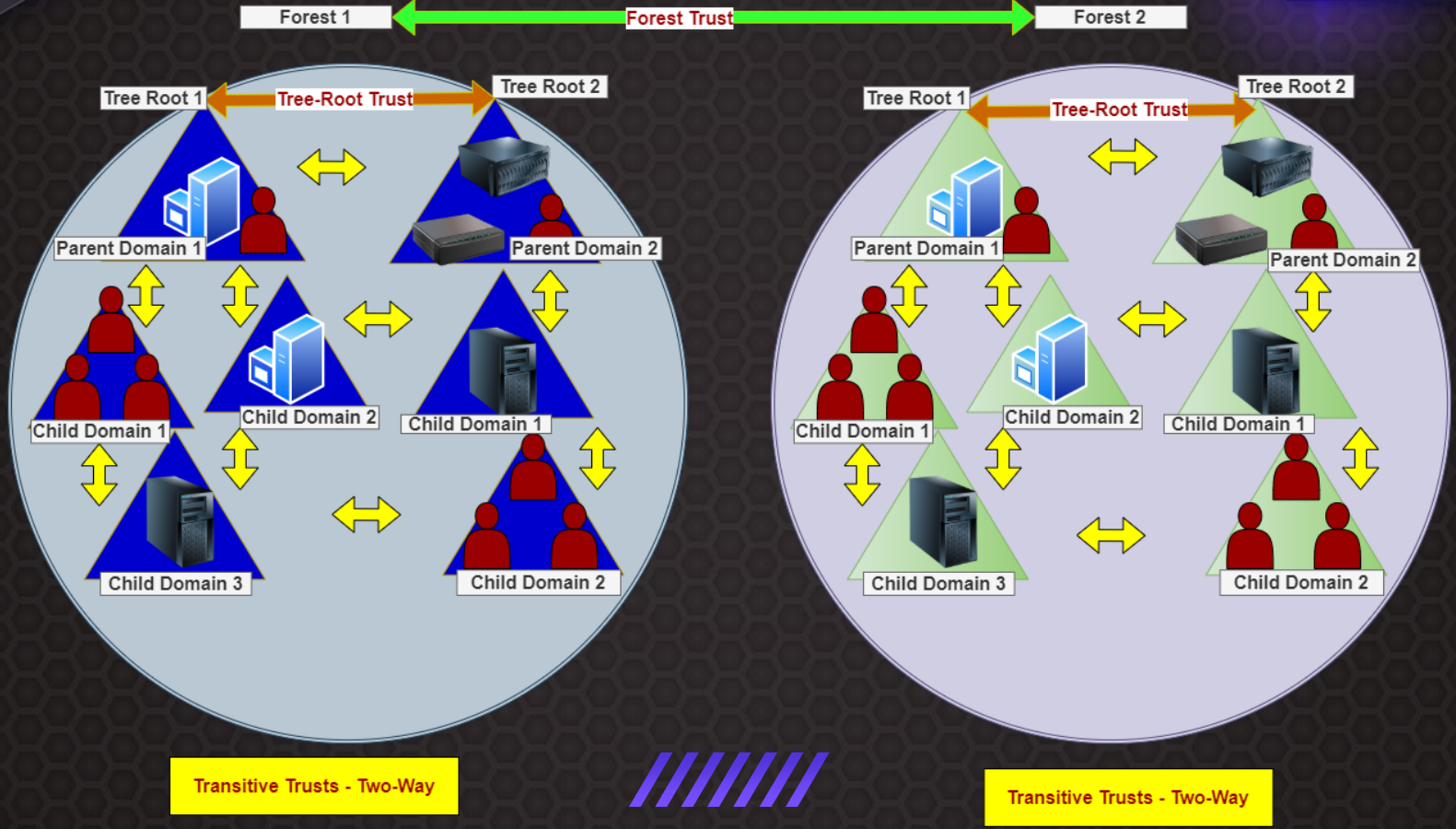
Organizational Unities (OU)

- Uma vez dentro da OU, o objeto herda todas as configurações de segurança da OU.

