Service FTP, FTPS, SFTP, gestion de droits et fichiers

Introduction :

La demande consiste à installer le service FTP Microsoft IIS, puis à configurer trois sites différents : un site FTP, un site FTPS (FTP sur SSL/TLS) et un site SFTP (FTP sur SSH). Pour chacun de ces sites, on veut configurer deux répertoires avec des permissions de lecture différentes, un site simple et un site avec authentification pour trois utilisateurs. Pour chaque site, on veut également capturer les échanges client-serveur via WireShark pour vérifier leur sécurité (en clair pour FTP, crypté pour FTPS et SFTP).

Les compétences :

Mettre en place et configurer des services de fichiers (partages)

Mettre en place et configurer des services de messagerie (SMTP, POP, IMAP, …)

Mettre en place et configurer des services de gestion de réseaux (DNS, DHCP, …)

Mettre en place et configurer des services d'authentification (LDAP, Kerberos, …)

Mettre en place et configurer des services de stockage (SAN, NAS, …)

Mettre en place et configurer des services de sécurité (firewall, VPN, …)

Mettre en place et configurer des services de sauvegarde et de restauration.

Sommaire :

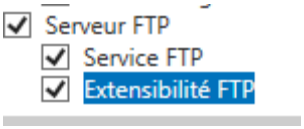
Partie 1 FTP :

Définition :

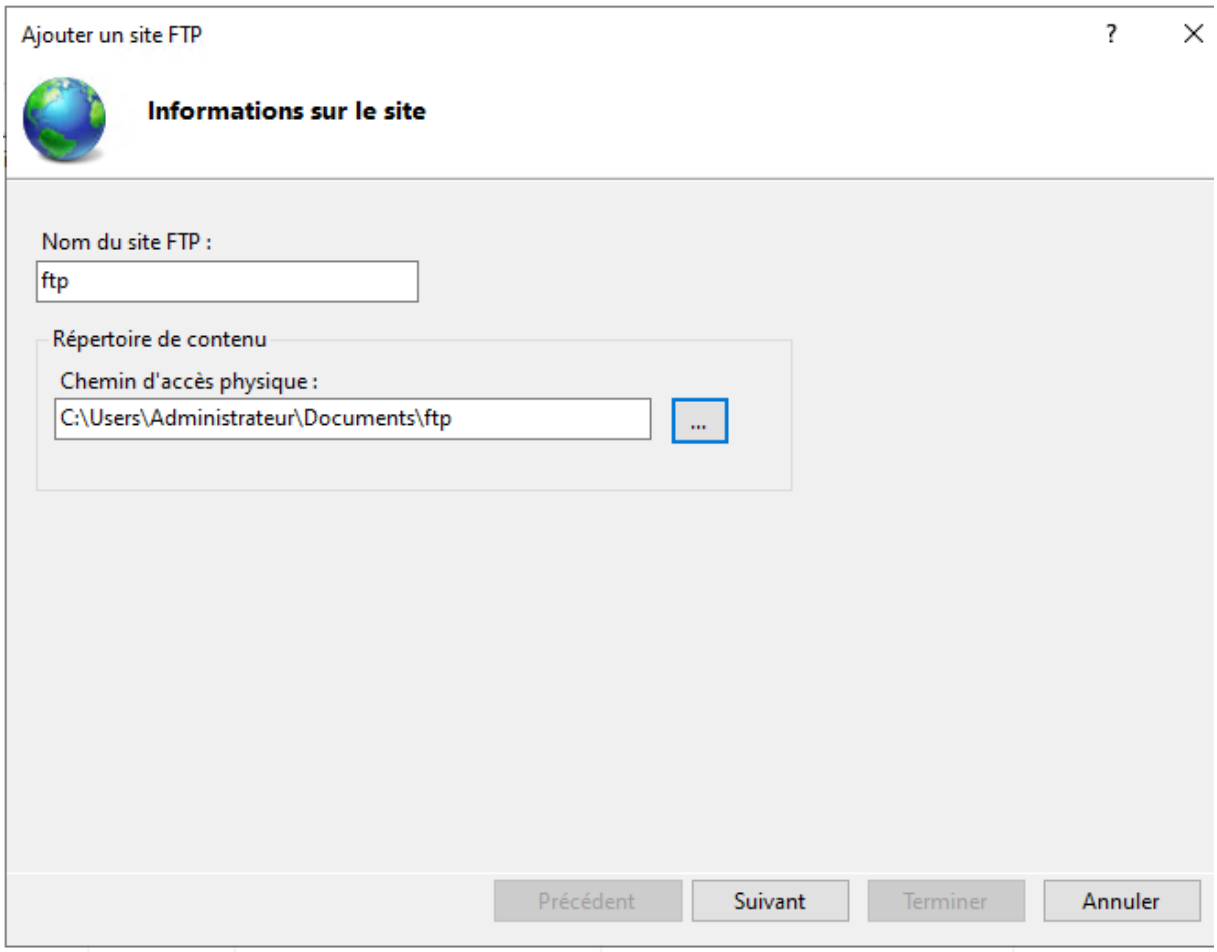
File Transfer Protocol, ou FTP, est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur.

