Université IBM i

7 novembre 2023

IBM Innovation Studio Paris

S06 – SSH : les clés du succès

11:15 / 12:15

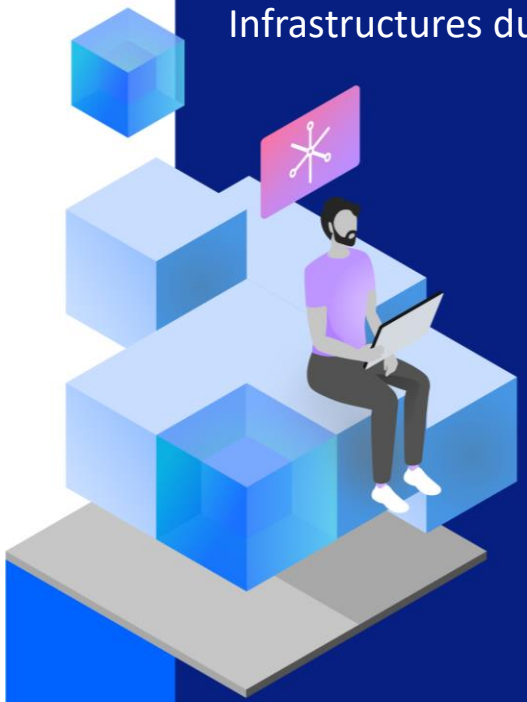
Julien Laurier
Gaia Mini Systèmes
julien.laurier@gaia.fr

infrasdufutur

#ibmi
#uii2023
#infrastructuredufuturIBM23

IBM

Infrastructures du futur



7 et 8 novembre 2023

Agenda

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

IBM

Infrastructures du futur

7 et 8 novembre 2023

Université IBM i

7 novembre 2023

IBM i 35 YEARS | Let's Create

1. Quoi, pour qui, pour quoi ?

Quoi ?

- SSH ➔ **S**ecure **Sh**ell
- Protocole de communication sécurisé
- Authentification et échanges sécurisés
- Couple de clés asymétriques
- Apparu en 1995, présent partout

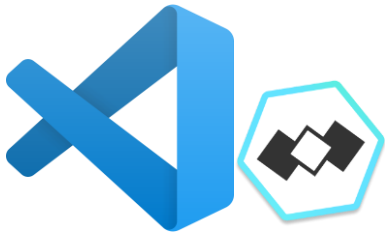
https://www.openssh.com/

Pour qui ?

Tout le monde !

Pour quoi ?

