Informações Gerais

**Sistema Operacional:** Microsoft Windows Server 2022 Standard

**Funções do Servidor:** Controlador de Domínio, DNS, DHCP, Arquivo, Impressão

Instalação do Windows Server

Language to install: English (United States)

Time and currency format: Portuguese (Brazil)

Keyboard or input method: ABNT2

Install Now

Instalar Windows Server 2022 Standard (Desktop Experience)

Custom: Install Microsoft Server Operating System only (advanced)

Particionar disco de acordo com a necessidade

Password: Xtr3m3!

Reenter password: Xtr3m3!

Configurações Iniciais

Abrir o Server Manager e clicar em Local Server

Computer name: srv-dc1

Remote management: Enable remote management of this server from other computers

Ethernet

IP: 172.20.10.10

Máscara de sub-rede: 255.255.255.0

Gateway: 172.20.10.254

DNS: 172.20.10.10

Desabilitar IPv6

IE Enhanced Security Configuration: Administrators: Off, Users: On

Time zone: (UTC-03:00) Brasilia

Product ID: Inserir a chave de ativação

Last checked for updates

UAC: Nunca notificar

System Properties (Windows Pause + Break)

Advanced, Performance: Adjust for best performance

Renomear conta de administrador para Thanos

Active Directory

Abrir o Server Manager, Manage, Add Roles and Features

Adicionar Função: Active Directory Domain Services

Promover este servidor a um controlador de domínio

Add a new forest: core.intra

Forest Functional Level: Windows Server 2016

Domain Functional Level: Windows Server 2016

DNS Server

Global Catalog

Senha Modo de Restauração dos Serviços de Diretório: Xtr3m3!

Nome NetBIOS: CORE

Depois de instalado o AD, o servidor irá reiniciar.

Será necessário trocar o endereço de DNS da placa de rede que está como 127.0.0.1 para 172.20.10.10

DNS

Abrir o Server Manager, Tools, DNS

Reverse Lookup Zones

New Zone

Primary Zone

Store the zone in Active Directory

To all DNS server running on domain controllers in this domain: core.intra

IPv4 Reverse Lookup Zone

172.20.10

Allow only secure dynamic updates

Forward Lookup Zones

core.intra

clicar com o botão direito do mouse em srv-dc1 e selecionar Properties

Marcar Update associated pointer (PTR) record

Clicar com o botão direito do mouse no Servidor srv-dc1 e depois clicar em Launch nslookup e verifique se aparece as informações do Default Server e do Address.

Clicar com o botão direito do mouse no Servidor srv-dc1 e depois clicar em Properties

Clique em Forwarders e insira os endereços abaixo:

1.1.1.1

8.8.8.8

208.67.222.222

1.0.0.1

8.8.4.4

Sites e Serviços

Abrir o Server Manager, Tools, Active Directory Sites and Services

Renomear Default-First-Site-Name para CORE

Clique com o botão direito do mouse em Subnets, New Subnet

Prefix: 172.20.10.0/24

Site Name: Core

Servidor DHCP

**Instalação**

Abrir o Server Manager, Manage, Add Roles and Features

Adicionar Função: DHCP Server

Marque a opção "Usar as seguintes credenciais do usuário"

Em Nome de usuário digite Core\Thanos

**Configuração**

Abrir o Server Manager, Tools, DHCP

Clique com o botão direito em IPv4 e selecione a opção New Scope

Nome do Escopo: SYSTEM-CORE

Descrição: Rede Corporativa da System Core

Start IP address: 172.20.10.100

End IP address: 172.20.10.200

Subnet mask: 255.255.255.0

Lease Duration: 8 dias

Gateway: 172.20.10.254

Parent domain: core.intra

DNS: 172.20.10.10

Arquivos, Pastas e Scripts

Copiar a pasta Scripts para C:\ do servidor srv-dc1

Copiar a pasta PolicyDefinitions para C:\Windows do servidor srv-dc1

Copiar a pasta core para \\core.intra\netlogon

Copiar a pasta GPO para C:\ do servidor srv-dc1

Populando o Active Directory

Executar o script 01-cria\_ou.bat em C:\Scripts\01-ou para criação da estrutura de Unidades Organizacionais

