

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	Erreur ! Signet non défini.
5.2 Materiel	Erreur ! Signet non défini.
5.3 privileges	3
5.4 Restart requirements.....	3
6. STANDARD OPERATING PROCEDURE	4
6.1 Téléchargement et Installation	Erreur ! Signet non défini.
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

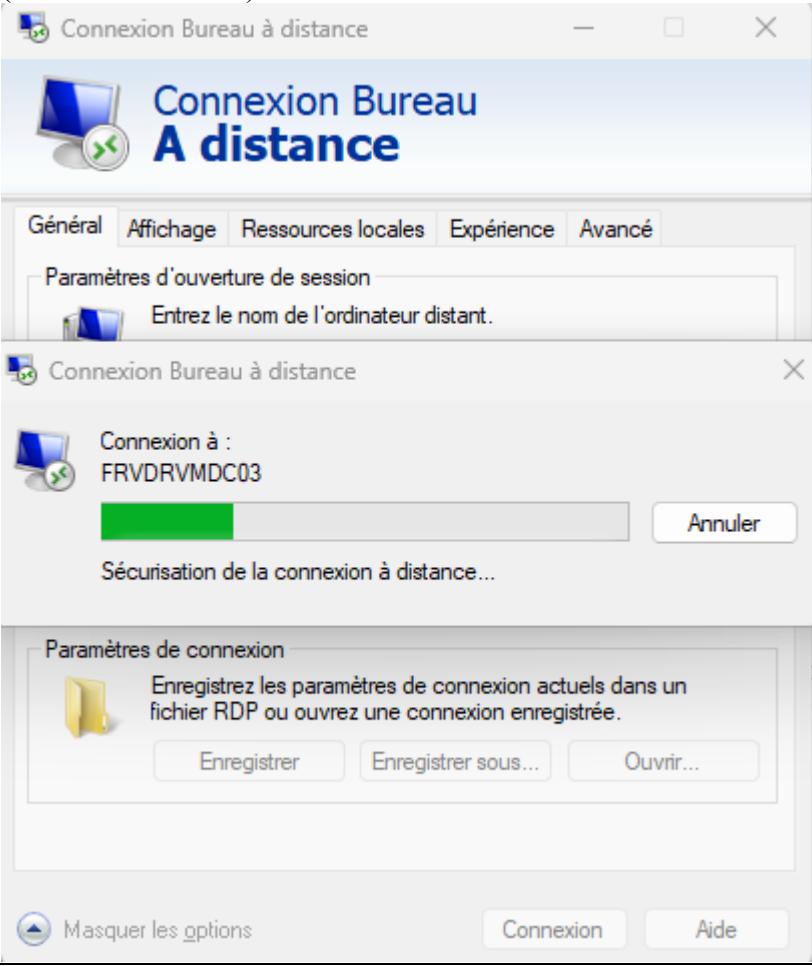
C	N/A	Description
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Workstation administrator <input checked="" type="checkbox"/> Server administrator <input type="checkbox"/> Active Directory administrator <input type="checkbox"/> Exchange administrator <input type="checkbox"/> 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.