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



IBM

Infrastructures du futur

7 et 8 novembre 2023

Université IBM i

7 novembre 2023

IBM i 35 YEARS

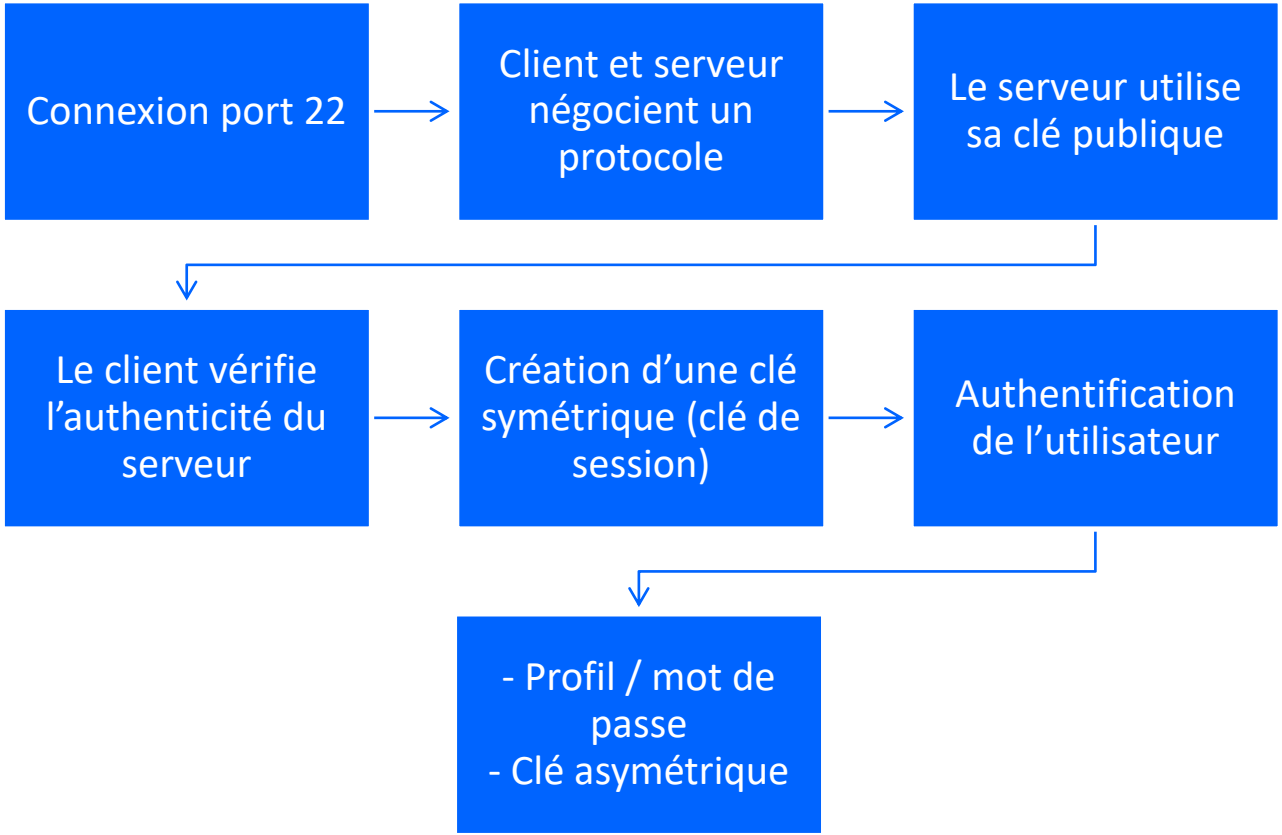
Let's Create

2. Protocoles

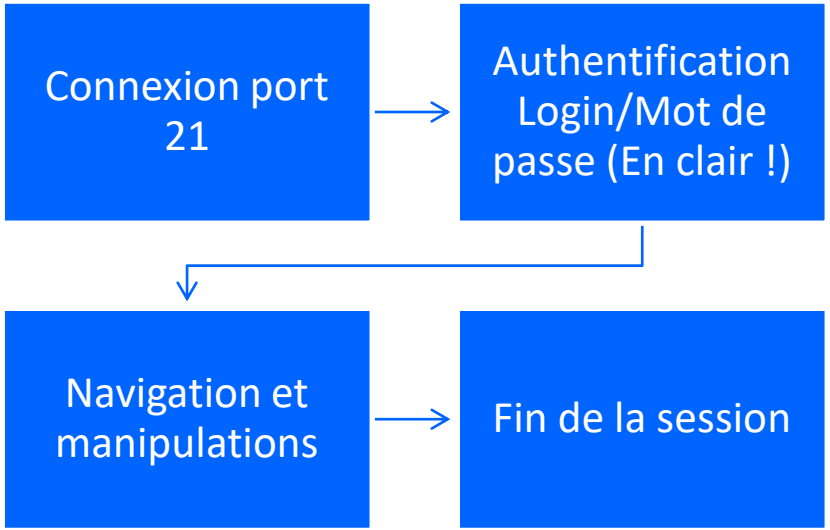
Protocoles - Sécurité

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

Protocoles - SSH

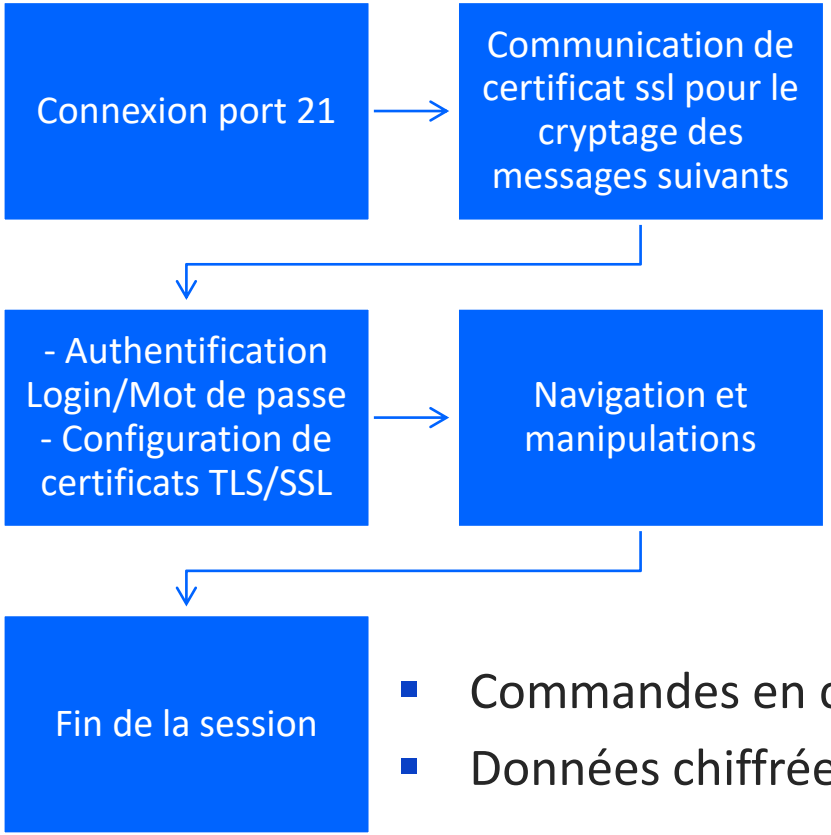


Protocoles - Transfert de fichiers - FTP




```
QSH
$ ftp server_name

$ user user_name
$ password **********

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

$ quit
```

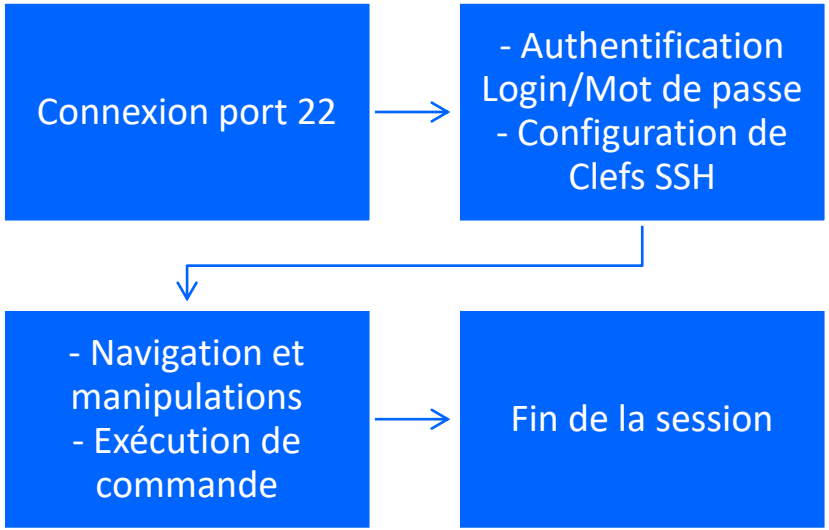
Protocoles - Transfert de fichiers - FTPS



- 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

IBM

Infrastructures du futur

7 et 8 novembre 2023

Université IBM i

7 novembre 2023

IBM i 35 YEARS

Let's Create

3. Prérequis

À ne jamais perdre de vue

- ~ ➔ Répertoire initial de l'utilisateur courant
- Les droits sur les répertoires et les fichiers doivent être le plus strict possible
  - (surtout les fichiers présents dans le répertoire .ssh)
- La commande which devient votre meilleur ami
- Attention à la version d'OpenSSH atteinte (QOpenSys/pkgs/bin ou QOpenSys/usr/bin)
- Attention au CCSID des fichiers de clés et au CRLF

Prérequis

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

```
5250
==> MKDIR DIR('/home/DemoUni1/')
==> CHGOWN OBJ('/home/DemoUni1/') NEWOWN(DemoUni1)
```