Executar o script cria\_usuarios.bat em C:\Scripts\02-users para criação dos usuários

Executar o script cria\_grupos\_ad.cmd em C:\Scripts\03-groups para criação dos grupos

Executar no Powershell o script adiciona-usuario-a-grupo.ps1 em C:\Scripts\03-groups para adicionar os usuários aos grupos correspondentes

Servidor de Arquivos

**Instalação de Role para o File Server**

Abra o Server Manager

Clique em Manage

Add Roles and Features

Next

Next

Next

File and Storage Services

File and iSCSI Services

File Server Resource Manager

Next

Next

Install

**Criação do RAID 5**

Pressionar as teclas Winkey + R e digitar diskmgmt.msc

Clicar com o botão direito do mouse e clicar em New RAID-5 volume

Selecionar 3 discos

Alocar todo o espaço disponível.

Formatar como NTFS e colocar o nome do Volume como Dados e atribuir a letra F:

para o novo volume

Aguardar a sincronização dos discos

**Removendo Herança do Volume**

Clique com o botão direito na unidade F: e clique em Properties

Clique em Security e depois em Edit...

Remova os grupos Users and Everyone para não precisar quebrar herança em todos

os diretórios filhos

Executar o script pastas.ps1 no Powershell localizado em C:\Scripts\04-file-server para executar as seguintes tarefas:

Criação e compartilhamento das pastas

Dar permissão nas pastas para os devidos grupos

**Pasta Base**

O diretório já foi criado com o Script pastas.ps1

**Atribuindo Permissões de Segurança**

Clique com o botão direito do mouse no diretório Home e clique em Properties

Clique na aba Security

Clique em Advanced

Na aba Permissions, clique em ADD

Selecione domain users

Em Applies to: This folder only

Basic permissions: Modify

No AD, vá até a OU core.intra/CORE/USERS e depois entre na OU de cada departamento e selecione todos os usuários

Clique com o botão direito e selecione Properties

Clique na aba Profile

Clique em Home Folder

Selecione Connect, escolha a unidade Z:

Digite \\srv-dc1\home$\%username%

**Enumeração**

Abra o Server Manager

Clique em File and Storage Services

Clique em Shares

Selecione o compartilhamento HOME$ e clique com o botão direito do mouse em Properties

Clique em Settings

Selecione a opção Enable access-based enumeration

**Cotas de Disco**

Abra o Server Manager

Clique em Tools

File Server Resource Manager

**Quota Management**

Quota Templates

Create Quota Template

Template Name: 10MB

Description: Cota de 10MB

Limit: 10MB

Hard quota: Do not allow users to exceed limit

**Cota em Pasta**

Quotas

Create Quota

Quota path: F:\Financeiro, F:\Marketing, F:\Publica, F:\RH, F:\Tecnologia, F:\Vendas

Create quota on path

Derive properties from this quota template (recommended):

10MB

Create

**Aplicar Cota na Pasta Base**

Quotas

Create Quota

Quota path: F:\HOME

Auto apply template and create quotas on existing and new subfolders

Derive properties from this quota template (recommended):

10MB

Create

**Triagem**

Executar script Prevent Ransomware.ps1 localizado em C:\Scripts\04-file-server para criar file group

Obs: Este script baixa da internet as principais extensões utilizadas pelos Ransomwares e é atualizado constantemente.

