

Power Week 2025

#pw2025

18 - 19 - 20 novembre 2025

IBM Innovation Studio Paris

S79 - SSH : les clefs du succès

20 novembre 13:45 - 14:45

Julien LAURIER
Gaia Mini Systèmes
julien.laurier@gaia.fr

IBM

common
FRANCE

Présentation

Julien LAURIER

Chez Gaia depuis 2020
Technicien IBM i



GAIA / VOLUBIS

Formation (débutant, perfectionnement)
Expertise IBM i
Centre de Services



Agenda

1. Quoi ? Pour qui ? Pour quoi ?
2. Protocoles
3. Prérequis
4. Première approche
5. Génération de clefs SSH
6. Seconde approche
7. Mise en place dans un programme
8. Contexte SSH
9. Gestion des logs
10. Récapitulatif

Power Week

18 -19 - 20 novembre 2025

IBM
common
FRANCE

IBM

Quoi, pour qui, pour quoi ?

Quoi ?

- **SSH** → **Secure SHell**
- Protocole de communication sécurisé
- Authentification et échanges sécurisés
- Couple de clés asymétriques
- Apparue en 1995, présent partout
- [OpenSSH 10.2](https://www.openssh.com/) released October 10, 2025

<https://www.openssh.com/>



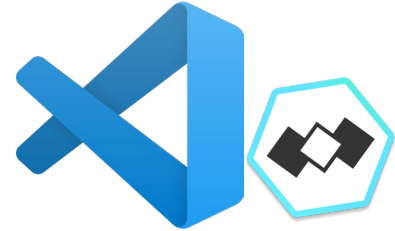
Pour qui ?

Tout le monde !



Pour quoi ?

- Sécurisation de flux ftp
- ACS (IBM Access Client Solution)
- FileZilla
- VSCode
- RDi (debug)
- Hosts Git
- ...



