

CAS PRÀCTIC 1 – EL SERVEI FTP a WINDOWS SERVER 2022

NOM DE L'ALUMNE/s: Nil Massó

OBJECTIU

- Configurar el servei d'FTP amb IIS/FTP en base a les premisses de l'enunciat per tal de complir els paràmetres establerts i fer les corresponents comprovacions.

INSTRUCCIONS

- L'activitat és de tipus individual.
- Cal realitzar-lo sobre les màquines virtuals proporcionades a l'inici del mòdul.
- Recordeu que caldrà configurar-les a nivell de *hostname*, usuaris, etc.
- Caldrà també que realitzeu les adients configuracions de xarxa amb IP estàtica dins la 'xarxa NAT' que utilitzem al MP.
- No hi ha problema en reutilitzar les de la UF1 o NF1 de la UF2. Tingueu en compte les configuracions que hi teniu per si us poden generar algun conflicte o variació.
- També podeu utilitzar les màquines de la plataforma IsardVDI degudament configurades i personalitzades.
- Per defecte, cal que justifiqueu les respostes amb captures de pantalla.
- Si a la captura no hi ha cap valor que la identifiqui de forma única, cal que es vegi el fons d'escriptori, *notepad* o eines similars amb el vostre nomcognom!
- Totes les captures que mostrin les comandes han d'incloure, a part del resultat, la comanda i/o els paràmetres, per tal de veure com la feu.

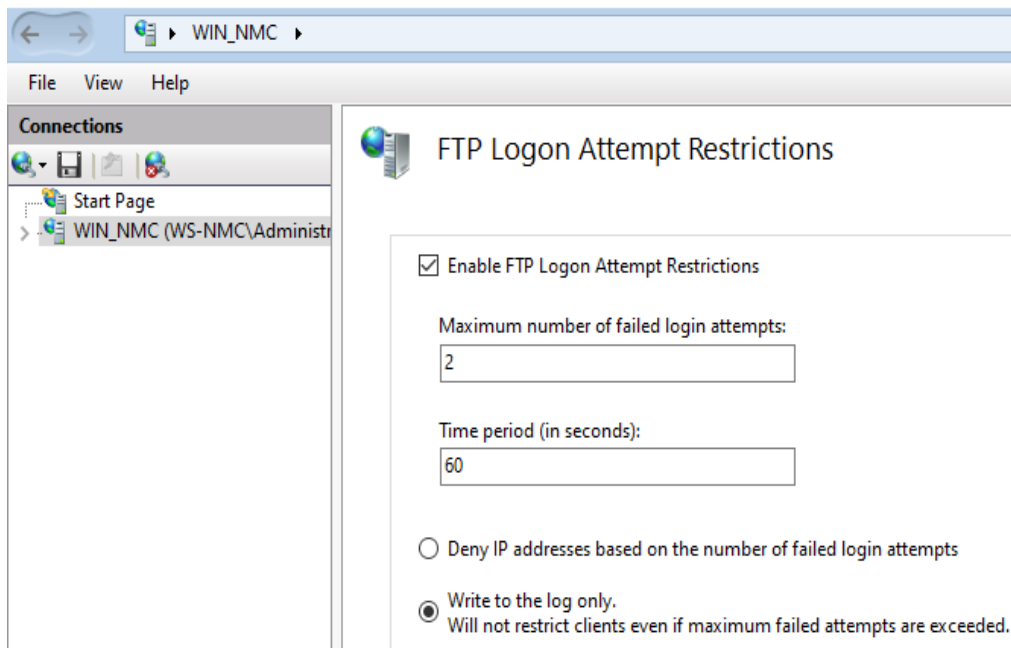
Utilitzant el Windows Server 2022 i el servei de FTP via IIS, caldrà configurar-ne el servei per tal que compleixi les premisses que a continuació es descriuran, i posteriorment, fer les comprovacions corresponents segons pertoquei. Com a client, sempre que no s'especifiqui el contrari, podeu fer servir qualsevol màquina, fins i tot fer les comprovacions amb el servidor actuant com a client a través del programa *ftp* via consola.