Estrutura Hierárquica



Estrutura Hierárquica



Functional Level

Functional Level	Domain Controller Operating System
Windows Server 2016	Windows Server 2022 Windows Server 2019 Windows Server 2016
Windows Server 2012R2	Windows Server 2022 Windows Server 2019 Windows Server 2016 Windows Server 2012 R2
Windows Server 2012	Windows Server 2022 Windows Server 2019 Windows Server 2016 Windows Server 2012 R2 Windows Server 2012

Functional Level	Domain Controller Operating System
Windows Server 2008R2	Windows Server 2022 Windows Server 2019 Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2
Windows Server 2008	Windows Server 2022 Windows Server 2019 Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 Windows Server 2008

Relações de Confiança

Transitividade

- http://marceloti.pe.hu/relacoes-de-confianca-active-directory/

Bidirecional

Unidirecional

05 Configuração AD DS

Atividade prática

06 DNS

Fundamentos de DNS
Tipos de serviço DNS
Como o DNS direciona o tráfego para a sua aplicação web?

Fundamentos do DNS

O DNS (Domain Name System – Sistema de nome de domínio) converte nomes de domínio legíveis por humanos (por exemplo, servidor.local) em endereços IP legíveis por máquina (por exemplo, 192.168.0.10).

Tipos de serviço DNS

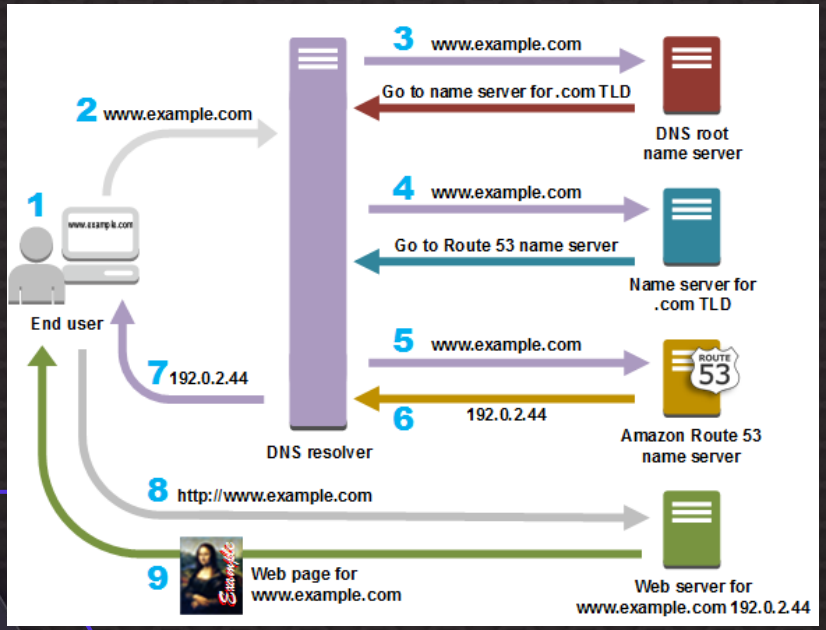
DNS autoritativo:

Responde a consultas do DNS, convertendo nomes de domínio em endereço IP.

DNS recursivo (DNS Resolver):

Atua como um intermediário que pode obter informações de DNS.

Como o DNS direciona o tráfego para a sua aplicação web?



07 DHCP

Por que usar DHCP?
Protocolo Cliente Servidor
Endereço IP
Máscara de sub-rede
Gateway padrão

Por que usar o DHCP?

Configuração Automática de IP

Incluindo máscara de sub-rede, gateway padrão e servidores de DNS. Imagina fazer isso manualmente.

Concessão e Recuperação automática

Recuperação automática dos endereços IP de computadores removidos da rede.

Manutenção e reserva de IPs

- IP Reservado a clientes DHCP específicos. Isso permite a atribuição de um único endereço IP por cliente DHCP.

Benefícios do DHCP

Configuração de endereço IP confiável.

O DHCP minimiza os erros de configuração causados pela configuração manual de endereço IP.

Administração de rede reduzida.

- Configuração TCP/IP centralizada e automatizada.
- A capacidade de definir configurações de TCP/IP de um local central.
- A capacidade de atribuir um intervalo completo de valores de configuração TCP/IP adicionais por meio de opções DHCP.
- Etc.