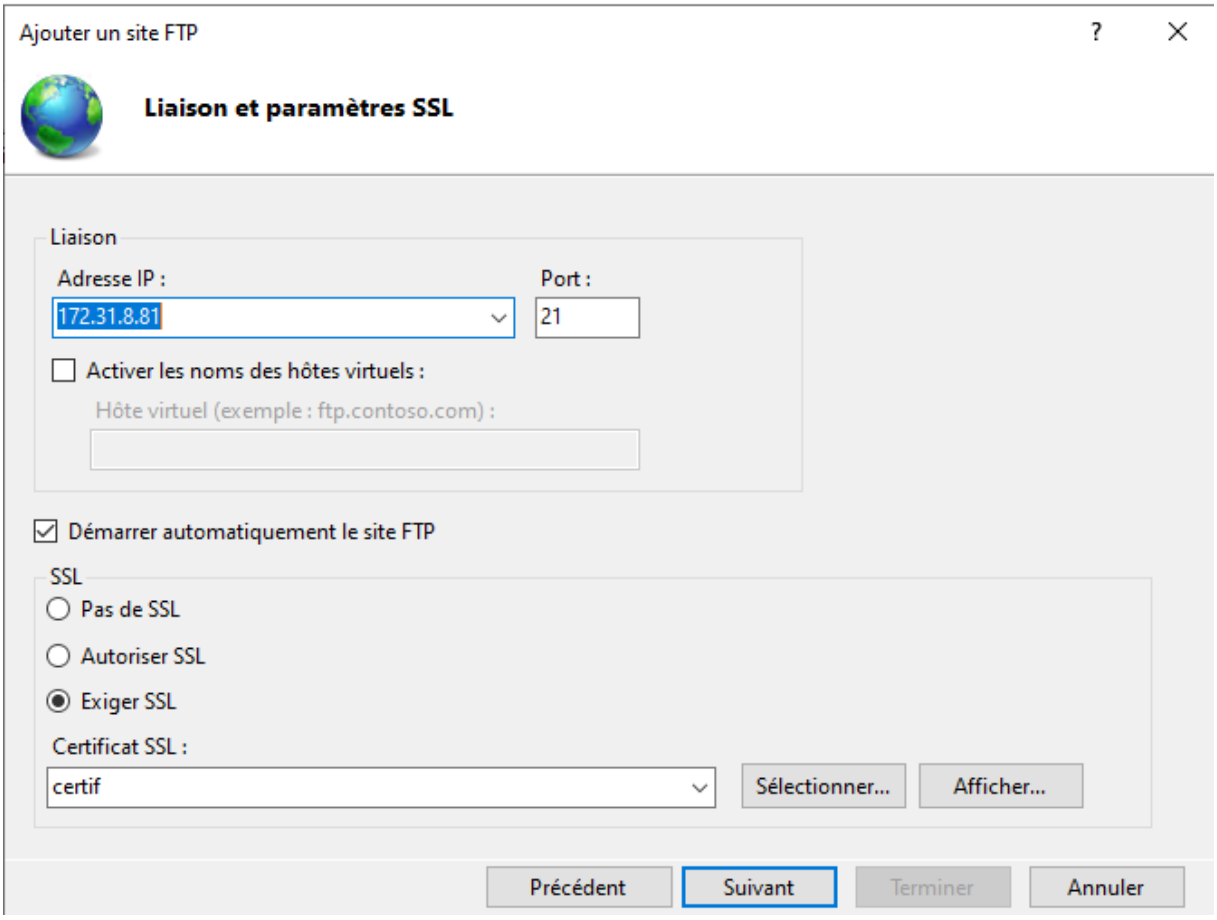
Installation du service FTP dans IIS :

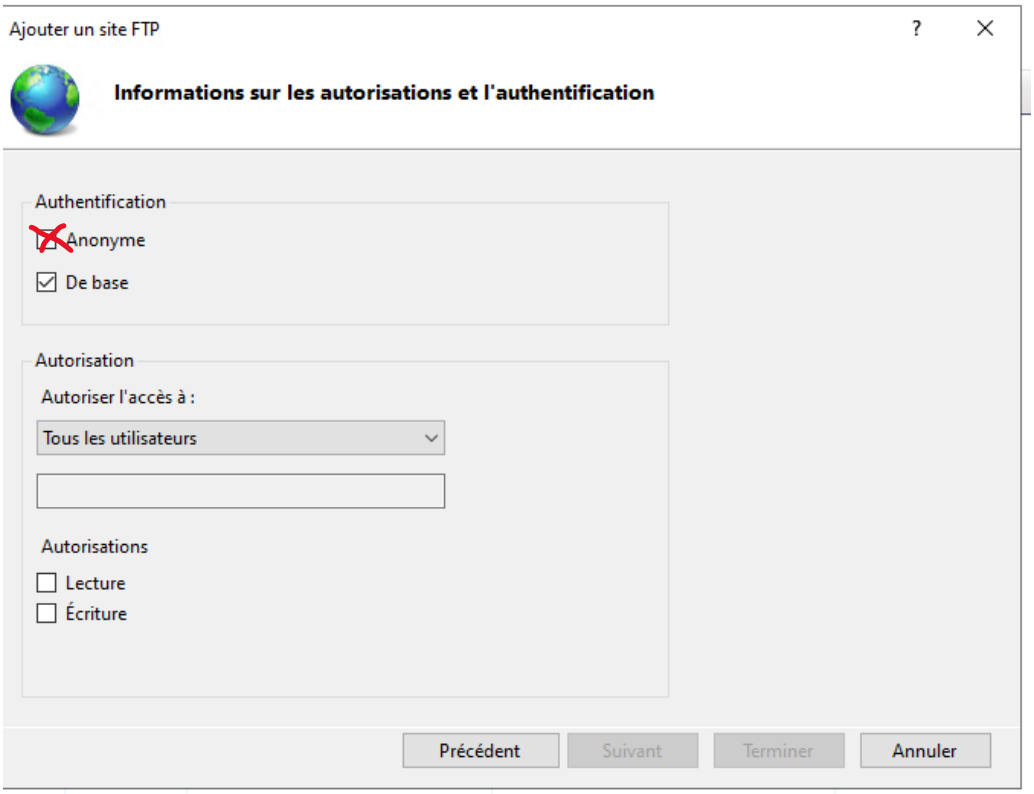
Quand on installe IIS dans les rôles on peut cocher serveur FTP.



