Procédures pour administrateurs pour faire un audit chez le client :

Si on a un compte admin fonctionnel sur tous les postes en Workgroup :

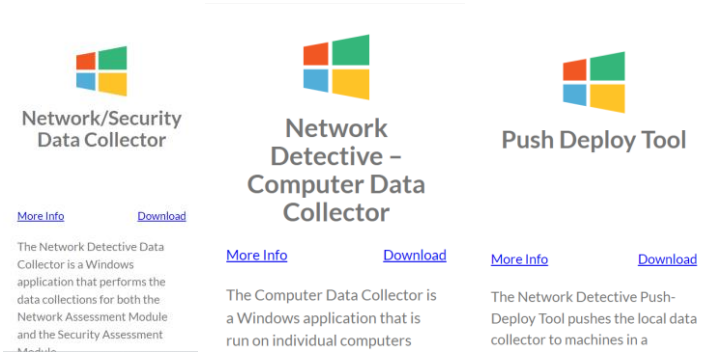
Exécuter **Network Detective Data Collector** (NDDC) avec l'analyse réseau (OBLIGATOIRE)

Exécutez le collecteur de données réseau sur n'importe quel poste de travail du réseau. Le collecteur de données doit être exécuté avec des privilèges d'administrateur et, si possible, avec une connexion commune à tous les ordinateurs du groupe de travail.

Faire un répertoire dans un dossier partagé sur le réseau. Exemple : C:\Users\exemple-chemin\Utilisateurs - Documents_Cyberallié\install

https://www2.rapidfiretools.com/nd-downloads/#network-security-assessment

Télécharger ces 3 applications:



Network Detective – Computer Data Collector : Le collecteur de données informatiques est une application Windows qui s'exécute sur des ordinateurs individuels (postes de travail ou serveurs) pour collecter des informations pour chaque système. **Utilisez cette option si/quand WMI et d'autres protocoles réseau sont bloqués pour fonctionner sur le réseau à partir de l'analys**e du collecteur de données réseau ou lors de l'analyse des réseaux hors domaine

Idéalement, on ferait une politique sur le réseau pour permettre l'accès WMI -> pourquoi et instructions

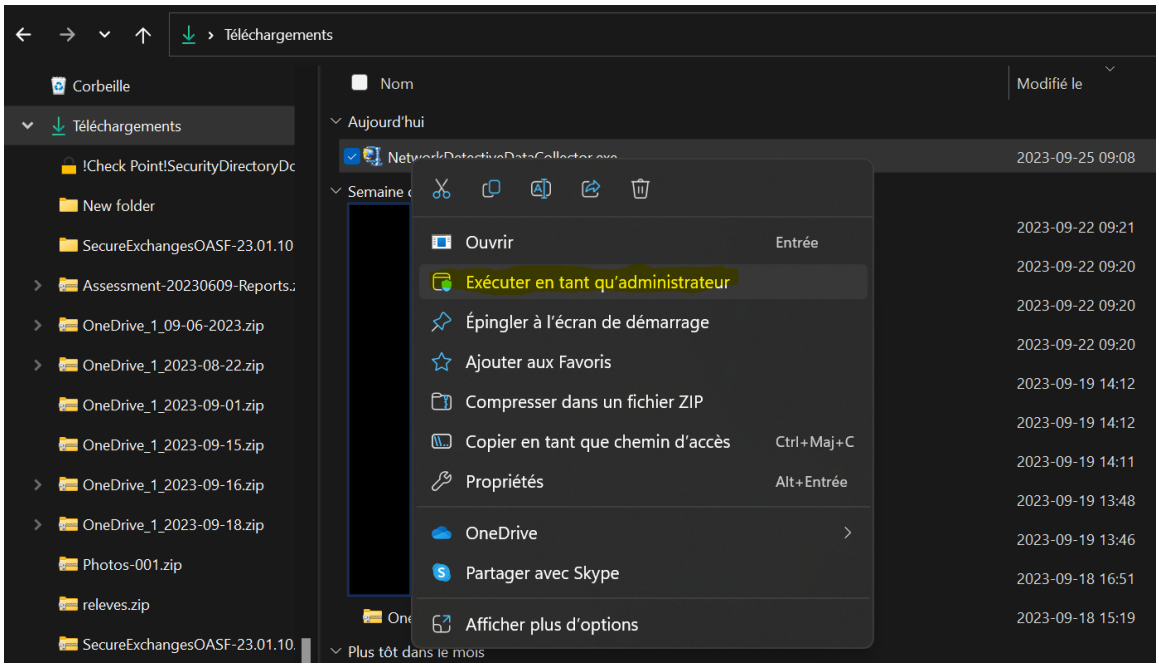
1. **NetworkDetectiveDataCollector.exe** sur tous les postes avec l'option réseau et sécurité activé. L'ors du préscan, une liste de postes accessibles sera affichée. **Pour obtenir de meilleurs résultats dans un groupe de travail, il est recommandé d'exécuter les collecteurs de données informatiques sur tous les ordinateurs du groupe de travail.**

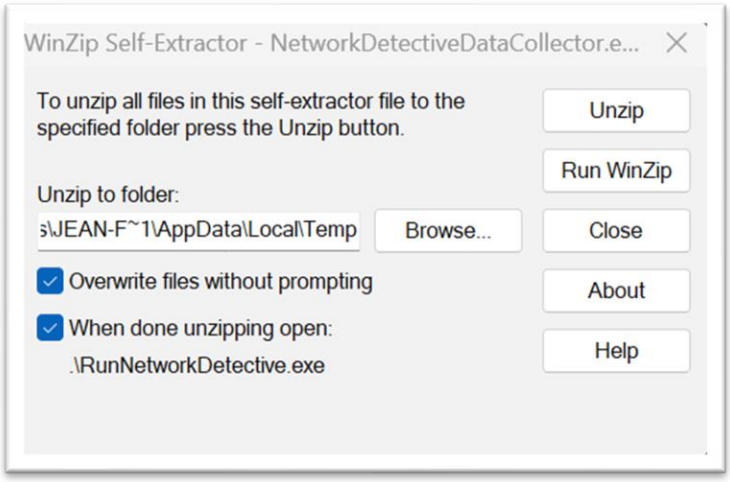
2. **NetworkDetectiveComputerDataCollector.exe**
   Exécutez le collecteur de données de l'ordinateur sur les ordinateurs qui ne peuvent pas être analysés à distance

   Si vous connaissez des ordinateurs qui ne peuvent pas être analysés à distance (c'est-à-dire bloqués par un pare-feu ou inaccessibles), vous devez exécuter le collecteur de données de l'ordinateur directement sur l'ordinateur lui-même.

3. Exécuter comme administrateur (Sur un seul poste) :
   NetworkDetectivePushDeployTool.zip

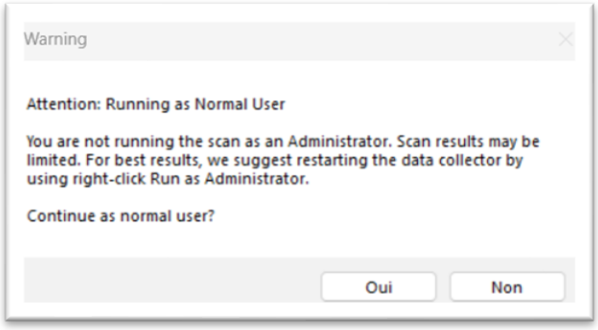
(Voir instructions à la fin du document pour Push Deploy)