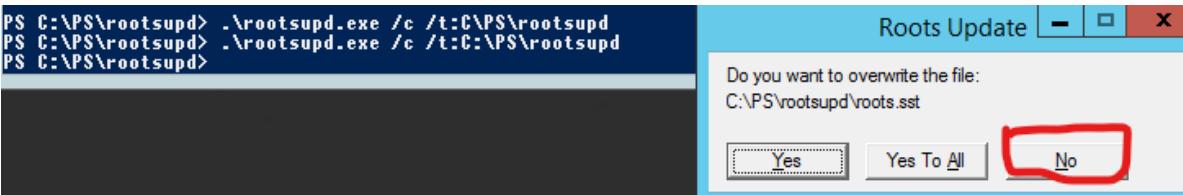
6. STANDARD OPERATING PROCEDURE

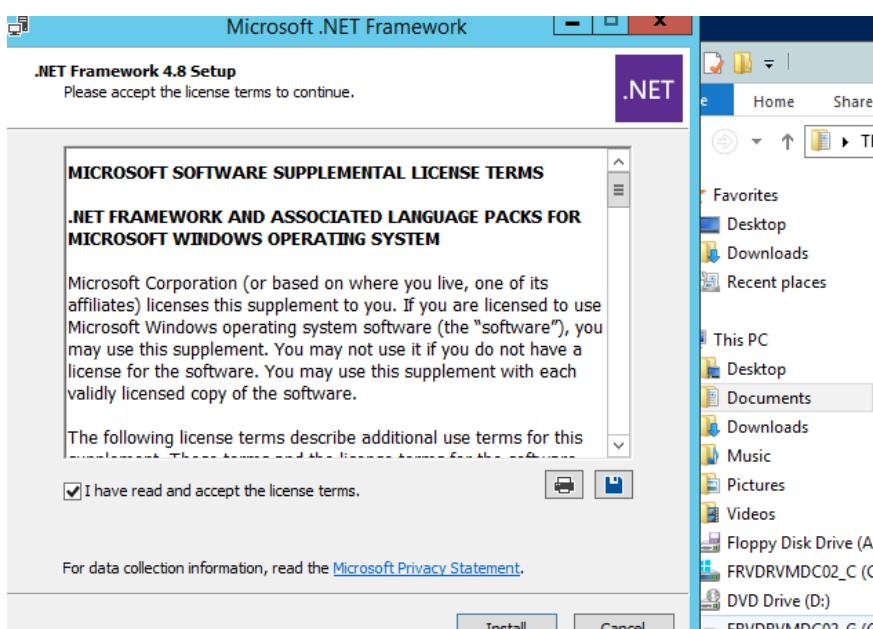
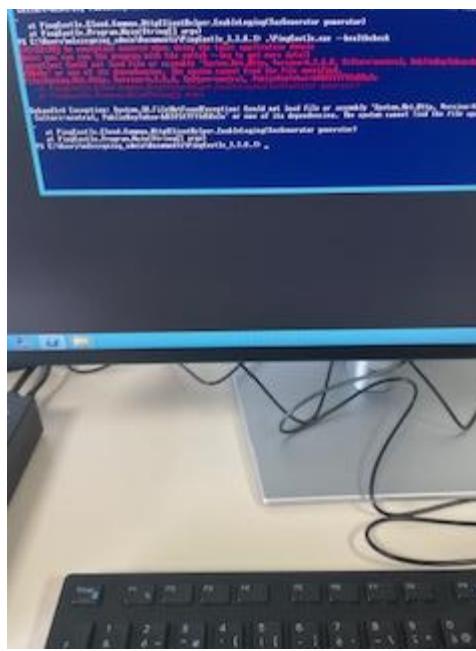
6.1 Téléchargement et Installation