Criar Tarefa agendada para atualizar a lista

**File Screen Templates**

Create File Screen Template

Template name: Bloqueio-de-Ransomware

Active screening: Do not allow users to save unauthorized Files

File groups: Anti-Ransomware File Groups

**File Screens**

Create File Screens

File Screen path: F:\

Derive properties from this file screen template (recommended): Bloqueio-de-Ransomware

Create

**Auditoria de Exclusão de arquivos e pastas**

Clique com o botão direito do mouse nas seguintes pastas F:\Financeiro, F:\Marketing, F:\Publica, F:\RH, F:\Tecnologia, F:\Vendas

e selecione Properties

Clique na aba Auditing e depois em ADD

Principal: Domain Users

Type: Success

Applies to: This folder, subfolders and files

Show Advanced permissions

Deixe marcado somente as opções:

Delete subfolders attributes

Delete

Testar melhor, achei que não funcionou corretamente

GPO

**GPO-COMP-MOTD**

GPO Status: User configuration settings disabled

Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/Security Options

Interactive logon: Message text for users attempting to log on: Este sistema é restrito a usuários autorizados.

Os indivíduos que tentarem acesso não autorizado poderão ser processados.

Se você não estiver autorizado, termine o acesso agora.

Clique em OK para indicar que aceita estas informações.

Interactive logon: Message title for users attempting to log on: Bem-vindo a Rede Corporativa da System Core

**GPO-COMP-ENERGIA**

GPO Status: User configuration settings disabled

Computer Configuration/Preferences/Control Panel Settings/Power Options/

New, Power Plan (At least Windows 7)

Action: Update

High performance

Set as the active power plan

When computer is: Plugged in Running on batteries

Require a password on wakeup: Yes Yes

Turn off hard disk after: Never Never

Sleep after: Never Never

Allow hybrid sleep: Off Off

Hibernate after: Never Never

Lid close action: Do nothing Do nothing

Power button action: Shutdown Shutdown

Start menu power button: Do nothing Do nothing

Link State Power Management: Off Off

Minimum processor state: 100% 5%

Maximum processor state: 100% 100%

Turn off display after: 15 5

Adaptive display: On On

Critical battery action: Do nothing Shutdown

Low battery level: 10 10

Critical battery level: 5 5

Low battery notification: Off Off

Low battery action: Do nothing Do nothing

**GPO-COMP-FIREWALL**

GPO Status: User configuration settings disabled

Computer Configuration/Policies/Windows Settings/Security Settings/Windows Firewall with Advanced Security

Properties

Domain Profile

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Private Profile

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Public Profile

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Inbound Rules, New Rule

Custom, Next

All Programs, Next

Protcol type: ICMPv4, Next

Next

Allow the connection, Next

Domain, Next

Name: PERMITE-PING

Description: PERMITE-PING, Finish

**GPO-COMP-BLOQUEIA-MIDIA-REMOVIVEL**

GPO Status: User configuration settings disabled

Computer Configuration/Policies/Administrative Templates/System/Removable Storage Access

All Removable Storage classes: Deny all access: Enabled

**GPO-COMP-REMOTE-DESKTOP**

GPO Status: User configuration settings disabled

Computer Configuration/Preferences/Control Panel Settings/Local Users and Groups

New Local Group

Action Update

Group Name: Remote Desktop Users (built-in)

Add

G-CORE-TI-REMOTE-DESKTOP

Computer Configuration/Policies/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Session Host/Connections

Allow users to connect remotely by using Remote Desktop Services: Enabled

Computer Configuration/Policies/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Session Host/Security

Require user authentication for remote connections by using Network-level authentication: Enabled

**GPO-COMP-DESABILITA-IPV6**

GPO Status: User configuration settings disabled

Computer Configuration/Preferences/Windows Settings/Registry/

Action: Update

Hive: HKEY\_LOCAL\_MACHINE

Key path: System\CurrentControlSet\Services\Tcpip6\Parameters

Value name: DisabledComponents

Value type: REG\_DWORD

Value data: 0xFF

**GPO-COMP-CERT-FIREFOX**

GPO Status: User configuration settings disabled

Computer Configuration/Preferences/Windows Settings/Files

Action: Update

Source file(s): \\core.intra\netlogon\core\umbrella.cfg

Destination file C:\Program Files\Mozilla Firefox\umbrella.cfg

Action: Update

Source file(s): \\core.intra\netlogon\core\umbrella.cfg

Destination file C:\Program Files (x86)\Mozilla Firefox\defaults\pref\local-settings.js