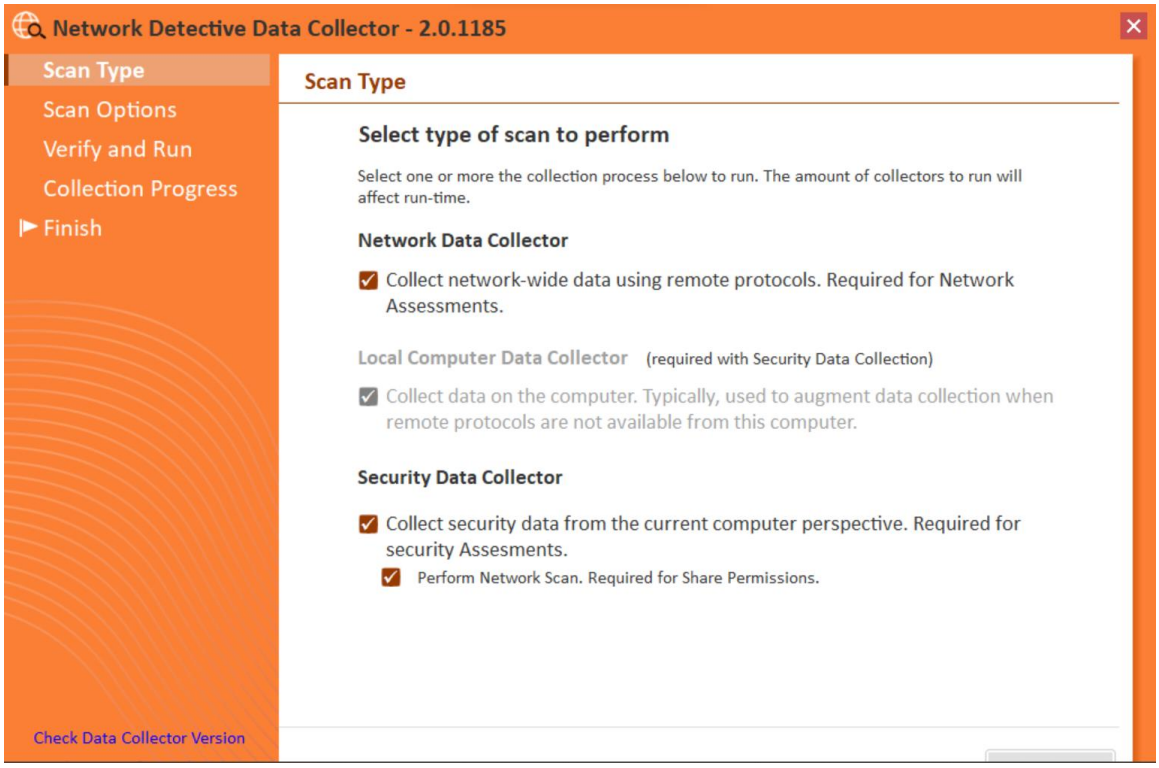


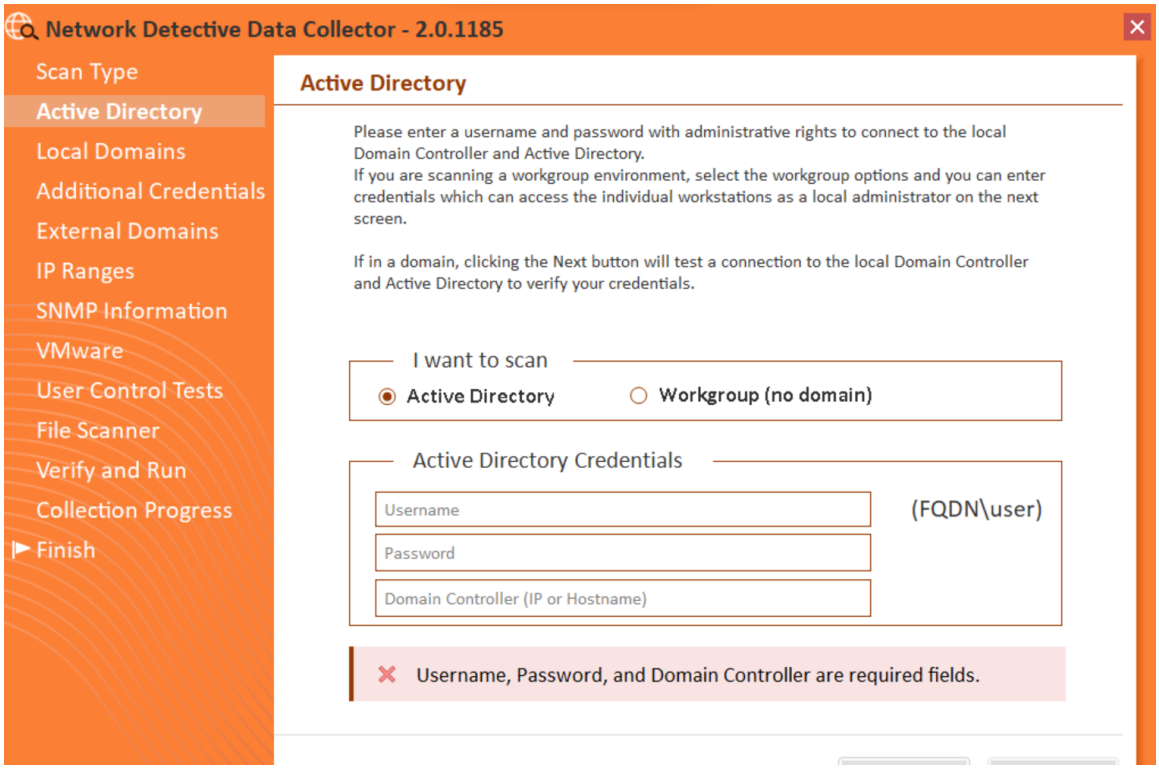


Unzip, … OK

Exécuter en administrateur sinon :



