Relatório de ASIST

Grupo 25

Turma 3DE

Relatório realizado por:

* Francisco Tavares nº1181844
* José Cunha nº1181494
* César Ferreira nº1180811
* Sérgio Carreirinha nº1180800

Índice

[Caso de Uso 1 3](#_Toc58158061)

[Problemática em causa: 3](#_Toc58158062)

[Resolução proposta: 3](#_Toc58158063)

[Caso de Uso 2 7](#_Toc58158064)

[Problemática em causa: 7](#_Toc58158065)

[Resolução proposta: 7](#_Toc58158066)

[Caso de Uso 3 10](#_Toc58158067)

[Problemática em causa: 10](#_Toc58158068)

[Resolução proposta: 10](#_Toc58158069)

[Caso de Uso 4 13](#_Toc58158070)

[Problemática em causa: 13](#_Toc58158071)

[Proposta de Resolução: 13](#_Toc58158072)

# Caso de Uso 1

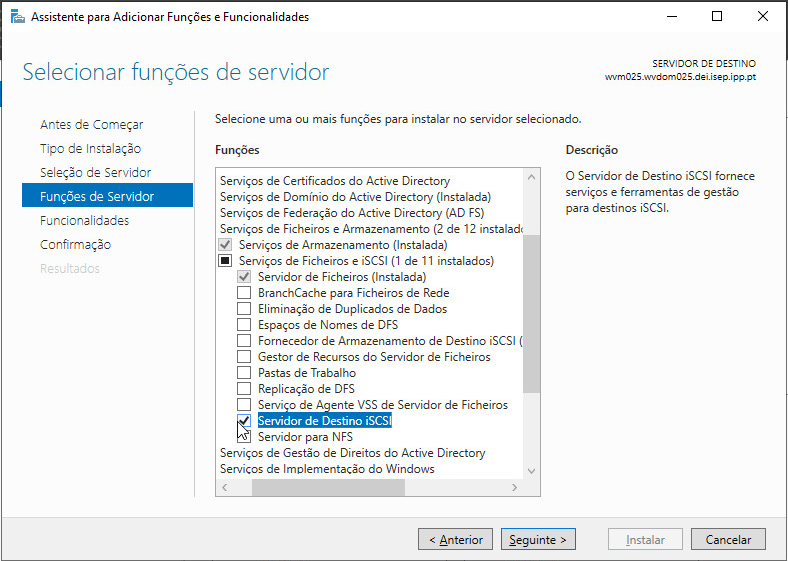
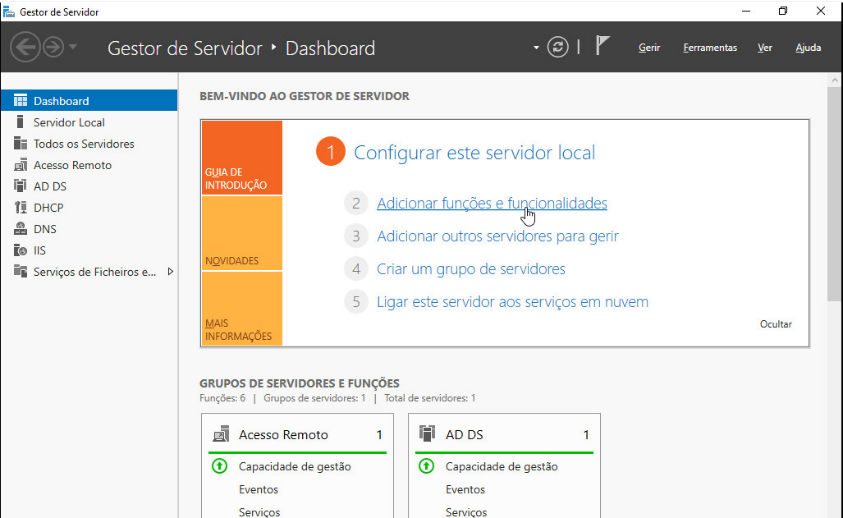
## Problemática em causa:

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

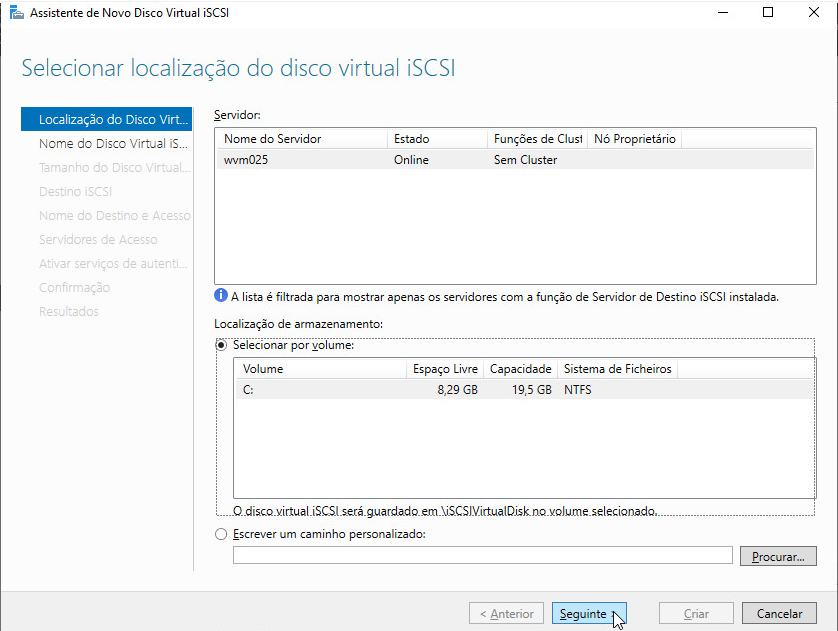
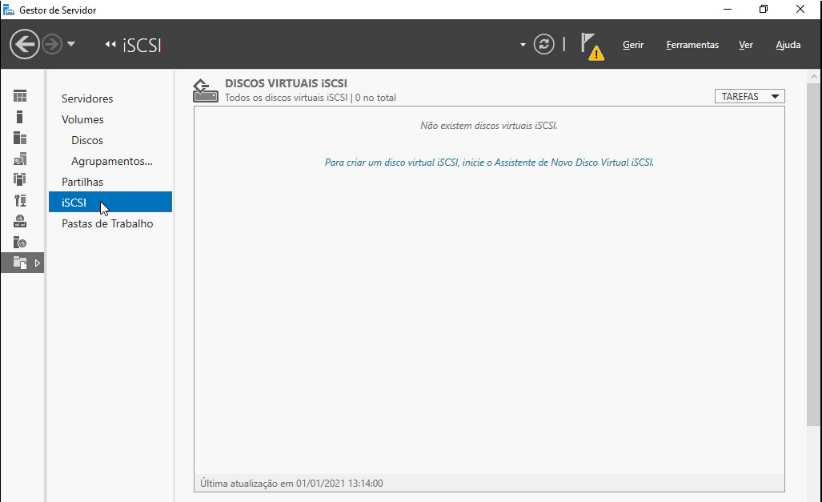
### Resolução proposta:

* Em Windows:

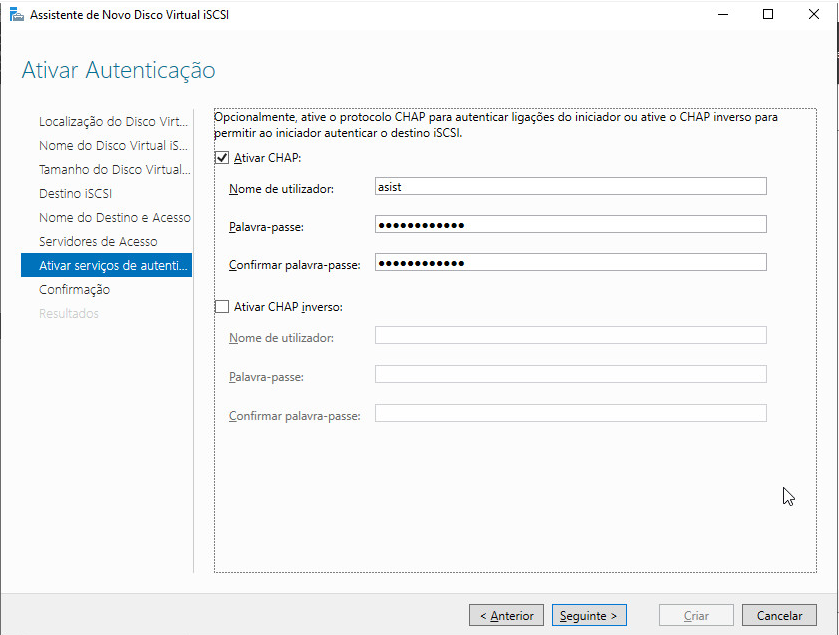
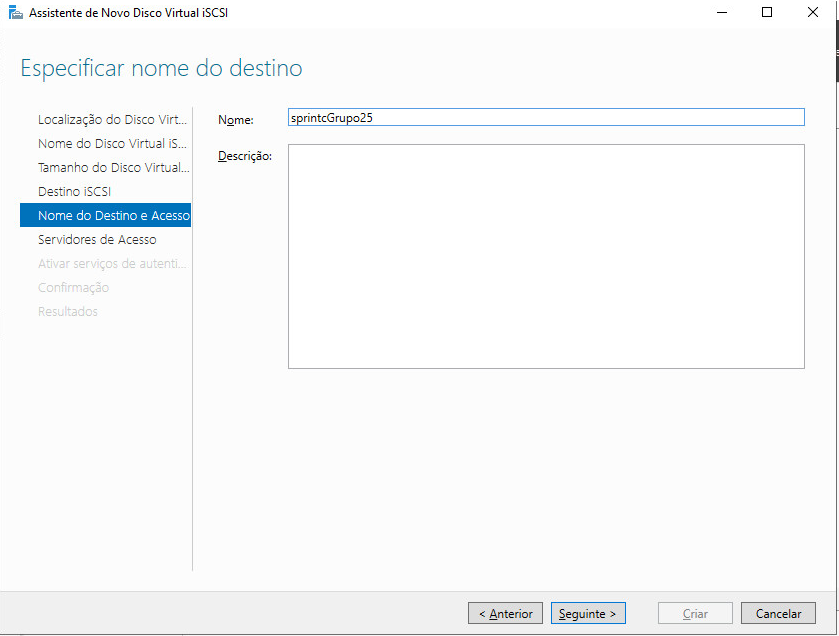
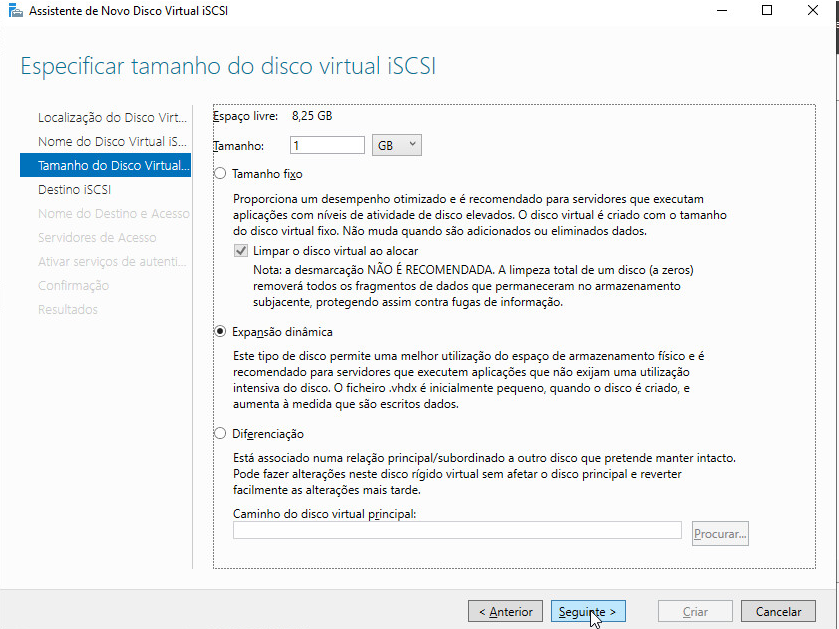
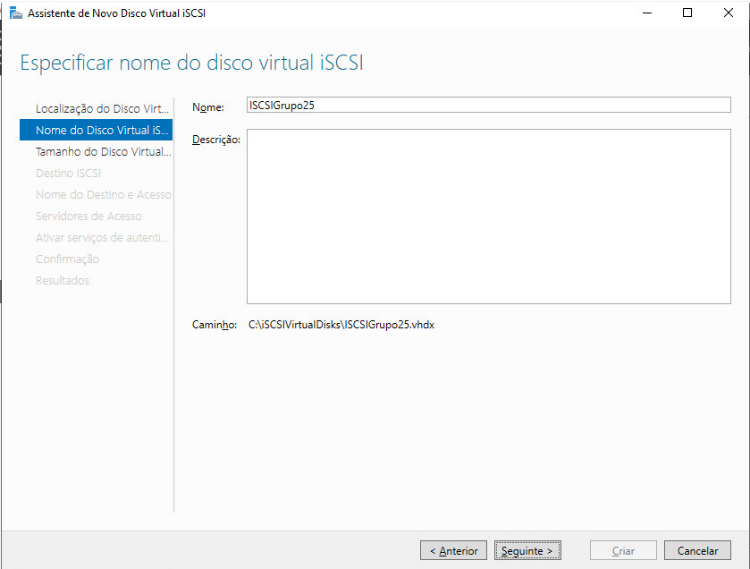
Em primeiro lugar, no *Dashboard* do Gestor de servidor, escolhemos a opção “Adicionar funções e funcionalidades”. De seguida, nas várias opções de funções a adicionar, selecionamos a “Servidor Destino ISCSI”.



