Sprint 2 (Sprint C)

ASIST

Turma 3DJ _ Grupo 57
1190903 _ Miguel Gonçalves
1191018 _ Rúben Rodrigues
1191042 _ Rui Pinto
1191106 _ Tomás Limbado

Data: 23/1/2022

Índice

US1

Como administrador da infraestrutura quero que seja criada uma SAN iSCSI nos servidores Linux e Windows disponíveis para qualquer utilizador autenticado

US2

Como administrador da infraestrutura quero que a SAN anterior esteja disponível sem necessidade de intervenção humana após um reboot de qualquer dos servidores

Nestes requisitos, é pedido a criação de uma SAN iSCSI nos servidores Windows e Linux, por isso apresentamos uma solução tendo como target a VM Linux e como initiator a VM Windows

Linux – configuração target

Para a concretização deste requisito foram seguidos os seguintes passos

Instalou-se o servidor iSCSI:

```
root@asist:~# apt install tgt
```

Criou-se um diretório onde irão estar os blocos dos ficheiros:

```
root@asist:~# mkdir -pv /iscsi/blocks
mkdir: pasta '/iscsi' criada
mkdir: pasta '/iscsi/blocks' criada
```

Criou-se um novo bloco no diretório anterior:

```
root@asist:~# dd if=/dev/zero of=/iscsi/blocks/www.img bs=1M count=1024 status=progress
```

Criou-se um novo ficheiro de configuração do target:

```
root@asist:~# nano /etc/tgt/conf.d/iscsi.conf
```

```
  GNU nano 5.4                          /etc/tgt/conf.d/iscsi.conf
<target iqn.2015-10.org.debian:uvm057.dei.isep.ipp.ptTgt>
        backing-store /iscsi/blocks/www.img
        initiator-name iqn.2015-11.com.microsoft:wvm057.dei.isep.ipp.pt
        incominguser asist Asist2122
</target>
```

Reiniciou-se o serviço iSCSI:

```
root@asist:~# systemctl restart tgt
```

Verificou-se o estado:

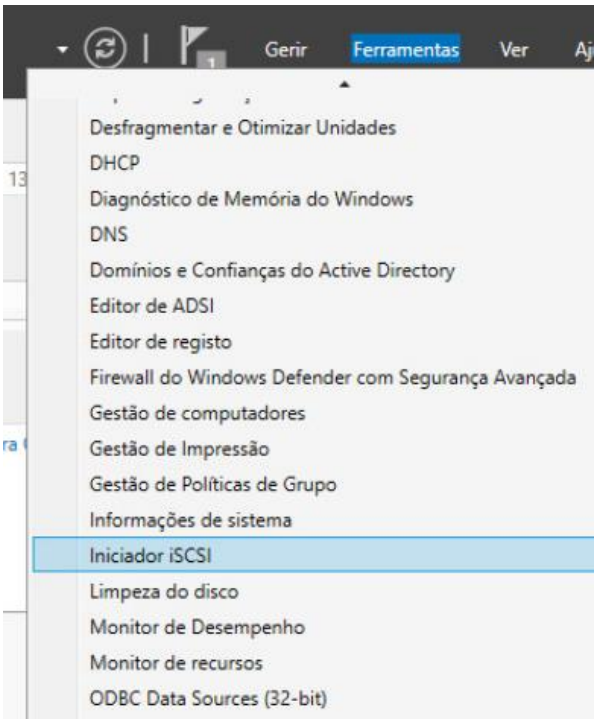
```
root@asist:~# systemctl status tgt
● tgt.service - (i)SCSI target daemon
     Loaded: loaded (/lib/systemd/system/tgt.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2022-01-19 18:01:23 WET; 1min 40s ago
```

Verificou-se que a porta 3260 está aberta para permitir acesso à SAN iSCSI

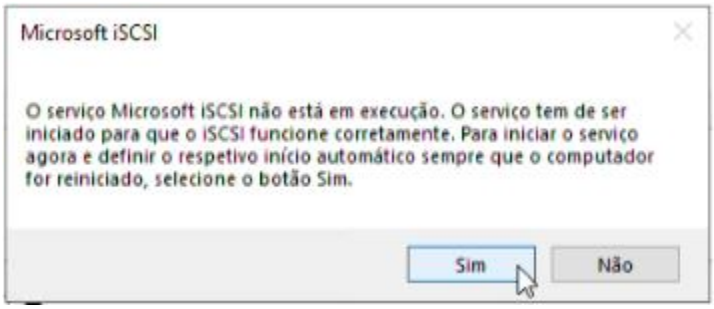
```
root@asist:~# netstat -tlpn
Conexões Internet Ativas (sem os servidores)
Proto Recv-Q Send-Q Endereço Local           Endereço Remoto         Estado      PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               OUÇA        536/sshd: /usr/sbin
tcp        0      0 0.0.0.0:3260            0.0.0.0:*               OUÇA        30480/tgtd
tcp6       0      0 :::22                   :::*                    OUÇA        536/sshd: /usr/sbin
tcp6       0      0 :::3260                 :::*                    OUÇA        30480/tgtd
```