- 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

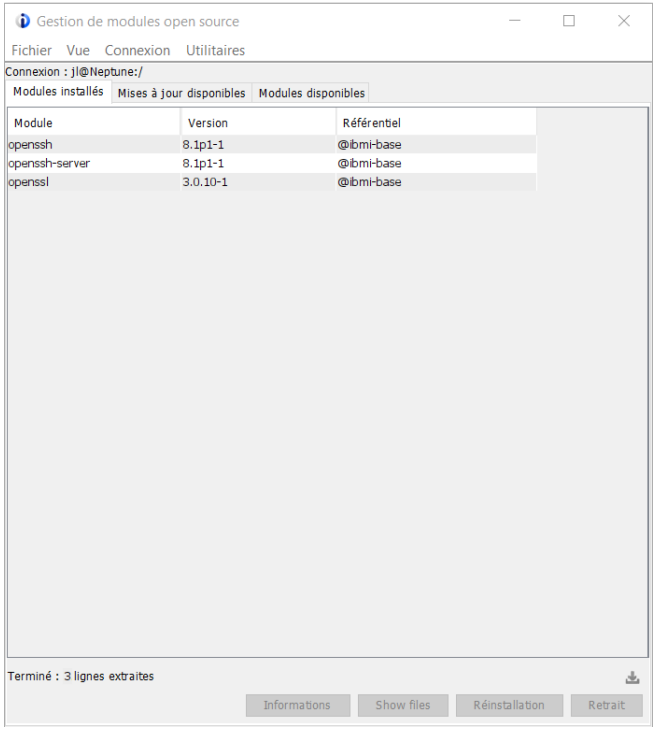
```
5250
==> WRKTCPSTS OPTION(*CNN)
```

➔

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

Prérequis

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



IBM

Infrastructures du futur

7 et 8 novembre 2023

Université IBM i

7 novembre 2023

IBM i 35 YEARS

Let's Create

4. Première approche

Validation de la communication

```
QP2TERM
$ ssh -T DemoUni1@uranus
The authenticity of host 'uranus (172.30.14.23)' 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 'uranus,172.30.14.23' (ECDSA) to the list of known hosts.
Connection closed by 172.30.14.23 port 22

$ ssh -T DemoUni1@uranus
DemoUni1@uranus's password:
$ **********

$ ls
ici_uranus
```

Transfert via scp

```
QP2TERM
$ cd /QOpenSys/pkgs/bin

$ sshpass -p '********' scp ~/slotA.txt demouni1@uranus:slotA_new.txt
```

```
(Uranus)/home/demouni1/slotA_new.txt
 **********Beginning of data**********
This is not a test!
 **********End of Data**********
```