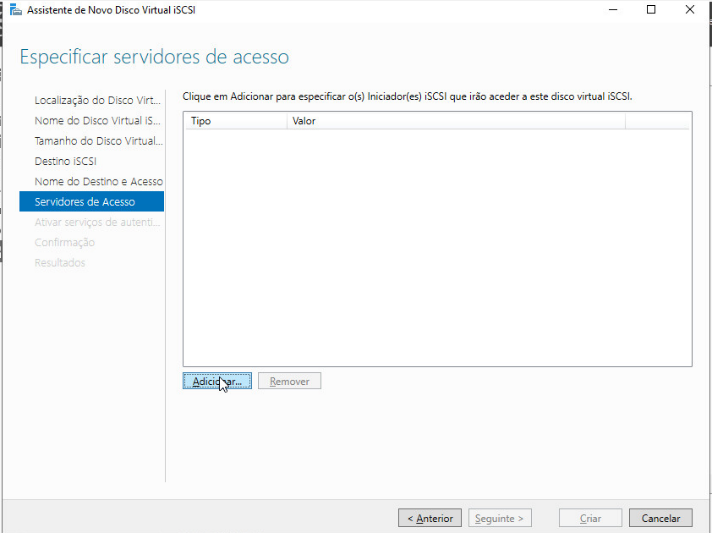
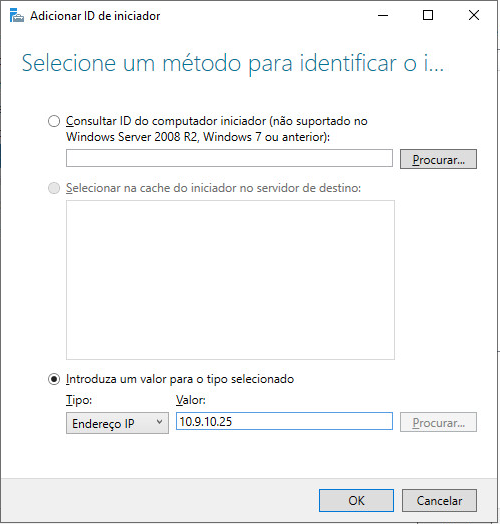
Finalizada a adição da função, procedemos à configuração da mesma. Primeiramente escolhemos a localização do disco virtual ISCSI.

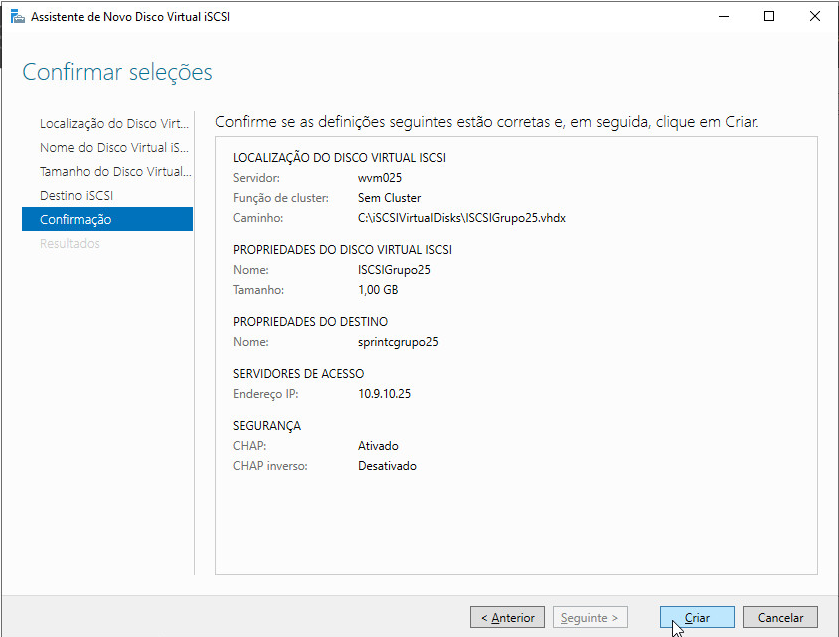


De seguida, introduzimos o nome pretendido para o disco, o seu espaço, o nome pretendido para a pasta de destino e a configuração de segurança CHAP.



