

Manual de apoio CSI - Fileshare





DIREÇÃO DE COMUNICAÇÕES E INFORMAÇÃO

Centro de Transmissões do Exército

Administração do serviço de Fileshare

Manual de Apoio CSI

Data:	Mar2024
Versão:	v. 01.01
Refª:	Manual CSI
Local	DCI - Lisboa

Registo de Alterações

Registo de Alterações

Versão	Data	Item	Observações/Pág.
01.00	Nov2022	Versão inicial	SAj Tm Filipe Simões
01.01	Mar2024	Revisão	Cap TM Filipe João

Índice

1. Fileshare.....	2
1.1 - ACL e tipos de permissões.....	2
1.1.1 - Leitura	2
1.1.2 - Escrita	3
1.1.3 - Controlo total	3
1.1.4 - Especiais	3
1.1.5 - Resumo	3
1.2 - Permissão versus Negação de permissão	4
1.3 - Herança de permissões	5
1.3.1 - Desativar herança de permissões.....	5
1.4 - Verificação de acesso efetivo.....	7
1.5 - Obtenção de propriedade sobre objetos.....	8
1.6 - Limitação de caracteres nos caminhos.....	9

Índice de Figuras

Figura 3.1 - Permissões não-herdadas (esquerda) e permissões herdadas (direita)	5
Figura 3.2 - Exemplo de pasta com herança de permissões desativada.....	6
Figura 3.3 - Verificação de acesso efetivo de um utilizador a uma pasta	7
Figura 3.4 - Utilizador sem acesso a um objeto	8

Índice de tabelas

Tabela 1 – Permissões especiais por grupos de permissões.....	4
---	---

Siglas e Acrónimos

ACL – *Access Control List*

ACE – *Access Control Entry*

AD – *Active Directory*

ARL – *Administrador de Redes local*

BD – *Base de dados*

DB – *Database*

DC – *Domain Controller*

DNS – *Domain Name System*

FQDN – *Fully Qualified Domain Name*

GPO – *Group Policy*

LAPS – *Local Administrator Password Solution*

LDAP – *Lightweight Directory Access Protocol*

NTFS – *New Technology File System*

OU – *Organizational Unit*

RDE – *Rede de Dados do Exército*

SID – *Security Identifier*

VPN – *Virtual Private Network*

Referências

- PDE 6.00 Comunicações e Informação – agosto 2023

Introdução

Pressupostos:

- Operações efetuadas por membros de GADMIN da unidade
- Pré-requisitos instalados
 - Windows 10/ Windows 11
 - Office instalado
 - Ferramentas administrativas

Consultar sempre as FAQ no portal <https://servicedesk.exercito.local>

1. Fileshare

Uma das formas de partilhar informação é através da utilização de um serviço de *fileshare* (pastas partilhadas). Este tipo de serviço permite que vários utilizadores possam criar, alterar (apenas um utilizador pode estar a alterar a informação ao mesmo tempo) e eliminar ficheiros alojados num servidor, habitualmente, na sua U/E/O.

Por norma, cada U/E/O terá uma partilha dedicada, providenciada pela DCI num servidor de *fileshare*. O acesso à partilha e correspondente pasta principal é da responsabilidade da DCSI, sendo o acesso às pastas nela contidas da responsabilidade dos ARL da U/E/O. O acesso aos ficheiros e pastas é restrito e da responsabilidade do administrador local que o deverá condicionar usando grupos de segurança.

O ARL deve fazer uma estrutura de pastas organizada de forma semelhante ao Quadro Orgânico da U/E/O (uma pasta por secção/subunidade), nunca devendo deixar todas as pastas desorganizadas na raiz.

1.1 - ACL e tipos de permissões

O sistema de ficheiros NTFS (atualmente o sistema de ficheiro nativo dos sistemas operativos da família Windows) trouxe consigo o controlo de acessos a objetos. Esse controlo encontra-se patente na lista de controlo de acessos (ACL) de cada objeto. A ACL é composta por entradas (ACE) de permissões a utilizadores ou grupos (preferencialmente grupos) garantindo ou negando um determinado tipo de acesso. O tipo de acesso é conferido utilizando tipos de permissões. De seguida referem-se os tipos de permissões existentes, descrevendo-os.

