

Title MO IT XXXX	Page 1 / 12
---------------------	----------------

Auteur Megane Lezegning	Signature	Date 20 Janvier 2026
Owner Jean-Marc MORVAN	Signature	Date 09-Feb-2026

1. IDENTIFICATION UNIQUE / SERVER ID .....	2
2. SUJET .....	3
3. SCOPE.....	3
4. DESCRIPTION .....	3
5. PRES-REQUIS / REQUIREMENTS.....	3
5.1    Logiciel .....	<b>Erreur ! Signet non défini.</b>
5.2    Materiel .....	<b>Erreur ! Signet non défini.</b>
5.3    privileges .....	3
5.4    Restart requirements.....	3
6. STANDARD OPERATING PROCEDURE .....	4
6.1    Téléchargement et Installation .....	<b>Erreur ! Signet non défini.</b>
7. SIGNATURES .....	10
8. CHANGE LOG - JOURNAL DES REVISIONS .....	11
9. CHANGE LOG – ANNULATION PROCEDURE .....	11

**1. IDENTIFICATION UNIQUE / SERVER ID****TITLE**

Name : Audit de sécurité  
Active Directory

Installer Name: Megane  
Lezegning

Date: Day / Month (full) / Year (4 digit)  
\_\_\_\_20\_\_\_\_ / \_\_\_\_01\_\_\_\_ / \_\_\_\_2026\_\_\_\_

## 2. SUJET

Audit d'annuaire AD – Guide de l'Administrateur

## 3. SCOPE

Ensemble des contrôleur de domaine (DC) et des objets (utilisateur, ordinateur, GPO)

## 4. DESCRIPTION

PingCastle est un outil d'audit de santé qui permet d'identifier les vecteurs d'attaques les plus courants sur AD et générer un rapport priorisé avec de risque sur 100

## 5. PRES-REQUIS / REQUIREMENTS

### 5.1 Logiciel

C	N/A	Description
<input type="checkbox"/>	<input type="checkbox"/>	PingCastle (version 3.3.0.1)
<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	

### 5.2 Materiel

C	N/A	Description
<input type="checkbox"/>	<input type="checkbox"/>	Contrôleur de domaine ou serveur membre du domaine

### 5.3 privileges

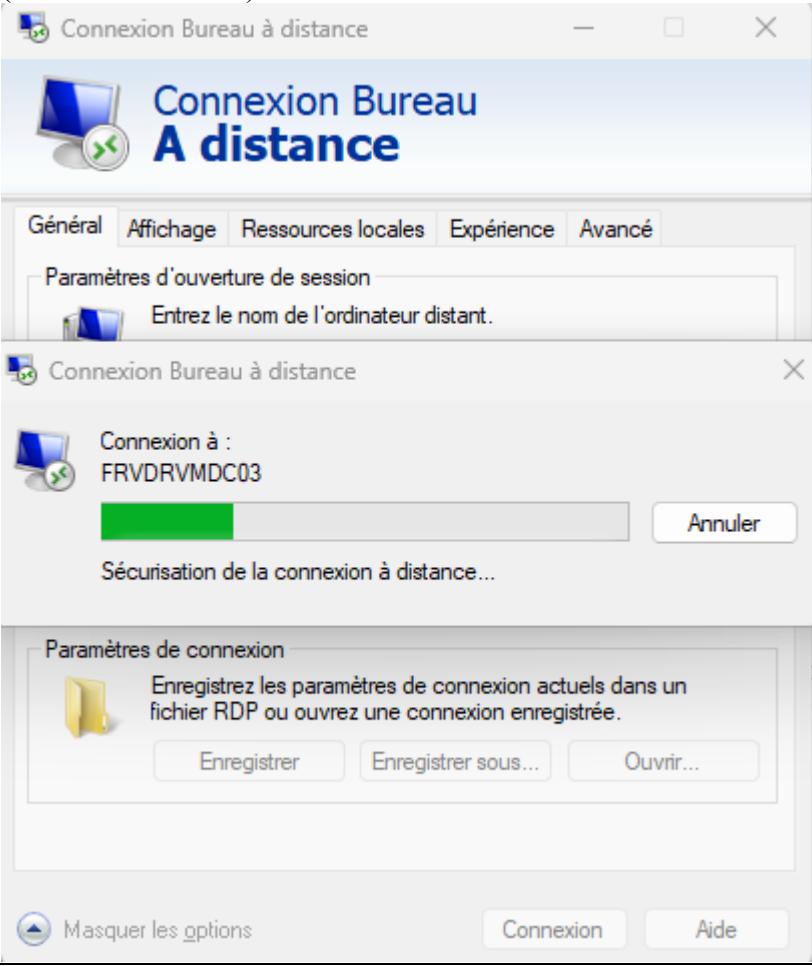
C	N/A	Description
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Workstation administrator <input checked="" type="checkbox"/> Server administrator <input type="checkbox"/> Active Directory administrator <input type="checkbox"/> Exchange administrator <input type="checkbox"/> Database administrator <input type="checkbox"/> SQL Server <input type="checkbox"/> Oracle <input type="checkbox"/> MySQL <input type="checkbox"/> Other: _____