Mais informações

DHCPDISCOVER

DHCPOFFER

DHCPREQUEST

DHCPACK

Source MAC addr	Dest MAC addr	Source IP addr	Dest IP addr	Packet Description
Client	Broadcast	0.0.0.0	255.255.255.255	DHCP Discover
DHCPsrvr	Broadcast	DHCPsrvr	255.255.255.255	DHCP Offer
Client	Broadcast	0.0.0.0	255.255.255.255	DHCP Request
DHCPsrvr	Broadcast	DHCPsrvr	255.255.255.255	DHCP ACK

08 GPMC

Objetos e OUs
Políticas de Grupo

Objetos e OUs

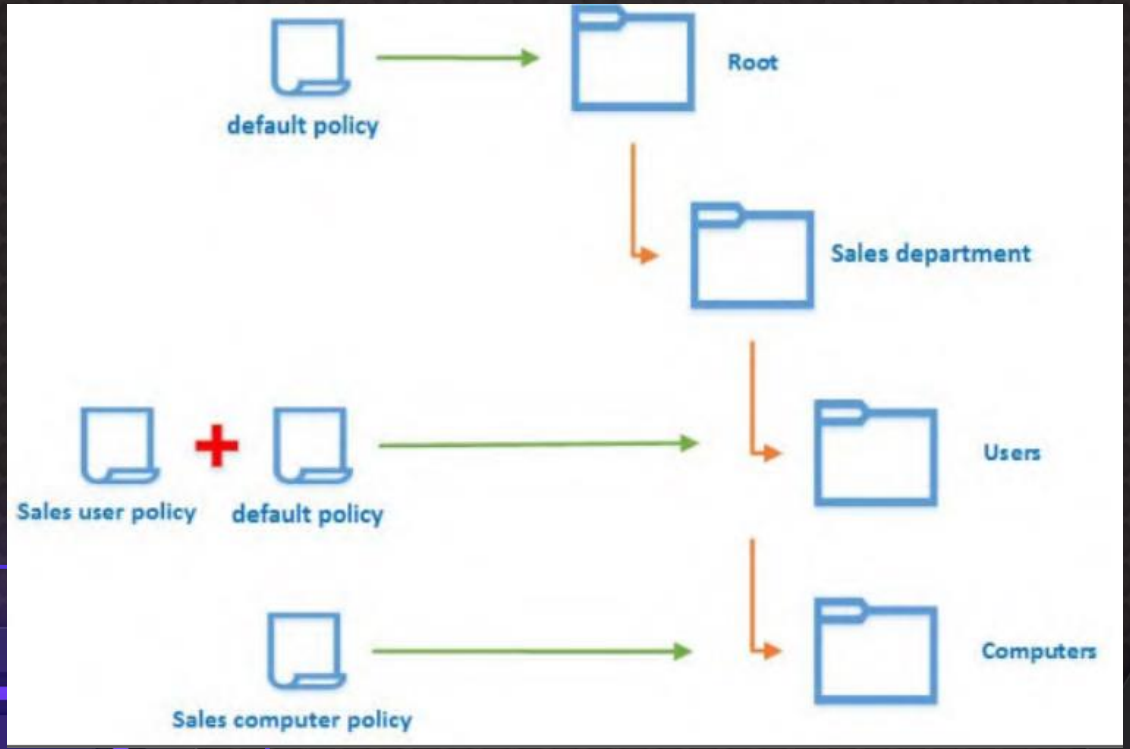
OU

- Container de usuários, grupos e computadores.
- Herda todas as configurações de segurança

Objetos

- Usuários
- Grupos de usuários
- Computadores

Objetos e OUs



Objetos e OU's

Atividade prática

- Configurar uma estrutura OU
- Configurar um usuário
- Logar em uma máquina cliente com a conta criada

Group Policy Management Console

Aplicando políticas a grupos

- Com o GPMC é possível configurar políticas que atingiram usuários ou OU's.

Group Policy Management Console

Atividade prática

- Aplicar uma política a uma OU que tenha um usuário.