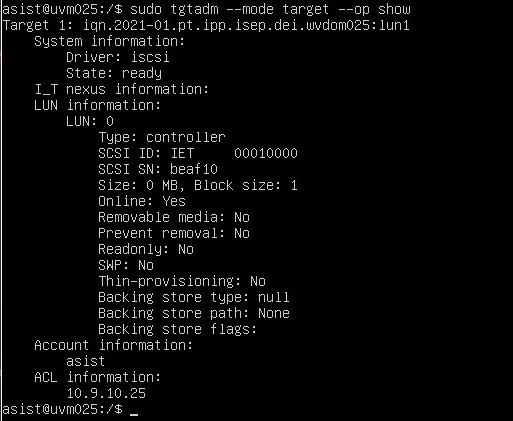
Por fim, foi dado acesso do servidor ao disco virtual, introduzindo o seu IP, e confirmada a criação do disco virtual ISCSI.





* Em Linux:

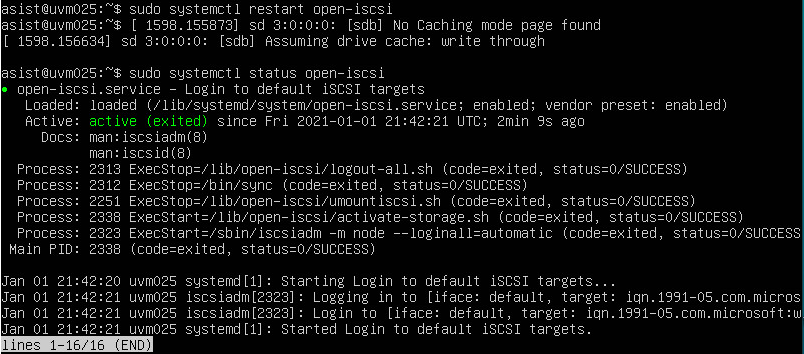
Em relação ao iSCSI Target, depois de instalar o pacote **tgt**, através do comando **sudo apt-get install tgt**, foi definido o target no ficheiro **/etc/tgt/conf.d/iscsi.conf**. Com o **comando sudo tgtadm --mode target --op show**, conseguimos verificar se a configuração foi bem feita.



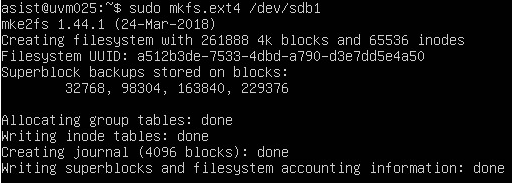
De seguida instalamos o pacote **open-iscsi**, de modo a ser configurado o iSCSI Initiator. Para isso foi usado o comando **sudo apt-get install open-iscsi**.

Depois do target configurado no servidor Windows, com ip **10.9.10.25**, é possível proceder à interligação entre os servidores, ou seja, permitir ao servidor Linux usar os discos lógicos disponibilizados pelo servidor Windows. Para isso, o primeiro passo é descobrir os nomes dos targets através do comando:

Com o nome do target pretendido, é possível configurar as definições de login para que o servidor Linux tenha acesso à informação partilhada pelo target:

Reiniciando o open-iscsi (**systemctl restart open-iscsi**) e verificando o estado do mesmo, é possível verificar se o login é feito com sucesso:

Com o comando **sudo** **fdisk /dev/sbd** é definida a partição.

E é formatada com o comando **sudo** **mkfs.ext4 /dev/sdb1**.

Finalmente, através do comando **sudo mount /dev/sdb1 /mnt**, a partição é montada no servidor Linux.

# Caso de Uso 2

## Problemática em causa:

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

### Resolução proposta:

 Foi definido ao a resolução deste exercício no método de autenticação para ligar o disco logico San iSCSI.

E foi usado editado o ficheiro /etc/fstab em ordem para dar mount, e foi colocado a seguinte linha.