Partint de la configuració per defecte del servei, caldrà que aneu realitzant les diferents configuracions i comprovacions. Tot i que es poden anar fent una darrera l'altra, us aconsello primer fer totes les configuracions i al final de tot, les corresponents comprovacions, per si alguna configuració en modifica alguna d'anterior.

Primer de tot, a nivell general, ens caldrà establir un mínim control de seguretat al servei davant de possibles intents d'atac de força bruta.

Caldrà doncs que establiu un control per tant que es permetin màxim un total de 2 intents fallits d'inici de sessió i es produeixi un *timeout* de 60 segons si això es sobrepassa. No obstant, no s'ha de bloquejar la IP, sinó que s'ha d'escriure als logs.

- a) Adjunteu una captura amb la configuració d'intents de login anterior i un registre del log conforme per un usuari es demana password i aquest és invàlid. *1 punt*.



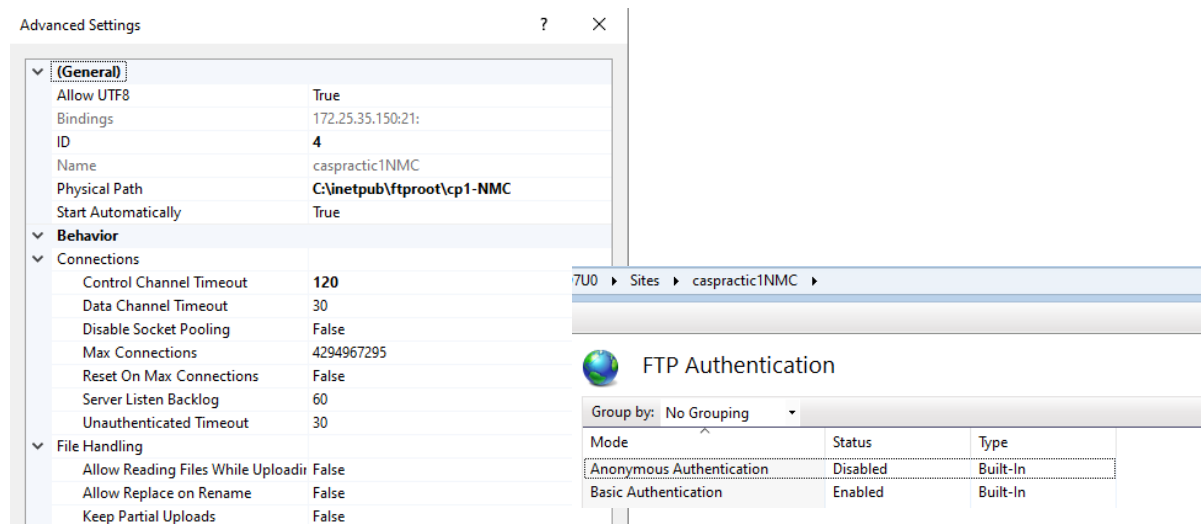
Tot seguit, caldrà que creeu un nou *site* FTP, que s'haurà de dir caspractic1XXX, on cal que substituïu les XXX per les vostres inicials de

treball. Aquest ha de tenir la carpeta c:\inetpub\ftproot\cp1-XXX com arrel del servei FTP. No us compliqueu la vida, via els permisos de Windows, feu una entrada 'Todos' amb permisos de lectura i escriptura tal com veieu a la imatge:

| Tipo | Entidad de seguridad | Acceso | Heredada de |
|---------|----------------------|--------------------------------|-------------|
| Perm... | Todos | Lectura, escritura y ejecución | Ninguno |