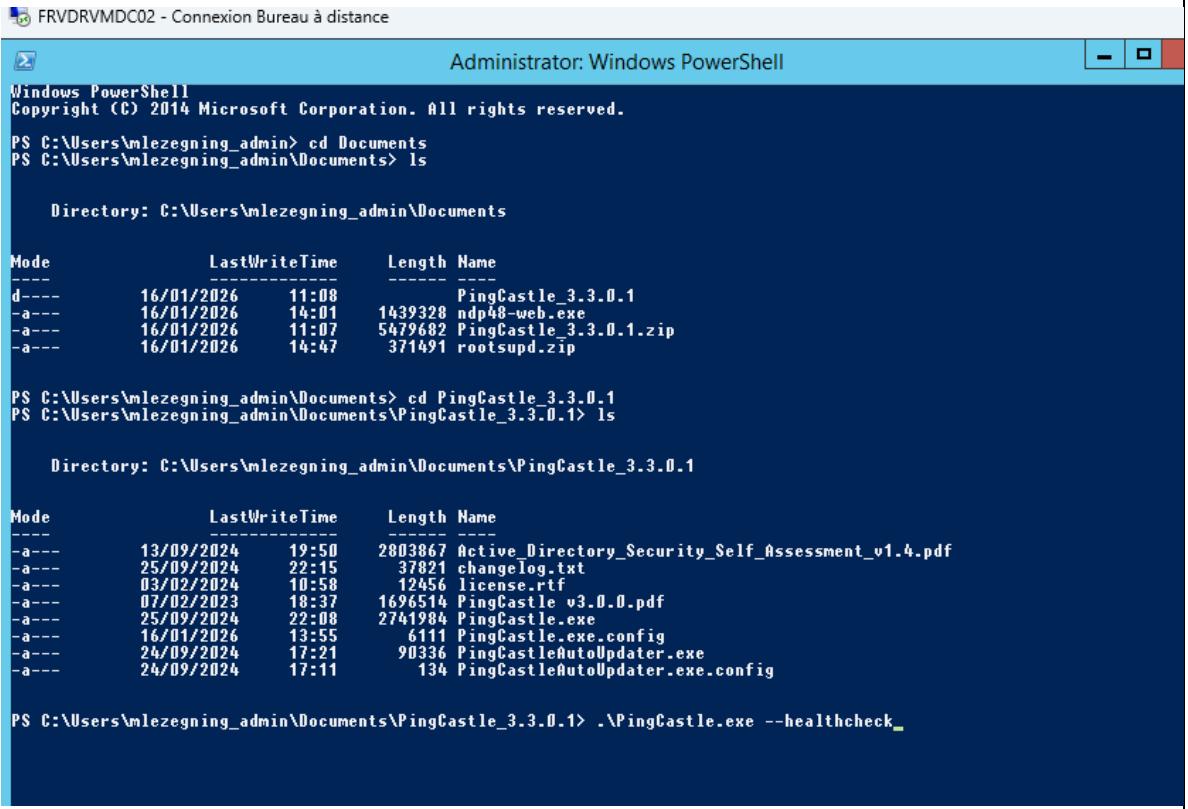
C	N/A	Item	Description
<input type="checkbox"/>	<input type="checkbox"/>	6.1.1	<p>Se connecter en RDP sur le serveur de gestion ou un contrôleur de domaine (FRVDRVMD03)</p> 
<input type="checkbox"/>	<input type="checkbox"/>	6.1.2	<ul style="list-style-type: none">Télécharger l'archive ZIP depuis le site officiel de PingCastle (https://www.pingcastle.com/download/)
<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><<certutil.exe -generateSSTFromWU roots.sst>></pre>

<input type="checkbox"/>	<input type="checkbox"/>	6.1.6	<p>Créer un Dossier C:\PS\rootsupd</p> <pre>PS C:\Users\mlezegeing_admin> 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> _</pre> <p>Enregistrer le fichier roots.sst dans le dossier créé</p> <pre>PS C:\Users\mlezegeing_admin> 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> _</pre>
<input type="checkbox"/>	<input type="checkbox"/>	6.1.7	<p>Téléchargez l'archive rootsupd.zip et extrayez le fichier rootsupd.exe.</p> <pre>PS C:\PS\rootsupd> 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 »																																				
			<pre>PS C:\PS\rootsupd> .\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	Apres l'executon , on verifie que le dossier contient l'utilitaire updroots.exe																																				
			<pre>PS C:\PS\rootsupd> ls</pre> <pre>Directory: C:\PS\rootsupd</pre> <table border="1"> <thead> <tr> <th>Mode</th> <th>LastWriteTime</th> <th>Length</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>-ar--</td> <td>04/03/2013 15:13</td> <td>132096</td> <td>ADVPACK.DLL</td> </tr> <tr> <td>-a---</td> <td>19/04/2013 18:43</td> <td>75116</td> <td>authroots.sst</td> </tr> <tr> <td>-a---</td> <td>19/04/2013 18:43</td> <td>17628</td> <td>delroots.sst</td> </tr> <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> <tr> <td>-a---</td> <td>03/04/2013 12:26</td> <td>1610</td> <td>rootsupd.inf</td> </tr> <tr> <td>-ar--</td> <td>04/03/2013 15:55</td> <td>5632</td> <td>updroots.exe</td> </tr> <tr> <td>-a---</td> <td>19/04/2013 18:43</td> <td>383419</td> <td>updroots.sst</td> </tr> </tbody> </table> <pre>PS C:\PS\rootsupd> .\updroots.exe roots.sst</pre>	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
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																																				