Power Week

18 -19 - 20 novembre 2025

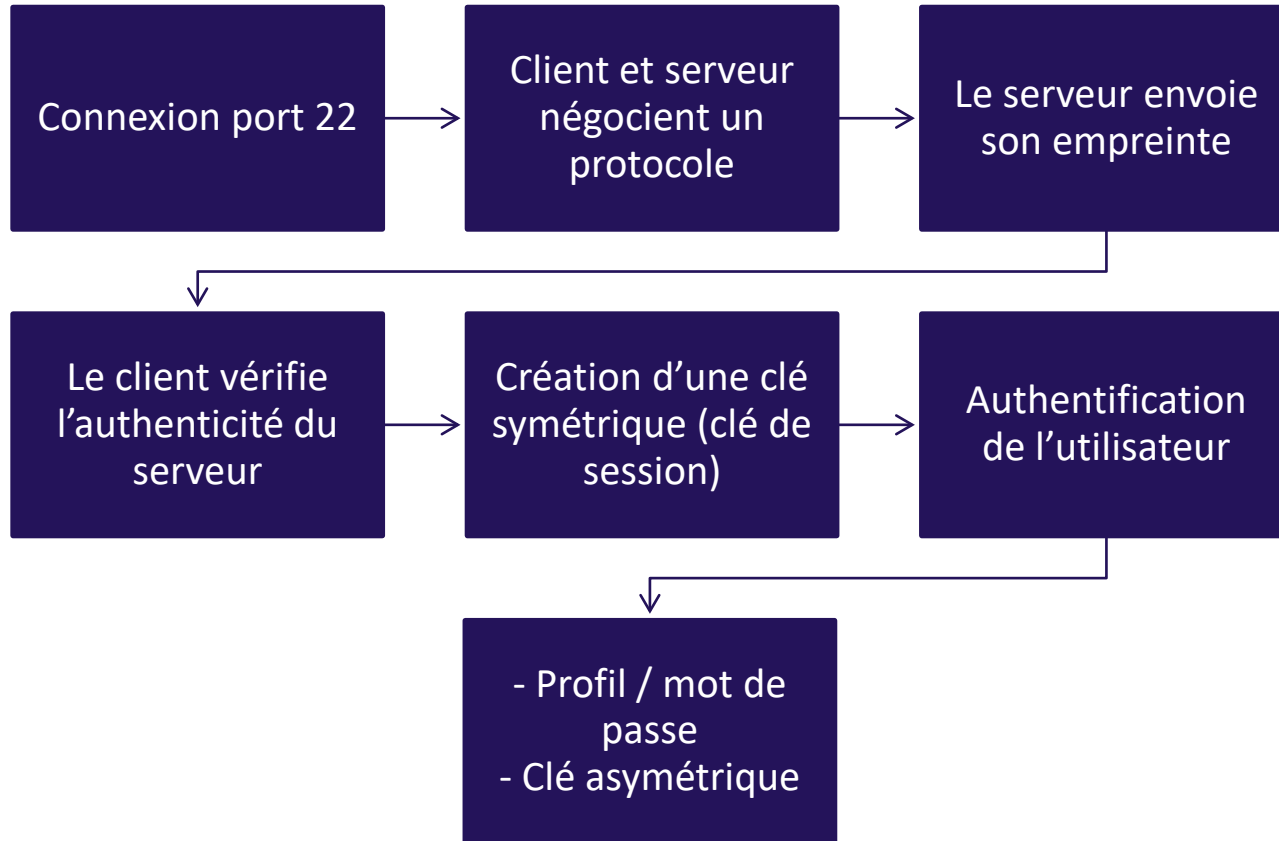


Protocoles

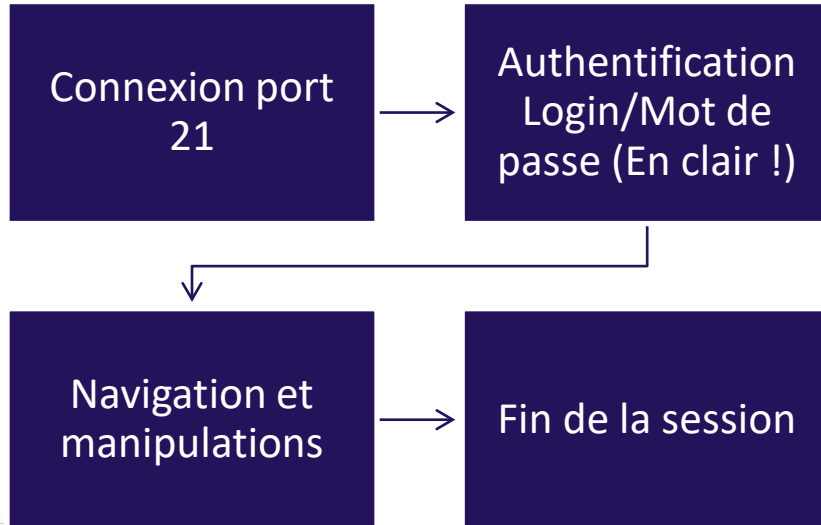
Protocoles - Sécurité

	SSL	TLS	SSH
Usage	Chiffage des échanges dans le web	Chiffage et sécurisation des échanges plus largement dans les échanges réseau	Chiffage et sécurisation des échanges et interactions avec un système distant + Son propre système d'authentification
Ports	443	443	22

Protocoles - SSH



Protocoles - Transfert de fichiers - FTP



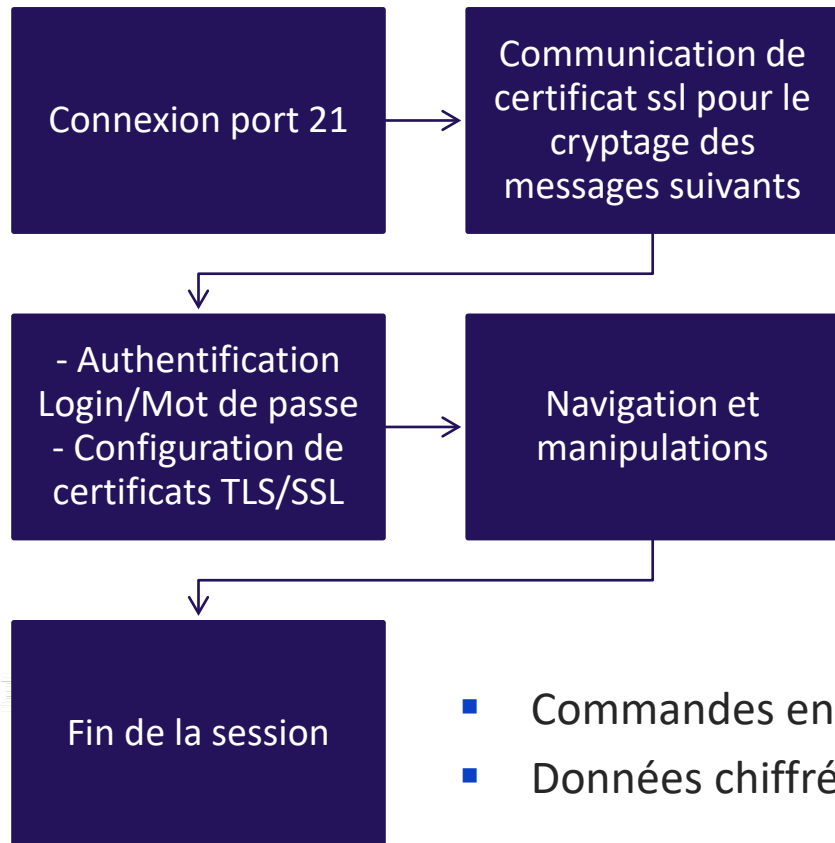
```
QSH
$ ftp server_name

$ user user_name
$ password *****

[ls / pwd / cd / lcd ...]
$ get file_path

$ quit
```