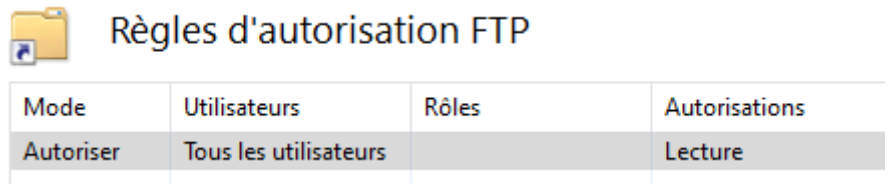
Configuration en mode anonyme :

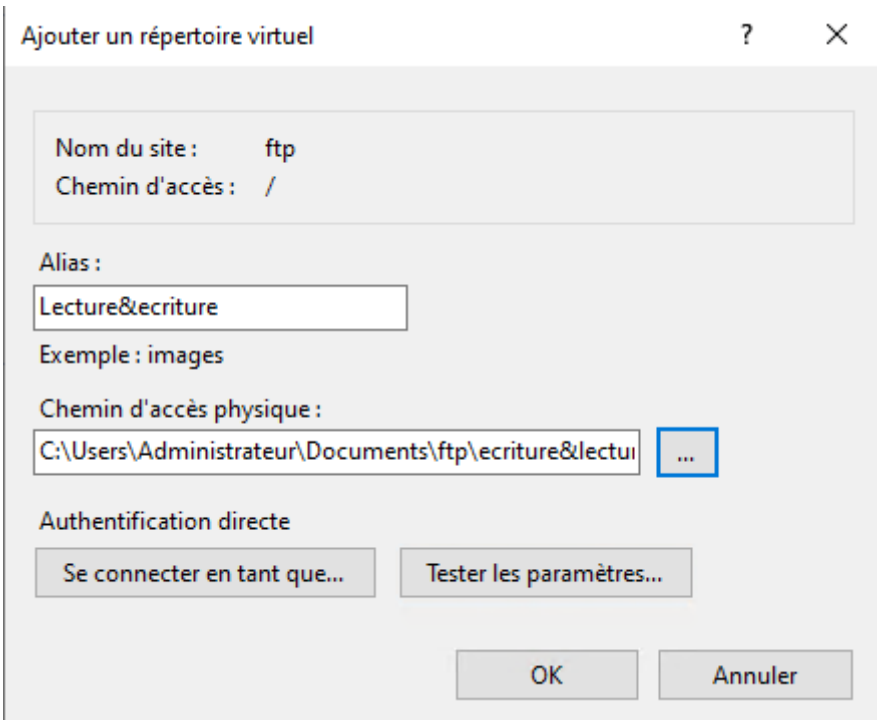


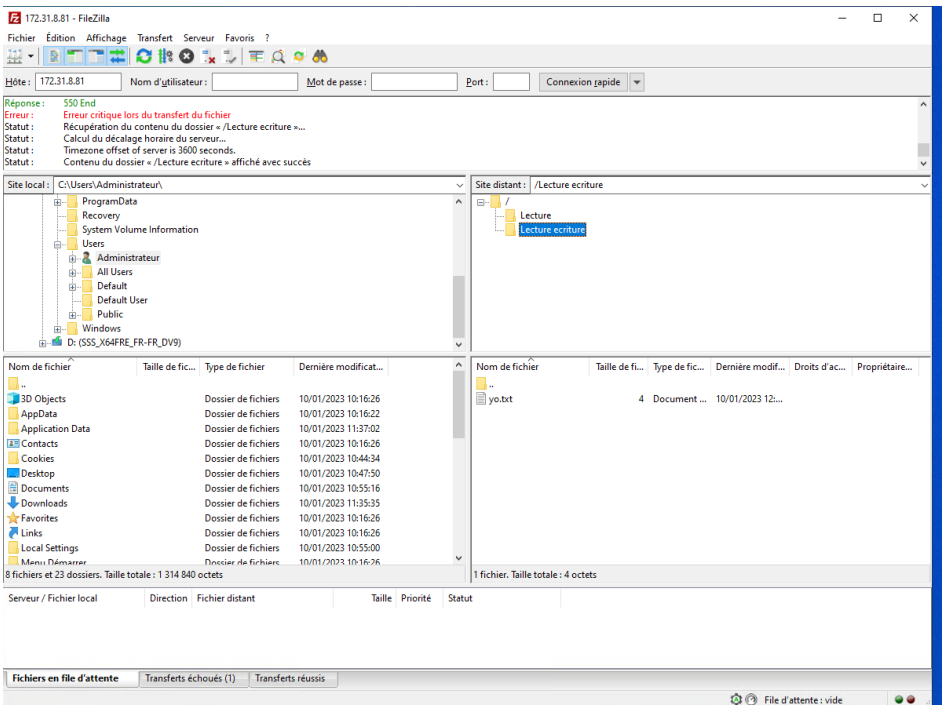

Ajouter un site FTP
Liaison et paramètres SSL
Liaison
Adresse IP :
172.31.8.81
Port :
21
Activer les noms des hôtes virtuels :
Hôte virtuel (exemple : ftp.contoso.com) :
Démarrer automatiquement le site FTP
SSL
Pas de SSL
Autoriser SSL
Exiger SSL
Certificat SSL :
certif
Sélectionner...
Afficher...
Précédent
Suivant
Terminer
Annuler


Ajouter un site FTP
Informations sur les autorisations et l'authentification
Authentification
Anonyme
De base
Autorisation
Autoriser l'accès à :
Tous les utilisateurs
Autorisations
Lecture
Écriture
Précédent
Suivant
Terminer
Annuler

