

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 controleur 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"/>	Controleur de domaine ou serveur membre du domaine

### 5.3 privileges

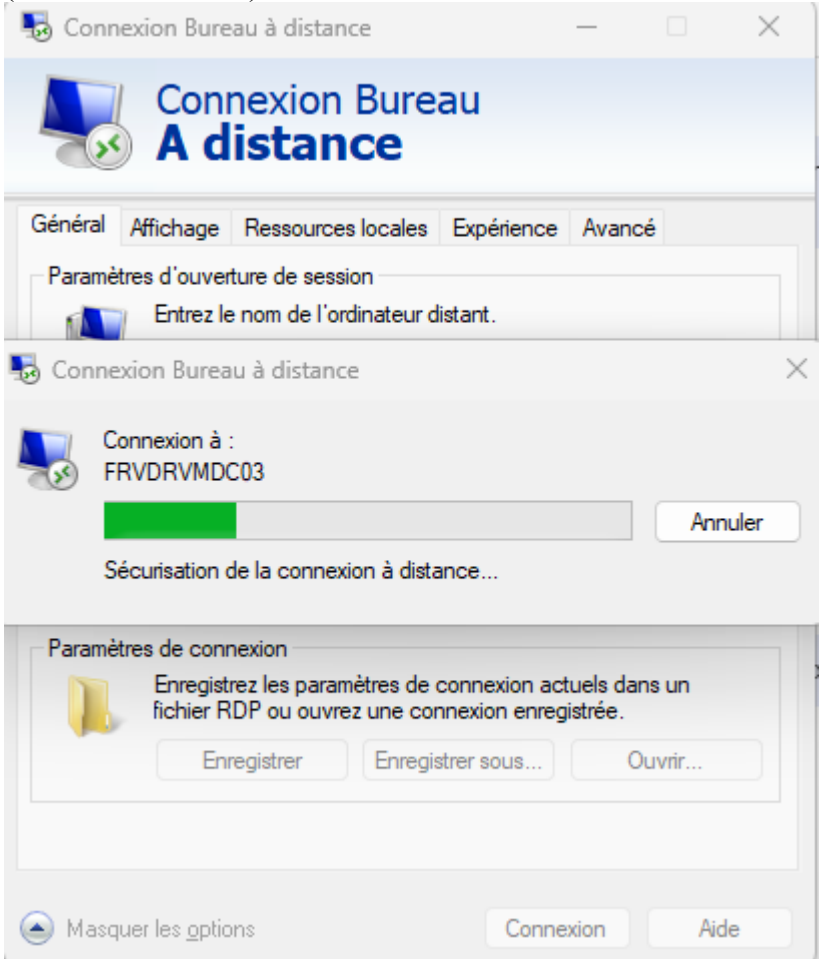
C	N/A	Description
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Workstation administrator <input checked="" type="checkbox"/> Server administrator <input type="checkbox"/> Active Directory administrator <input type="checkbox"/> Exchange administrator <input type="checkbox"/>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

### 5.4 Restart requirements

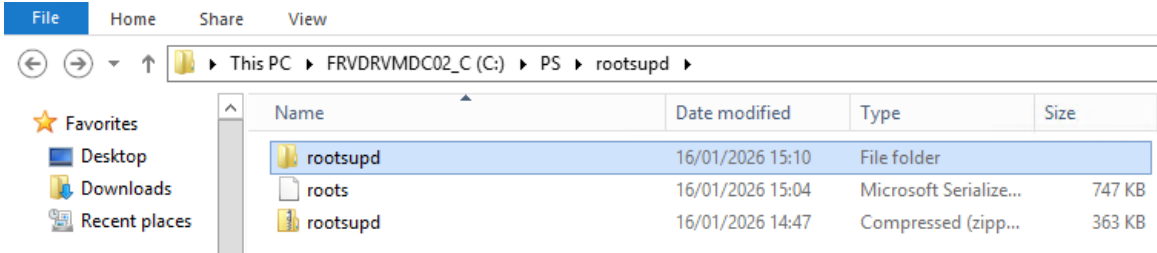
There is no restart requirement during restore operations.