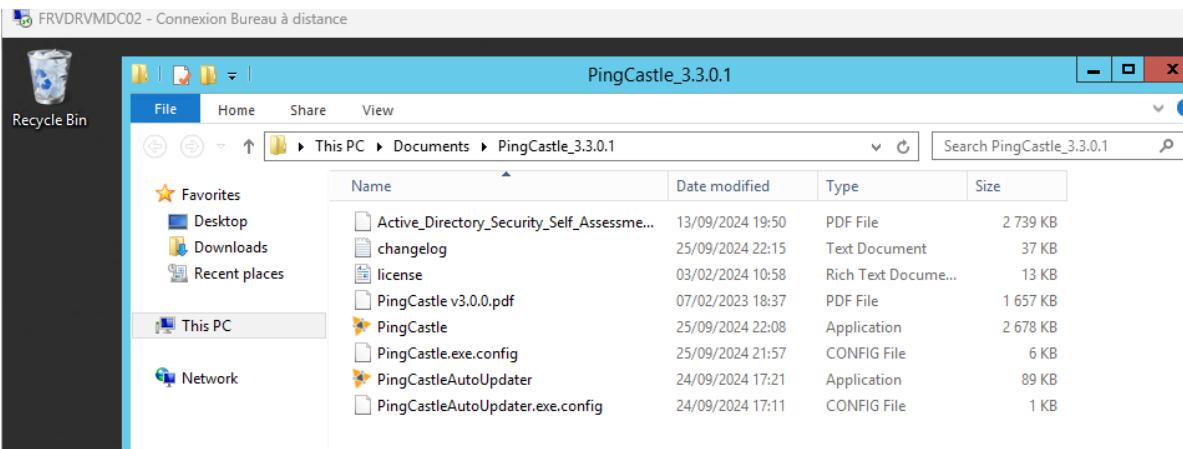
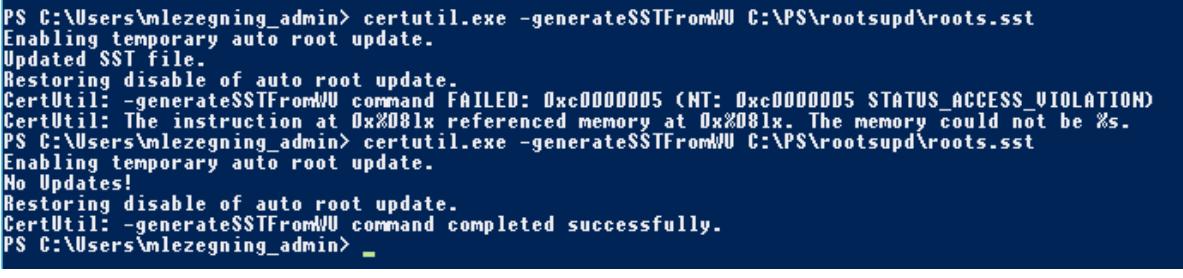
### 5.4 Restart requirements

There is no restart requirement during restore operations.