1.1.1 - Leitura

As permissões de leitura permitem visualizar os objetos e seu conteúdo, mas não permitem alterá-los ou eliminá-los. Normalmente compreendem os seguintes grupos:

- **Leitura (Read)** – permite abrir um ficheiro e ver os seus atributos
- **Ler e Executar (Read & Execute)** – permite abrir um ficheiro, ver os seus atributos e executá-lo, caso seja um ficheiro executável
- **Listar o conteúdo da pasta (List folder contents)** – permite ver o conteúdo de uma pasta

Habitualmente, as permissões de leitura, quando conferidas a um utilizador/grupo, são atribuídas usando os 3 grupos anteriores.

1.1.2 - Escrita

Para dar permissões para criar, eliminar ou alterar os objetos, usam-se as permissões de escrita. Não é possível atribuir permissões de escrita sem atribuir permissões de leitura. As permissões de escrita dividem-se em dois grupos:

- **Escrita** – Permite a criação de ficheiros e pastas e a alteração de ficheiros. Não permite a eliminação de ficheiros e implica ter permissões de leitura.
- **Modificar** – Permite a eliminação dos objetos.

1.1.3 - Controlo total

Para além de compreender todas as restantes permissões, quem tiver permissões de Controlo Total pode gerir as permissões dos outros utilizadores/grupos sobre um objeto. Este tipo de permissões apenas deve ser atribuído aos ARL das U/E/O, usando o grupo “GADMIN” correspondente.

1.1.4 - Especiais

As permissões especiais são permissões mais granulares e específicas de operações. Apenas devem ser usadas quando os tipos de permissões anteriores não satisfazem o pretendido. A Tabela 1 tem a lista das permissões especiais

1.1.5 - Resumo

A Tabela 1 faz a relação entre as permissões especiais e os tipos de permissões existentes.

Tabela 1 – Permissões especiais por grupos de permissões¹

Permissões especiais	Controlo total	Modificar	Ler e executar	Listar conteúdo de pastas	Leitura	Escrita
Atravessar pasta/Executar ficheiro	X	X	X	X		
Listar pasta/Ler dados	X	X	X	X	X	
Ler atributos	X	X	X	X	X	
Ler atributos estendidos	X	X	X	X	X	
Criar ficheiros/Escrever dados	X	X				X
Criar pastas/Acrescentar dados	X	X				X
Escrever atributos	X	X				X
Escrever atributos estendidos	X	X				X
Eliminar subpastas e ficheiros	X	X				
Eliminar	X	X				
Ler permissões	X	X	X	X	X	X
Alterar permissões	X					
Obter propriedade	X					
Sincronizar	X	X	X	X	X	X

1.2 - Permissão versus Negação de permissão

Um determinado utilizador/grupo, em termos de acesso a um objeto, estará num dos seguintes casos:

- **Tem acesso:**
 - Explícito – o utilizador/grupo encontra-se listado na ACL estando-lhe permitido o acesso
 - Herdado – o utilizador/grupo pertence a um dos grupos listado na ACL com permissões de acesso
- **Não tem acesso:**
 - Explícito – o utilizador/grupo encontra-se listado na ACL, sendo-lhe negada a permissão

¹ Baseada na tabela “NTFS Access Limitations” em <https://blog.foldersecurityviewer.com/understanding-ntfs-permissions/>, consultada em 06JUN22

Grupo de Controlo e Gestão de Sistemas 4

- Herdado – foi negado o acesso a um grupo na ACL ao qual o utilizador/grupo pertence

Salienta-se que as permissões de negação têm prevalência sobre as permissões atribuídas.