Protocoles - Transfert de fichiers - FTPS



- Commandes en clair
- Données chiffrées

QSH

```
$ ftp -e server_name
```

```
$ user user_name
```

```
$ password *****
```

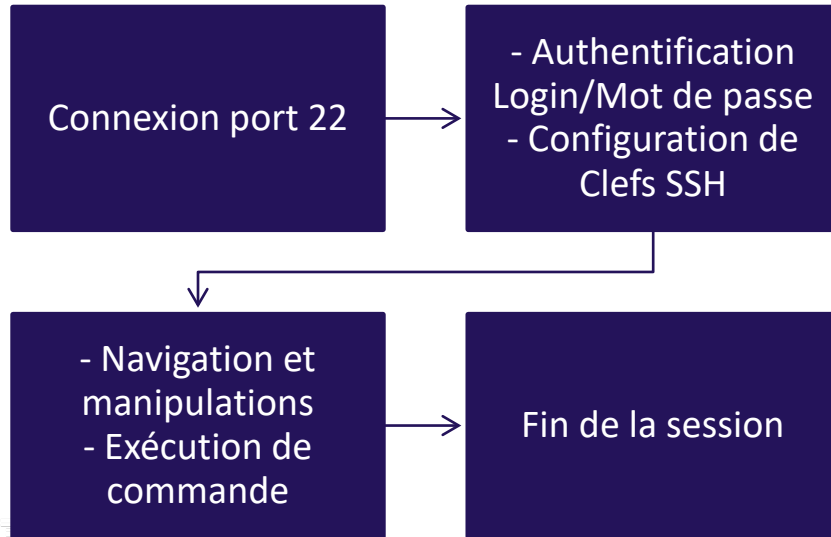
```
$ AUTH SSL  
(chiffrement des commandes  
et données en SSL)
```

```
[ls / pwd / cd / lcd ...]
```

```
$ get file_path
```

```
$ quit
```

Protocoles - Transfert de fichiers - SFTP



```
QSH
$ sftp server_name

$ user user_name

[ls / pwd / cd / lcd ...]
$ get file_path

$ exit
```

Protocoles - Transfert de fichiers

	FTP	FTPS	SFTP / SCP
Niveau de sécurité	Inexistant	Moyen	Fort
Port(s)	21	990 (contrôle) 989 (données)	22
Authentification	Profil / mot de passe	Profil / mot de passe	Profil / couple de clés
Chiffrage	Néant	Chiffrage des données via SSL/TLS	Chiffrage complet via tunnel SSH
Intégrité des données	Non garantie	Garantie via SSL/TLS	Garantie via SSH

Power Week

18 -19 - 20 novembre 2025



Prérequis

À ne jamais perdre de vue

- ~ → Répertoire initial de l'utilisateur courant
- Les droits sur les répertoires et les fichiers doivent être les plus stricts possibles (surtout les fichiers présents dans le répertoire .ssh)
- Attention à la version d'OpenSSH atteinte (/QOpenSys/pkgsrc/bin ou /QOpenSys/usr/bin)
- Attention au CCSID des fichiers de clés et au CRLF
- Si l'IBM i est la cible le profile QSSHD doit être *ENABLED