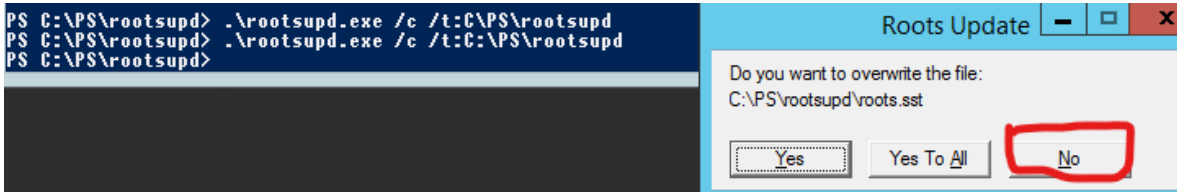
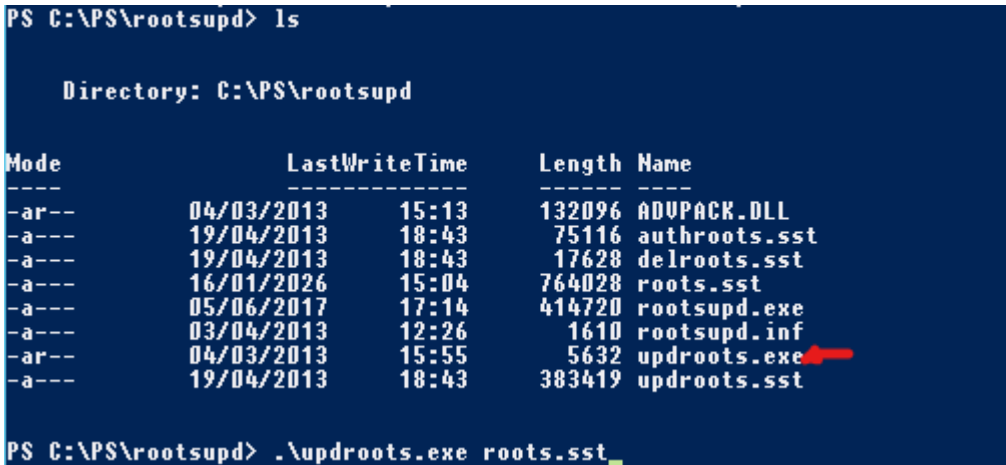
## 6. STANDARD OPERATING PROCEDURE

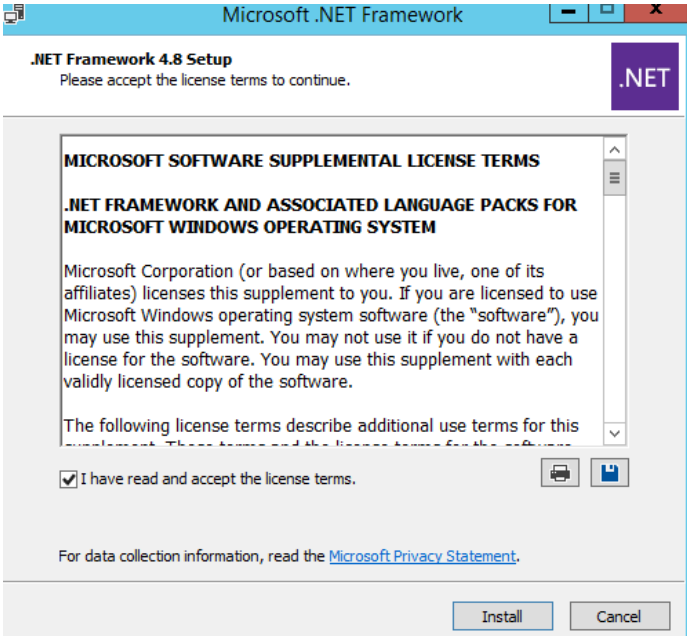
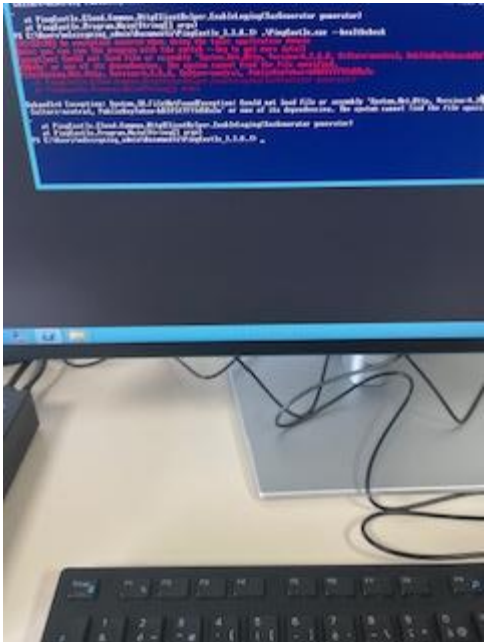
### 6.1 Téléchargement et Installation