<input type="checkbox"/>	<input type="checkbox"/>	6.1.11	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"/>	6.1.12	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> cd Documents PS C:\Users\mlezechning_admin\Documents> 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> cd PingCastle_3.3.0.1 PS C:\Users\mlezechning_admin\Documents\PingCastle_3.3.0.1> 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> .\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> .\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> </pre>

<input type="checkbox"/>	<input type="checkbox"/>	6.1.15	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"/>	6.1.16	Ouvre le fichier HTML et la on'a notre analyse								
			<p>frvdr.com - Analyse de bilan de santé 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. ? 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>Indicateurs Active Directory</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>Indicateurs</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>Comparer avec les statistiques Avis de confidentialité</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

Title MO IT xxxx_LAPS	Page 1 / 25
--------------------------	----------------

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

1. IDENTIFICATION UNIQUE / SERVER ID	2
2. SUJET/SUBJECT.....	3
3. SCOPE.....	3
4. DESCRIPTION	3
5. PRES-REQUIS / REQUIREMENTS.....	3
5.1 Software	3
5.2 Hardware	3
5.3 Required privileges	3
5.4 Restart requirements.....	3
6. STANDARD OPERATING PROCEDURE	4
6.1 Téléchargement et Installation LAPS	Erreur ! Signet non défini.
7. SIGNATURES	24
8. CHANGE LOG - JOURNAL DES REVISIONS	24
9. CHANGE LOG – ANNULATION PROCEDURE	24

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

Name: FRVDRVMDC02

Installer Name: Megane
Lezegning

Date:

Day / Month (full) / Year (4 digit)

_____ 30 _____ / _____ 01 _____ / _____ 2002 _____

2. SUJET/SUBJECT

Installation de LAPS Sur le serveur frvdrvmdc02– Guide de l'Administrateur

3. SCOPE

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

4. DESCRIPTION

Microsoft LAPS est utilisé pour gérer les mots de passe des administrateurs locaux sur vos appareils joints au domaine Active Directory.

LAPS (Local Administrator Password Solution), crée un mot de passe unique, fort et aléatoire pour chaque poste de travail, serveur et stocke le mot de passe dans Active Directory.

5. PRES-REQUIS / REQUIREMENTS

5.1 Software

C	N/A	Description
<input type="checkbox"/>	<input type="checkbox"/>	LAPS.X64.msi
<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	

5.2 Hardware

C	N/A	Description
<input type="checkbox"/>	<input type="checkbox"/>	Serveur AD & CLIENT