1.3 - Herança de permissões

Por omissão, no Windows, as pastas propagam as suas permissões aos objetos nelas contidos (ficheiros e pastas). Esta é uma forma de manter os acessos aos ficheiros/pastas consistente e facilmente gerível. No entanto, nem sempre é conveniente que tal aconteça. Um exemplo disso mesmo será nas pastas das secções dentro da “pasta-mãe” da U/E/O. Não é conveniente que as secções acedam às pastas das outras secções. Ainda assim, não deverá ser usado em muitos mais casos a fim de ser mantida a consistência das permissões e não se cair no risco de se perder o controlo dos acessos nos objetos contidos noutros objetos.

As permissões herdadas aparecem a cinzento e não são alteráveis e as permissões não-herdadas aparecem a preto na ACL.

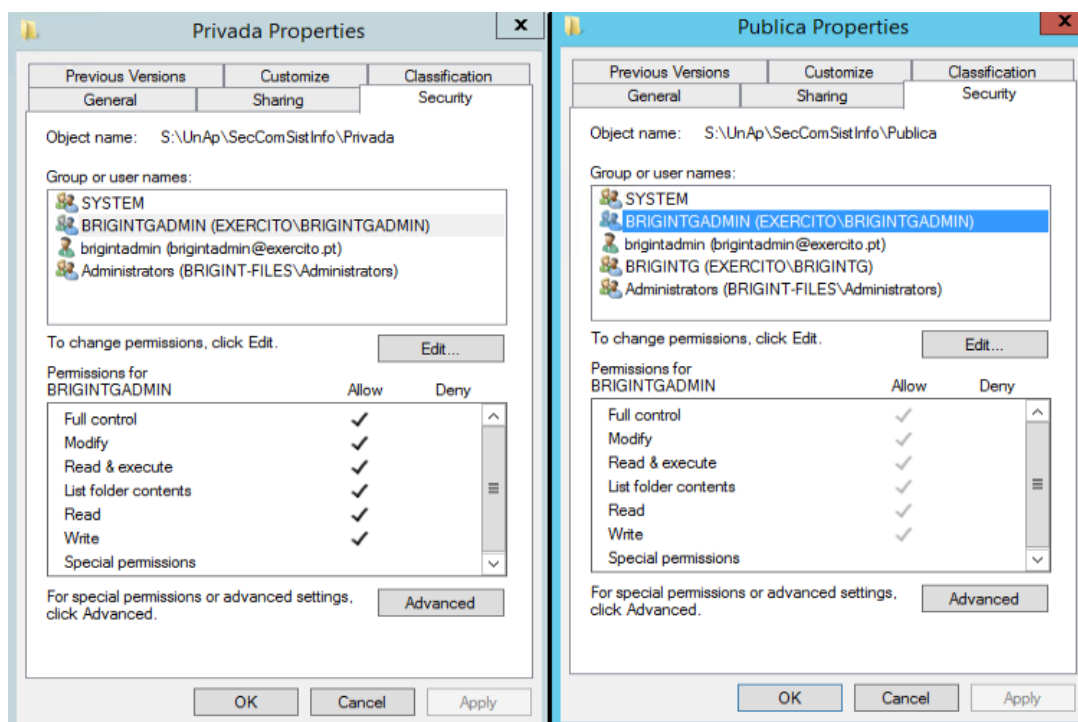


Figura 1.1 - Permissões não-herdadas (esquerda) e permissões herdadas (direita)

1.3.1 - Desativar herança de permissões

Para que um objeto deixe de herdar as permissões da “pasta-mãe” é necessário desativar a herança de permissões. Apesar de poder ser efetuado sobre ficheiros, este

tipo de operações, apenas deve ser efetuado sobre pastas e apenas pode ser levado a cabo por quem tenha permissões de Controlo Total sobre a pasta. Para desativar a herança de permissões é necessário:

1. Aceder às propriedades da pasta
2. Aceder às permissões avançadas, clicando no botão “Avançadas” (*Advanced*) no separador “Segurança” (*Security*)
3. Na nova janela, clicar no botão “Desativar herança” (*Disable inheritance*)
4. Responder se é pretendido manter e alterar as permissões herdadas, convertendo-as para permissões explícitas sobre o objeto ou, se é pretendido remover todas as permissões do objeto. Ressalva-se que, caso se removam as permissões herdadas, deverão ser dadas novas permissões de controlo total aos administradores por essas terem sido removidas.
5. Adicionar as permissões pretendidas aos grupos à pasta
6. Escolher se as permissões de todos os objetos contidos na pasta devem herdar as suas permissões substituídas pelas novas permissões, ativando o visto na *checkbox* de substituição das permissões dos objetos subordinados pelas permissões da pasta

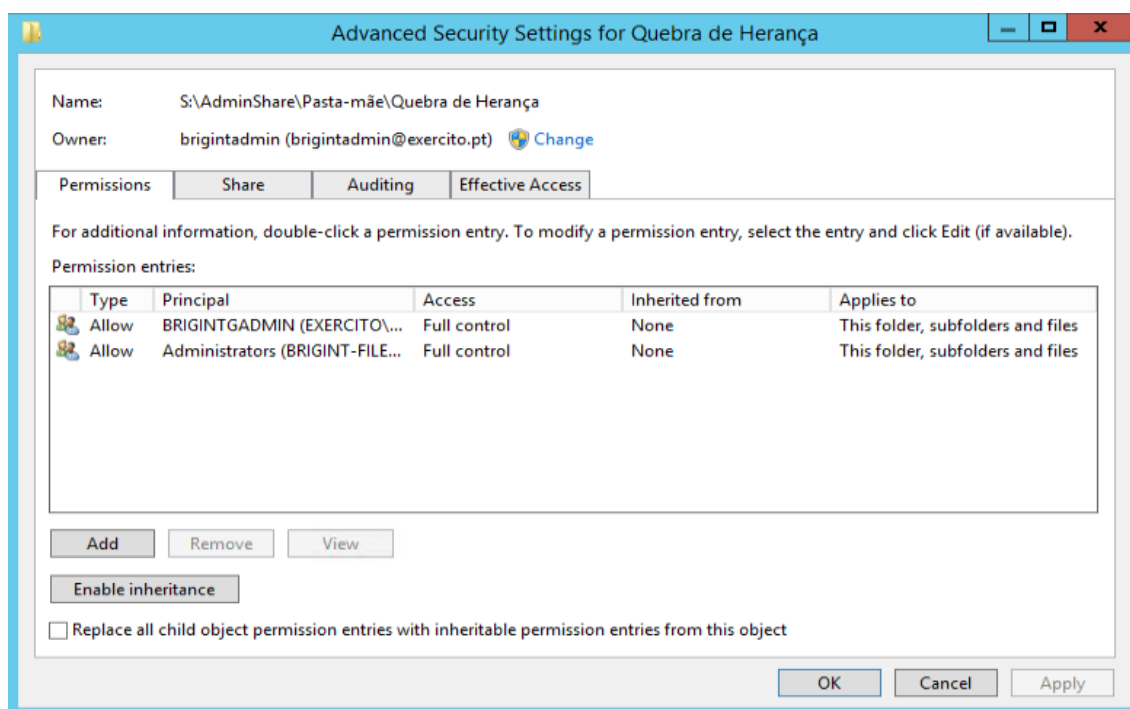


Figura 1.2 - Exemplo de pasta com herança de permissões desativada

1.4 - Verificação de acesso efetivo

Para confirmação da configuração dos acessos, é possível verificar que tipo de acesso tem um determinado utilizador/grupo a um objeto, devendo-se:

1. Aceder às propriedades do objeto
2. Escolher o separador “Segurança” (*Security*) e usar o botão “Avançadas” (*Advanced*)
3. Na nova janela, escolher o separador “Acesso efetivo” (*Effective Access*)
4. Abrir a hiperligação “Selecionar um utilizador” (*Select a user*) e escolher o utilizador/grupo pretendido
5. Clicar em “Ver acesso efetivo” (*View effective access*)

O resultado deverá ser semelhante à Figura 1.3.