C	N/A	Item	Description
<input type="checkbox"/>	<input type="checkbox"/>	6.1.1	<p>Se connecter en RDP sur le serveur de gestion ou un contrôleur de domaine (FRVDRVMDC03)</p> 
<input type="checkbox"/>	<input type="checkbox"/>	6.1.2	<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"/>	6.1.3	Créer un dossier dédié (ex : C:\Users\Admin\Documents\PingCastle)

C	N/A	Item	Description
<input type="checkbox"/>	<input type="checkbox"/>	6.1.4	<p>Extraire le contenu de l'archive dans ce dossier</p>
<input type="checkbox"/>	<input type="checkbox"/>	6.1.5	<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> <pre>PS C:\Users\mlezegning_admin&gt; certutil.exe -generateSSTFromWU C:\PS\rootsupd\roots.sst Enabling temporary auto root update. Updated SST file. Restoring disable of auto root update. CertUtil: -generateSSTFromWU command FAILED: 0xc0000005 (NT: 0xc0000005 STATUS_ACCESS_VIOLATION) CertUtil: The instruction at 0x%08lx referenced memory at 0x%08lx. The memory could not be %s. PS C:\Users\mlezegning_admin&gt; certutil.exe -generateSSTFromWU C:\PS\rootsupd\roots.sst Enabling temporary auto root update. No Updates! Restoring disable of auto root update. CertUtil: -generateSSTFromWU command completed successfully. PS C:\Users\mlezegning_admin&gt; _</pre>

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

<input type="checkbox"/>	<input type="checkbox"/>	6.1.8	<p>Executer le fichier rootsupd.exe avec les parametres : « \rootsupd.exe /c /t :C:\PS\rootsupd »</p> <pre>PS C:\PS\rootsupd&gt; .\rootsupd.exe /c /t:C:\PS\rootsupd</pre> <p>Un page va apparaitre et on clique sur No</p> 
<input type="checkbox"/>	<input type="checkbox"/>	6.1.9	<p>Après l'exécution , on verifie que le dossier contient l'utilitaire updroots.exe</p> 
<input type="checkbox"/>	<input type="checkbox"/>	6.1.10	<p>On installe les certificats racine à jour à l'aide de l'utilitaire updroots.exe en executant la commande suivante : « \updroots.exe roots.sst » »</p> <pre>PS C:\PS\rootsupd&gt; .\updroots.exe roots.sst PS C:\PS\rootsupd&gt;</pre>

<input type="checkbox"/>	<input type="checkbox"/>	6.1.11	<p>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</p> 
<input type="checkbox"/>	<input type="checkbox"/>	6.1.12	<p>On relance notre outil PingCastle mais si notre Os est à jour pas besoin de faire une config manuelle des certificats racine</p> <p>Car moi en voilancer mon PingCastle j'ai une erreur à cause des certificats qui n'étais pas à jour</p> 

☐ ☐ **6.1.13** Ouvrir un powershell et naviguer jusqu'au dossier

```

FRVDRVMDC02 - Connexion Bureau à distance

Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\mlezeqning_admin> cd Documents
PS C:\Users\mlezeqning_admin\Documents> ls

    Directory: C:\Users\mlezeqning_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\mlezeqning_admin\Documents> cd PingCastle_3.3.0.1
PS C:\Users\mlezeqning_admin\Documents\PingCastle_3.3.0.1> ls

    Directory: C:\Users\mlezeqning_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\mlezeqning_admin\Documents\PingCastle_3.3.0.1> .\PingCastle.exe --healthcheck_

```

☐ ☐ **6.1.14** Lancer le Script avec la commande : « « .\PingCastle.exe --healthcheck » »

```

PS C:\Users\mlezeqning_admin\Documents\PingCastle_3.3.0.1> .\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 approximately 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
[15:53:50] - Initialize
[15:53:50] - 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] - Export completed
[15:53:51] Gathering delegation data
[15:53:51] Gathering gpo data
[15:53:53] Gathering pki data
[15:53:53] Gathering scm 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 --inter
tive --level Full)
[15:54:02] Done
Task Perform analysis for frvdr.com completed
PS C:\Users\mlezeqning_admin\Documents\PingCastle_3.3.0.1>

