Installation infrastructure RDS sur Windows server

> Installer Windows Serveur datacenter sans interface graphique, **sauf pour le serveur de broker qui lui sera installé avec interface graphique**. Le choix ce présente au début de l'installation de Windows Serveur. Toutes les commandes ci-dessous sont exécutés en PowerShell

Serveurs

- 1 serveur Gateway et web access
- 1 serveur Broker
- 2 serveurs d'applications & bureaux

Réseau

Topologie

Le serveur Gateway sera installé dans la zone réseau “ab-publique”

Les autres serveurs seront dans la zone réseau “ab-privé”

Configuration

IP

- Lancer powershell

```
Powershell
```

- Afficher les cartes disponible avec leurs index

```
Get-NetIPInterface
```

```
ifIndex InterfaceAlias                 AddressFamily NlMtu(Bytes) InterfaceMetric Dhcp     ConnectionState PolicyStore
------- --------------                 ------------- ------------ --------------- ----     --------------- -----------
11      Ethernet                       IPv6                  1500              25 Enabled  Connected       ActiveStore
1       Loopback Pseudo-Interface 1    IPv6            4294967295              75 Disabled Connected       ActiveStore
11      Ethernet                       IPv4                  1500              25 Disabled Connected       ActiveStore
1       Loopback Pseudo-Interface 1    IPv4            4294967295              75 Disabled Connected       ActiveStore
```

- Récupérer avec le code sous “ifIndex” et utiliser le code si dessous pour ajouter une IP et une Gateway à l'inteface Ethernet choisie.

```
New-NetIPAddress –InterfaceIndex XX –IPAddress 10.248.XX.XX –PrefixLength 24 –DefaultGateway 10.
```

- Ajouter un DNS à l'interface Ethernet choisie. Préciser toujours ifIndex.

```
Set-DnsClientServerAddress -InterfaceIndex XX -ServerAddresses 192.168.198.100,10.248.XX.XX
```

Configuration de Windows Update

- Installation du module

```
Install-Module PSWindowsUpdate -Confirm -Force
```

- Répondre oui aux questions posées

```
PS C:\Users\Administrateur> Install-Module pswindowsupdate -confirm -force

Le fournisseur NuGet est requis pour continuer
PowerShellGet requiert le fournisseur NuGet, version 2.8.5.201 ou ultérieure, pour interagir avec les référentiels
NuGet. Le fournisseur NuGet doit être disponible dans « C:\Program Files\PackageManagement\ProviderAssemblies » ou «
C:\Users\Administrateur\AppData\Local\PackageManagement\ProviderAssemblies ». Vous pouvez également installer le
fournisseur NuGet en exécutant la commande « Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force ».
Voulez-vous que PowerShellGet installe et importe le fournisseur NuGet maintenant ?
[O] Oui  [N] Non  [S] Suspendre  [?] Aide (la valeur par défaut est « O ») : o

Confirmer
Êtes-vous sûr de vouloir effectuer cette action ?
Opération « Installer le package » en cours sur la cible « Package nuget, version 2.8.5.208 de
https://onegetcdn.azureedge.net/providers/nuget-2.8.5.208.package.swidtag. ».
[O] Oui  [T] Oui pour tout  [N] Non  [U] Non pour tout  [S] Suspendre  [?] Aide (la valeur par défaut est « O ») : o

Confirmer
Êtes-vous sûr de vouloir effectuer cette action ?
Opération « Install-Module » en cours sur la cible « Version 2.1.1.2 du module PSWindowsUpdate ».
[O] Oui  [T] Oui pour tout  [N] Non  [U] Non pour tout  [S] Suspendre  [?] Aide (la valeur par défaut est « O ») : o
PS C:\Users\Administrateur>
```

- Installation des MAJ disponible

```
Get-WindowsUpdate -Install -Acceptall -IgnoreReboot
```

Répéter la commande jusqu’à ce qu'il n’y est plus de mise a jour disponible

- Changer le nom du serveur

```
Rename-Computer -NewName XXXXXXXXX
Restart-Computer
```