Prérequis – Répertoire utilisateur

- L'utilisateur doit avoir un répertoire initial dans l'ifs

```
5250  
==> MKDIR DIR(' /home/PW2025/')  
==> CHGOWN OBJ(' /home/PW2025/') NEWOWN(PW2025)
```

- Le service SSH serveur doit être démarré sur le serveur à atteindre

```
5250  
==> STRTCPSVR SERVER(*SSHD)
```

```
PowerShell  
C:\> start-service sshd
```

- Vérifier son fonctionnement sur IBM

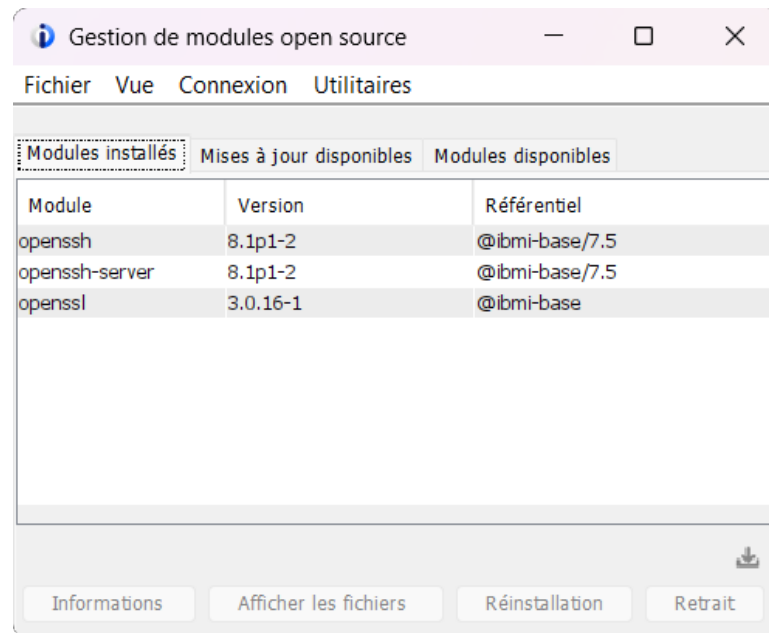
```
5250  
==> WRKTCPSVS OPTION(*CNN)
```



Remote Address	Remote Port	Local Port	Idle Time	State
*	*	ssh	003:56:09	Listen

Prérequis – Modules Open Source

- Modules Open Sources (À jour !)
- OpenSSH (ssh, sftp, scp ...)
- OpenSSL (Crypto)



The screenshot shows a window titled 'Gestion de modules open source' with a menu bar containing 'Fichier', 'Vue', 'Connexion', and 'Utilitaires'. Below the menu bar are three tabs: 'Modules installés' (selected), 'Mises à jour disponibles', and 'Modules disponibles'. The 'Modules installés' tab displays a table with three columns: 'Module', 'Version', and 'Référentiel'. The table lists three installed modules: 'openssh' (version 8.1p1-2, reference @ibmi-base/7.5), 'openssh-server' (version 8.1p1-2, reference @ibmi-base/7.5), and 'openssl' (version 3.0.16-1, reference @ibmi-base). At the bottom of the window, there are four buttons: 'Informations', 'Afficher les fichiers', 'Réinstallation', and 'Retrait', along with a download icon.

Module	Version	Référentiel
openssh	8.1p1-2	@ibmi-base/7.5
openssh-server	8.1p1-2	@ibmi-base/7.5
openssl	3.0.16-1	@ibmi-base

Power Week

18 -19 - 20 novembre 2025

Première approche



Validation de la communication

```
QP2TERM
```

```
$ ssh -T pw2025@ibmi.local.lan
```

```
The authenticity of host 'ibmi (192.168.xxx.xxx)' can't be established.
```

```
ECDSA key fingerprint is SHA256:aXBtTJpae8buntUbfX8YVm0Byz7C37bEcYLNrtpBC1s.
```

```
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

```
$ yes
```

```
Warning: Permanently added 'ibmi,192.168.xxx.xxx' (ECDSA) to the list of known hosts.
```