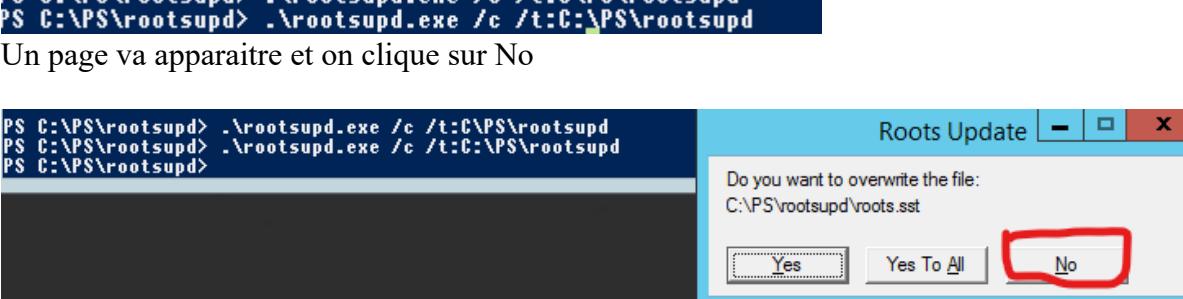
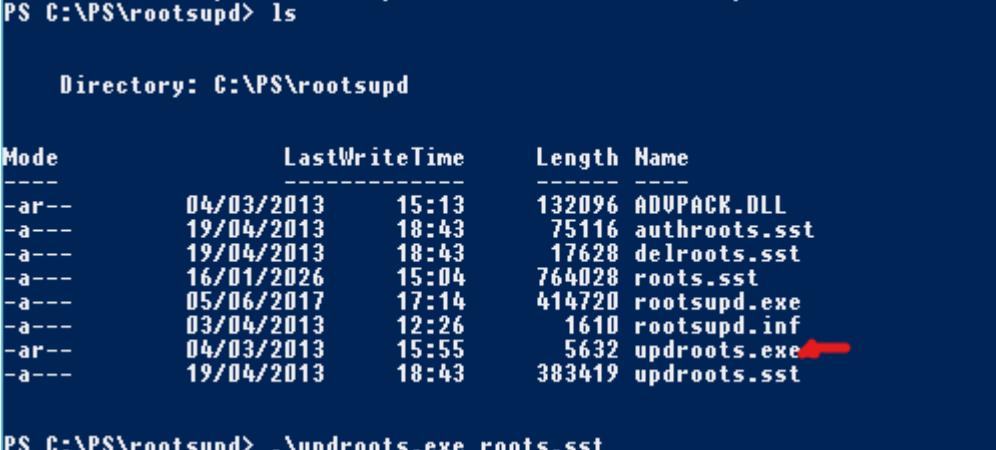
## 6. STANDARD OPERATING PROCEDURE

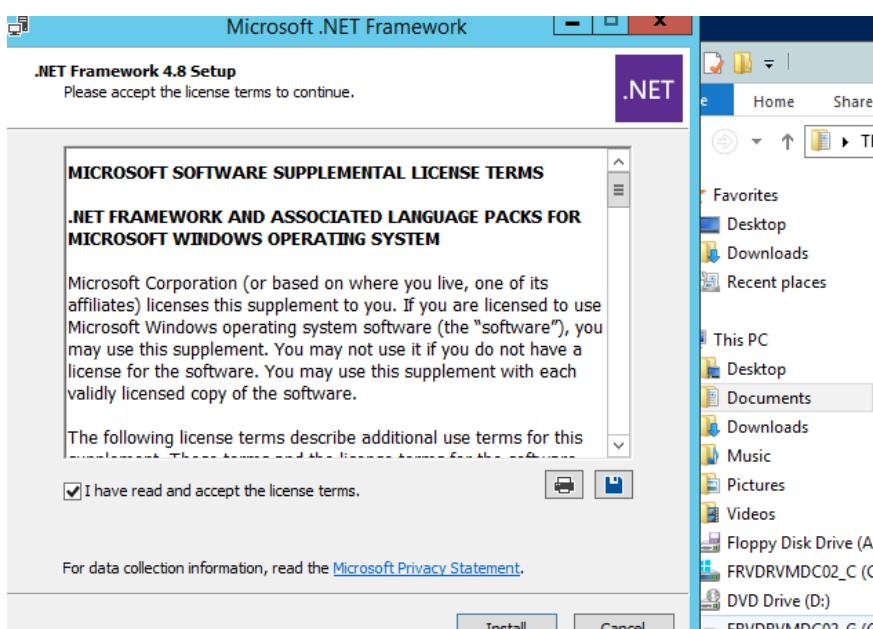
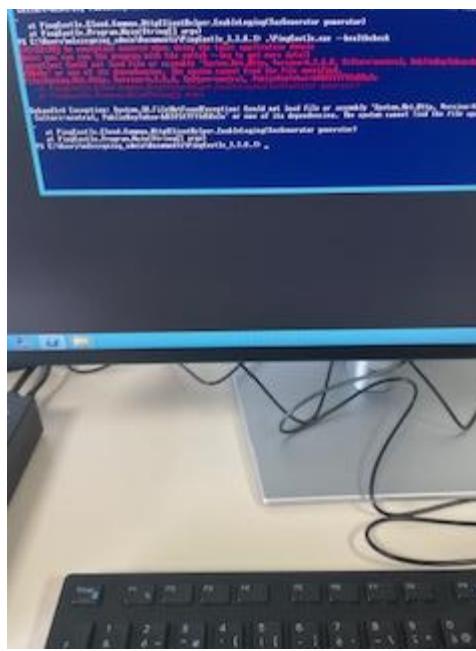
### 6.1 Téléchargement et Installation