Action: Update

Source file(s): \\core.intra\netlogon\core\local-settings.js

Destination file C:\Program Files\Mozilla Firefox\defaults\pref\local-settings.js

Action: Update

Source file(s): \\core.intra\netlogon\core\local-settings.js

Destination file C:\Program Files (x86)\Mozilla Firefox\defaults\pref\local-settings.js

**GPO-USERS-NAVEGADORES**

GPO Status: Computer configuration settings disabled

Edge

User Configuration/Policies/Administrative Templates/Microsoft Edge

Microsoft Edge/Startup, home page and new tab page

Configure the home page URL: Enabled

Home page URL: http://www.uol.com.br

Show Home button on toolbar: Enabled

Action to take on startup: Enabled

Open a list of URLs

Sites to open when the browser starts

Value: http://www.uol.com.br

Set the new tab page as the home page: Enabled

Configure the new tab page URL: Enabled

New tab page URL: http://www.uol.com.br

Firefox

User Configuration/Policies/Administrative Templates/Mozilla/Firefox/Home page

URL for Home page: Enabled

URL: http://www.uol.com.br

Don't allow the homepage to be changed

Show Home button on toolbar: Enabled

Start Page: Enabled

Homepage (Locked)

Chrome

User Configuration/Policies/Administrative Templates/Google/Google Chrome

Startup, home page and new tab page

Action on startup: Enabled

Open a list of URLs

URLs to open on startup: Enabled

Show: http://www.uol.com.br

Show Home button on toolbar: Enabled

Configure the home page URL: Enabled

Home page URL: http://www.uol.com.br

Use New Tab Page as homepage: Disabled

**GPO-USERS-PROXY**

GPO Status: Computer configuration settings disabled

IE

User Configuration/Preferences/Control Panel Settings/Internet Settings

New

Internet Explorer 10

Connections

LAN Settings

Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 172.20.10.254 Port: 3128

Bypass proxy server for local addresses

Firefox

User Configuration/Policies/Administrative Templates/Mozilla/Firefox/Proxy Settings

Don't allow proxy settings to be changed: Enabled

Connection Type: Manual proxy configuration

HTTP Proxy: 172.20.10.254:3128

Use this proxy server for all protocols: Enabled

SOCKS Version: SOCKS v5

No proxy for: 172.20.10.0/24, .core.intra

Evitar alterações nas configurações de Proxy

User Configuration/Policies/Administrative Templates/Windows Components/Internet Explorer

Prevent changing proxy settings: Enabled

**GPO-COMP-AVISO-TROCA-DE-SENHA**

GPO Status: User configuration settings disabled

Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/Security Options

Interactive logon: Prompt user to change password before expiration

Define this policy setting

Begin prompting this many days before passwords expires: 90 days

**GPO-COMP-COPIA-ARQUIVOS**

GPO Status: User configuration settings disabled

Computer Configuration/Preferences/Windows Settings/Folders

Action: Update

Path: C:\TI

Computer Configuration/Preferences/Windows Settings/Files

Action: Update

Source file(s): \\core.intra\NETLOGON\core\Bginfo.exe

Destination File: C:\TI\Bginfo.exe

Action: Update

Source file(s): \\core.intra\NETLOGON\core\desktops.bgi

Destination File: C:\TI\desktops.bgi

Action: Update

Source file(s): \\core.intra\NETLOGON\core\logo1.jpg

Destination File: C:\TI\logo1.jpg

Action: Update

Source file(s): \\core.intra\NETLOGON\core\logon-desktop.vbs

Destination File: C:\TI\logon-desktop.vbs

**GPO-USERS-BGINFO-DESKTOPS**

GPO Status: Computer User configuration settings disabled

User Configuration/Policies/Windows Settings/Scripts/Logon

Add

Script Name: C:\TI\logon-desktop.vbs

**GPO-USERS-BGINFO-SERVERS**

GPO Status: Computer User configuration settings disabled

User Configuration/Policies/Windows Settings/Scripts/Logon

Add

Script Name: C:\TI\logon-server.vbs

**Default Domain Policy**

Computer Configuration/Policies/Windows Settings/Security Settings/Account Policies/Password Policy