09 Segurança

Vulnerabilidades Conhecidadas

Vulnerabilidades Conhecidas

PrintSpooler / Print Nightmare

Windows Print Spooler Elevation of Privilege Vulnerability

CVE-2021-1675 / CVE-2021-34527

Similar porém Distinto

Softwares Afetados

cpe:2.3:o:microsoft:windows_server_2008:-:sp2:*:*:*:*:*:*:*

Show Matching CPE(s)

cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:x64:*

Show Matching CPE(s)

cpe:2.3:o:microsoft:windows_server_2012:-:*:*:*:*:*:*:*

Show Matching CPE(s)

cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:*:*

Show Matching CPE(s)

cpe:2.3:o:microsoft:windows_server_2016:-:*:*:*:*:*:*:*

Show Matching CPE(s)

cpe:2.3:o:microsoft:windows_server_2019:-:*:*:*:*:*:*:*

Show Matching CPE(s)

CVE-2021-1675

08/06/2021

- Microssoft solta nota de correção da vulnerabilidade

21/06/2021

- Microssoft muda a classificação para: RCE (Remote Code Executions)

xx/xx/2021

- Grupo de pesquisadores disponibiliza uma PoC (Proof of concept) explorando essa vulnerabilidade.

Resposta:

Desabilitar função:

- `> net stop spooler`

Desabilitar a inicialização:

- `> sc config spooler start=disabled`

Provas de Conceito (PoC)

Packet Storm Security

https://packetstormsecurity.com/files/167261/Print-Spooler-Remote-DLL-Injection.html

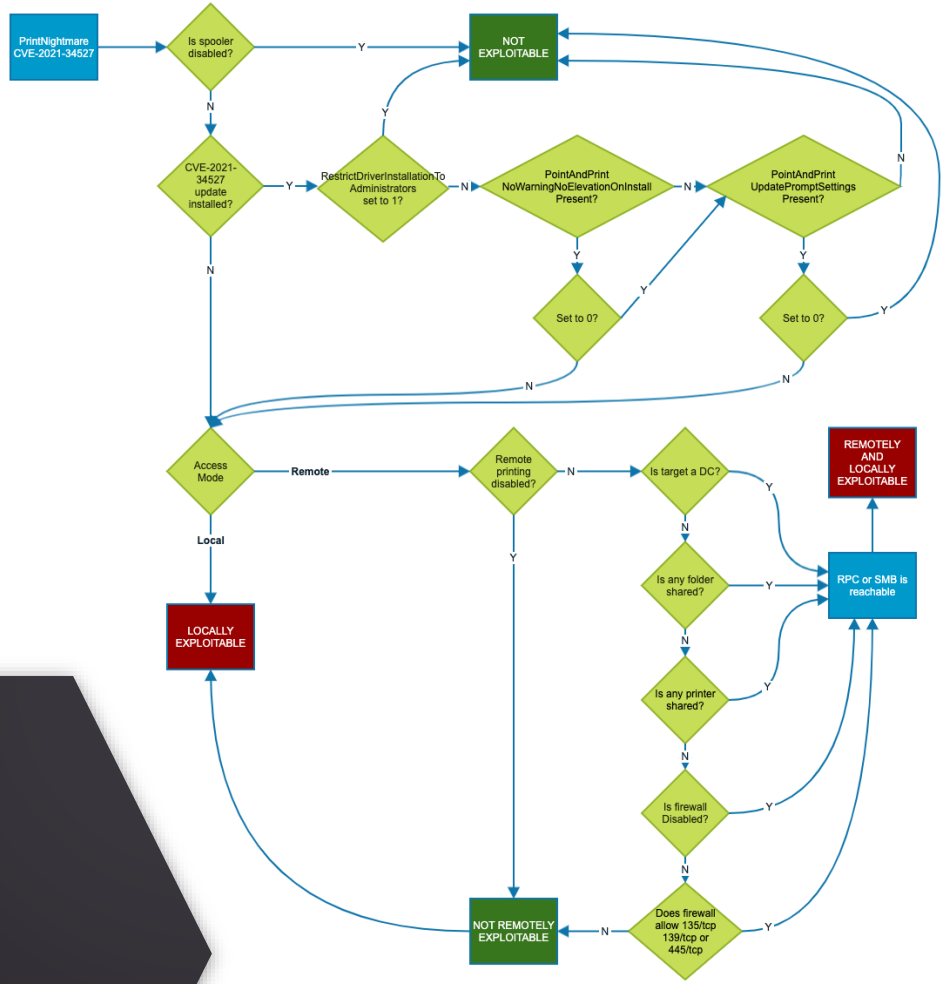
Carnegie Mellon University

https://www.kb.cert.org/vuls/id/383432

MSRC - Microsoft Security Response Center

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1675

Prova de Conceito (PoC)



Fim

Charles Neves Epifanio de Oliveira charles.oliveira@facens.br
Leonardo dos Reis Souza leonardo.souza@facens.br