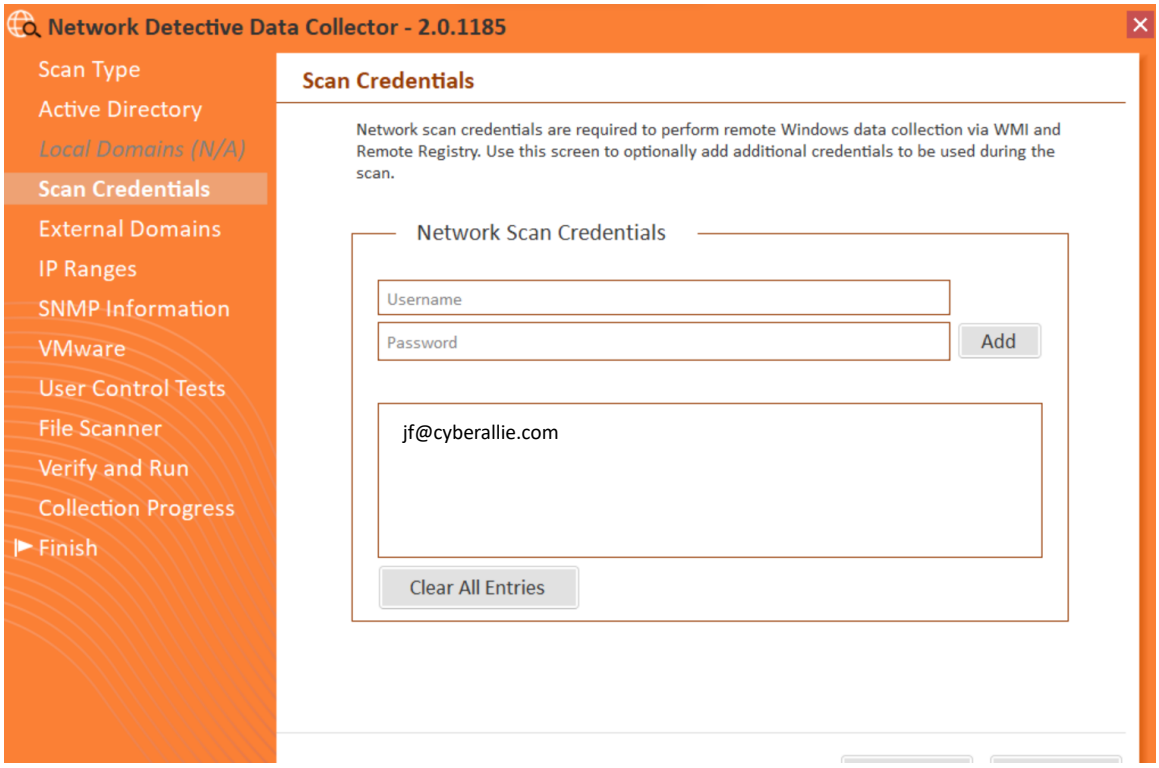


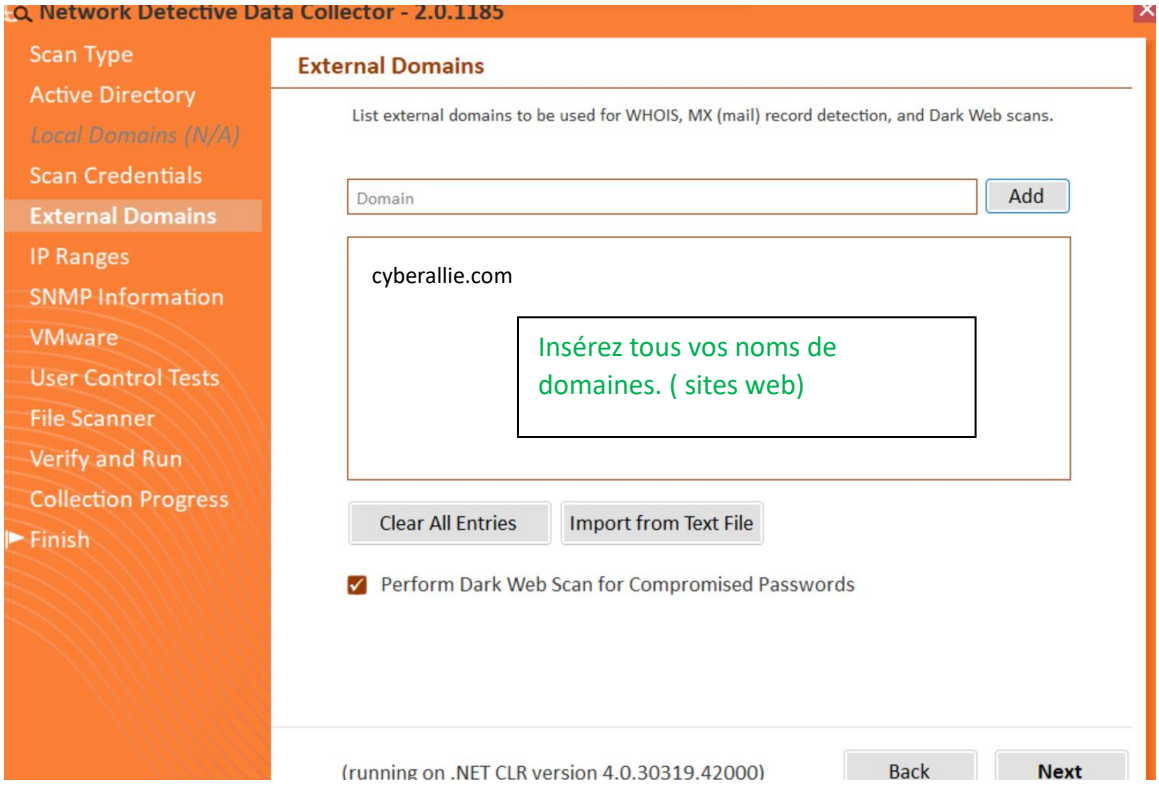


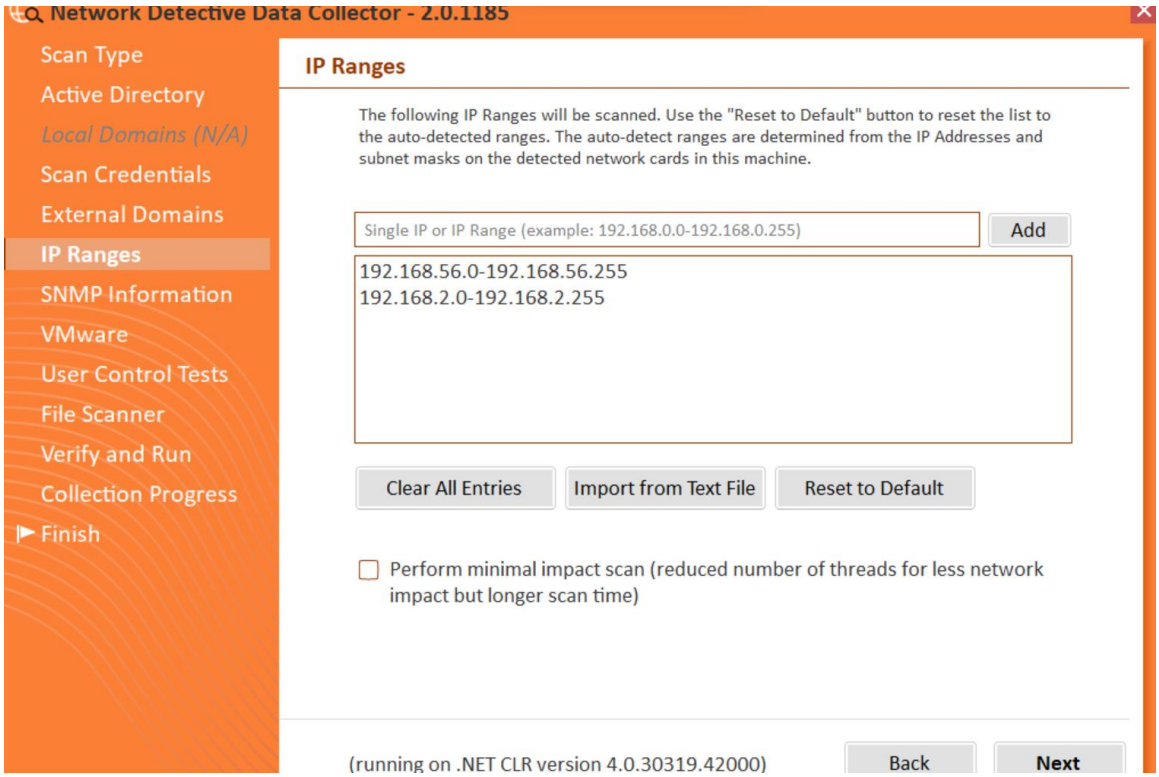
Remplir les informations du domaine pour les serveurs. (FQDN\user), mot de passe, Domain controller (IP ou hostname) ou choisir Workgroup pour les groupes de travail.

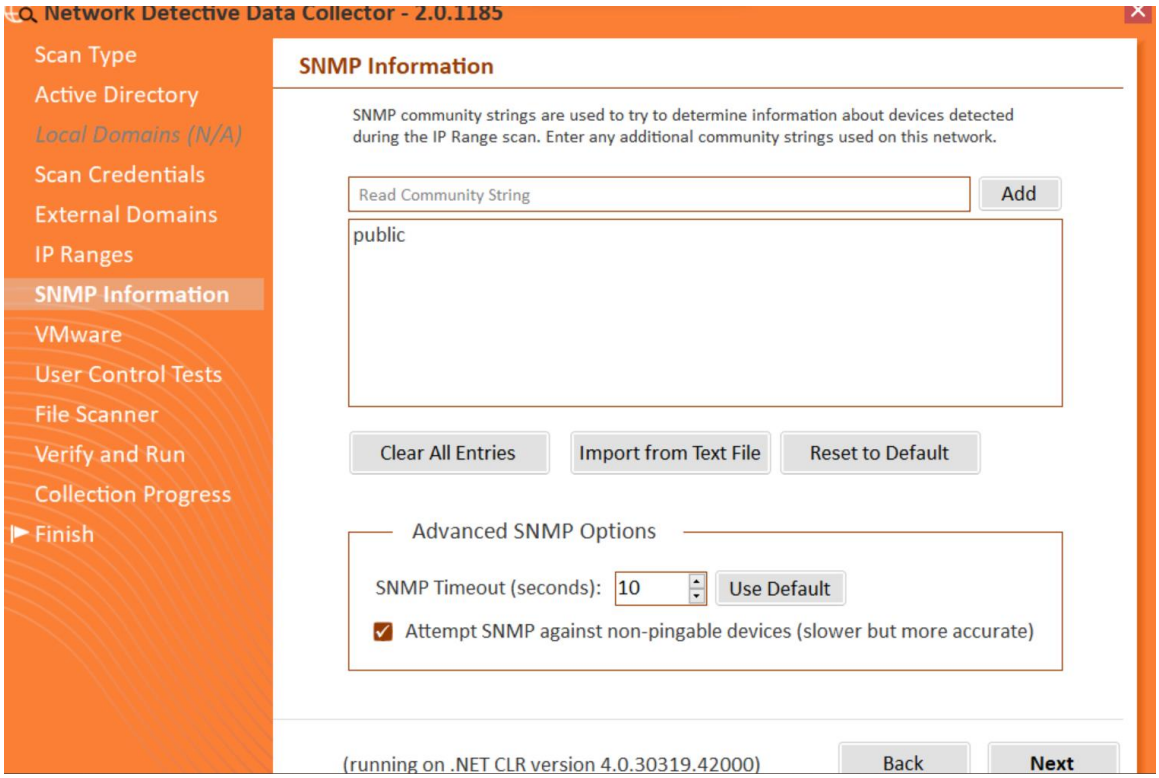
exemple: corp.domaineclient.com\username.

Ou Workgroup et faire le tour de tous les postes.




Network Detective Data Collector - 2.0.1185
Scan Type
Active Directory
Local Domains (N/A)
Scan Credentials
External Domains
IP Ranges
SNMP Information
VMware
User Control Tests
File Scanner
Verify and Run
Collection Progress
Finish
External Domains
List external domains to be used for WHOIS, MX (mail) record detection, and Dark Web scans.
Domain
Add
cyberallie.com
Insérez tous vos noms de domaines. (sites web)
Clear All Entries
Import from Text File
Perform Dark Web Scan for Compromised Passwords
(running on .NET CLR version 4.0.30319.42000)
Back
Next


Network Detective Data Collector - 2.0.1185
Scan Type
Active Directory
Local Domains (N/A)
Scan Credentials
External Domains
IP Ranges
SNMP Information
VMware
User Control Tests
File Scanner
Verify and Run
Collection Progress
Finish
IP Ranges
The following IP Ranges will be scanned. Use the "Reset to Default" button to reset the list to the auto-detected ranges. The auto-detect ranges are determined from the IP Addresses and subnet masks on the detected network cards in this machine.
Single IP or IP Range (example: 192.168.0.0-192.168.0.255)
Add
192.168.56.0-192.168.56.255
192.168.2.0-192.168.2.255
Clear All Entries
Import from Text File
Reset to Default
Perform minimal impact scan (reduced number of threads for less network impact but longer scan time)
(running on .NET CLR version 4.0.30319.42000)
Back
Next



Insérer les mots de passe des routeurs, commutateurs, … (un à un ou importer d'un CSV)