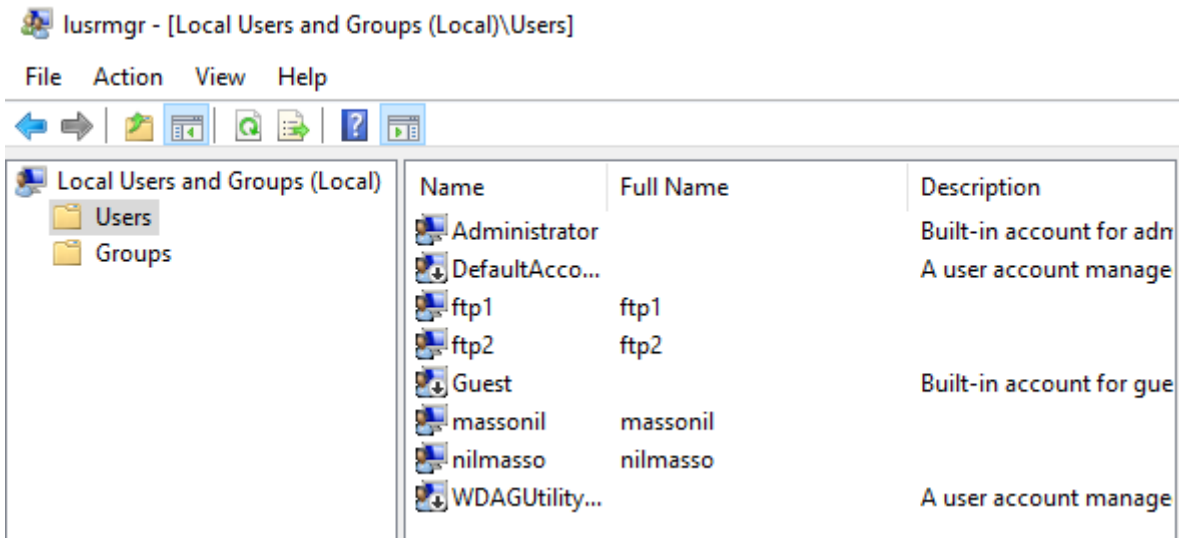
Aquest *site* ha de funcionar sense SSL, ha d'estar activat únicament per l'accés d'usuaris bàsics, i ha de tenir els permisos de llegir i escriure activats.

- b) Adjunteu una captura de la 'Configuración avanzada' del *site* i dels usuaris d'autenticació FTP permesos. *1 punt*.



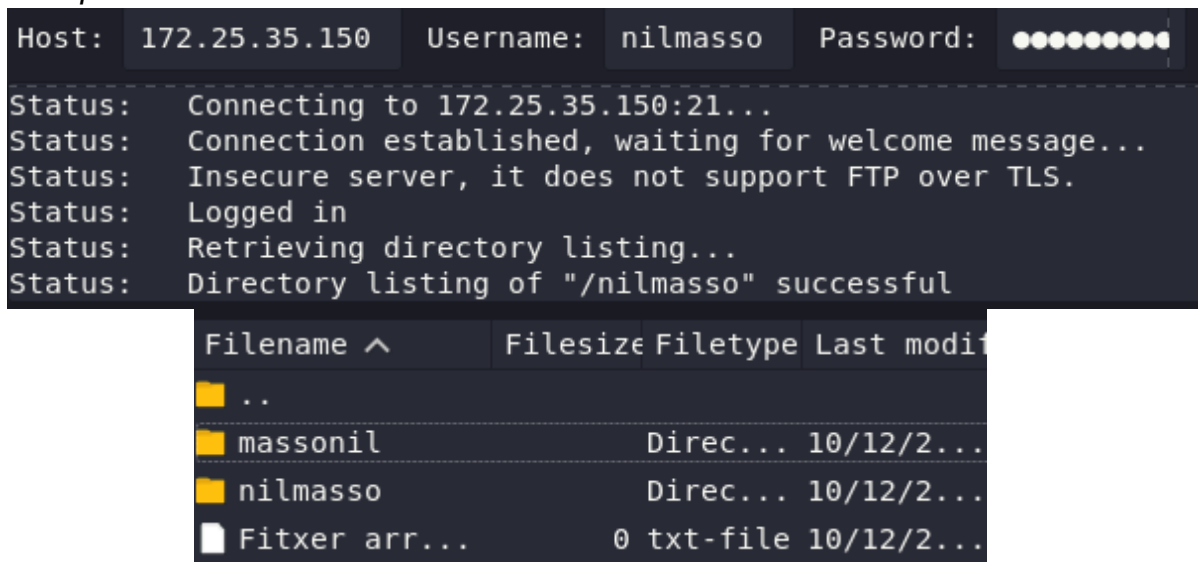
Per altra banda, cal crear 2 usuaris de sistema, un que sigui *nomcognom* i un que sigui *cognomnom*. Evidentment substituïu *nomcognom* i *cognomnom* pels vostres.