Enforce password history 10 passwords remembered

Maximum password age 90 days

Minimum password age 7 days

Minimum password length 7 characters

Password must meet complexity requirements Enabled

Store passwords using reversible encryption Disabled

**GPO-COMP-POWERSHELL-EXECUTION-POLICY**

GPO Status: User configuration settings disabled

Computer Configuration/Policies/Administrative Templates/Windows Components/Windows PowerShell

Turn on script execution: Enabled

Execution Policy: Allow all scripts

**GPO-COMP-FIREFOX-PADRAO**

GPO Status: User configuration settings disabled

Computer Configuration/Policies/Administrative Templates/Windows Components/File Explorer/

Set a default associations configuration file: Enabled

Default associations configuration file: \\core.intra\netlogon\core\firefox.xml

**GPO-USERS-MOSTRA-EXTENSAO-DE-ARQUIVO**

GPO Status: Computer configuration settings disabled

User Configuration/Preferences/Control Panel Settings/Folder Options

New

Folder Options (At least Windows Vista)

Desmarcar Hide extensions for known file types

**GPO-USERS-REGISTRA-LOGON-LOGOFF**

GPO Status: Computer configuration settings disabled

User Configuration/Policies/Windows Settings/Scripts/Logon

\\core.intra\netlogon\core\logon.exe

User Configuration/Policies/Windows Settings/Scripts/Logoff

\\core.intra\netlogon\core\logoff.exe

GPO para Configuração de NTP nos Clientes

WMI Filters, New

Name: LOCALIZA-PDC

ADD

Query: Select \* from Win32\_ComputerSystem where DomainRole = 5

OK

**GPO-SRV-NTP**

Details: This GPO is linked to the following WMI filter:

LOCALIZA-PDC

GPO Status: User configuration settings disabled

Computer Configuration/Policies/Administrative Templates/System/Windows Time Service/Time Providers

Configure Windows NTP Client: Enabled

NtpServer a.st1.ntp.br,0x9 b.st1.ntp.br,0x9 c.st1.ntp.br,0x9

Type NT5DS

CrossSiteSyncFlags 2

ResolvePeerBackoffMinutes 15

ResolvePeerBackoffMaxTimes 7

SpecialPollInterval 1024

EventLogFlags 0

Enable Windows NTP Client: Enabled

Aplicar na OU Domain Controllers

**GPO-COMP-VNC**

GPO Status: User configuration settings disabled

Computer Configuration/Policies/Windows Settings/Scripts/Startup

\\core.intra\netlogon\core\ultravnc.exe

Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/Security Options

User Account Control: Detect application installations and prompt for elevation: Disabled

User Account Control: Run all administrators in Admin Approval Mode: Disabled

User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode: Elevate without prompting

**GPO-COMP-AUDITORIA**

GPO Status: User configuration settings disabled

Computer Configuration/Policies/Windows Settings/Security Settings/ Local Policies/Audit Policy

Audit object access: Success, Failure

Para restaurar as GPOs executar o script restaura-gpo.ps1 localizado em C:\GPO

\*\*\*Precisa validar

Servidor de Impressão

IMP-FINANCEIRO-001

IP: 172.20.10.201

IMP-MARKETING-001

IP: 172.20.10.202

IMP-RH-001

IP: 172.20.10.203

IMP-TI-001

IP: 172.20.10.204

IMP-VENDAS-001

IP: 172.20.10.205