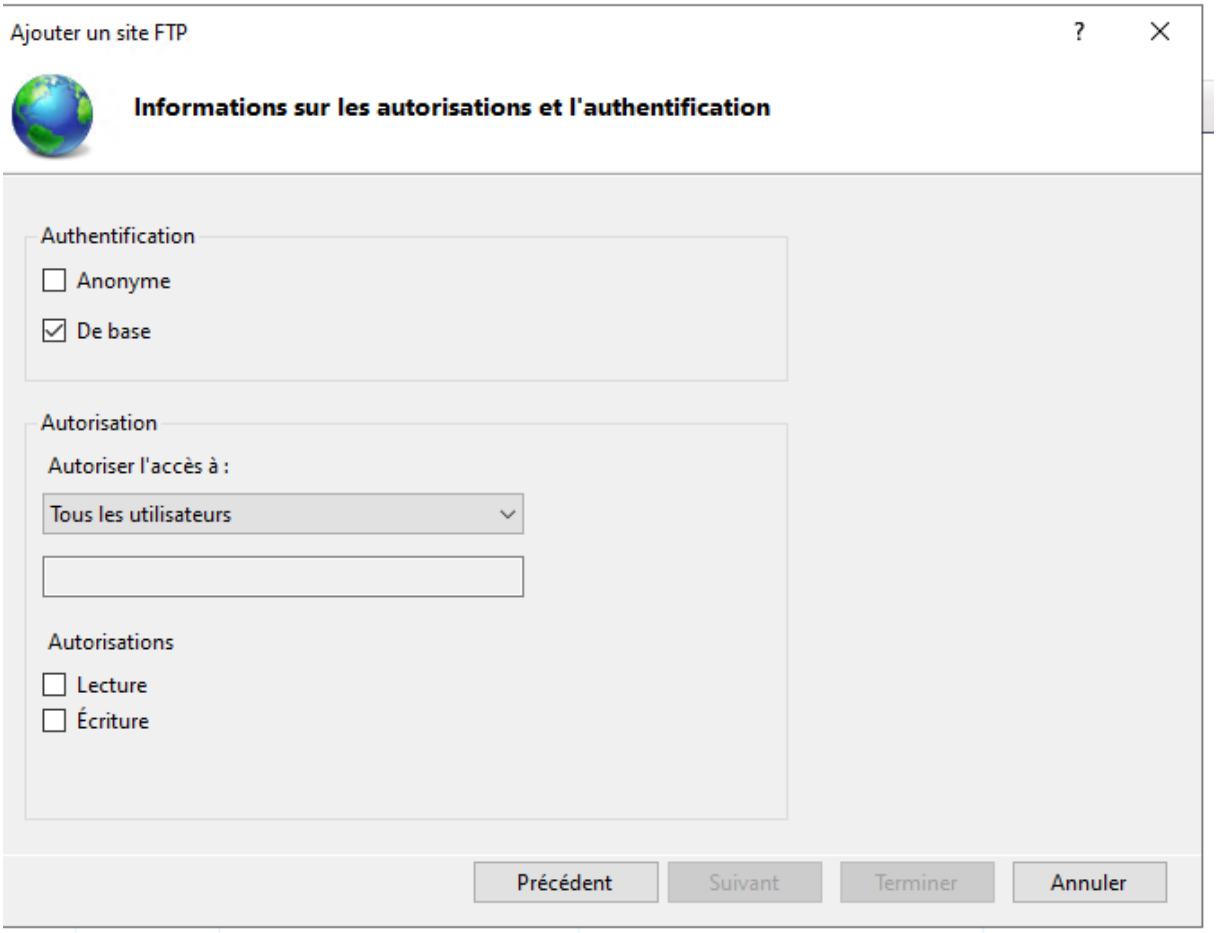
Droit accès au répertoire :







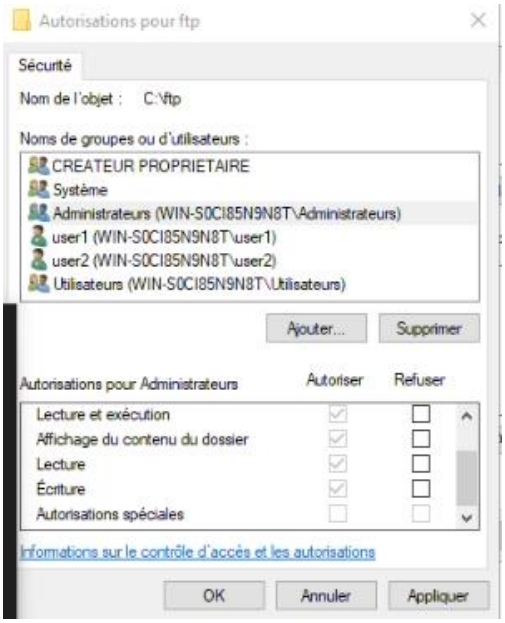
Configuration avec authentification :