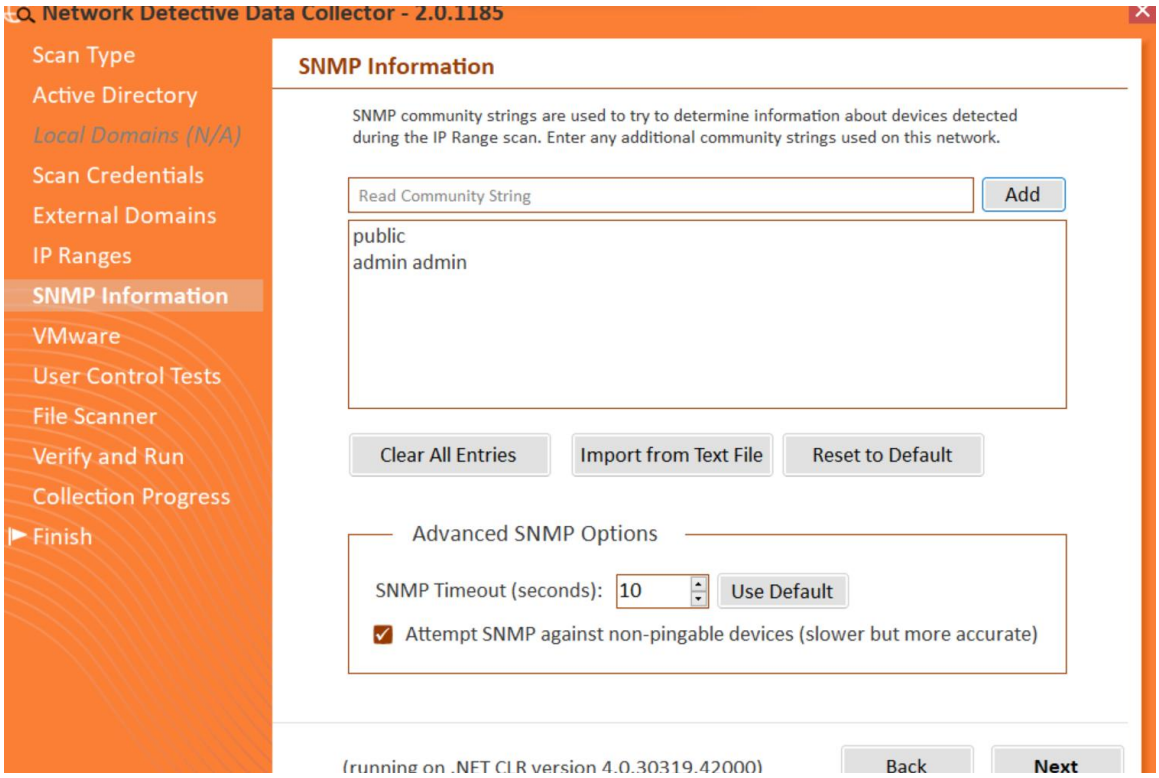
Les chaînes de communauté SNMP (Simple Network Management Protocol) sont essentiellement des mots de passe ou des informations d'identification utilisés pour authentifier et contrôler l'accès aux appareils activés par SNMP, tels que les routeurs, les commutateurs et les dispositifs réseau. Il existe deux types de chaînes de communauté SNMP :

1. **Chaîne de communauté en lecture seule (RO Community String)** : Cette chaîne permet un accès en lecture seule aux informations SNMP sur l'appareil. Les utilisateurs ayant cette chaîne peuvent récupérer des données telles que les informations système, les statistiques du trafic réseau et d'autres paramètres surveillés, mais ils ne peuvent pas effectuer de modifications de configuration.

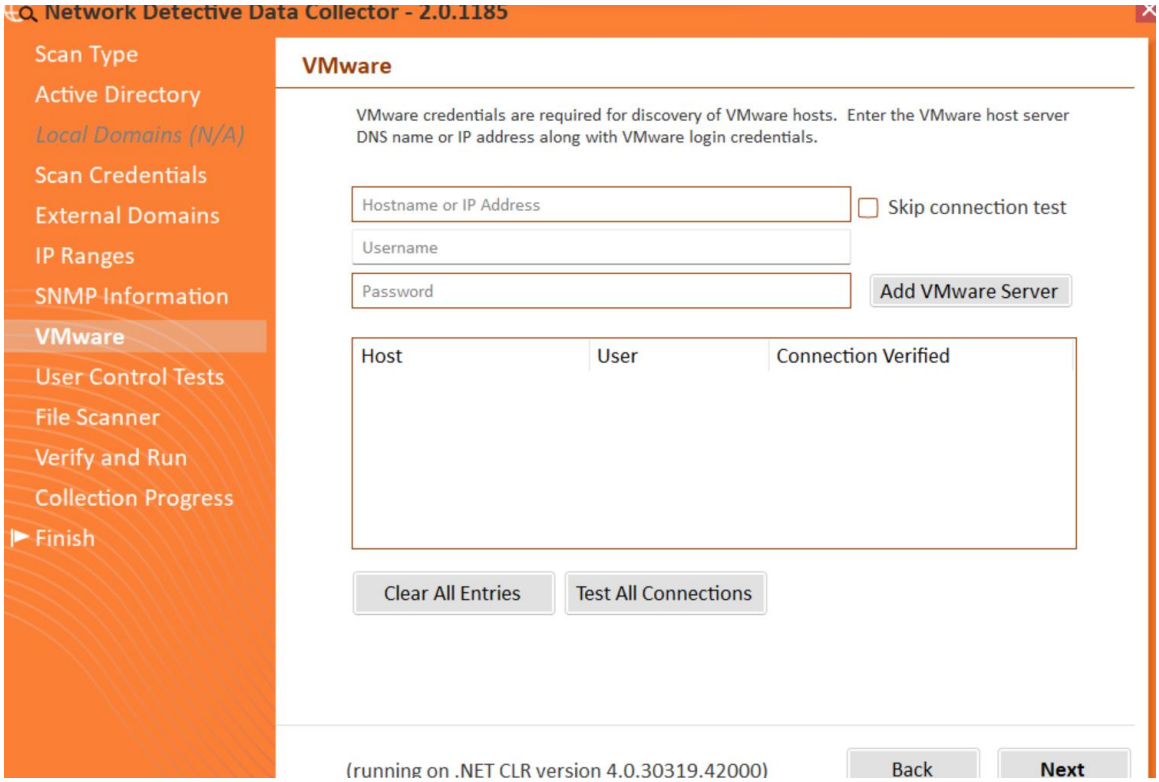
2. **Chaîne de communauté en lecture-écriture (RW Community String)** : Cette chaîne permet à la fois un accès en lecture et en écriture aux informations SNMP. Les utilisateurs ayant cette chaîne peuvent non seulement récupérer des données, mais également modifier les configurations de l'appareil, ce qui comprend la modification des paramètres ou l'exécution d'actions sur l'appareil.

Il est important de sécuriser ces chaînes de communauté, car un accès non autorisé peut entraîner des risques potentiels pour la sécurité. Dans les implémentations SNMP modernes, il est recommandé d'utiliser SNMPv3, qui offre des fonctionnalités de sécurité plus robustes telles que l'authentification et le chiffrement, plutôt que de se fier uniquement aux chaînes de communauté.

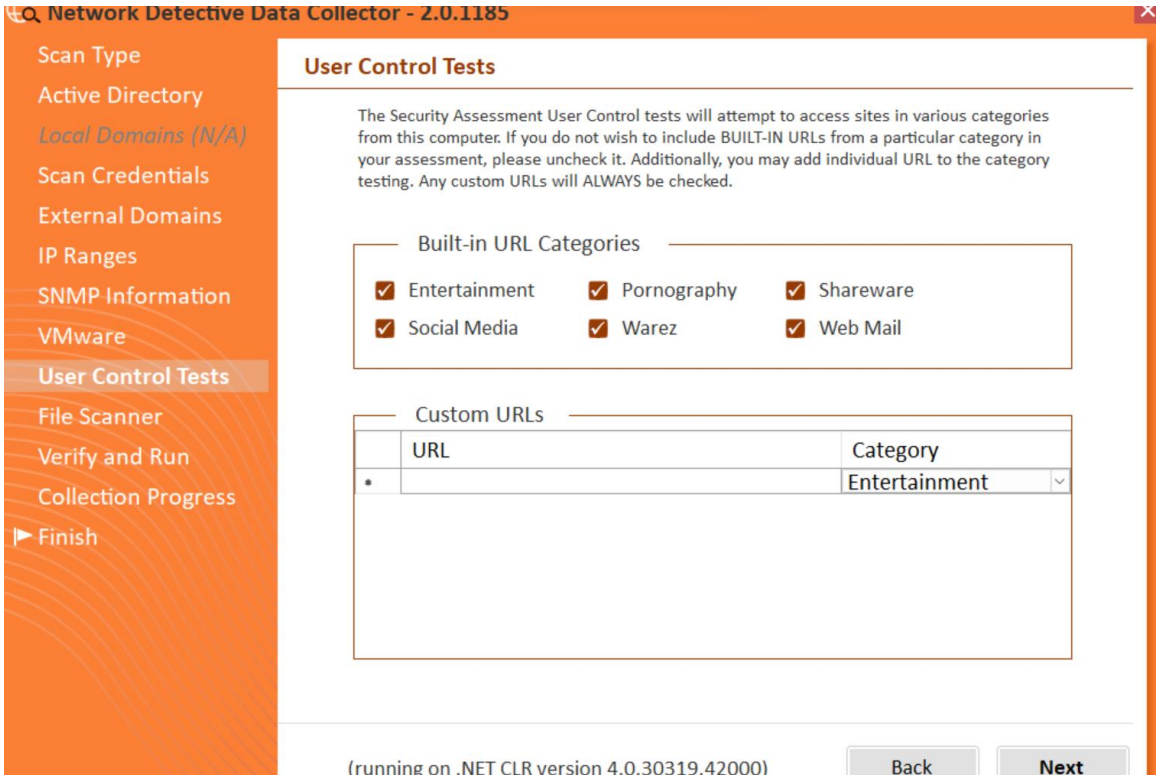
Ici j'ai ajouté Admin (utilisateur) Admin (Mot de passe) espérons que ça n'existe pas sur votre réseau!