Windows – configuração initiator
Para a concretização deste requisito foram seguidos os seguintes passos

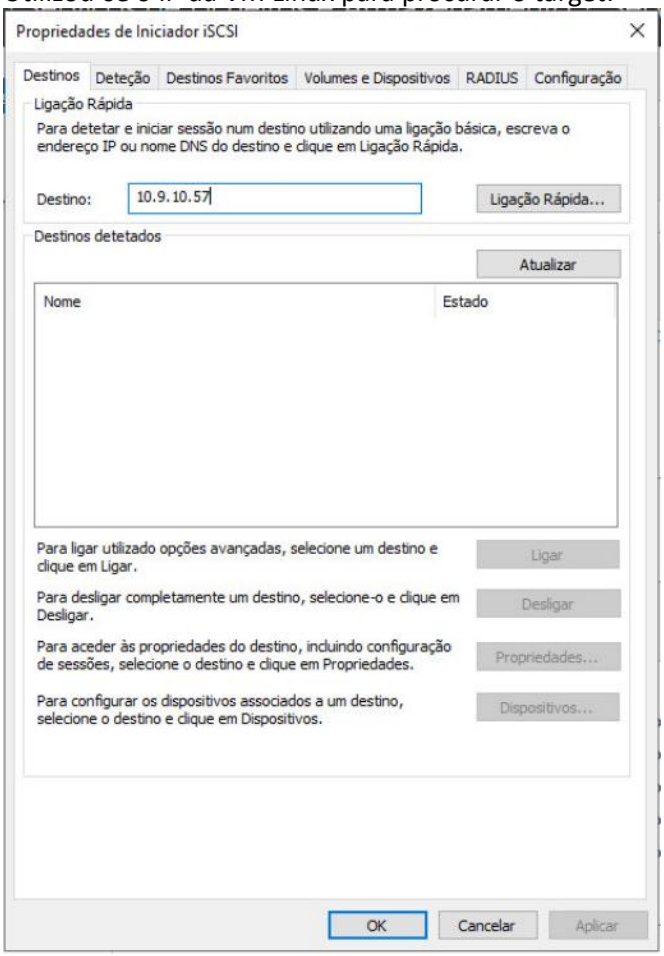
Através do das ferramentas do gestor de servidor selecionou-se a opção Iniciador iSCSI:



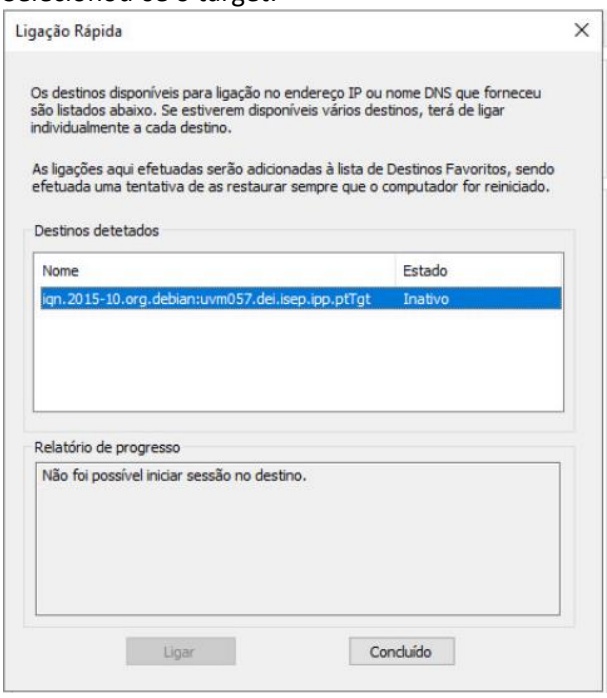
Selecionou-se sim:



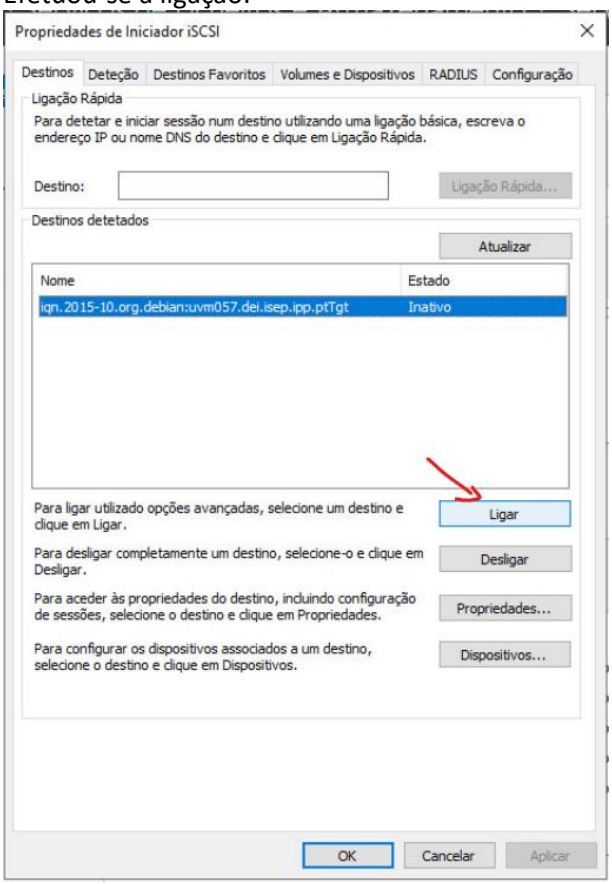
Utilizou-se o IP da VM Linux para procurar o target:



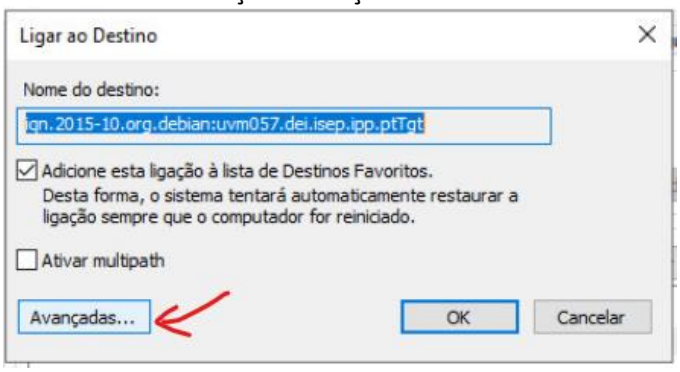
Selecionou-se o target:



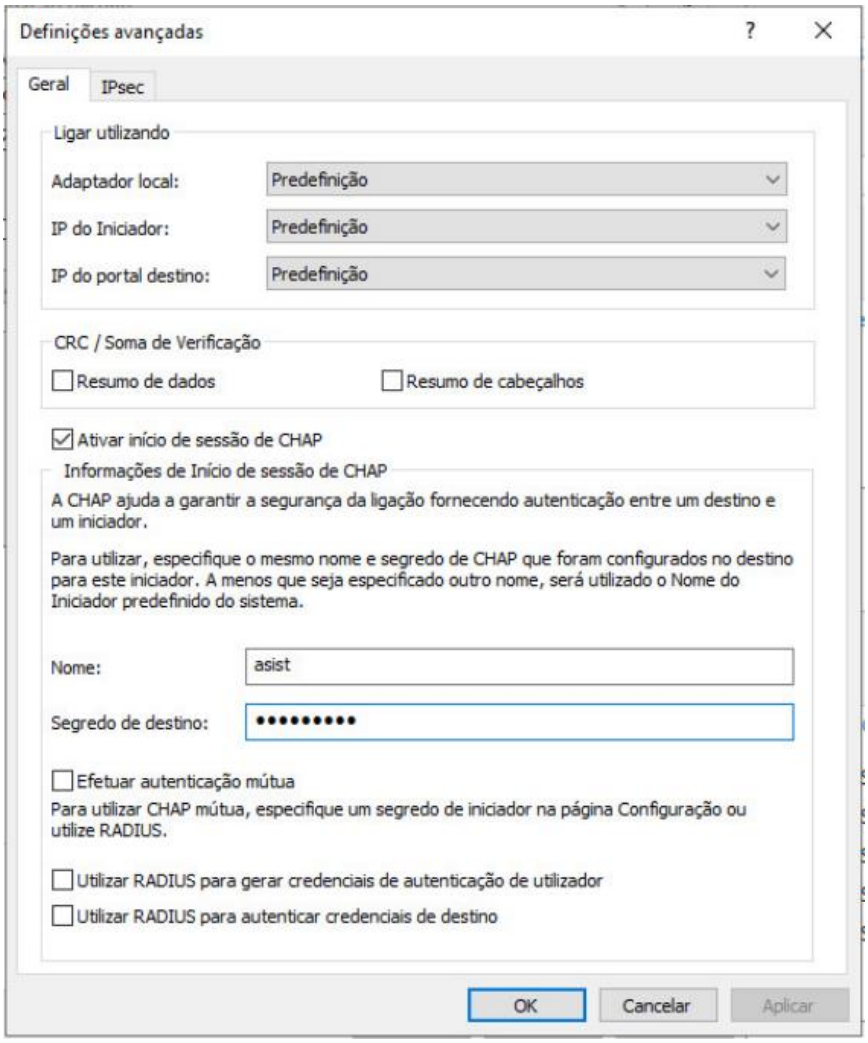
Efetuou-se a ligação:



Acedeu-se as definições avançadas:



Inseriu-se as credenciais definidas no target:



Depois de concluídas todas as configurações, acedeu-se o gestor de discos, tornando o disco online e inicializando-o, criando uma nova partição

US3

Como administrador do servidor Linux quero que semanalmente seja verificado se todos os utilizadores registados em */etc/passwd* possuem uma entrada no */etc/shadow*, se o grupo primário existe, se a *homedir* existe e pertence ao dono e grupo correto. Qualquer inconformidade deve ser registada em */tmp/auth_errors*

Neste requisito, realizou-se um script que irá ser executado uma vez por semana graças ao ficheiro em /etc/crontab que permite que os scripts localizados no diretório /etc/cron.weekly sejam executados semanalmente. Para isto criou-se o ficheiro verif:

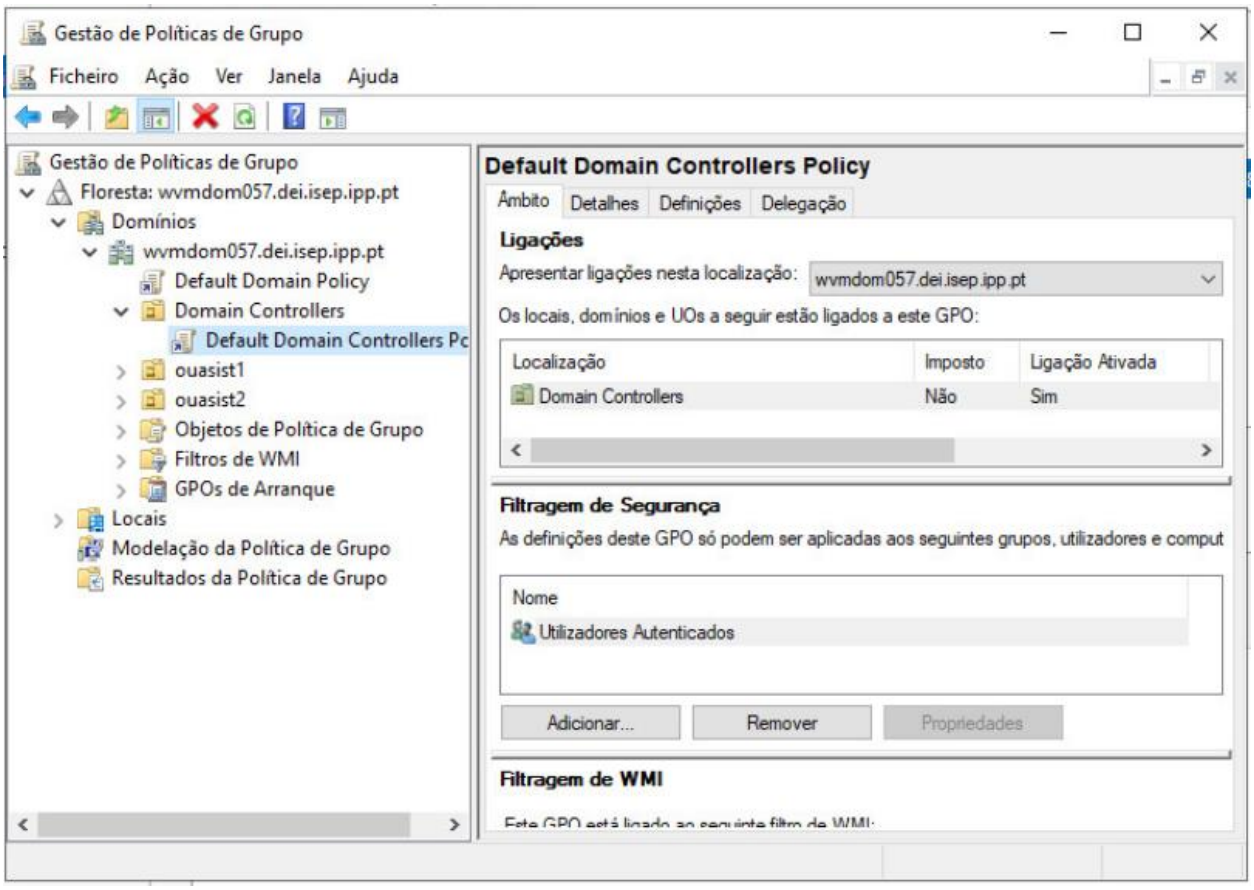
```
root@asist:~# nano /etc/cron.weekly/verif
```