Configuration de SSH

- Recherche de la version de SSH en ligne

```
Get-WindowsCapability -Online | ? Name -like 'OpenSSH*'
```

- Installation de SSH server

```
Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0
```

- Démarrage sur service SSH

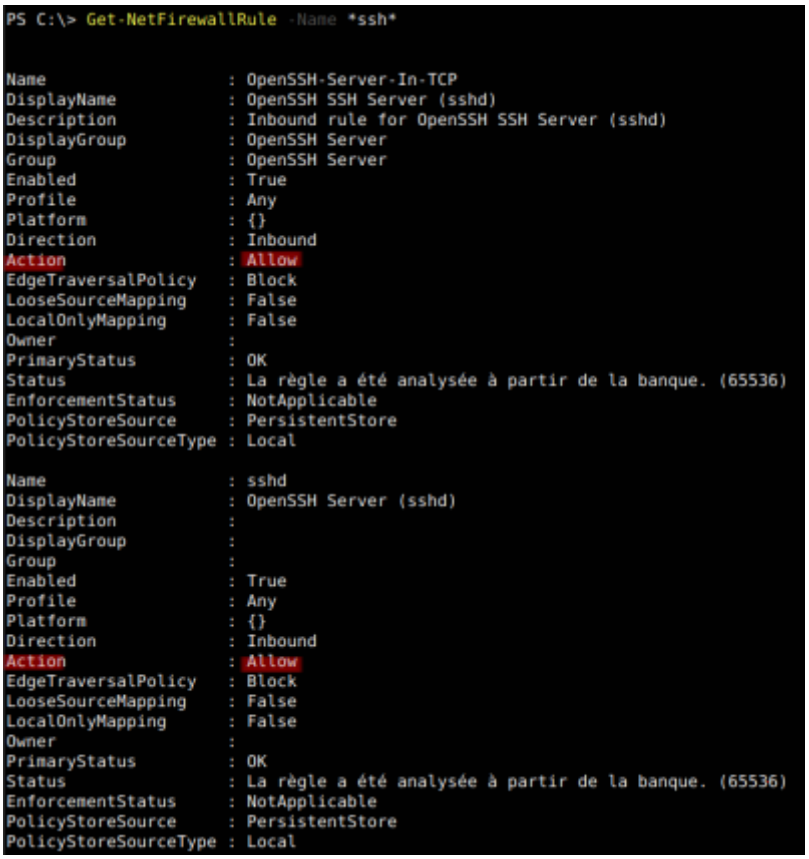
```
Start-Service sshd
```

- Démarrage automatique du service SSH

```
Set-Service -Name sshd -StartupType 'Automatic'
```

- Confirmer que la régle de firewall est bien active et autorise le SSH

```
Get-NetFirewallRule -Name *ssh*
```



Règles

A déployer sur le serveur Gateway

```
netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol="icmpv4:
netsh advfirewall firewall add rule name="allow DNS" dir=out protocol=TCP localport=53 action=al
netsh advfirewall firewall add rule name="allow Epmap" dir=out protocol=TCP localport=135 action
netsh advfirewall firewall add rule name="allow kerberos 1" dir=out protocol=TCP localport=88 ac
netsh advfirewall firewall add rule name="allow kerberos 1" dir=out protocol=UDP localport=88 ac
netsh advfirewall firewall add rule name="allow kerberos 2" dir=out protocol=TCP localport=464 a
netsh advfirewall firewall add rule name="allow kerberos 2" dir=out protocol=UDP localport=464 a
netsh advfirewall firewall add rule name="allow LDAP" dir=out protocol=TCP localport=389 action=
netsh advfirewall firewall add rule name="allow LDAP-GC" dir=out protocol=TCP localport=3268 act
netsh advfirewall firewall add rule name="allow LDAP-GCSSL" dir=out protocol=TCP localport=3269
netsh advfirewall firewall add rule name="allow LDAP" dir=out protocol=UDP localport=389 action=
netsh advfirewall firewall add rule name="allow LDAPS" dir=out protocol=TCP localport=636 action
netsh advfirewall firewall add rule name="allow MS-ds" dir=out protocol=TCP localport=445 action
netsh advfirewall firewall add rule name="allow Netbios-dgm" dir=out protocol=UDP localport=138
netsh advfirewall firewall add rule name="allow Netbios-ms-udp" dir=out protocol=UDP localport=1
netsh advfirewall firewall add rule name="allow Netbios-ms-ssn" dir=out protocol=TCP localport=1
netsh advfirewall firewall add rule name="allow Port-1024" dir=out protocol=TCP localport=1024 a
netsh advfirewall firewall add rule name="allow port_R_20000-59999" dir=out protocol=TCP localpo
netsh advfirewall firewall add rule name="allow port_R_20000-59999" dir=out protocol=UDP localpo
```