```

<input type="checkbox"/>	<input type="checkbox"/>	<b>6.1.15</b>	Sa nous générer deux fichier  <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <div> ad_hc_frvdr.com</div> <div>16/01/2026 15:54</div> <div>HTML Document</div> <div>1 623 KB</div> </div> <div style="display: flex; justify-content: space-between; align-items: center;"> <div> ad_hc_frvdr.com</div> <div>16/01/2026 15:54</div> <div>XML Document</div> <div>67 KB</div> </div> </div>				
<input type="checkbox"/>	<input type="checkbox"/>	<b>6.1.16</b>	Ouvre le fichier HTML et la on'a notre analyse  <div style="border: 1px solid #ccc; padding: 10px; margin: 5px 0;"> <div style="display: flex; justify-content: space-between; align-items: center; border-bottom: 1px solid #ccc; padding-bottom: 5px;"> <div> frvdr.com</div> <div>16/01/2026</div> <div>À propos</div> </div> <div style="text-align: center; margin-top: 10px;"> <h2 style="color: #f96;">frvdr.com - Analyse de bilan de santé</h2> <p style="color: #f96;">Date : 16/01/2026 - Version du moteur : 3.3.0.1</p> </div> <div style="background-color: #e0f7fa; padding: 5px; margin: 5px 0; font-size: 0.9em;"> <p>Ce rapport a été généré avec l'édition de base de PingCastle. <a href="#">?</a></p> <p><b>L'intégration de ce document à des fins commerciales</b> (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> </div> <div style="background-color: #ffeb3b; padding: 5px; margin: 5px 0; font-weight: bold;">Indicateurs Active Directory</div> <p style="font-size: 0.8em; margin: 5px 0;">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> <div style="display: flex; align-items: center; margin: 10px 0;"> <div style="text-align: center;"> <h3 style="color: #f96;">Indicateurs</h3> </div> <div style="margin-left: 20px;"> <p>Niveau de risque du domaine : 100/100</p> <p style="font-size: 0.8em;">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> <div style="border: 1px solid #ccc; padding: 2px 5px; margin: 5px 0;">Comparer avec les statistiques</div> <p style="font-size: 0.8em; color: #f96;"><a href="#">Avis de confidentialité</a></p> </div> </div> <table border="1" style="width: 100%; border-collapse: collapse; font-size: 0.8em; margin: 10px 0;"> <tr> <td style="width: 25%; text-align: center; vertical-align: top;"> <p>Objet périmé : 68/100</p> <p style="font-size: 0.7em;">Il s'agit d'opérations liées aux objets utilisateur ou ordinateur</p> </td> <td style="width: 25%; text-align: center; vertical-align: top;"> <p>17 règles correspondent</p> </td> <td style="width: 25%; text-align: center; vertical-align: top;"> <p>Fiducies : 6/100</p> <p style="font-size: 0.7em;">Il s'agit des connexions entre deux annuaires Active Directory.</p> </td> <td style="width: 25%; text-align: center; vertical-align: top;"> <p>Anomalies : 100/100</p> <p style="font-size: 0.7em;">Il s'agit de points de contrôle de sécurité spécifiques</p> </td> </tr> </table> </div>	<p>Objet périmé : 68/100</p> <p style="font-size: 0.7em;">Il s'agit d'opérations liées aux objets utilisateur ou ordinateur</p>	<p>17 règles correspondent</p>	<p>Fiducies : 6/100</p> <p style="font-size: 0.7em;">Il s'agit des connexions entre deux annuaires Active Directory.</p>	<p>Anomalies : 100/100</p> <p style="font-size: 0.7em;">Il s'agit de points de contrôle de sécurité spécifiques</p>
<p>Objet périmé : 68/100</p> <p style="font-size: 0.7em;">Il s'agit d'opérations liées aux objets utilisateur ou ordinateur</p>	<p>17 règles correspondent</p>	<p>Fiducies : 6/100</p> <p style="font-size: 0.7em;">Il s'agit des connexions entre deux annuaires Active Directory.</p>	<p>Anomalies : 100/100</p> <p style="font-size: 0.7em;">Il s'agit de points de contrôle de sécurité spécifiques</p>				

## 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.**

MO IT XXXX	Page 11 / 12
------------	-----------------

**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