```
Connection closed by 192.168.xxx.xxx port 22
```

```
$ ssh -T pw2025@ibmi.local.lan
```

```
pw2025@ibmi's password:
```

```
$ *****
```

```
$ ls
```

```
ici_ibmi
```

Transfert via scp

```
QP2TERM
```

```
$ cd /QOpenSys/pkgsrc/bin
```

```
$ sshpass -p '*****' scp ~/fileA.txt pw2025@ibmi:fileA_new.txt
```

```
(ibmi_target)/home/pw2025/fileA_new.txt
```

```
*****Beginning of data*****
```

```
This is not a test!
```

```
*****End of Data*****
```

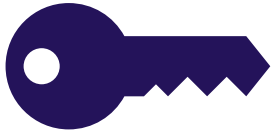
Power Week

18 -19 - 20 novembre 2025

Génération d'une clef



Concept de clefs SSH



Clef privée




Clef publique



Serveur (empreinte)

PuTTY Key Generator

 PuTTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
AAAAB3NzaC1yc2EAAAADAQABAAQACg0EvXiUwiiKPhAO1SAPPcs0xiUfbmGg2znAGvbvh6rcp9gDw1yicalaJ9Ck0y  
Bvdipor/kexBxPQIKWOfCix4hQObTtuFns1VmKJhDofr8Qy2aZPnuH7B7xKKNesS96A1Zwk83g2pFGf/1682ATqD5WH1E3c  
pPN0qwQ1zuSng3OezUWCUALoHfn7vYgp+55YSDxJQPEk5tkOzrW3E9PcRRaF  
+6ML94qFY6QDFFSyUPi4hxqnextctRMMCDIV2tG3wpBHq9Yy4lwhYr3VlcJJRm4bBER  
+6Ay1QOiPv4IJE2PToT3nCZkrLLlutoU55YqfFy/Yvo1AjTSS9XwxUu1rhp rsa-key-20231106
```

Key fingerprint: ssh-rsa 2048 SHA256:6Max1fiT+DDHmtFIQpMY3XK6TSUU9Y+zpyq+S6jaLdw

Key comment: rsa-key-20231106

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair Generate

Load an existing private key file Load

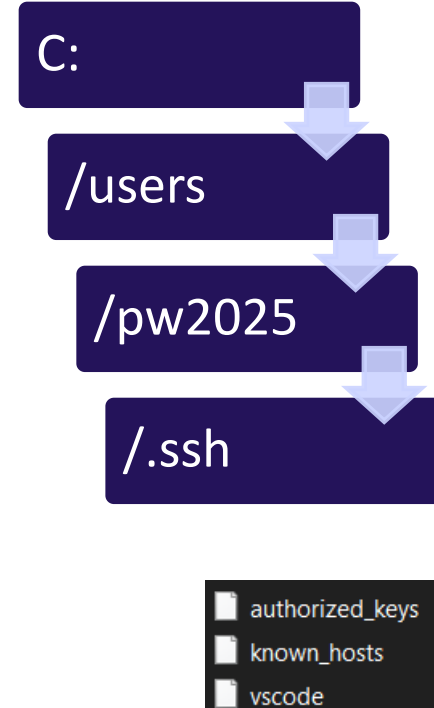
Save the generated key Save public key Save private key

Parameters

Type of key to generate:

☒ RSA ☐ DSA ☐ ECDSA ☐ EdDSA ☐ SSH-1 (RSA)

Number of bits in a generated key: 2048



Génération manuelle - 1

```
QP2TERM
```

```
$ ssh-keygen
```

```
Generating public/private rsa key pair.
```

```
Enter file in which to save the key
```

```
(/home/pw2025/.ssh/id_rsa):
```

```
$ ~/.ssh/monkey
```

```
Enter passphrase (empty for no passphrase):
```

```
$
```

```
Your identification has been saved in uranus.
```

```
Your public key has been saved in uranus.pub.
```



Génération manuelle - 2

The key fingerprint is:

SHA256:qtRtBIACHGwtlUNhZDanYRmUSZ6FDROIoP02TeBoXvg pw2025@IBMI.LOCAL.LAN

The key's randomart image is:

```
+---[RSA 3072]-----+
|*..++X^%O          |
|o+o=*%O.           |
|..= =++            |
|  o = o .          |
|   . E . S         |
|    . o +          |
|    . o o          |
|    . . .          |
|    .              |
+-----[SHA256]-----+
```

Génération manuelle en une ligne !

QP2TERM

```
$ ssh-keygen -t rsa -b 3072 -f ~/.ssh/monkey -N ''
```

Generating public/private rsa key pair.