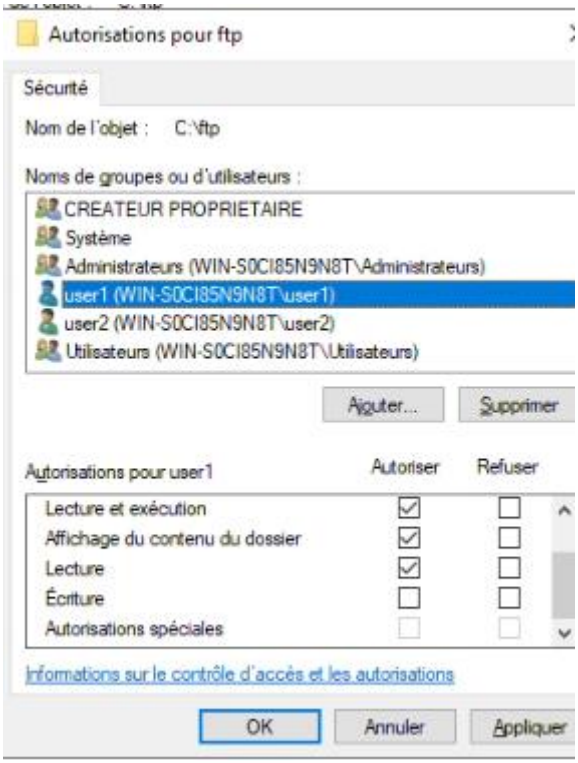


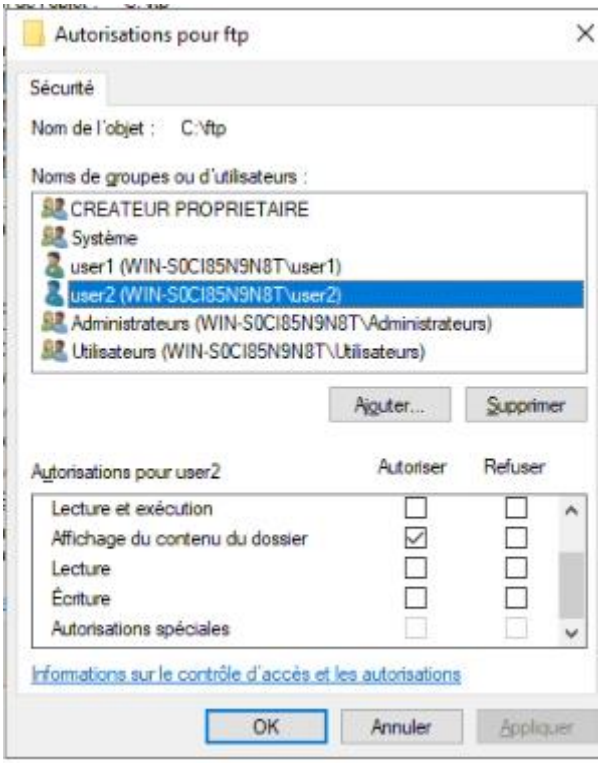
Création de 3 utilisateurs :

J'ai créé 3 utilisateurs 1 : Administrateur, 2 : user1 et 3 : user2.

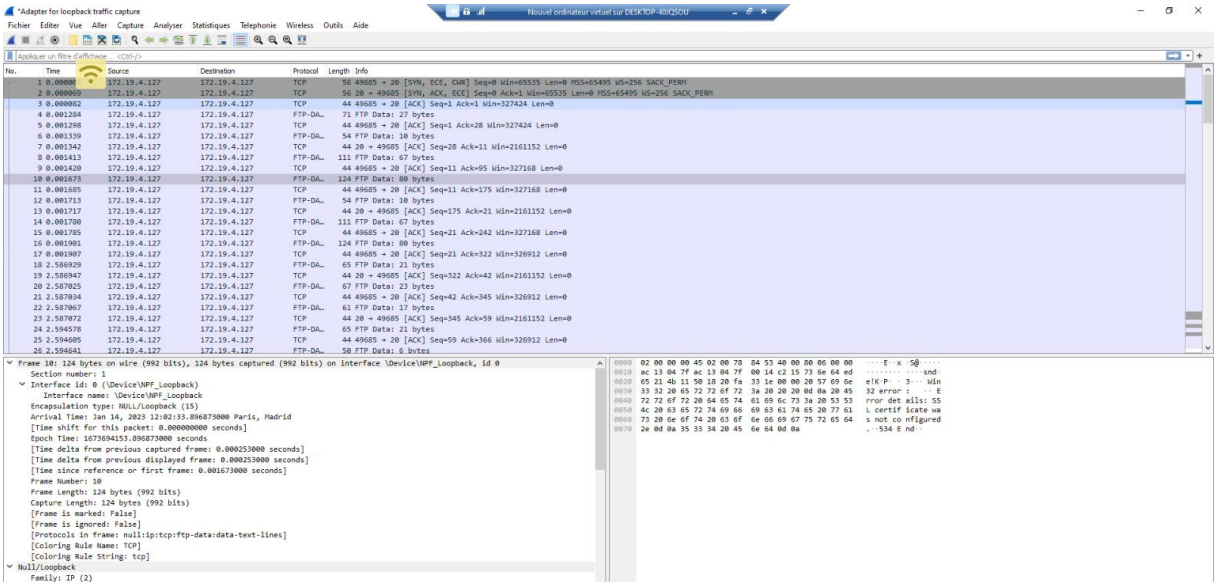
Droits accès au répertoire :




Autorisations pour ftp
Sécurité
Nom de l'objet : C:\ftp
Noms de groupes ou d'utilisateurs :
CREATEUR PROPRIETAIRE
Système
Administrateurs (WIN-S0CI85N9N8T\Administrateurs)
user1 (WIN-S0CI85N9N8T\user1)
user2 (WIN-S0CI85N9N8T\user2)
Utilisateurs (WIN-S0CI85N9N8T\Utilisateurs)
Ajouter...
Supprimer
Autorisations pour user1
Autoriser
Refuser
Lecture et exécution
Affichage du contenu du dossier
Lecture
Écriture
Autorisations spéciales
Informations sur le contrôle d'accès et les autorisations
OK
Annuler
Appliquer


Autorisations pour ftp
Sécurité
Nom de l'objet : C:\ftp
Noms de groupes ou d'utilisateurs :
CREATEUR PROPRIETAIRE
Système
user1 (WIN-S0CI85N9N8T\user1)
user2 (WIN-S0CI85N9N8T\user2)
Administrateurs (WIN-S0CI85N9N8T\Administrateurs)
Utilisateurs (WIN-S0CI85N9N8T\Utilisateurs)
Ajouter...
Supprimer
Autorisations pour user2
Autoriser
Refuser
Lecture et exécution
Affichage du contenu du dossier
Lecture
Écriture
Autorisations spéciales
Informations sur le contrôle d'accès et les autorisations
OK
Annuler
Appliquer

Capture Wireshark :