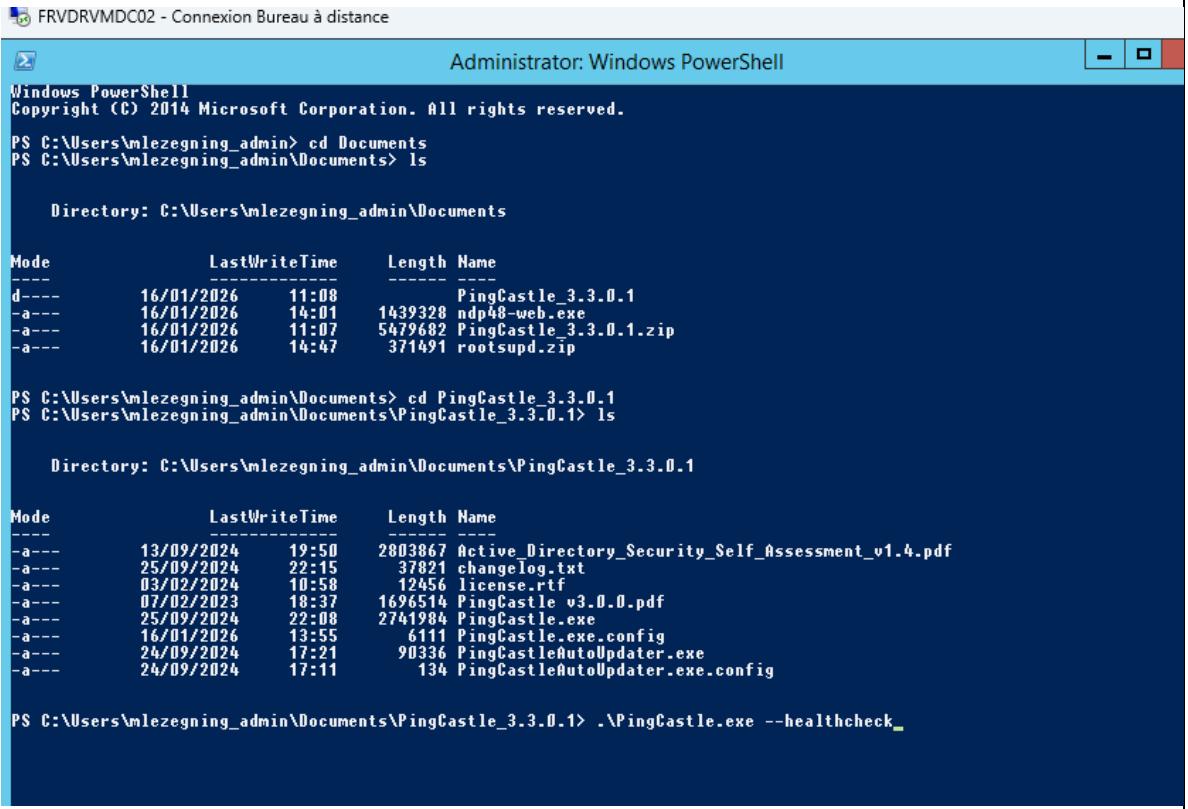
C	N/A	Item	Description
<input type="checkbox"/>	<input type="checkbox"/>	<b>6.1.1</b>	<p>Se connecter en RDP sur le serveur de gestion ou un contrôleur de domaine (FRVDRVMD03)</p> 
<input type="checkbox"/>	<input type="checkbox"/>	<b>6.1.2</b>	<ul style="list-style-type: none"><li>Télécharger l'archive ZIP depuis le site officiel de PingCastle (<a href="https://www.pingcastle.com/download/">https://www.pingcastle.com/download/</a>)</li></ul>
<input type="checkbox"/>	<input type="checkbox"/>	<b>6.1.3</b>	Créer un dossier dédié (ex : C:\Users\Admin\Documents\PingCastle)