IBM

Infrastructures du futur

7 et 8 novembre 2023

Université IBM i

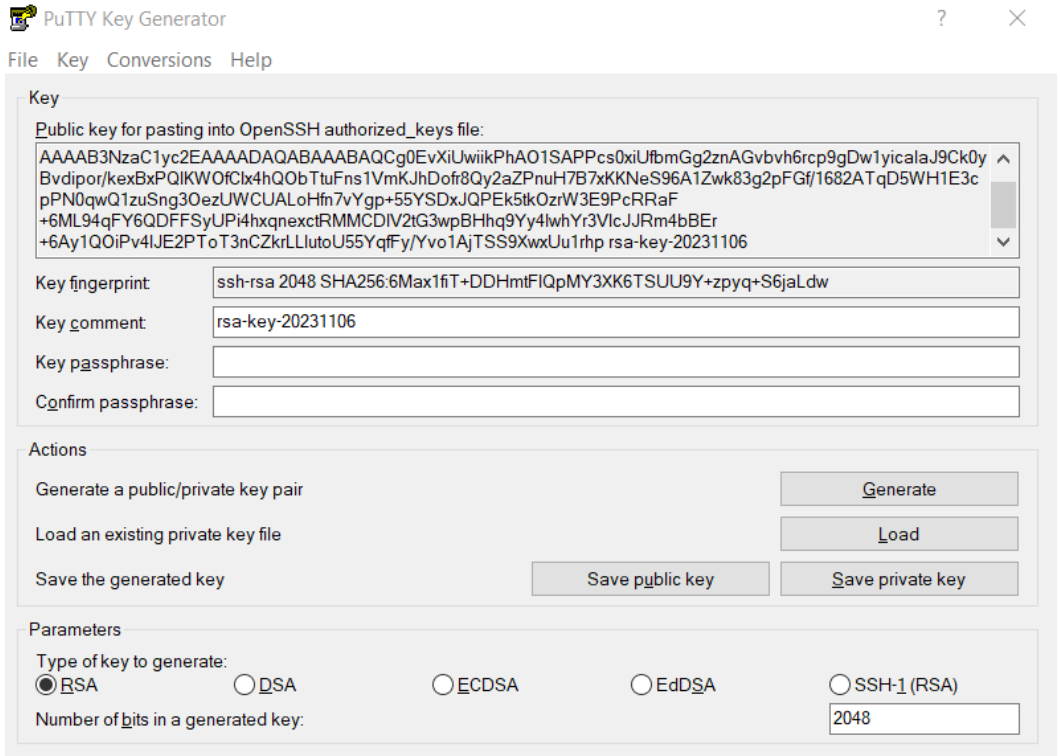
7 novembre 2023

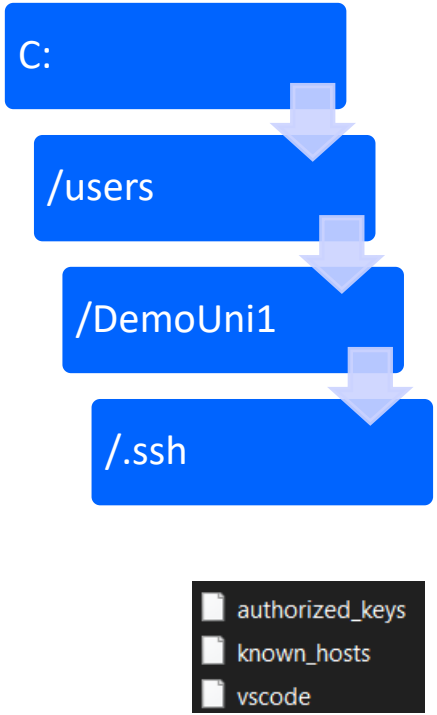
IBM i 35 YEARS

Let's Create

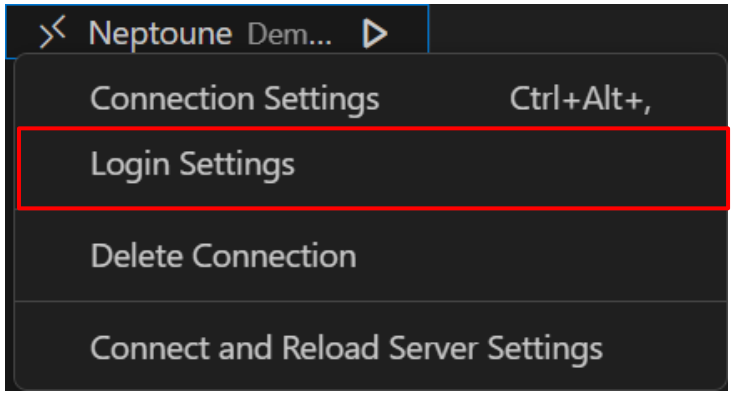
5. Génération d'une clé

PuTTY Key Generator

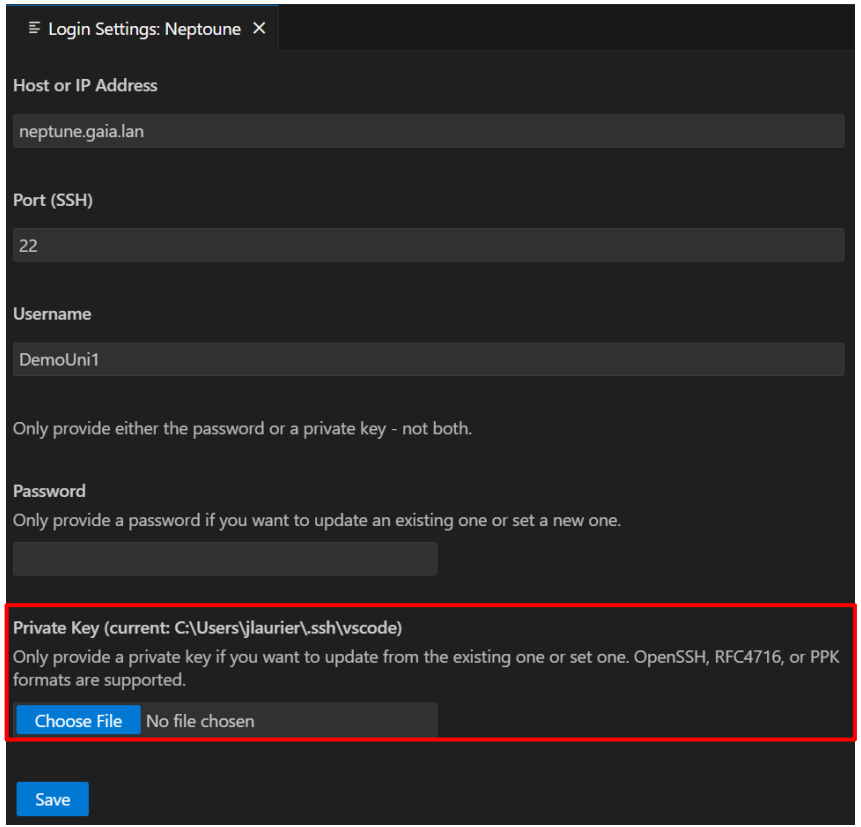




Mise en place clé sur VSCode - Privée



- ~/.ssh/vscode



Mise en place clé sur VSCode - Publique

- Créer le fichier authorized_keys et accorder directement les droits

```
QP2TERM
$ mkdir ~/.ssh
$ chmod 700 ~/.ssh

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

- Copier la valeur de la clé publique sur le serveur: ~/.ssh/vscode.pub
  ➔ ~/.ssh/authorized_keys

Génération manuelle - 1