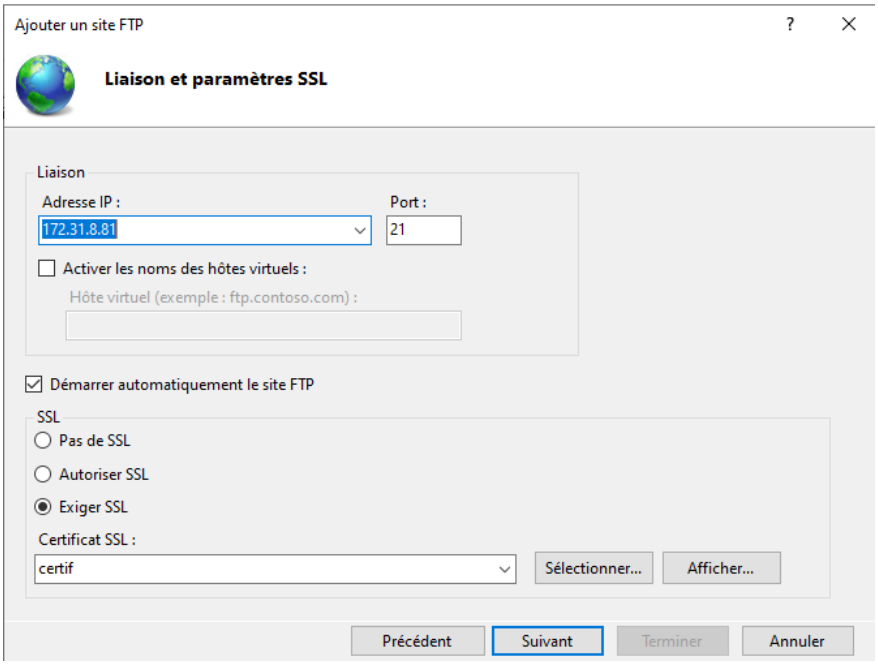
Partie 2 FTPS :

Définition :

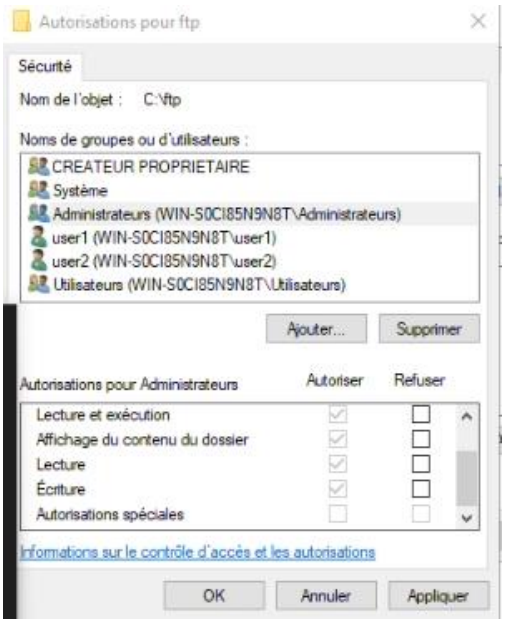
Le File Transfer Protocol Secure, abrégé FTPS, est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP, variante du FTP, sécurisé avec les protocoles SSL ou TLS.

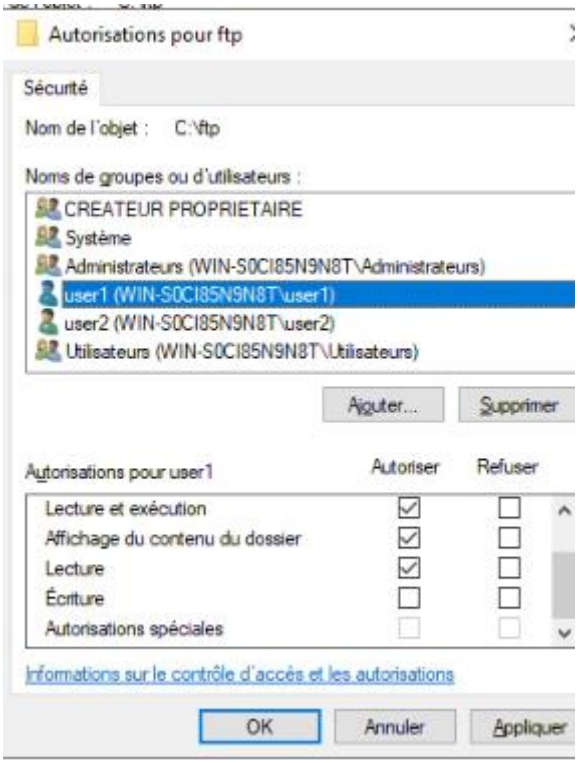
Mise en place de la sécurité FTPS :

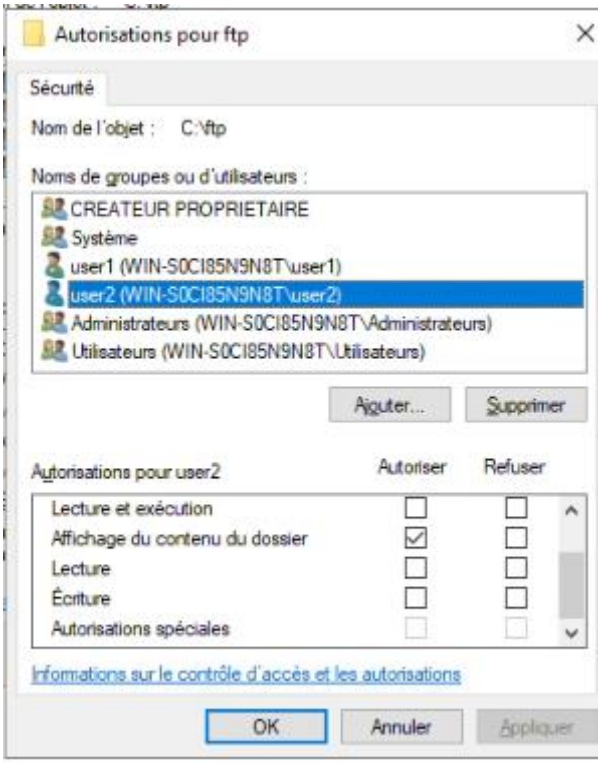
Pour cela on met une certification SSL :