C	N/A	Item	Description
<input type="checkbox"/>	<input type="checkbox"/>	<b>6.1.4</b>	<p>Extraire le contenu de l'archive dans ce dossier</p> 
<input type="checkbox"/>	<input type="checkbox"/>	<b>6.1.5</b>	<p>Mettre à jour manuellement les certificats racine pour pouvoir lancer pingCastle (OS obsolète)</p> <p>Crée une liste des certificats racine à jour. Pour ce faire, exécute la commande :</p> <pre>&lt;&lt;certutil.exe -generateSSTFromWU roots.sst&gt;&gt;</pre> 

<input type="checkbox"/>	<input type="checkbox"/>	6.1.6	<p>Créer un Dossier C:\PS\rootsupd</p> <pre>PS C:\Users\mlezegeing_admin&gt; New-Item -ItemType Directory -Force -path "C:\PS\rootsupd"      Directory: C:\PS  Mode                LastWriteTime     Length Name ----                -----          ----  d---        16/01/2026      15:02           rootsupd  PS C:\Users\mlezegeing_admin&gt; _</pre> <p>Enregistrer le fichier roots.sst dans le dossier créé</p> <pre>PS C:\Users\mlezegeing_admin&gt; ls C:\PS\rootsupd\      Directory: C:\PS\rootsupd  Mode                LastWriteTime     Length Name ----                -----          ----  -a---        16/01/2026      15:04    764028 roots.sst  PS C:\Users\mlezegeing_admin&gt; _</pre>
<input type="checkbox"/>	<input type="checkbox"/>	6.1.7	<p>Téléchargez l'archive <a href="#">rootsupd.zip</a> et extrayez le fichier rootsupd.exe.</p> <pre>PS C:\PS\rootsupd&gt; ls      Directory: C:\PS\rootsupd  Mode                LastWriteTime     Length Name ----                -----          ----  -a---        16/01/2026      15:04    764028 roots.sst -a---        05/06/2017      17:14   414720 rootsupd.exe</pre>

<input type="checkbox"/>	<input type="checkbox"/>	6.1.8	Executer le fichier rootsupd.exe avec les parametres : « .\rootsupd.exe /c /t:C:\PS\rootsupd »   Un page va apparaitre et on clique sur No
<input type="checkbox"/>	<input type="checkbox"/>	6.1.9	Apres l'executon , on verifie que le dossier contient l'utilitaire updroots.exe   PS C:\PS\rootsupd> ls  Directory: C:\PS\rootsupd  Mode LastWriteTime Length Name ---- -- -- -- -- -ar-- 04/03/2013 15:13 132096 ADVPACK.DLL -a--- 19/04/2013 18:43 75116 authroots.sst -a--- 19/04/2013 18:43 17628 delroots.sst -a--- 16/01/2026 15:04 764028 roots.sst -a--- 05/06/2017 17:14 414720 rootsupd.exe -a--- 03/04/2013 12:26 1610 rootsupd.inf -ar-- 04/03/2013 15:55 5632 updroots.exe -a--- 19/04/2013 18:43 383419 updroots.sst  PS C:\PS\rootsupd> .\updroots.exe roots.sst
<input type="checkbox"/>	<input type="checkbox"/>	6.1.10	On installe les certificats racine à jour à l'aide de l'utilitaire updroots.exe en executant la commande suivante : « « .\updroots.exe roots.sst » »   PS C:\PS\rootsupd> .\updroots.exe roots.sst PS C:\PS\rootsupd>

<input type="checkbox"/>	<input type="checkbox"/>	<b>6.1.11</b>	On lance l'installation du .NetFramework 4.8 que j'ai telechargers sur le site officiel sur mon PC et copier coller sur mon serveur
			
<input type="checkbox"/>	<input type="checkbox"/>	<b>6.1.12</b>	On relance notre outil PingCastle mais si notre Os est à jour pas besion de faire une config manuelle des certificats racine  Car moi en voilancer mon PingCastle j'ai une erreur à cause des certificats qui n'etais pas à jour  