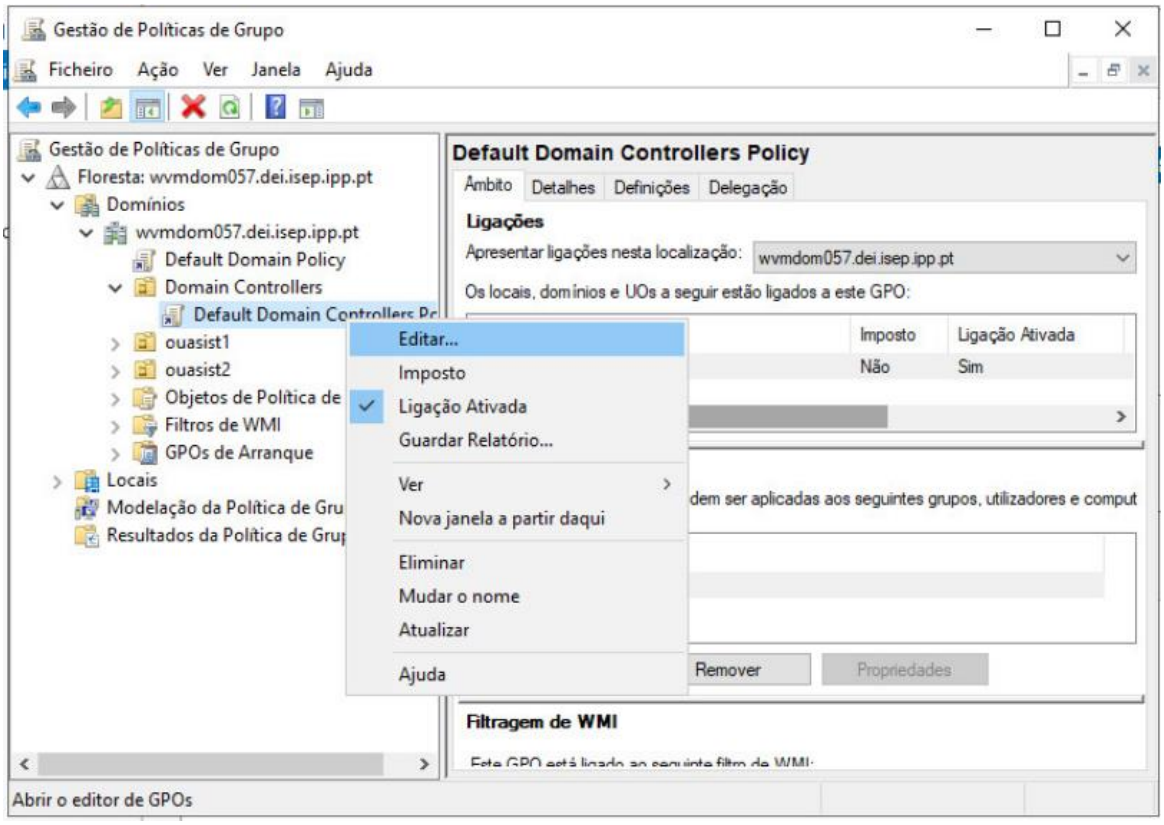
```
 GNU nano 5.4                                /etc/cron.weekly/verif
#!/bin/bash
sudo pwck > /tmp/auth_error/log
while read line; do
    while IFS=':' read -ra lineComponents; do
        user=${lineComponents[0]};
        usergid=${lineComponents[3]};
        userhome=${lineComponents[5]};
        userGroupName=`getent group "%usergid"| cut -d: -f1`;
        verifyHomeOwner=`stat -c "%U" "$userhome" > /dev/null | grep -w "$user"`;
        if [ -z "$verifyHomeOwner" ]; then
            echo "Owner do homedir do $user incorreto." >> /tmp/auth_error/log;
        fi
        verifyGroupOwner=`stat -c "%G" "$userhome" > /dev/null | grep -w "$userGroupName"`;
        if [ -z "$verifyGroupOwner" ]; then
            echo "Group Owner do homedir do $user incorreto." >> /tmp/auth_error/log;
        fi
    done <<< "$line"
done < /etc/passwd
```