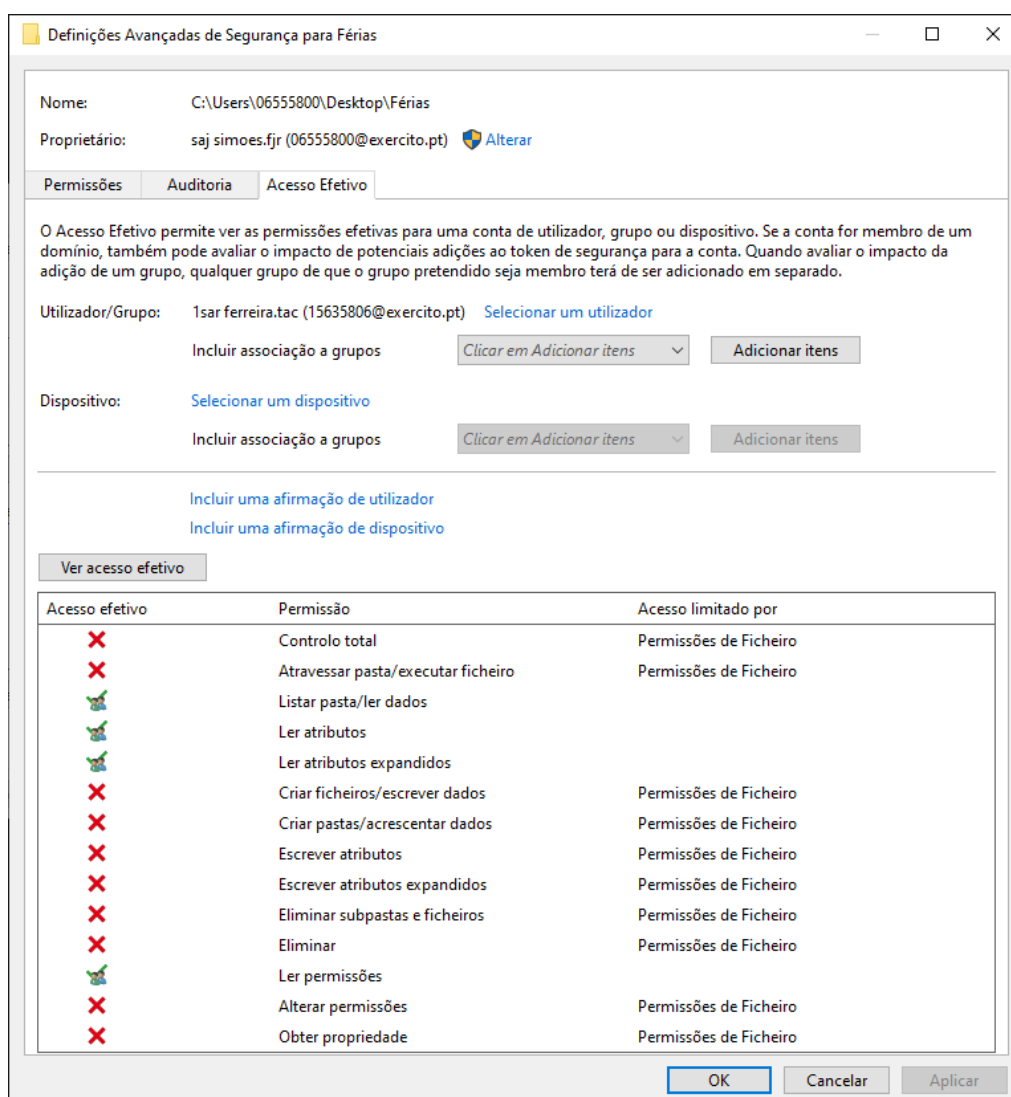


Figura 1.3 - Verificação de acesso efetivo de um utilizador a uma pasta

1.5 - Obtenção de propriedade sobre objetos

Provavelmente por más configurações anteriores ou enganos na configuração das permissões, pode acontecer que um administrador não tenha acesso a determinado objeto. Nestes casos, o administrador, pode tornar-se proprietário do objeto e, consequentemente, limpar a ACL do objeto para a poder reconfigurar. Quando um caso destes acontece, a janela das propriedades do objeto apresenta algo semelhante à Figura 1.4 e não é possível aceder ao objeto.