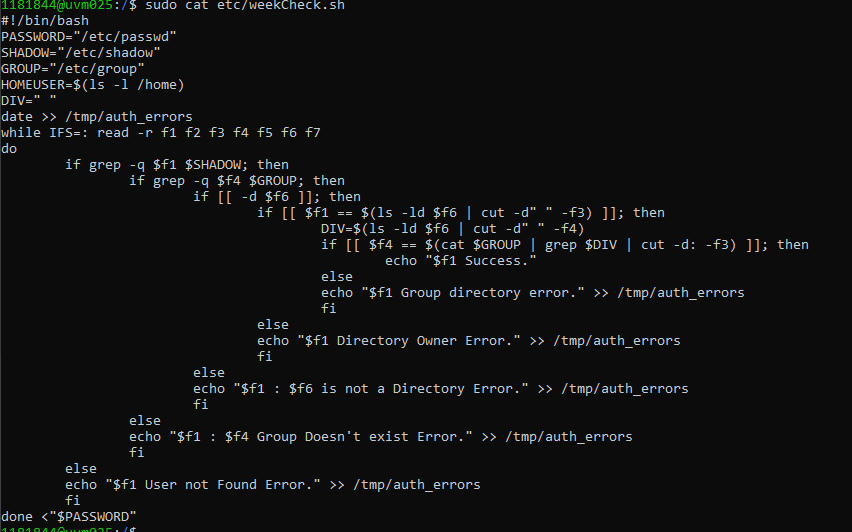
# Caso de Uso 3

## Problemática em causa:

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\_error

### Resolução proposta:

Para resolver a problemática em causa foi criado um Script que verifica inicialmente se os utilizadores têm entrada no /etc/shadow, caso alguns utilizadores não possuam entradas são criados erros. Depois de se verificar a entrada no /etc/shadow será confirmado se existe o grupo primário, mais uma vez, se este não existir são criados erros. Seguidamente confirmamos se existe o diretório, se o dono do diretório está correto e se pertence ao grupo correto. Depois de ser feito script foi necessário implementar a scheduled execution. Para isso editamos o ficheiro /etc/crontab e garantimos que todos os domingos hás 19:22 o script é corrido e são verificadas as pastas em causa. Nos prints a baixo é possível observar os resultados obtidos da execução do script mostrando os sucessos e os insucessos armazenados no auth\_errors.