```
QP2TERM
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key
(/home/DEMOUNI1/.ssh/id_rsa):

$ ~/.ssh/uranus
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
demouni1@NEPTUNE.GAIA.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 2048 -f ~/.ssh/monkey -N ''
Generating public/private rsa key pair.
Your identification has been saved in /home/demouni1/.ssh/monkey.
Your public key has been saved in /home/demouni1/.ssh/monkey.pub.
The key fingerprint is:
SHA256:9l+JLyHKBbXWqqsCF7JbtzSs6YxWh8nN1Hw4vf2NaZk demouni1@NEPTUNE.GAIA.LAN
The key's randomart image is:
+---[RSA 2048]----+
|                 |
|          .      |
|       o + o     |
|  . . . * = .    |
|   + O  S= +     |
|  o B O. .= o. . |
|   * * + +...oo* |
|  oo+ . +  ..oE .|
| ...o.....  .o.  |
+----[SHA256]-----+
```

Points clés de la génération de… clés

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

Type	Tailles possibles	Statut
dsa	1024	Déprécié
rsa	2048 - 4096	Le plus courant
ecdsa	256 - 384 - 521	
ed25519	256	

IBM

Infrastructures du futur

7 et 8 novembre 2023

Université IBM i

7 novembre 2023

IBM i 35 YEARS

Let's Create

6. Approche réelle

Protocoles - Transfert de fichiers

- scp -i ~/.ssh/monkey ~/slotC.txt demouni1@uranus:slotC_new.txt

```
QP2TERM
$ scp -i ~/.ssh/monkey ~/slotC.txt demouni1@uranus:slotC_new.txt
```

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

```
(Uranus)/home/demouni1/slotC_new.txt
 ************Beginning of data**************
I'm just a useless file...
 ************End of Data**********************
```

Infrastructures du futur

7 et 8 novembre 2023

Université IBM i

7 novembre 2023

IBM i 35 YEARS

Let's Create

7. Intégration dans un programme

Programme – SCP

```
PGM
/* Variables */
DCL         VAR(&SRCFILE) TYPE(*CHAR) LEN(50) VALUE('/home/DemoUni1/slotC.txt')
DCL         VAR(&USER) TYPE(*CHAR) LEN(3) VALUE('DEMONUI1')
DCL         VAR(&TARGET) TYPE(*CHAR) LEN(30) VALUE('iTest9')
DCL         VAR(&RMTFILE) TYPE(*CHAR) LEN(50) VALUE('/home/DemoUni1/slotC-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 &RMTFILE)
STRQSH      CMD(&CMD)

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

ENDPGM
```

IBM

Infrastructures du futur

7 et 8 novembre 2023

Université IBM i

7 novembre 2023

IBM i 35 YEARS

Let's Create

8. 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/demouni1/.ssh/github
    Identity added: /home/demouni1/.ssh/github

// Vérification de la connexion à GitHub
$ ssh -T git@github.com
    Hi DemoUni! You've successfully authenticated, but GitHub
does not provide shell access.
```

Fichier config

```
~/.ssh/config
host Uranus
    hostname uranus.gaia.lan
    user demouni1
    port 22
    identityFile ~/.ssh/monkey
```

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

```
QP2TERM
$ scp slotC.txt Uranus:slotC_new.txt
```

IBM

Infrastructures du futur

7 et 8 novembre 2023

Université IBM i

7 novembre 2023

IBM i 35 YEARS | Let's Create

9. 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 ~/slotC.txt demouni1@uranus:slotC_new.txt
OpenSSH_8.0p1, OpenSSL 3.0.10 1 Aug 2023
debug1: Reading configuration data /home/demouni1/.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
```

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

- Sous Windows
- \ProgramData\ssh\sshd_config

- \ProgramData\ssh\logs\sshd.log

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

- 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

42