<input type="checkbox"/>	<input type="checkbox"/>	6.1.13	Ouvre un powershell et navigue jusqu'au dossier
			 <pre> FRVDRVMDC02 - Connexion Bureau à distance Administrator: Windows PowerShell Windows PowerShell Copyright (C) 2014 Microsoft Corporation. All rights reserved.  PS C:\Users\mlezechning_admin&gt; cd Documents PS C:\Users\mlezechning_admin\Documents&gt; ls      Directory: C:\Users\mlezechning_admin\Documents  Mode LastWriteTime Length Name ---- -- -- -- -- d--- 16/01/2026 11:08 PingCastle_3.3.0.1 -a-- 16/01/2026 14:01 1439328 ndp48-web.exe -a-- 16/01/2026 11:07 5479682 PingCastle_3.3.0.1.zip -a-- 16/01/2026 14:47 371491 rootsupd.zip  PS C:\Users\mlezechning_admin\Documents&gt; cd PingCastle_3.3.0.1 PS C:\Users\mlezechning_admin\Documents\PingCastle_3.3.0.1&gt; ls      Directory: C:\Users\mlezechning_admin\Documents\PingCastle_3.3.0.1  Mode LastWriteTime Length Name ---- -- -- -- -- -a-- 13/09/2024 19:50 2803867 Active_Directory_Security_Self_Assessment_v1.4.pdf -a-- 25/09/2024 22:15 37821 changelog.txt -a-- 03/02/2024 10:58 12456 license.rtf -a-- 07/02/2023 18:37 1696514 PingCastle_v3.0.0.pdf -a-- 25/09/2024 22:08 2741984 PingCastle.exe -a-- 16/01/2026 13:55 6111 PingCastle.exe.config -a-- 24/09/2024 17:21 90336 PingCastleAutoUpdater.exe -a-- 24/09/2024 17:11 134 PingCastleAutoUpdater.exe.config  PS C:\Users\mlezechning_admin\Documents\PingCastle_3.3.0.1&gt; .\PingCastle.exe --healthcheck_ </pre>
<input type="checkbox"/>	<input type="checkbox"/>	6.1.14	Lance le Script avec la commande : « « .\PingCastle.exe –healthcheck » »
			<pre> PS C:\Users\mlezechning_admin\Documents\PingCastle_3.3.0.1&gt; .\PingCastle.exe --healthcheck Free Edition of PingCastle 3.3.0 - Not for commercial use Starting the task: Perform analysis for frvdr.com [15:53:46] Getting domain information (frvdr.com) [15:53:48] Gathering general data [15:53:49] This domain contains approximatively 2993 objects [15:53:49] Gathering user data [15:53:49] Gathering computer data [15:53:49] Gathering trust data [15:53:50] Gathering privileged group and permissions data   - Initialize   - Searching for critical and infrastructure objects [15:53:50] - Collecting objects - Iteration 1 [15:53:50] - Collecting objects - Iteration 2 [15:53:50] - Collecting objects - Iteration 3 [15:53:50] - Collecting objects - Iteration 4 [15:53:50] - Collecting objects - Iteration 5 [15:53:50] - Collecting objects - Iteration 6 [15:53:50] - Completing object collection [15:53:50] Gathering delegation data [15:53:51] Gathering gpo data [15:53:51] Gathering pki data [15:53:53] Gathering sccm data [15:53:53] Gathering exchange data [15:53:53] Gathering anomaly data [15:53:53] Gathering dns data [15:53:53] Gathering WSUS data [15:53:53] Gathering MSOL data [15:53:53] Gathering domain controller data (including null session) (including RPC tests) [15:54:01] Gathering network data [15:54:01] Computing risks [15:54:02] Export completed [15:54:02] Generating html report [15:54:02] Generating xml file for consolidation report [15:54:02] Export level is Normal [15:54:02] Personal data will NOT be included in the .xml file (Add --level Full to add it. Ex: PingCastle.exe --interactive --level Full) [15:54:02] Done Task Perform analysis for frvdr.com completed PS C:\Users\mlezechning_admin\Documents\PingCastle_3.3.0.1&gt; </pre>