A déployer sur les autres serveurs de la ferme RDS

```
netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol="icmpv4:
netsh advfirewall firewall add rule name="allow port_5985" dir=out protocol=TCP localport=5985 a
netsh advfirewall firewall add rule name="allow port_5986" dir=out protocol=TCP localport=5986 a
netsh advfirewall firewall add rule name="allow Epmap" dir=out protocol=TCP localport=135 action
netsh advfirewall firewall add rule name="allow DNS" dir=out protocol=TCP localport=53 action=al
netsh advfirewall firewall add rule name="allow kerberos 1" dir=out protocol=TCP localport=88 ac
netsh advfirewall firewall add rule name="allow kerberos 1" dir=out protocol=UDP localport=88 ac
netsh advfirewall firewall add rule name="allow kerberos 2" dir=out protocol=TCP localport=464 a
netsh advfirewall firewall add rule name="allow kerberos 2" dir=out protocol=UDP localport=464 a
netsh advfirewall firewall add rule name="allow LDAP" dir=out protocol=TCP localport=389 action=
netsh advfirewall firewall add rule name="allow LDAP-GC" dir=out protocol=TCP localport=3268 act
netsh advfirewall firewall add rule name="allow LDAP-GCSSL" dir=out protocol=TCP localport=3269
netsh advfirewall firewall add rule name="allow LDAP" dir=out protocol=UDP localport=389 action=
netsh advfirewall firewall add rule name="allow LDAPS" dir=out protocol=TCP localport=636 action
netsh advfirewall firewall add rule name="allow MS-ds" dir=out protocol=TCP localport=445 action
netsh advfirewall firewall add rule name="allow Netbios-dgm" dir=out protocol=UDP localport=138
netsh advfirewall firewall add rule name="allow Netbios-ms-udp" dir=out protocol=UDP localport=1
netsh advfirewall firewall add rule name="allow Netbios-ms-ssn" dir=out protocol=TCP localport=1
netsh advfirewall firewall add rule name="allow Port-1024" dir=out protocol=TCP localport=1024 a
```

- Joindre le serveur au domaine ISYREL.FR

```
Add-Computer -DomainName isyrel.fr -Restart
```

Déploiement des Rôles RDS

Ligne de commande à entrer sur l'un des serveurs

- Rôle broker, Web Access, et le(s) serveur(s) d'application (-SessionHost)

```
New-RDSessionDeployment -ConnectionBroker "nom_duserveur.domain.lan" -WebAccessServer "nom_duser
```

- Rôle Gateway sur le même serveur que le Web Access

```
Add-RDServer -Server "nom_duserveur.domain.lan_web_access" -Role "RDS-GATEWAY" -ConnectionBroker
```

- Ajouter un serveur sessions d'hosts ultérieurement à la ferme RDS

```
Add-RDServer -Server "nom_duserveur.domain.lan_sessions_hosts " -Role "RDS-RD-SERVER" -Connectic
```

- Vérification des rôles installer sur les serveurs.
- A exécuter sur le serveur de broker, il affichera tous les rôles serveurs par serveurs

```
Get-RDserver
```

```
PS C:\> Get-RDserver

Server                                          Roles
------                                          -----
BTOINOUBKR01.TOINOU879.LAN                      {RDS-CONNECTION-BROKER}
btoinourdsgw01.toinou879.lan                    {RDS-WEB-ACCESS, RDS-GATEWAY}
btoinourdsapp01.toinou879.lan                   {RDS-RD-SERVER}
```