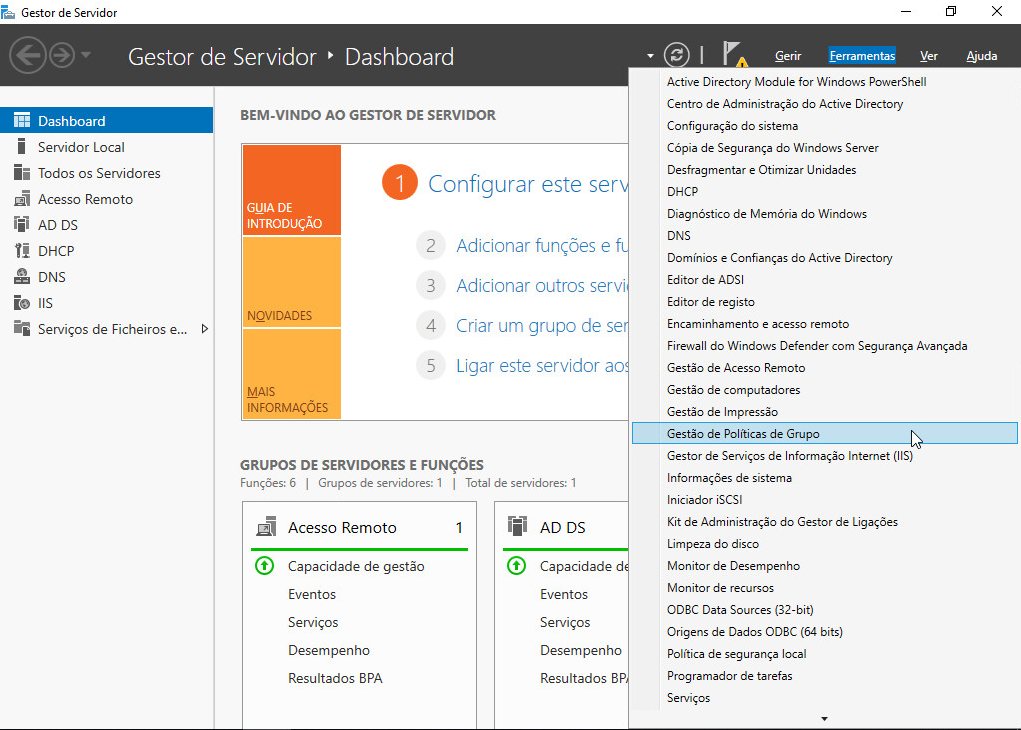
# Caso de Uso 4

## Problemática em causa:

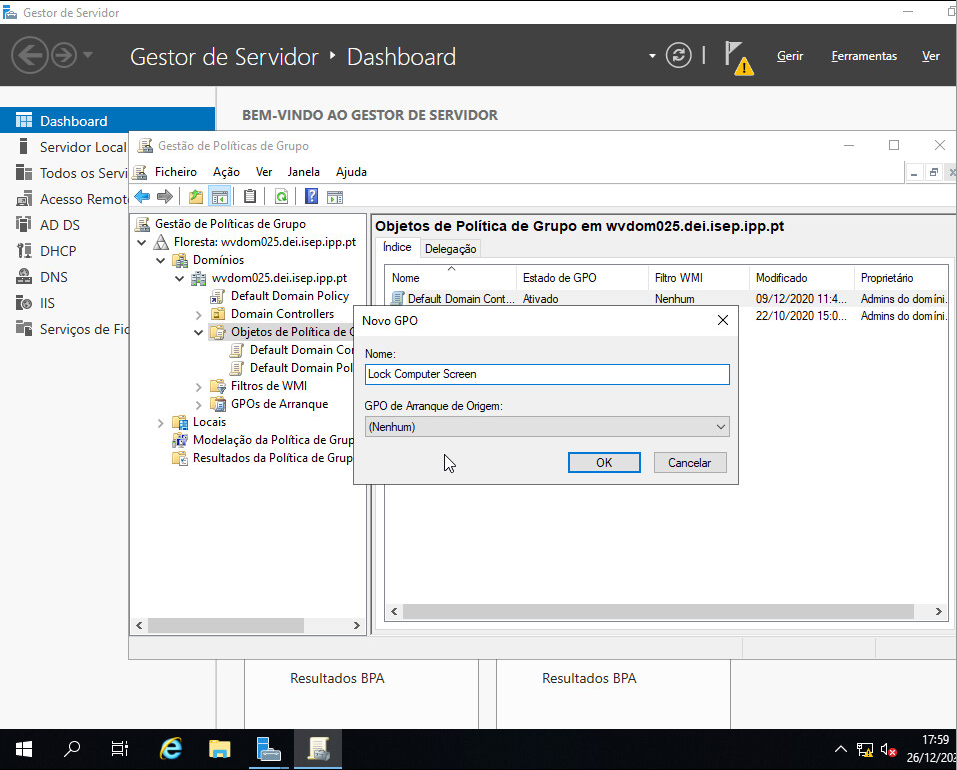
Como administrador da infraestrutura quero que todos os utilizadores registados no DC Windows tenham a sessão bloqueada ao fim de 3 minuto de inatividade

### Resolução proposta:

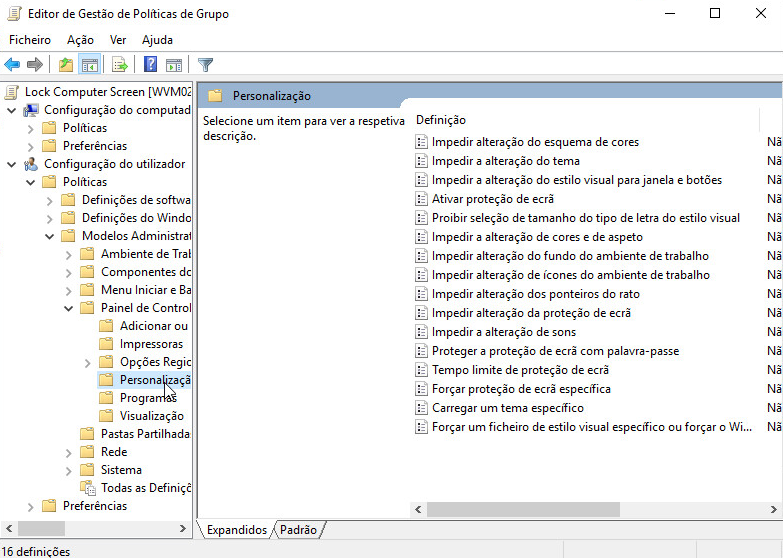
Primeiramente abrimos o gestor de servidor, selecionamos Ferramentas e de seguida Gestão de Políticas de Grupo.