Droit accès au répertoire :







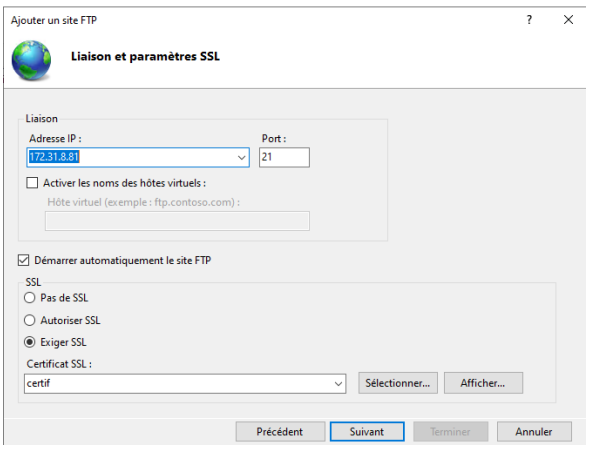
Partie 3 SFTP :

Différence en FTPS et SFTP :

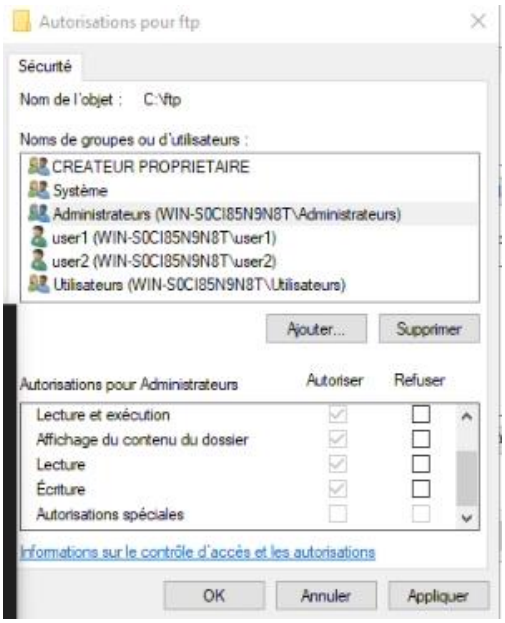
Une différence entre FTPS et SFTP est comment ces protocoles utilisent les ports. SFTP a besoin d'un seul port pour toutes les communications SFTP, ce qui permet de le protéger facilement. FTPS utilise plusieurs ports, ce qui représente une différence essentielle avec SFTP. Et FTPS encode les données et on le voit grâce à wireshark alors que SFTP encode les données mais on ne voit pas l'encodage sur wireshark.

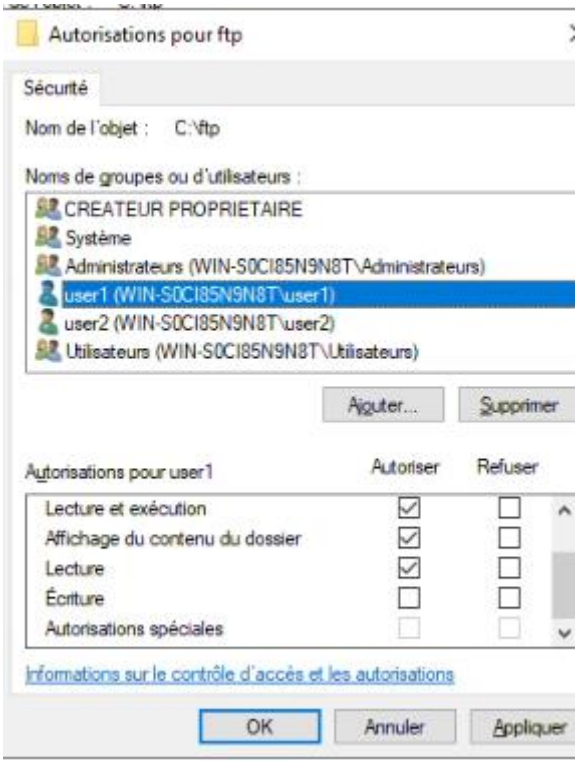
Mise en place de la sécurité SFTP :

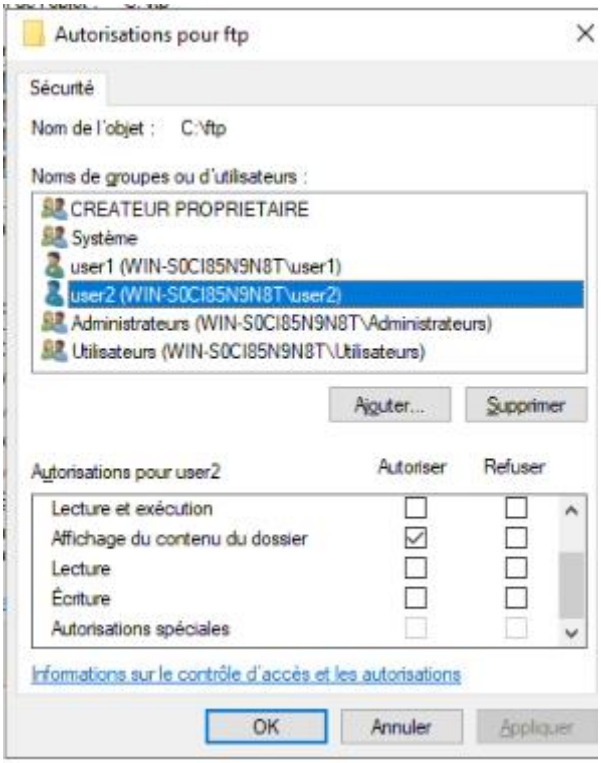
Pour cela on met une certification SSL et on change le port et on peut le voir dans filezilla dans l'ip on peut voir sftp :