Certificats

Serveur Broker

- Pour le Broker il faut créer un serveur auto-signé. pour cela exécuter la commande ci-dessous sur le serveur broker. Windows 2019

```
New-SelfSignedCertificate -certstorelocation cert:\localmachine\my -Subject "isyrel-rds"
```

- Récupérer le “Thumbprint”

```
PS C:\Users\administrateur.TOINOU879> New-SelfSignedCertificate -certstorelocation cert:\localmachine\my -Subject "isyrel"


   PSParentPath : Microsoft.PowerShell.Security\Certificate::LocalMachine\my

Thumbprint                                Subject
----------                                -------
E4179F308E584A9A44DF255CB3A54F9424A49510  CN=isyrel
```

- Installation du certificat auto-signé pour la connexion RDS broker

```
Set-RDCertificate -Role RDRedirector -Thumbprint "renseigner_le_Thumbprint" -ConnectionBroker "r
```

Windows 2016

```
$Password = ConvertTo-SecureString -String "password" -AsPlainText -force
```

```
new-RDCertificate -Role RDRedirector -exportpath "C:\certificates\RDSRedirectorisyrel.pfx" -Pass
el.fr"
```

```
Serveur "Gateway" broker
```

Création de collection d'application ou bureaux

```
New-RDSessionCollection -CollectionName "nom_de_la_collection" -SessionHost @("nom_duserveur.dom
```

Publication d'une application

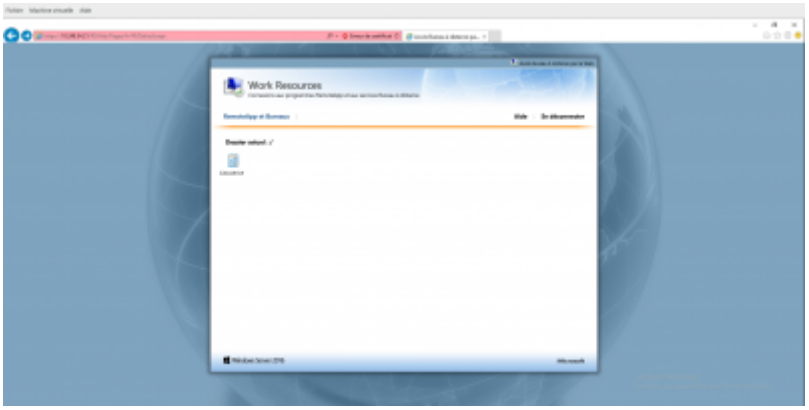
- Exemple avec une application

```
New-RDRemoteApp -CollectionName "nom_d'une_collection_existante" -DisplayName "Notepad" -FilePat
```

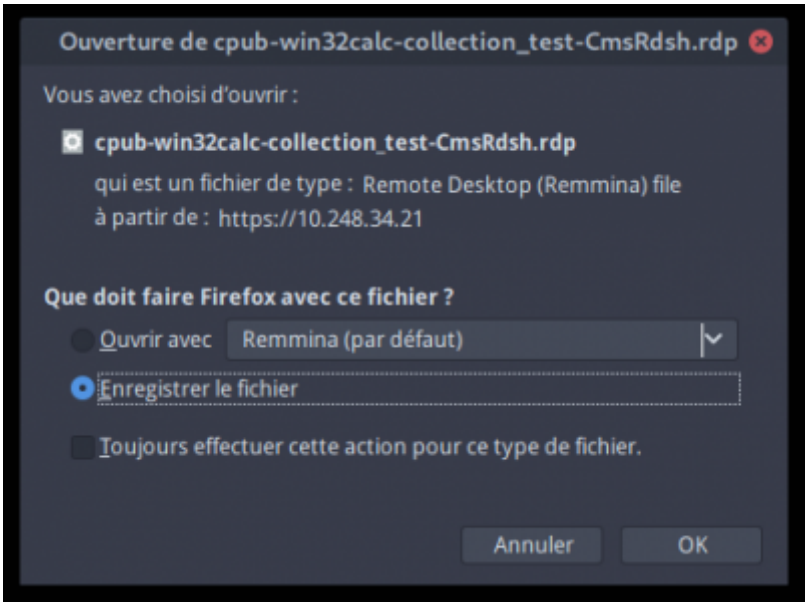
Créer le raccourci de l'application déployée