5.3 Required privileges

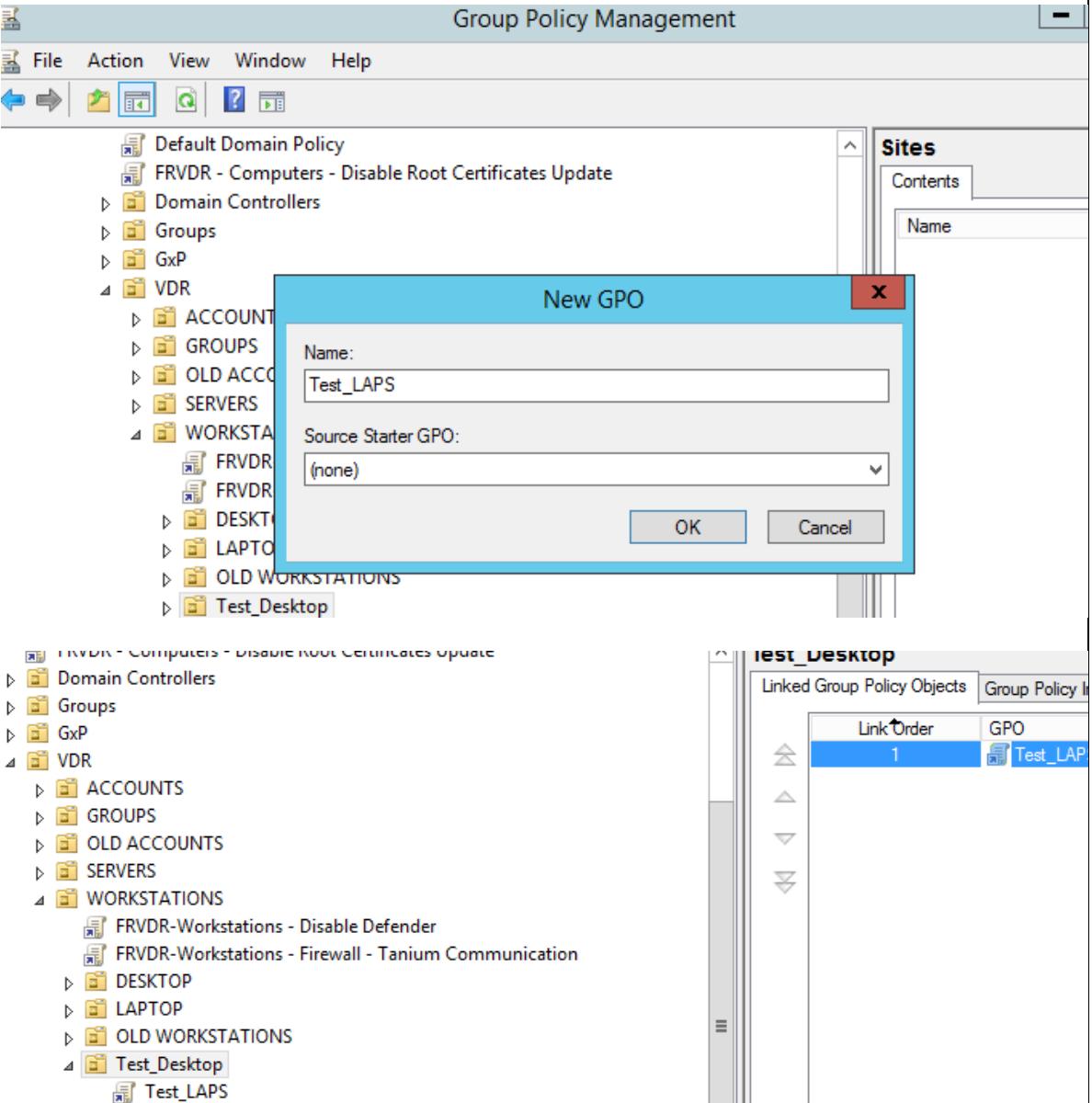
C	N/A	Description
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Workstation administrator <input checked="" type="checkbox"/> Server administrator <input type="checkbox"/> Active Directory administrator <input type="checkbox"/> Exchange administrator <input type="checkbox"/>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