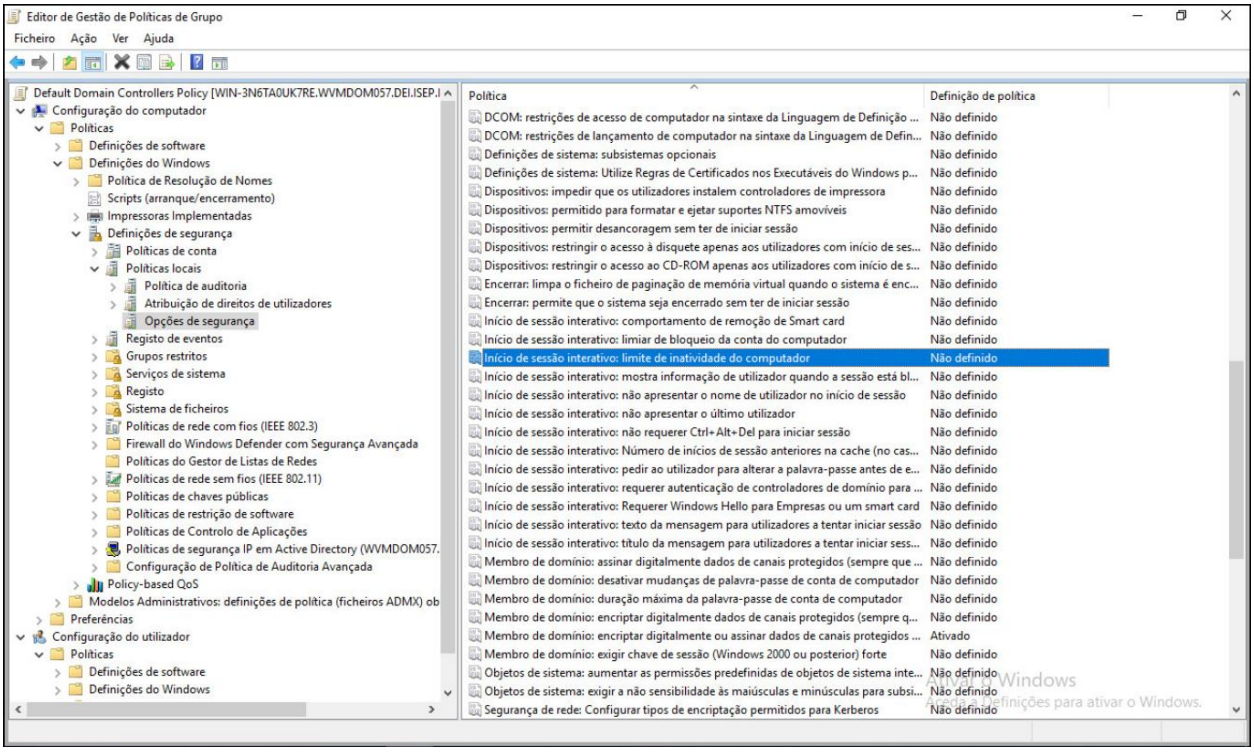
US4

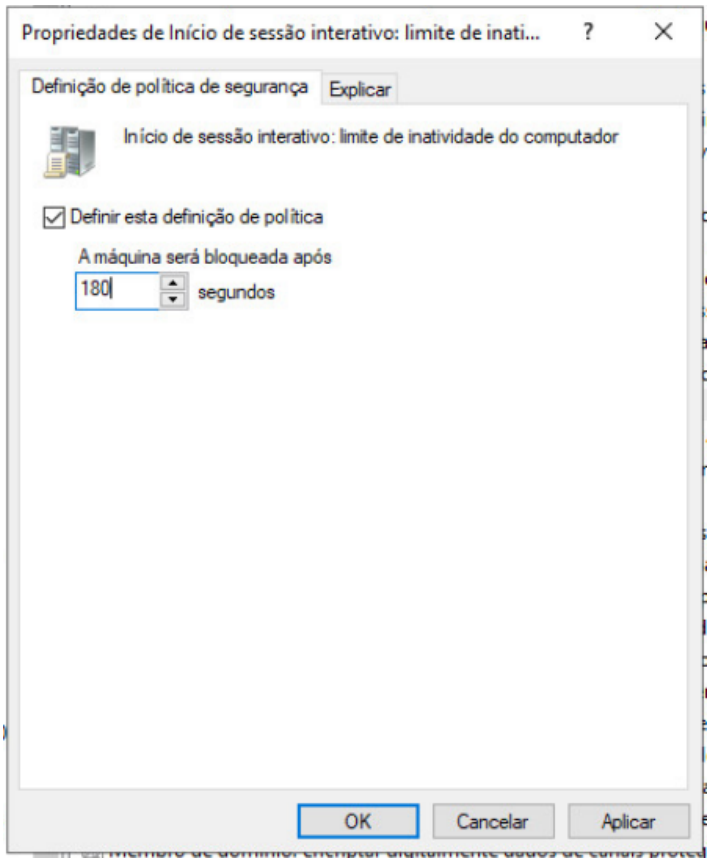
Como administrador da infraestrutura quero que todos os utilizadores registados no DC Windows tenham a sessão bloqueada ao fim de 3 minutos de inatividade

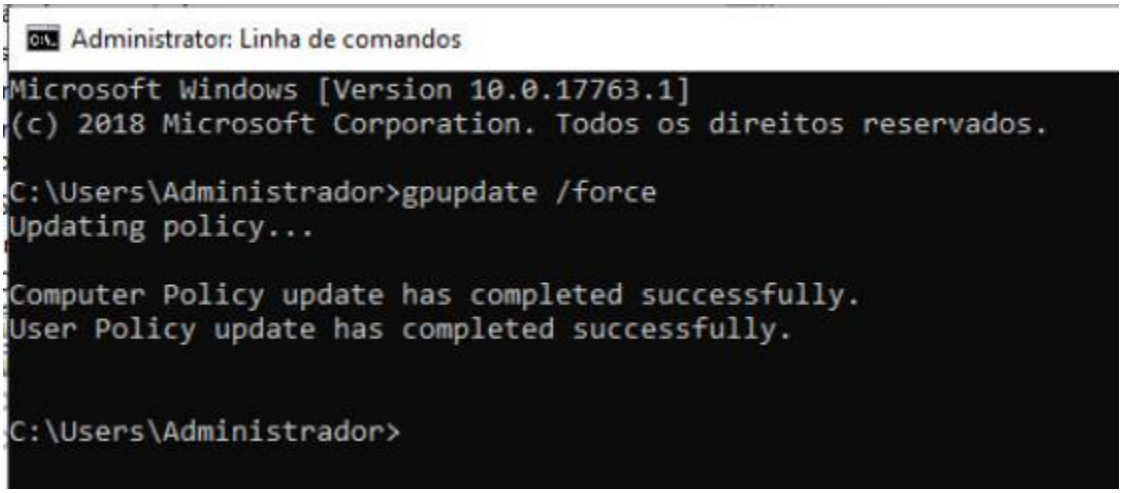
Para concretizar este requisito utilizamos o Gestor de Políticas de Grupo e seguimos os seguintes passos




Gestão de Políticas de Grupo
Ficheiro Ação Ver Janela Ajuda
Gestão de Políticas de Grupo
Floresta: wvmdom057.dei.isep.ipp.pt
Domínios
wvmdom057.dei.isep.ipp.pt
Default Domain Policy
Domain Controllers
Default Domain Controllers Pc
ouasist1
ouasist2
Objetos de Política de
Filtros de WMI
GPOs de Arranque
Locais
Modelação da Política de Gru
Resultados da Política de Grup
Default Domain Controllers Policy
Âmbito Detalhes Definições Delegação
Ligações
Apresentar ligações nesta localização: wvmdom057.dei.isep.ipp.pt
Os locais, domínios e UOs a seguir estão ligados a este GPO:
Imposto Ligação Ativada
Não Sim
Editar...
Imposto
Ligação Ativada
Guardar Relatório...
Ver
Nova janela a partir daqui
Eliminar
Mudar o nome
Atualizar
Ajuda
dem ser aplicadas aos seguintes grupos, utilizadores e comput
Remover
Propriedades
Filtragem de WMI
Abrir o editor de GPOs