Your identification has been saved in /home/pw2025/.ssh/monkey.

Your public key has been saved in /home/pw2025/.ssh/monkey.pub.

The key fingerprint is:

SHA256:9l+JLyHKBBxWqqsCF7JbtzSs6YxWh8nN1Hw4vf2NaZk pw2025@IBMI.LOCAL.LAN

The key's randomart image is:

+---[RSA 3072]-----+

```
|
|      .
|      o + o
|      . . . * = .
|      + 0 S= +
|      o B 0. .= o. .
|      * * + +...oo*
|      oo+ . + ..oE .
|      ...o..... .o.
|
```

+-----[SHA256]-----+

Points clefs de la génération de... clefs

Options	Description
-t	Type de clef créée
-b	Nombre de bits composant la clef
-f	Fichier de sortie
-N	Phrase de chiffrement

Type	Tailles possibles
dsa	Déprécié
rsa	min. 1024 - dft. 3072
ecdsa	256 - 384 - 521
ed25519	Taille fixe



<https://man.openbsd.org/ssh-keygen>

Exemple de mise en place sur VSCode



Clef privée

Login Settings: Neptoune X

Host or IP Address

Port (SSH)

22

Username

Only provide either the password or a private key - not both.

Password

Only provide a password if you want to update an existing one or set a new one.

Private Key

Only provide a private key if you want to update from the existing one or set one. OpenSSH, RFC4716, or PPK formats are supported.

Choose File No file chosen

Save



Clef publique

- Créer le fichier `authorized_keys` et accorder les bons droits

```
QP2TERM
```

```
$ mkdir ~/.ssh
```

```
$ chmod 700 ~/.ssh
```

```
$ touch authorized_keys
```

```
$ chmod 600 ~/.ssh/authorized_keys
```

- Copier la valeur de la clef publique sur le serveur: `~/.ssh/vscode.pub` → `~/.ssh/authorized_keys`

Power Week

18 -19 - 20 novembre 2025



Approche réelle

Protocoles - Transfert de fichiers

- `scp -i ~/.ssh/monkey ~/fileB.txt pw2025@ibmi_target:fileB_new.txt`

QP2TERM

```
$ scp -i ~/.ssh/monkey ~/fileB.txt pw2025@ibmi:fileB_new.txt
```

- `scp -i [clé privée] [fichier local] [profil]@[cible]:[fichier destination]`

```
(ibmi)/home/pw2025/fileB_new.txt
```

```
*****Beginning of data*****
```

```
I'm just a useless file...
```

```
*****End of Data*****
```

Power Week

18 -19 - 20 novembre 2025



Intégration dans un programme

Programme – SCP

```
PGM
/* Variables */
DCL      VAR(&SRCFILE) TYPE(*CHAR) LEN(50) VALUE('/home/pw2025/fileC.txt')
DCL      VAR(&USER) TYPE(*CHAR) LEN(3) VALUE('PW2025')
DCL      VAR(&TARGET) TYPE(*CHAR) LEN(30) VALUE('ibmi')
DCL      VAR(&RMFILE) TYPE(*CHAR) LEN(50) VALUE('/home/pw2025/fileC_new.txt')
DCL      VAR(&CMD) TYPE(*CHAR) LEN(500)

/* Mise en place d'un fichier de log */
ADDENVVAR ENVVAR(QIBM_QSH_CMD_OUTPUT) VALUE('FILEAPPEND=~/.scplog.txt') REPLACE(*YES)

/* Passage en gestion erreur IBM i */
ADDENVVAR ENVVAR(QIBM_QSH_CMD_ESCAPE_MSG) VALUE(Y) REPLACE(*YES)

/* Exécution de la commande QSH */
CHGVAR    VAR(&CMD) VALUE('scp' *BCAT &SRCFILE *BCAT &USER *TCAT '@' *TCAT &TARGET *TCAT ':' *TCAT &RMFILE)
STRQSH    CMD(&CMD)

/* Gestion des erreurs éventuelles */
MONMSG    MSGID(QSH0000) EXEC(DO)
    SNDPGMMSG MSGID(CPF9898) MSGF(QCPFMSG) MSGDTA('Fichier' *BCAT &FICSRC *BCAT 'non transmis') MSGTYPE(*ESCAPE)
ENDDO

ENDPGM
```