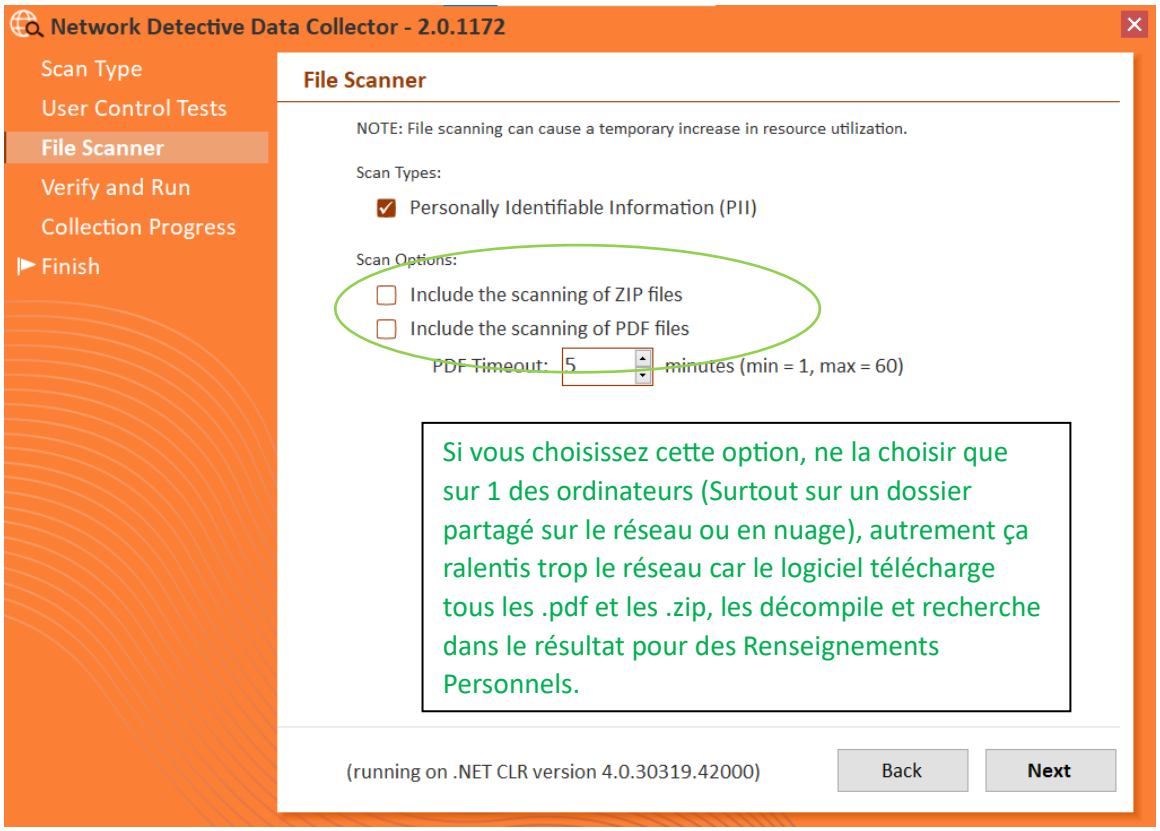


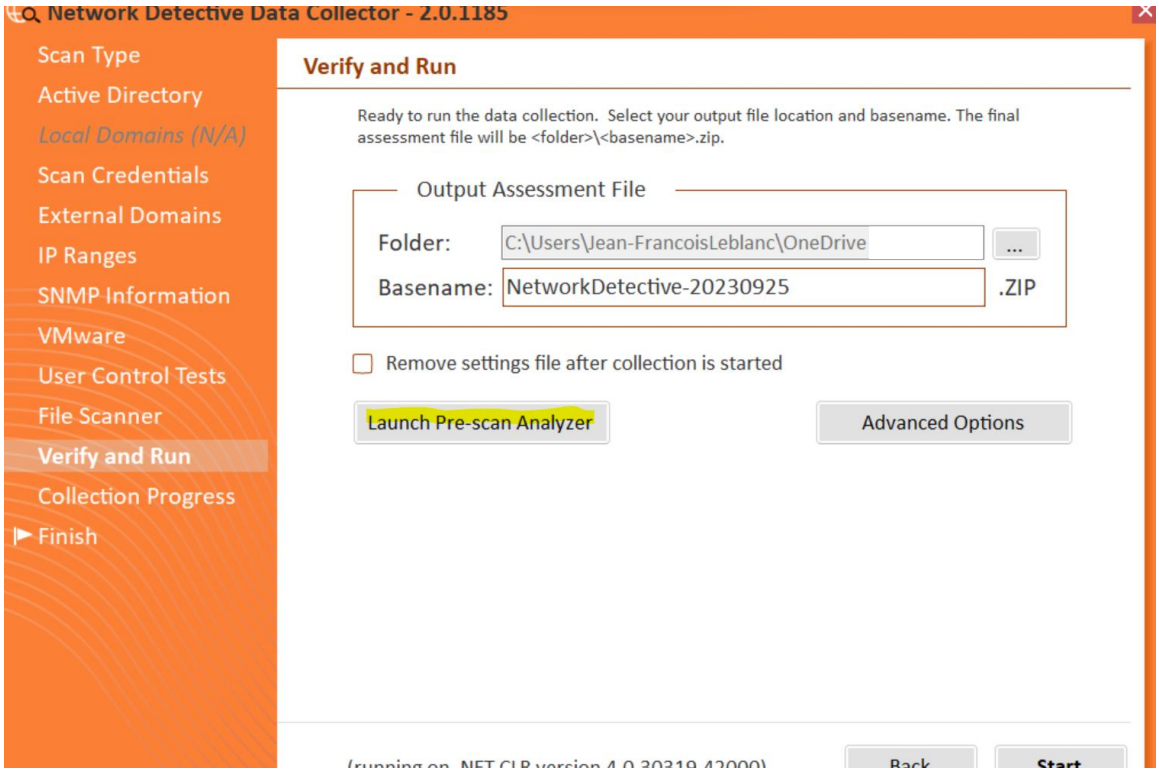
Si vous avez des machines virtuelles :

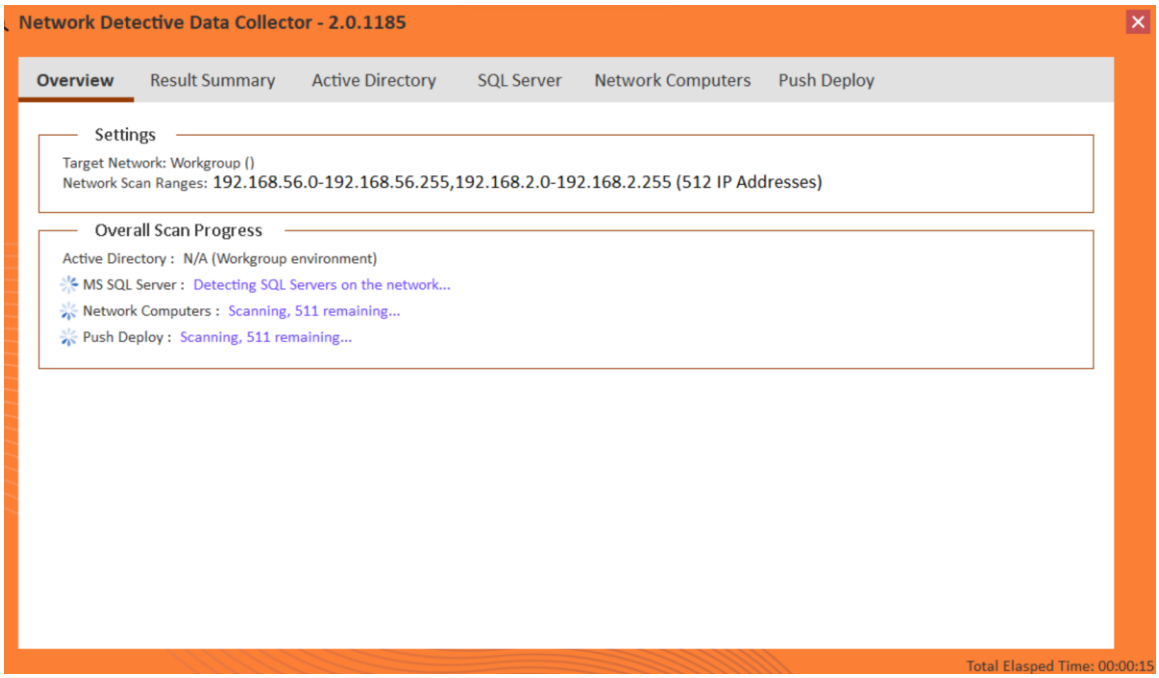


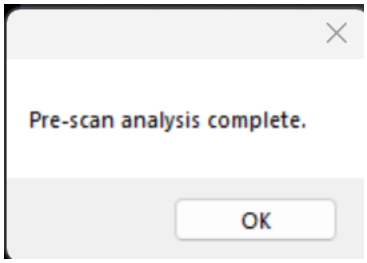
Si non : Next



1. 
Network Detective Data Collector - 2.0.1172
Scan Type
User Control Tests
File Scanner
Verify and Run
Collection Progress
Finish
File Scanner
NOTE: File scanning can cause a temporary increase in resource utilization.
Scan Types:
Personally Identifiable Information (PII)
Scan Options:
Include the scanning of ZIP files
Include the scanning of PDF files
PDF Timeout: 5 minutes (min = 1, max = 60)
Si vous choisissez cette option, ne la choisir que sur 1 des ordinateurs (Surtout sur un dossier partagé sur le réseau ou en nuage), autrement ça ralentis trop le réseau car le logiciel télécharge tous les .pdf et les .zip, les décompile et recherche dans le résultat pour des Renseignements Personnels.
(running on .NET CLR version 4.0.30319.42000)
Back
Next