- c) Un cop ho tingueu, adjunteu una captura del llistat d'usuaris del sistema on consten aquests usuaris. *0,5 punts*.



A més a més, el servei FTP ha de fer que cada usuari comenci a la seva carpeta particular dins del directori FTP però sense aïllament.

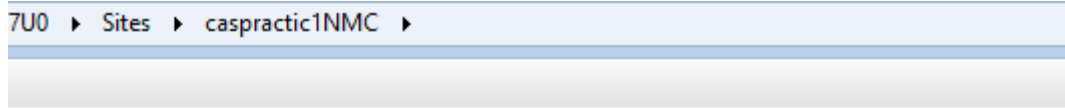
- d) Demostreu amb una captura a quin directori entra un dels usuaris creats quan feu login i que es pot moure per la resta de directoris. *1 punt*.



També cal que configureu els ports passius del servei FTP perquè específicament vagin del 4550 al 4560.

- e) Adjunteu una captura que en demostra la configuració i a més, amb el Wireshark, demostreu la comunicació entre client i servidor en mode passiu amb una captura de la part on, via el canal de control es

negocia el servei sota passiu, i després, del canal de dades, on es veu per quins ports es transfereix el fitxer. *1,5 punts.*



FTP Firewall Support

The settings on this page let you configure your FTP server to accept passive connections from an external firewall.

Data Channel Port Range:

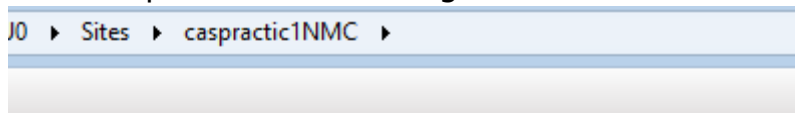
4550-4560

Example: 5000-6000

En aquesta única captura es veu tant, com es negocia el servei sota passiu primera i segona linea, com el port que s'utilitza per transferir les dades, marcat en vermell

A nivell d'autorització d'usuaris, cal que, denegueu l'escriptura d'usuaris anònims (encara que no estiguin habilitats, és prevenció pel futur), i que la resta mantinguin l'accés de lectura i escriptura.