<input type="checkbox"/>	<input type="checkbox"/>	<b>6.1.15</b>	Sa nous générer deux fichier								
			<table border="1"> <tr> <td> ad_hc_frvdr.com</td> <td>16/01/2026 15:54</td> <td>HTML Document</td> <td>1 623 KB</td> </tr> <tr> <td> ad_hc_frvdr.com</td> <td>16/01/2026 15:54</td> <td>XML Document</td> <td>67 KB</td> </tr> </table>	ad_hc_frvdr.com	16/01/2026 15:54	HTML Document	1 623 KB	ad_hc_frvdr.com	16/01/2026 15:54	XML Document	67 KB
ad_hc_frvdr.com	16/01/2026 15:54	HTML Document	1 623 KB								
ad_hc_frvdr.com	16/01/2026 15:54	XML Document	67 KB								
<input type="checkbox"/>	<input type="checkbox"/>	<b>6.1.16</b>	Ouvre le fichier HTML et la on'a notre analyse								
			<p><b>frvdr.com - Analyse de bilan de santé</b> Date : 16/01/2026 - Version du moteur : 3.3.0.1</p> <p>Ce rapport a été généré avec l'édition de base de PingCastle. <a href="#">?</a> L'intégration de ce document à des fins commerciales (vente des informations contenues dans le rapport) est interdite. Si vous êtes auditeur, vous devez obligatoirement acquérir une licence d'auditeur pour participer au développement de ce document.</p> <p><b>Indicateurs Active Directory</b></p> <p>Cette section se concentre sur les indicateurs de sécurité essentiels. Identifiez le sous-processus qui détermine le score et modifiez certaines règles dans ce domaine pour améliorer ce score.</p> <p><b>Indicateurs</b></p> <p>Niveau de risque du domaine : 100/100 Il s'agit du score maximal des 4 indicateurs, et aucun score ne peut dépasser 100. Plus le score est bas, mieux c'est.</p> <p><a href="#">Comparer avec les statistiques</a> <a href="#">Avis de confidentialité</a></p> <table border="1"> <tr> <td>Objet périmé : 68/100 Il s'agit d'opérations liées aux objets utilisateur ou ordinateur</td> <td>17 règles correspondantes</td> <td>Fiducies : 6/100 Il s'agit des connexions entre deux annuaires Active Directory.</td> <td>2 règles correspondantes</td> </tr> <tr> <td>Comptes privilégiés : 65/100 Il s'agit des administrateurs d'Active Directory</td> <td>7 règles correspondantes</td> <td>Anomalies : 100/100 Il s'agit de points de contrôle de sécurité spécifiques</td> <td>18 règles correspondantes</td> </tr> </table>	Objet périmé : 68/100 Il s'agit d'opérations liées aux objets utilisateur ou ordinateur	17 règles correspondantes	Fiducies : 6/100 Il s'agit des connexions entre deux annuaires Active Directory.	2 règles correspondantes	Comptes privilégiés : 65/100 Il s'agit des administrateurs d'Active Directory	7 règles correspondantes	Anomalies : 100/100 Il s'agit de points de contrôle de sécurité spécifiques	18 règles correspondantes
Objet périmé : 68/100 Il s'agit d'opérations liées aux objets utilisateur ou ordinateur	17 règles correspondantes	Fiducies : 6/100 Il s'agit des connexions entre deux annuaires Active Directory.	2 règles correspondantes								
Comptes privilégiés : 65/100 Il s'agit des administrateurs d'Active Directory	7 règles correspondantes	Anomalies : 100/100 Il s'agit de points de contrôle de sécurité spécifiques	18 règles correspondantes								

## 7. SIGNATURES

**Installateur : Je confirme que cette installation a été exécutée suivant les instructions de cette check-list.**

**Installer : I certify that this installation was done following the instructions provided in this checklist.**

Installer Signature: Megane Lezegning	Date: 20 Janvier 2026
Printed Name	

**Vérificateur / Manager : Je confirme que cette installation a été exécutée suivant les instructions de cette check-list.**

**Verifier/Manager : I certify that this installation was done following the instructions provided in this checklist**

Verifier Signature	Date
Printed Name	

## 8. CHANGE LOG - JOURNAL DES REVISIONS

Version	Auteur	Description des modifications	Raison / Commentaries
1.0	Megane Lezegning	Création initiale du MO IT	Mise ne place audit annuel

## 9. CHANGE LOG – ANNULATION PROCEDURE

Effective	Version	Author	Change Description	Reason / Comment
			Cancellation	
SOP Owner Approval – Name		Signature		Date