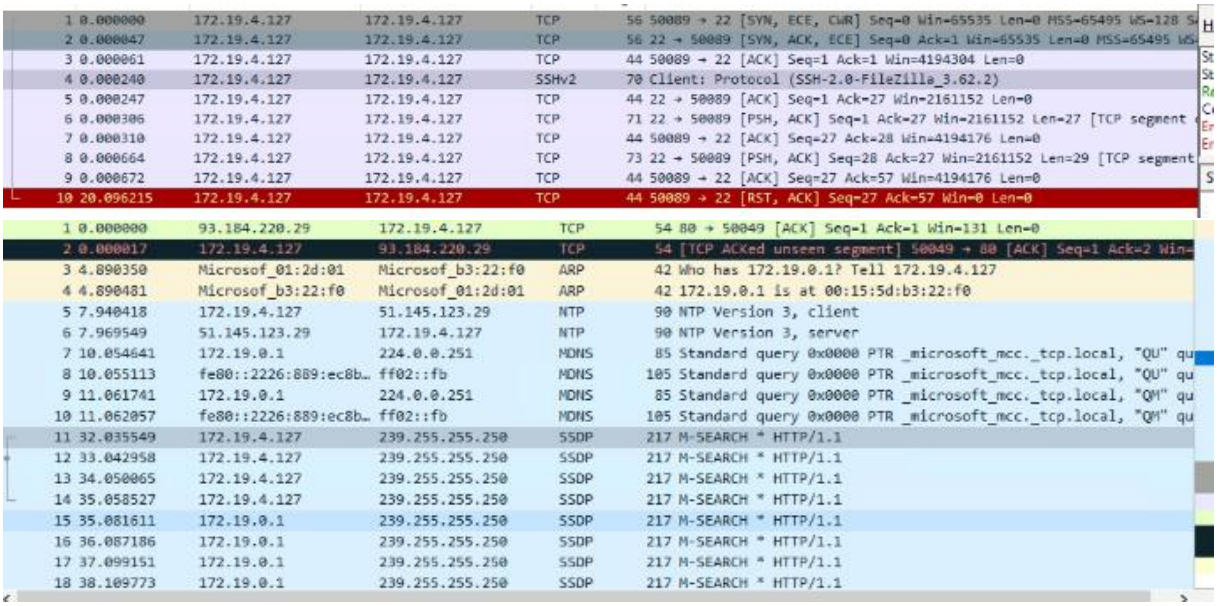
Droit accès au répertoire :







Capture wireshark :



1	0.000000	172.19.4.127	172.19.4.127	TCP	56 50089 → 22 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=65495 WS=128 S
2	0.000047	172.19.4.127	172.19.4.127	TCP	56 22 → 50089 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS
3	0.000061	172.19.4.127	172.19.4.127	TCP	44 50089 → 22 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
4	0.000240	172.19.4.127	172.19.4.127	SSHv2	70 Client: Protocol (SSH-2.0-FileZilla_3.62.2)
5	0.000247	172.19.4.127	172.19.4.127	TCP	44 22 → 50089 [ACK] Seq=1 Ack=27 Win=2161152 Len=0
6	0.000306	172.19.4.127	172.19.4.127	TCP	71 22 → 50089 [PSH, ACK] Seq=1 Ack=27 Win=2161152 Len=27 [TCP segment
7	0.000310	172.19.4.127	172.19.4.127	TCP	44 50089 → 22 [ACK] Seq=27 Ack=28 Win=4194176 Len=0
8	0.000664	172.19.4.127	172.19.4.127	TCP	73 22 → 50089 [PSH, ACK] Seq=28 Ack=27 Win=2161152 Len=29 [TCP segment
9	0.000672	172.19.4.127	172.19.4.127	TCP	44 50089 → 22 [ACK] Seq=27 Ack=57 Win=4194176 Len=0
10	20.096215	172.19.4.127	172.19.4.127	TCP	44 50089 → 22 [RST, ACK] Seq=27 Ack=57 Win=0 Len=0

1	0.000000	93.184.220.29	172.19.4.127	TCP	54 80 → 50049 [ACK] Seq=1 Ack=1 Win=131 Len=0
2	0.000017	172.19.4.127	93.184.220.29	TCP	54 [TCP ACKed unseen segment] 50049 → 80 [ACK] Seq=1 Ack=2 Win=
3	4.890350	Microsof_01:2d:01	Microsof_b3:22:f0	ARP	42 Who has 172.19.0.1? Tell 172.19.4.127
4	4.890481	Microsof_b3:22:f0	Microsof_01:2d:01	ARP	42 172.19.0.1 is at 00:15:5d:b3:22:f0
5	7.940418	172.19.4.127	51.145.123.29	NTP	90 NTP Version 3, client
6	7.969549	51.145.123.29	172.19.4.127	NTP	90 NTP Version 3, server
7	10.054641	172.19.0.1	224.0.0.251	MDNS	85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" qu
8	10.055113	fe80::2226:889:ec8b…	ff02::fb	MDNS	105 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" qu
9	11.061741	172.19.0.1	224.0.0.251	MDNS	85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" qu
10	11.062057	fe80::2226:889:ec8b…	ff02::fb	MDNS	105 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" qu
11	32.035549	172.19.4.127	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
12	33.042958	172.19.4.127	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
13	34.050065	172.19.4.127	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
14	35.058527	172.19.4.127	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
15	35.081611	172.19.0.1	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
16	36.087186	172.19.0.1	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
17	37.099151	172.19.0.1	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
18	38.109773	172.19.0.1	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1