L’objectif des manipulations suivantes est de faire en sorte que l'utilisateur puisse se connecter a son application, sans avoir a rentrer son identifiant et mot de passe.

- Se connecter a la passerelle RDP



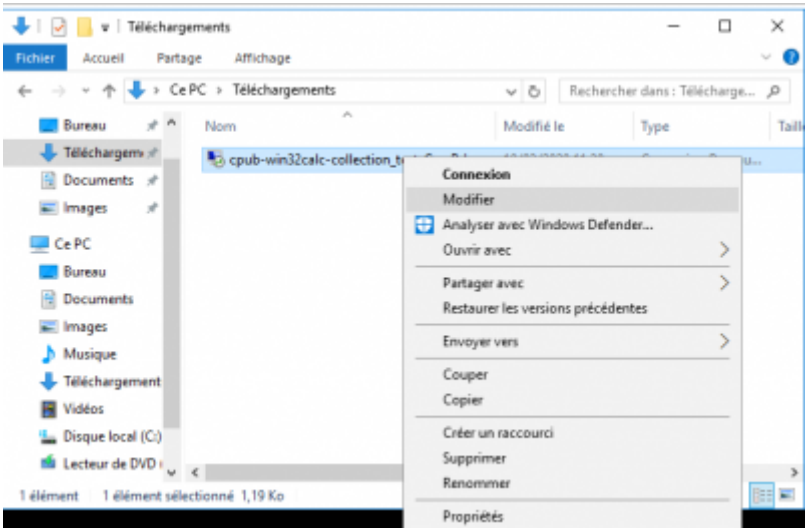
- Enregistrer le raccourci .rdp



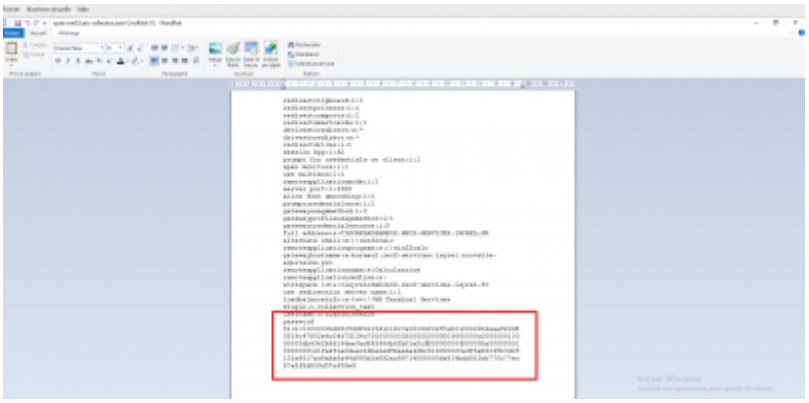
Avant de modifier le fichier, on génère le chiffrage du mot de passe utilisateur avec la commande suivante:

```
("MyPassword!" | ConvertTo-SecureString -AsPlainText -Force) | ConvertFrom-SecureString;
```

- Cliquer droit sur le fichier .rdp puis “modifier”



Rentrer l'option username:s:monutilisateur et password 51:b:<copier la sortie du mot de passe généré précédemment>



En double cliquant sur le raccourci pour ouvrir l'application, l'utilisateur n'a plus besoin d'entrer son identifiant et mot de passe.

Revision #3
Created 25 August 2022 07:56:08 by Aurélie Leturcq
Updated 22 September 2022 12:37:09 by Aurélie Leturcq