Pre-scan Results and Recommendations

Execution Date: 2023-09-25 09:47:25 (UTC-05:00) Est (É.-U. et Canada)
Total Elapsed Time: 00:09:45

Scan Configuration

Target Network: Workgroup ()
192.168.56.0-192.168.56.255,192.168.2.0-192.168.2.255 (512 IP Addresses)

Results Summary

Domains Found: 0
Computers in Active Directory: 0
Active Directory computers that can be scanned remotely: 0
Active Directory computers that cannot be scanned remotely: 0
Users in Active Directory: 0
Computers that can be scanned remotely (including non-A/D computers): 0

Issue Summary

Overall:	**2 Critical Issues, 4 recommendations**
Active Directory:	0 Critical Issues, 0 recommendations
SQL Server:	0 Critical Issues, **1 recommendations**
Network Computers:	**1 Critical Issues, 2 recommendations**
Push Deploy:	**1 Critical Issues, 1 recommendations**

Recommendations

[CRITICAL] No computers were accessible via WMI or Remote Registry within the environment. This most likely points to a configuration issue or blocking by a local or remote firewall. For best results, please ensure that either WMI or Remote Registry is accessible remotely. Alternatively, the local data collector can be used to collect data on computers that are not remotely accessible.

[CRITICAL] No computers were accessible via the Push Deploy Tool. The tool is used to remotely run Local Data Collectors. Computers that are not accessible can still be scanned by manually running the Local Data Collector on those individual systems. To make systems accessible to push deploy, systems should respond to WMI, have access to Admin$ share, and have at least .NET 3.5 installed.

No SQL Servers were detected remotely. This could be due to SQL Servers not configured to broadcast or local firewalls blocking remote access. If there are known SQL Servers, the administrator should assure they are broadcasting properly and appropriate ports are open to allow access for inclusion in reports.

Partial Access is available to the following computers. Please review the notes next to each system to determine if additional access can be granted for more complete reporting.

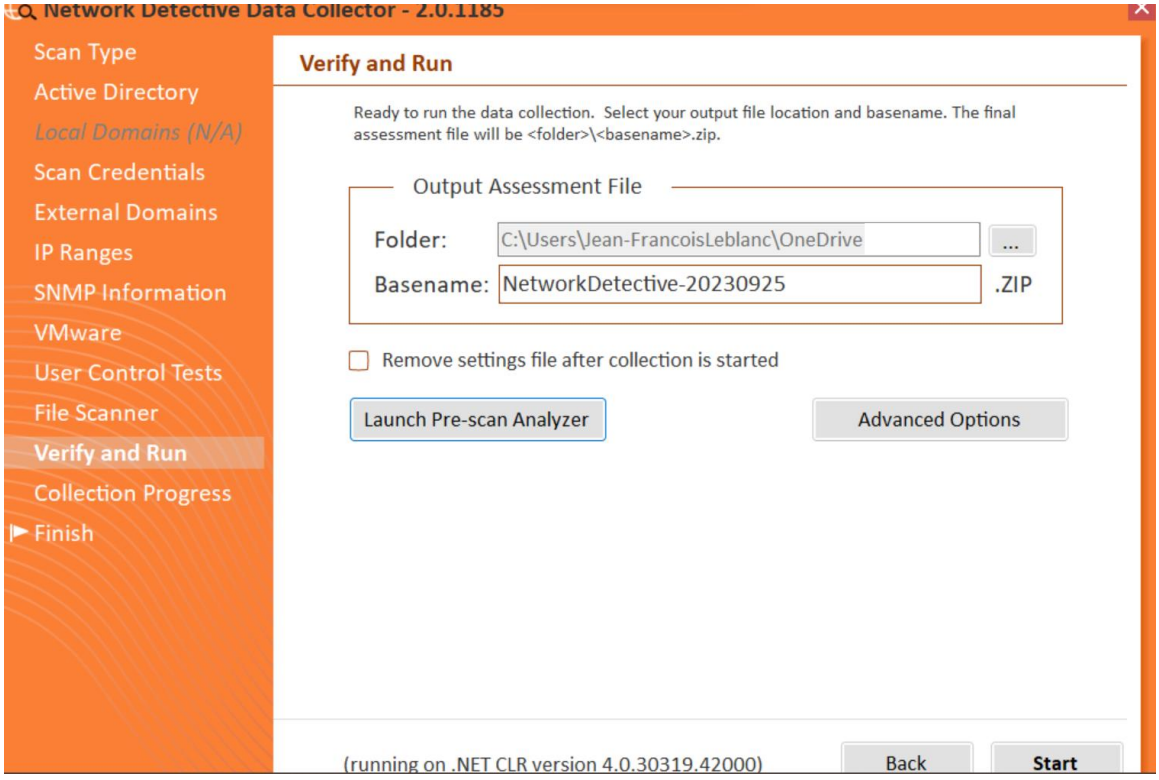
- DESKTOP-ULC0M10 (192.168.56.1) - Les références utilisateur ne peuvent pas être utilisées pour des connexions locales

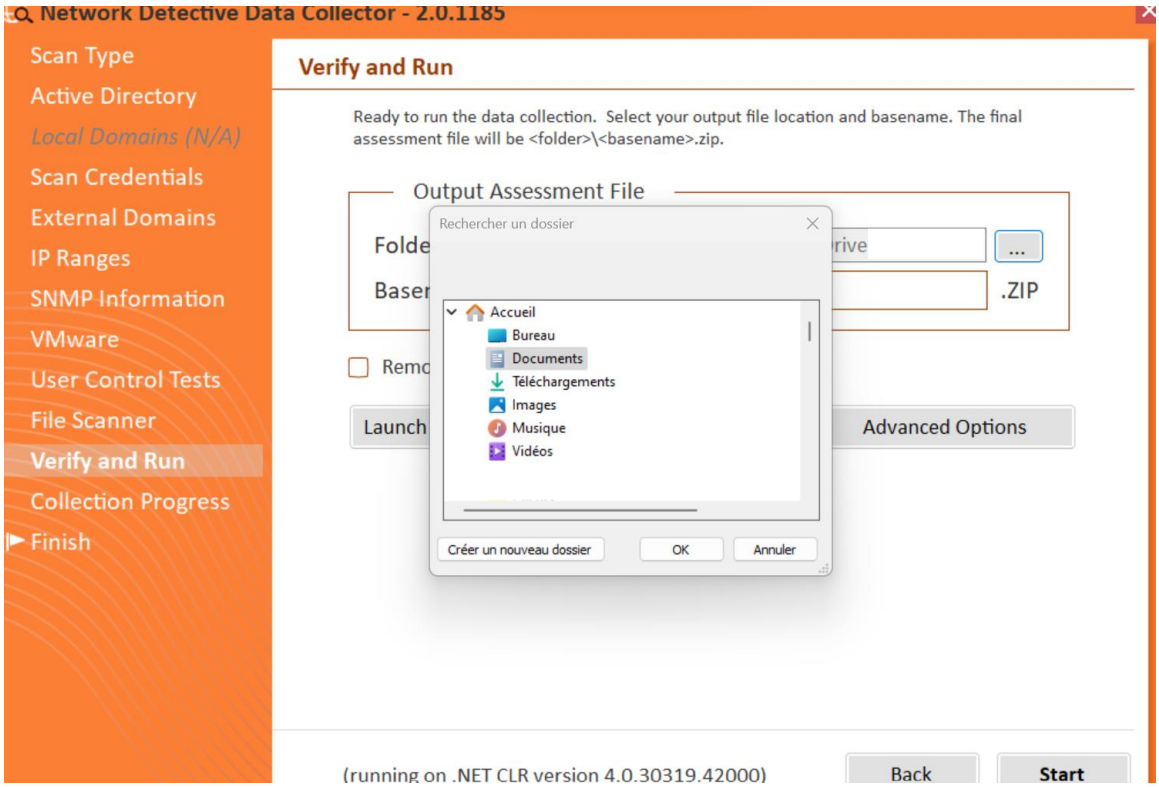
Report Notes

When computers are listed in light gray, those are to indicate computers where ping has failed. These computers in many cases are offline, but in some cases might be set to not respond to ping or firewalled.