f) Adjunteu una captura amb la configuració d'autoritzacions. *1 punt.*



FTP Authorization Rules

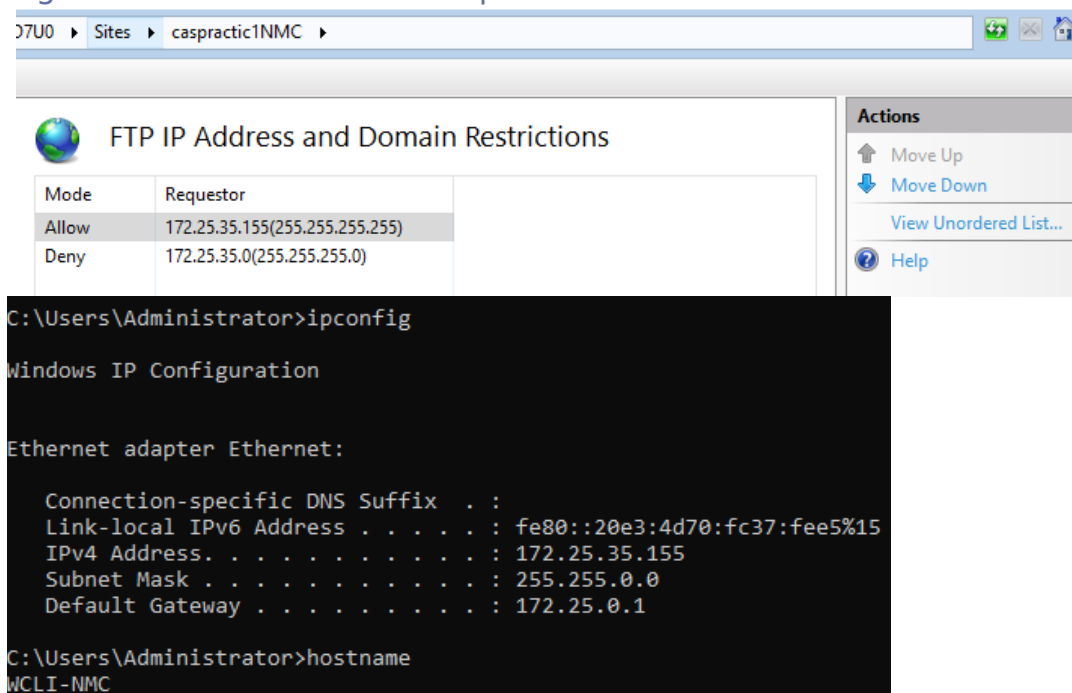
| Mode | Users | Roles | Permissions |
|-------|-----------------|-------|-------------|
| Deny | Anonymous Users | | Write |
| Allow | All Users | | Read, Write |

Per anar acabant, cal que restringiu l'accés al servei a només la IP del vostre client i la IP 172.25.X.155/32. La resta d'IPs del rang, han de quedar bloquejades a nivell de servei FTP.

g) Cal que adjunteu una captura d'un *ipconfig* i *hostname* des del vostre client, i posteriorment, la captura de la llista ordenada de IPs permeses/bloquejades al servei FTP. *1 punt.*

Entenc que del rang et refereixes al meu, .35, i per tant només /24, en cas de que fos del rang general ficaria /32(255.255.0.0).

Curiosament el meu WCLI te assignada la .155 com a conseqüència no em cal afegir un altre allow a la seva ip.



The screenshot shows the IIS Manager console with the 'caspractic1NMC' site selected. The 'FTP IP Address and Domain Restrictions' feature is expanded, showing a table with two entries: 'Allow' for '172.25.35.155(255.255.255.255)' and 'Deny' for '172.25.35.0(255.255.255.0)'. To the right, the 'Actions' pane shows 'Move Up', 'Move Down', 'View Unordered List...', and 'Help'.