Editor de Gestão de Políticas de Grupo
Ficheiro Ação Ver Ajuda
Default Domain Controllers Policy [WIN-3N6TA0UK7RE.WVMDOM057.DEI.ISEP.I
Configuração do computador
Políticas
Definições de software
Definições do Windows
Política de Resolução de Nomes
Scripts (arranque/encerramento)
Impressoras Implementadas
Definições de segurança
Políticas de conta
Políticas locais
Política de auditoria
Atribuição de direitos de utilizadores
Opções de segurança
Registo de eventos
Grupos restritos
Serviços de sistema
Registo
Sistema de ficheiros
Políticas de rede com fios (IEEE 802.3)
Firewall do Windows Defender com Segurança Avançada
Políticas do Gestor de Listas de Redes
Políticas de rede sem fios (IEEE 802.11)
Políticas de chaves públicas
Políticas de restrição de software
Políticas de Controlo de Aplicações
Políticas de segurança IP em Active Directory (WVMDOM057.
Configuração de Política de Auditoria Avançada
Policy-based QoS
Modelos Administrativos: definições de política (ficheiros ADMX) ob
Preferências
Configuração do utilizador
Políticas
Definições de software
Definições do Windows
Política
Definição de política
DCOM: restrições de acesso de computador na sintaxe da Linguagem de Definição ... Não definido
DCOM: restrições de lançamento de computador na sintaxe da Linguagem de Defin... Não definido
Definições de sistema: subsistemas opcionais Não definido
Definições de sistema: Utilize Regras de Certificados nos Executáveis do Windows p... Não definido
Dispositivos: impedir que os utilizadores instalem controladores de impressora Não definido
Dispositivos: permitido para formatar e ejetar suportes NTFS amovíveis Não definido
Dispositivos: permitir desancoragem sem ter de iniciar sessão Não definido
Dispositivos: restringir o acesso à disquete apenas aos utilizadores com início de ses... Não definido
Dispositivos: restringir o acesso ao CD-ROM apenas aos utilizadores com início de s... Não definido
Encerrar: limpa o ficheiro de paginação de memória virtual quando o sistema é enc... Não definido
Encerrar: permite que o sistema seja encerrado sem ter de iniciar sessão Não definido
Início de sessão interativo: comportamento de remoção de Smart card Não definido
Início de sessão interativo: limiar de bloqueio da conta do computador Não definido
Início de sessão interativo: limite de inatividade do computador Não definido
Início de sessão interativo: mostra informação de utilizador quando a sessão está bl... Não definido
Início de sessão interativo: não apresentar o nome de utilizador no início de sessão Não definido
Início de sessão interativo: não apresentar o último utilizador Não definido
Início de sessão interativo: não requerer Ctrl+Alt+Del para iniciar sessão Não definido
Início de sessão interativo: Número de inícios de sessão anteriores na cache (no cas... Não definido
Início de sessão interativo: pedir ao utilizador para alterar a palavra-passe antes de e... Não definido
Início de sessão interativo: requerer autenticação de controladores de domínio para ... Não definido
Início de sessão interativo: Requerer Windows Hello para Empresas ou um smart card Não definido
Início de sessão interativo: texto da mensagem para utilizadores a tentar iniciar sessão Não definido
Início de sessão interativo: título da mensagem para utilizadores a tentar iniciar sess... Não definido
Membro de domínio: assinar digitalmente dados de canais protegidos (sempre que ... Não definido
Membro de domínio: desativar mudanças de palavra-passe de conta de computador Não definido
Membro de domínio: duração máxima da palavra-passe de conta de computador Não definido
Membro de domínio: encriptar digitalmente dados de canais protegidos (sempre q... Não definido
Membro de domínio: encriptar digitalmente ou assinar dados de canais protegidos ... Ativado
Membro de domínio: exigir chave de sessão (Windows 2000 ou posterior) forte Não definido
Objetos de sistema: aumentar as permissões predefinidas de objetos de sistema inte... Não definido
Objetos de sistema: exigir a não sensibilidade às maiúsculas e minúsculas para subsi... Não definido
Segurança de rede: Configurar tipos de encriptação permitidos para Kerberos Não definido
Ativar o Windows
Aceda a definições para ativar o Windows.


Propriedades de Início de sessão interativo: limite de inati...
Definição de política de segurança
Explicar
Início de sessão interativo: limite de inatividade do computador
Definir esta definição de política
A máquina será bloqueada após
180
segundos
OK
Cancelar
Aplicar


Administrator: Linha de comandos
Microsoft Windows [Version 10.0.17763.1]
(c) 2018 Microsoft Corporation. Todos os direitos reservados.
C:\Users\Administrador>gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.
C:\Users\Administrador>