Power Week

18 -19 - 20 novembre 2025



Contexte SSH

Utilisation d'un agent

```
QP2TERM
```

```
// Démarrage de l'agent
```

```
$ eval "$(ssh-agent -s)"  
Agent pid 9102
```

```
// Ajout de la clé SSH privée
```

```
$ ssh-add /home/pw2025/.ssh/github  
Identity added: /home/pw2025/.ssh/github
```

```
// Vérification de la connexion à GitHub
```

```
$ ssh -T git@github.com  
Hi PW2025! You've successfully authenticated, but GitHub  
does not provide shell access.
```

Fichier config

```
~/.ssh/config
host ibmiB
    hostname ibmiB.local.lan
    user pw2025
    port 22
    identityFile ~/.ssh/monkey
```

```
QP2TERM
$ chmod 600 ~/.ssh/config
```

```
QP2TERM
$ scp fileC.txt ibmiB:fileC_new.txt
```

Power Week

18 -19 - 20 novembre 2025

IBM
common
FRANCE

IBM

Logs

Mode verbose côté client

- 3 niveaux de log
- Ajouter -v ou -vv ou -vvv
(v minuscule, -V majuscule indique la version des outils)

```
QP2TERM
$ scp -v -i ~/.ssh/monkey ~/fileC.txt pw2025@ibmi2:fileC_new.txt
OpenSSH_8.0p1, OpenSSL 3.0.10 1 Aug 2023
debug1: Reading configuration data /home/pw2025/.ssh/config
debug1: Reading configuration data
/QOpenSys/QIBM/ProdData/SC1/OpenSSH/etc/ssh_config
...
debug1: client_input_channel_req: channel 0 rtype exit-status reply 0
debug1: channel 0: free: client-session, nchannels 1
Transferred: sent 2760, received 2488 bytes, in 0.8 seconds
Bytes per second: sent 3484.0, received 3140.6
debug1: Exit status 0
```

Activation de la log côté serveur

- Sous IBM i
- /QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config
- + ajouter la ligne suivante

```
/QOpenSys/etc/syslog.conf  
auth.info /var/auth.log
```

- Sous Windows
- \ProgramData\ssh\sshd_config
- \ProgramData\ssh\logs\sshd.log

```
sshd_config  
...  
# Logging  
SyslogFacility LOCAL0  
LogLevel Debug3  
...
```

Power Week

18 -19 - 20 novembre 2025



Récapitulatif

Récapitulatif des droits - Côté client

Élément	Droits	chmod	Description
.ssh	drwx-----	700	Droit de lecture, d'écriture et d'exécution uniquement pour le propriétaire.
config	-rw-----	600	Droit de lecture et d'écriture uniquement pour le propriétaire.
[privateKey]	-rw-----	600	Droit de lecture et d'écriture uniquement pour le propriétaire.



Récapitulatif des droits - Côté serveur

Élément	Droits	chmod	Description
.ssh	drwx-----	700	Droit de lecture, d'écriture et d'exécution uniquement pour le propriétaire.
authorized_keys	-rw-----	600	Droit de lecture et d'écriture uniquement pour le propriétaire.



Récapitulatif des commandes - Sans configFile

- `ssh -T -i [privateKey] [remoteUserName]@[serverName]`
- `sftp -i [privateKey] [remoteUserName]@[serverName]`
- `scp -i [privateKey] [file] [remoteUserName]@[serverName]:[remoteDirectory]`

Option	Description
-T	Désactiver l'allocation de pseudo-terminal
-i	Fichier de clé privée

Récapitulatif des commandes - Avec configFile

- `ssh -T [alias]`
- `sftp [alias]`
- `scp [file] [alias]:[remoteDirectory]`

Option	Description
-T	Désactiver l'allocation de pseudo-terminal
-F	Fichier de config spécifique

Liens utiles

- Droits
 - https://fr.wikipedia.org/wiki/Permissions_UNIX
- OpenSSH
 - <https://www.openssh.org/>
- Articles dédiés au SSH sur l'IBM i
 - <https://www.seidengroup.com/how-to-configure-and-use-ssh-on-ibm-i/>
 - <https://www.seidengroup.com/2020/11/16/getting-started-with-ssh-for-ibm-i/>
 - <https://www.gaia.fr/...>
- CVE
 - <https://www.ibm.com/support/pages/bulletin/search/?q=ibm%20i>

MERC