Below the IIS Manager window, a Windows Command Prompt shows the following output:

```
C:\Users\Administrator>ipconfig

Windows IP Configuration

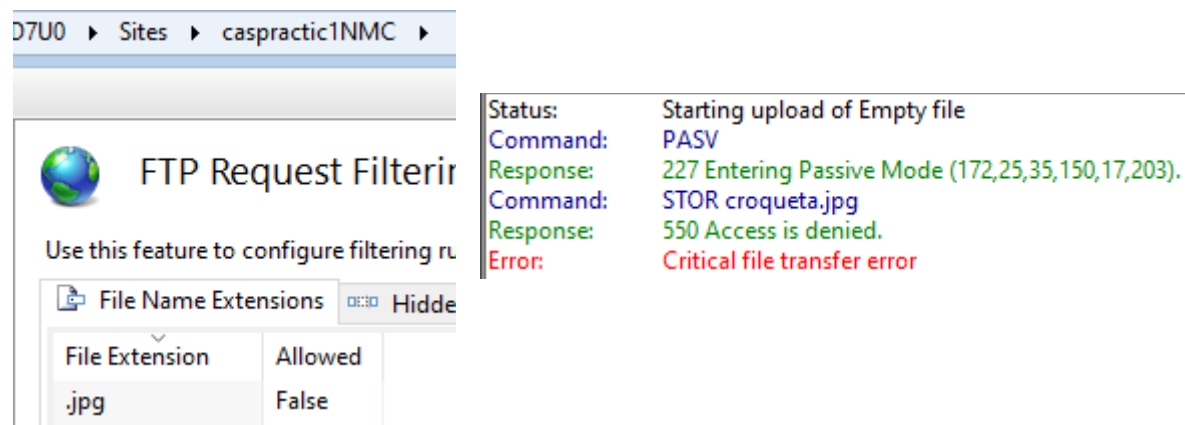
Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::20e3:4d70:fc37:fee5%15
    IPv4 Address. . . . . : 172.25.35.155
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 172.25.0.1

C:\Users\Administrator>hostname
WCLI-NMC
```

També cal que fer no es puguin crear directoris amb qualsevol usuari via FTP i que a més, no es puguin penjar imatges de tipus .JPG.

- h) Adjunteu les captures corresponents als paràmetres de configuració i les comprovacions des de client conforme no podeu penjar les imatges ni crear directoris. *2 punts.*

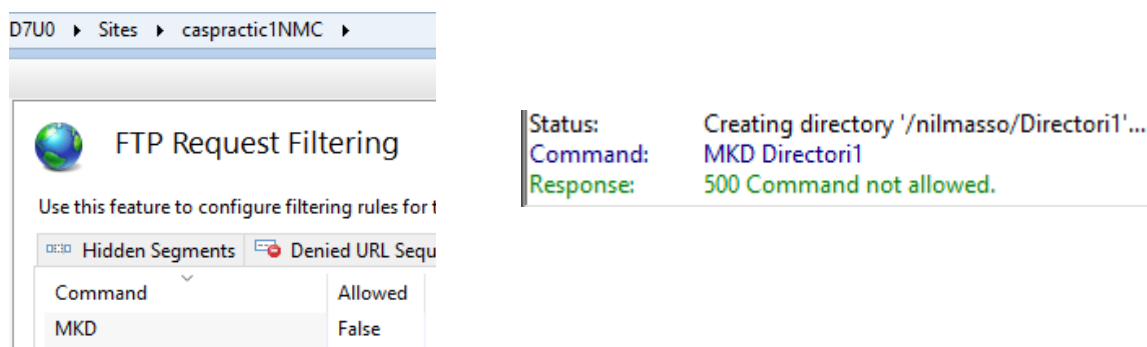


The screenshot shows the IIS Manager console with the 'caspractic1NMC' site selected. The 'FTP Request Filtering' feature is expanded, showing the 'File Name Extensions' tab. A table shows that '.jpg' is not allowed (False). To the right, the 'Status' pane shows the following output:

```
Status: Starting upload of Empty file
Command: PASV
Response: 227 Entering Passive Mode (172,25,35,150,17,203).
Command: STOR croqueta.jpg
Response: 550 Access is denied.
Error: Critical file transfer error
```

Per acabar, cal comprovar l'estructura de directoris del servei FTP.

- i) Per tant, cal que adjunteu una captura de c:\inetpub\ftproot\cp1-XXX\ *1 punt.*



The screenshot shows the IIS Manager console with the 'caspractic1NMC' site selected. The 'FTP Request Filtering' feature is expanded, showing the 'Hidden Segments' tab. A table shows that 'MKD' is not allowed (False). To the right, the 'Status' pane shows the following output:

```
Status: Creating directory '/nilmasso/Directori1'...
Command: MKD Directori1
Response: 500 Command not allowed.
```