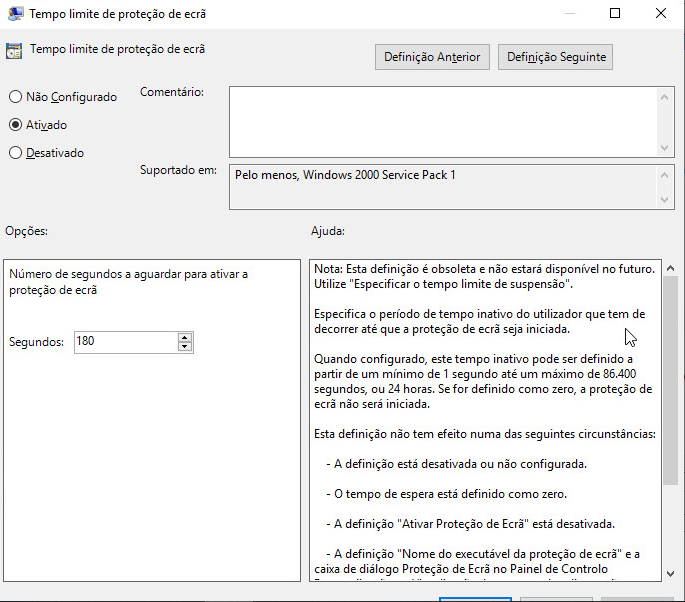


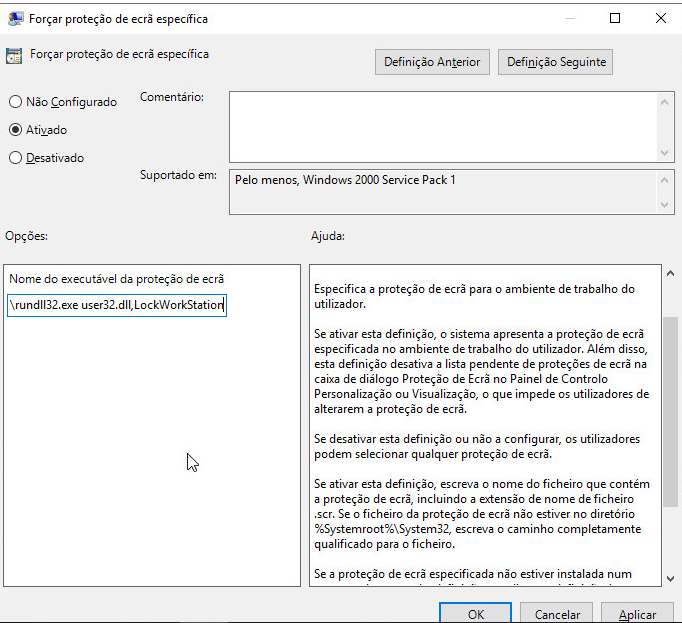
Para que possamos bloquear a sessão depois de 3 minutos temos que criar um novo objeto de política de grupo à qual chamamos de “Lock Computer Screen”.



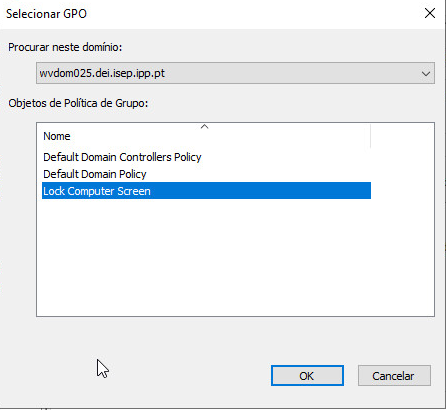
Carregando com o botão direito do mouse em cima do Objeto de Política de Grupo criado selecionamos o “Editar” e seguimos o seguinte caminho:



Dentro do personalização temos que ativar o: “ativar proteção de ecrã”, “Proteger a proteção de ecrã com palavra-passe”, “Tempo limite de proteção de ecrã” onde colocamos o tempo que pretendemos que a sessão seja bloqueada após a inatividade (neste caso 180 segundos) e “Forçar proteção de ecrã com palavra-passe” onde colocamos o nome executável..



Seguidamente adicionamos ao domínio o GPO criado.



Por fim podemos verificar as definições alteradas anteriormente no “Lock Computer Screen” o qual nos diz que o bloqueio por inatividade do utilizador está ativo e que o tempo de inatividade máximo é de 180 segundos ou seja, 3 minutos.