Considérez les recommandations!

Si tout est beau, lancez le scan.





Important pour les groupes de travail (Workgroups):

Créez un répertoire Logs sur un lecteur réseau et mettez tous les logs des postes dans ce répertoire. Ainsi, vous n'aurez pas à faire le tour de tous les postes une seconde fois pour récupérer les logs.

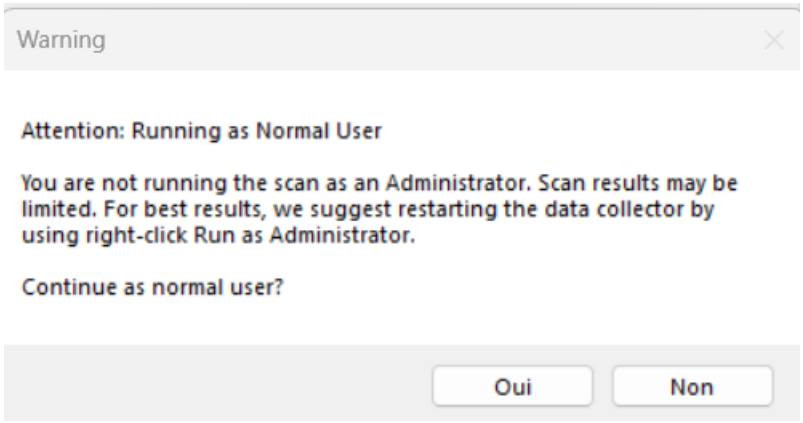
Si vous avez un Domaine – Active Directory (Avec serveur)

Pour les réseaux avec serveurs, faire cette démarche sur le serveur avec un compte administrateur du domaine.

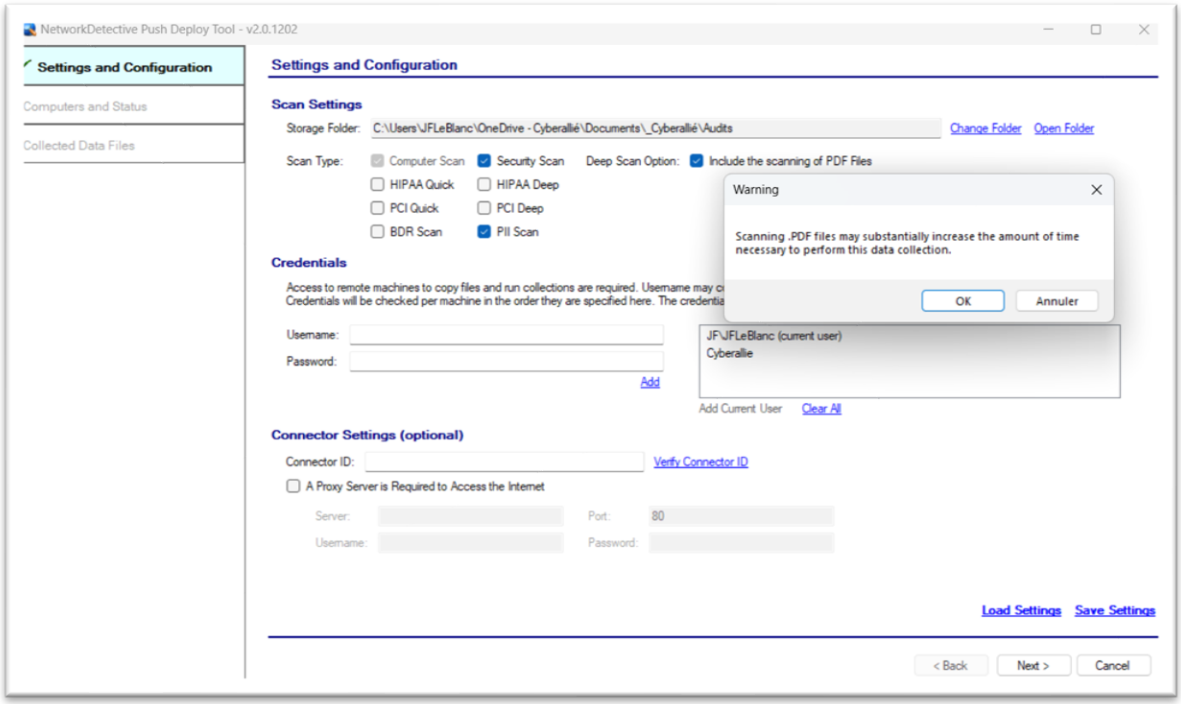
Pour les groupes de travail, faire cette démarche sur tous les postes.

NetworkDetectivePushDeployTool.zio instructions :

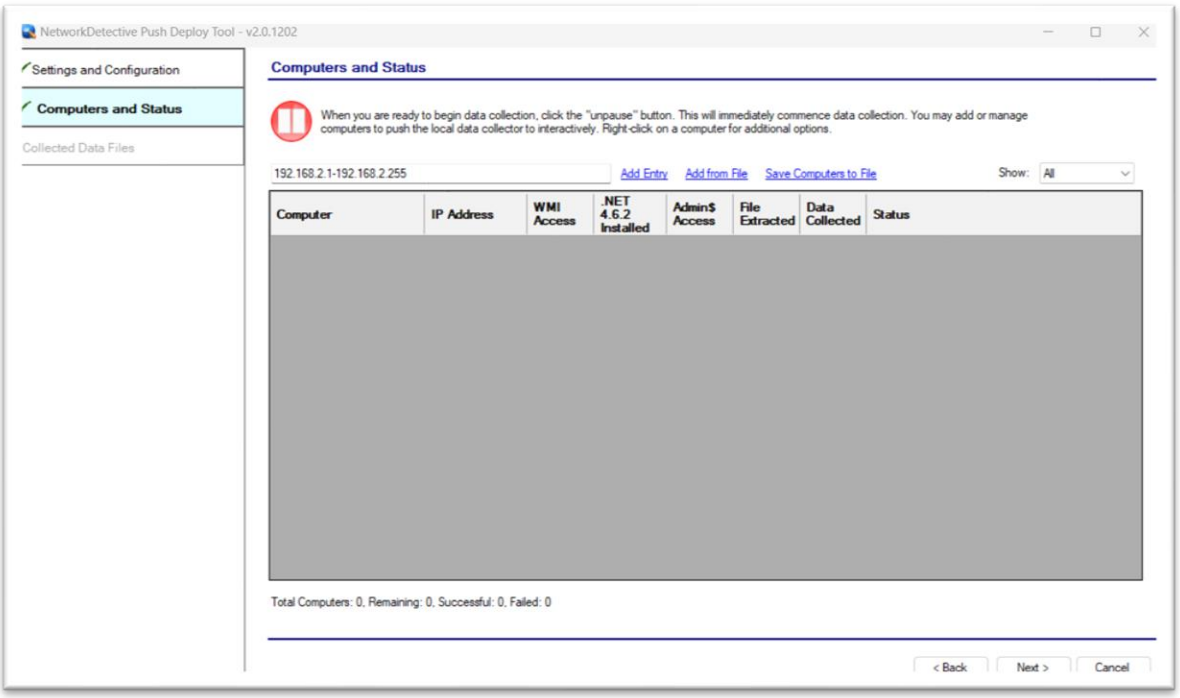
Choisir un PC disponible et performant, Extraire, exécuter en Admin sinon **:**