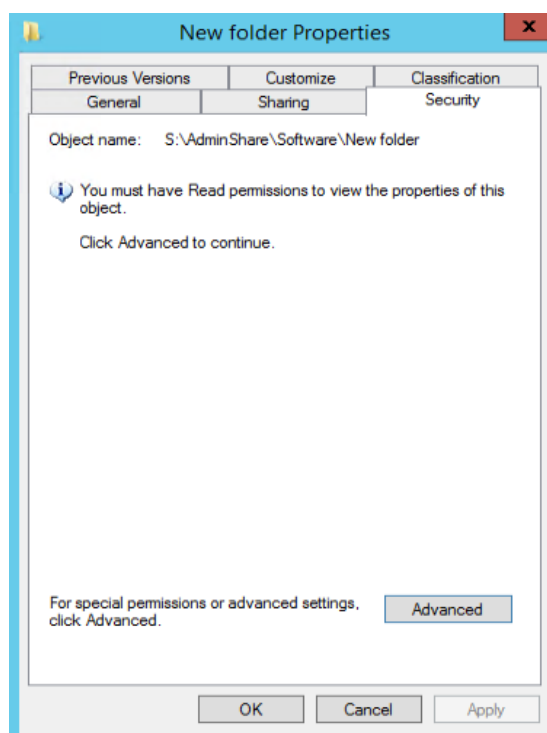


Figura 1.4 - Utilizador sem acesso a um objeto

Uma vez que um administrador deverá ter sempre acesso aos objetos, só assim garantindo os acessos devidos à informação e objetos, pode obter propriedade sobre o objeto ao:

1. Abrir o separador “Segurança” nas propriedades do objeto e clicar em “Avançadas”
2. Clicar na hiperligação “Alterar” o proprietário do objeto e escolher o novo proprietário. Pode ser o seu próprio nome de utilizador ou do grupo de administração da U/E/O (GADMIN da U/E/O)
3. Deverá “Substituir o proprietário em subcontentores e objetos”
4. Aplicar as definições escolhidas, clicando no botão “Aplicar”
5. Confirmar que pretende substituir as permissões obtendo permissões de Controlo Total

-
6. Fechar as permissões do objeto
 7. Voltar a aceder às propriedades do objeto e reformular a ACL do objeto com as permissões devidas

1.6 - Limitação de caracteres nos caminhos

O Windows tem uma limitação de 256 caracteres nos caminhos dos ficheiros/pastas. Não deveria ser um problema, no entanto, verifica-se que os utilizadores tendem a escrever caminhos nas pastas extremamente longos. Este é um problema aparentemente inócuo, mas de extrema gravidade para os backups que falharão ao fim de algumas falhas de acessos a ficheiros. Repare-se no exemplo seguinte dum caminho do ficheiro (o nome do servidor e outras pastas anteriores foi propositadamente removido):

(...)02 - Estado Maior\02.04 - SecrcMD\10_ARQUIVO
PRIMÁRIO\ARQUIVO\ARQUIVO\Arquivo Primário\lei arquivo\Lei 8_95, de 29 de Março
- 1ª Alteração à Lei 65_93, de 26 de Agosto sobre o Regime de acesso aos
documentos da Administração Pública.pdf

Podem daqui surgir algumas dúvidas que só o utilizador poderá responder:

- Será que existe necessidade de 5 pastas de denominação “Arquivo”?
- Só o nome do ficheiro tem 137 caracteres (mais de metade da limitação de caracteres). Não será possível encurtá-lo?

O Comandante do CTE

Rogério Morgado Ferreira
Cor TM



Direção de Comunicações e Informação / Centro de Transmissões do Exército

Rua de Sapadores, 1199-015 | Lisboa

Email: dcinfo@exercito.pt | Telefone: 218 117 030