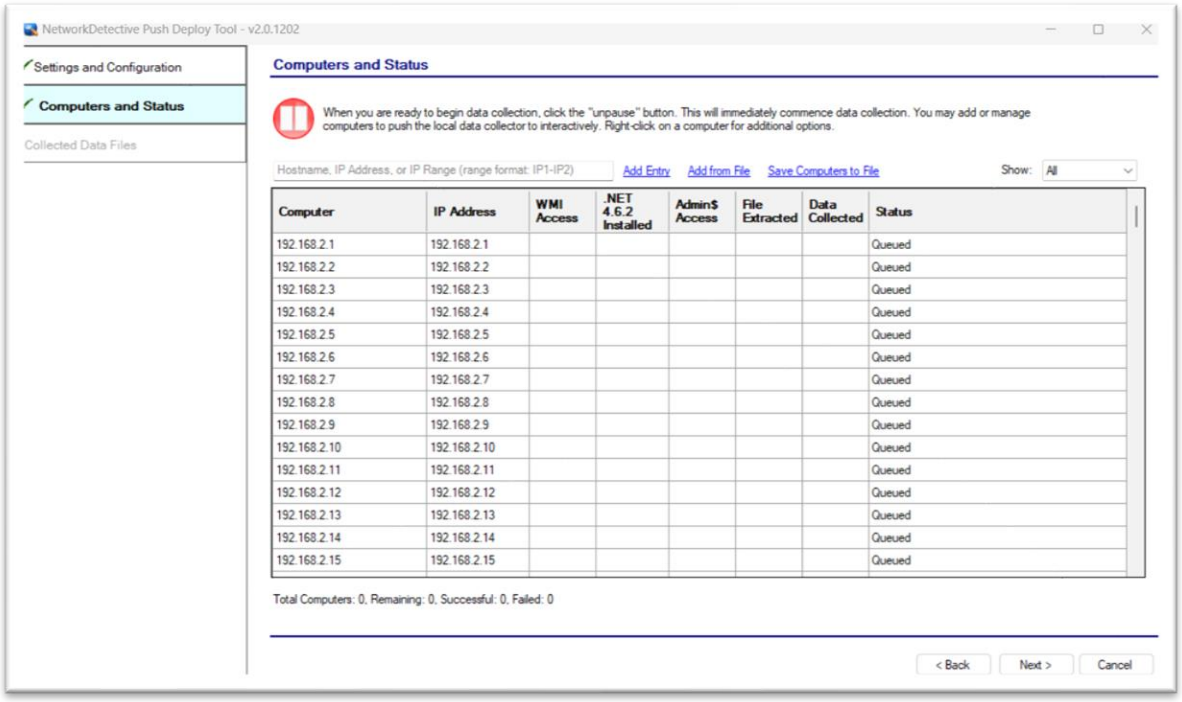


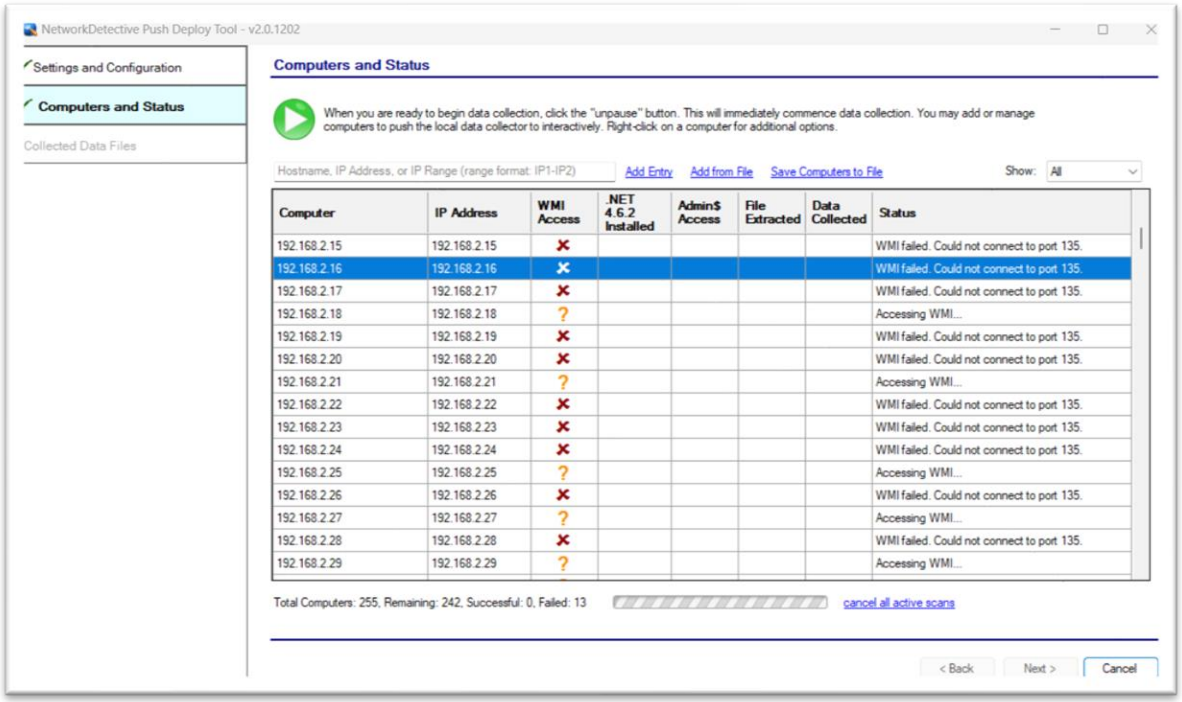
Cyberallie = compte Admin :



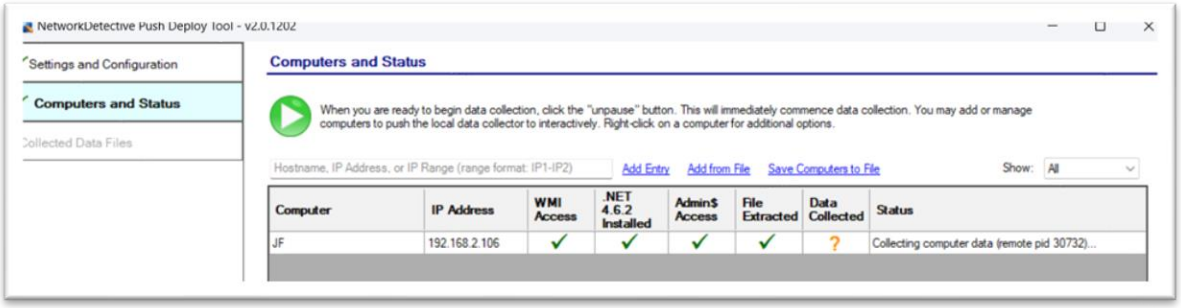
```
C:\Users\JFLeBlanc>ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte réseau sans fil Connexion au réseau local* 1 :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte réseau sans fil Connexion au réseau local* 2 :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . : home
   Adresse IPv6 de liaison locale. . . . .: fe80::2532:3feb:d54d:9a06%7
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.2.106
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.2.1
```

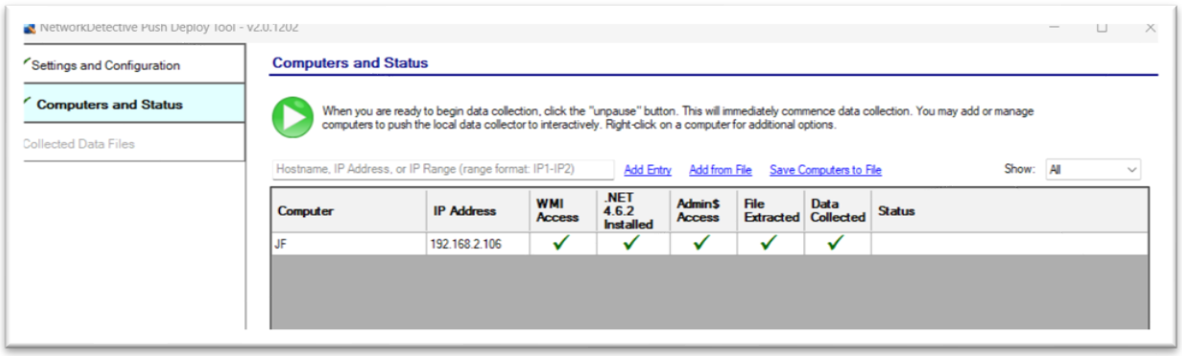




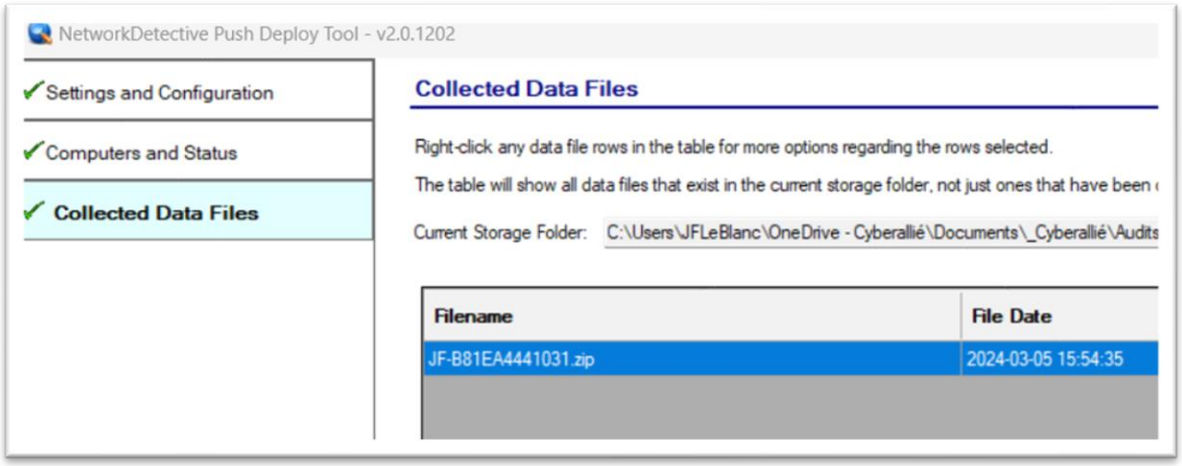


Exemple d'un bon scan :





Récupérer ce fichier et tous le .zip (1 par PC) et le mettre dans votre répertoire partagé :



Prendre en note l'adresse IP publique de l'entreprise.

Merci de m'aviser lorsque le tout sera terminé jf@cyberallie.com

Je suis toujours disponible pour vous accompagner avec ce processus.

Jean-François LeBlanc

Expert-conseils en sécurité informatique

Cybersécurité | Cyberallié

DONNÉES SÉCURISÉES, AFFAIRES ASSURÉES

819-955-7400

jf@cyberallie.com

www.cyberallie.com

Planifiez une rencontre avec moi

Fier membre du BNI Les Aristôts, de l'APEO et de la Chambre de Commerce de Gatineau

La sécurité n'est pas seulement un de nos produits. C'est notre fondement.