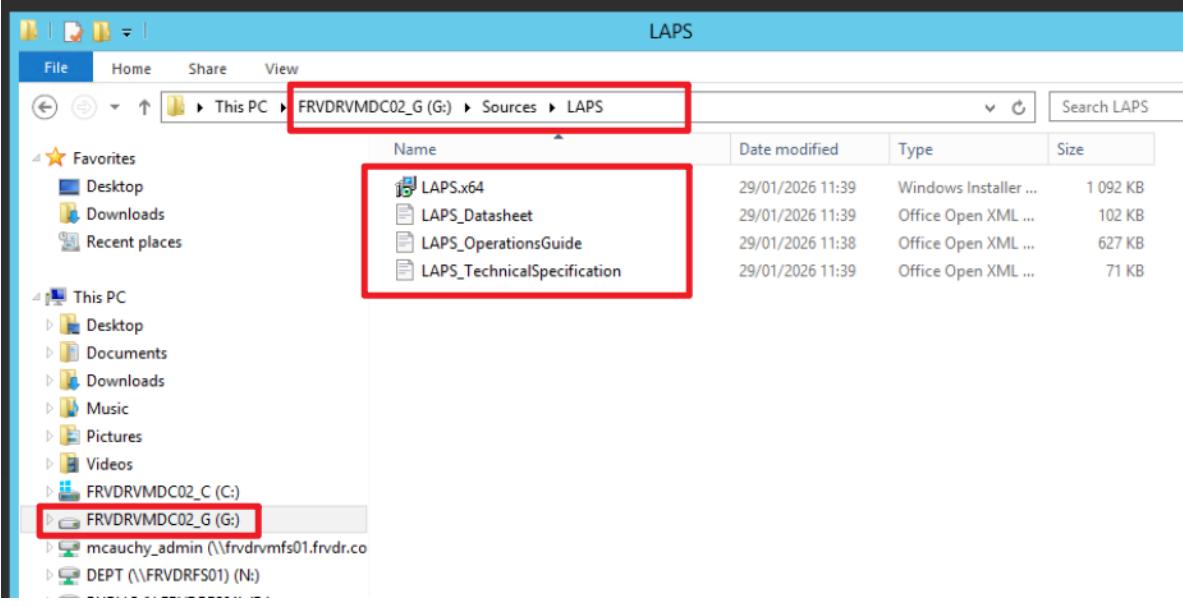
5.4 Restart requirements

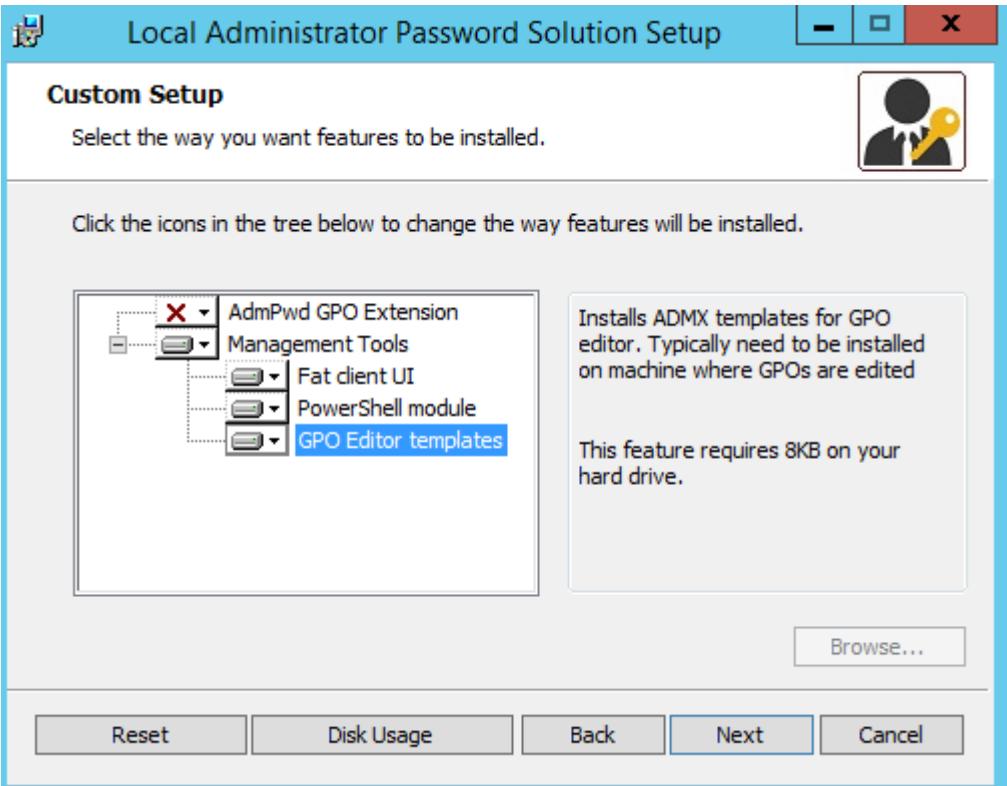
There is no restart requirement during restore operations.

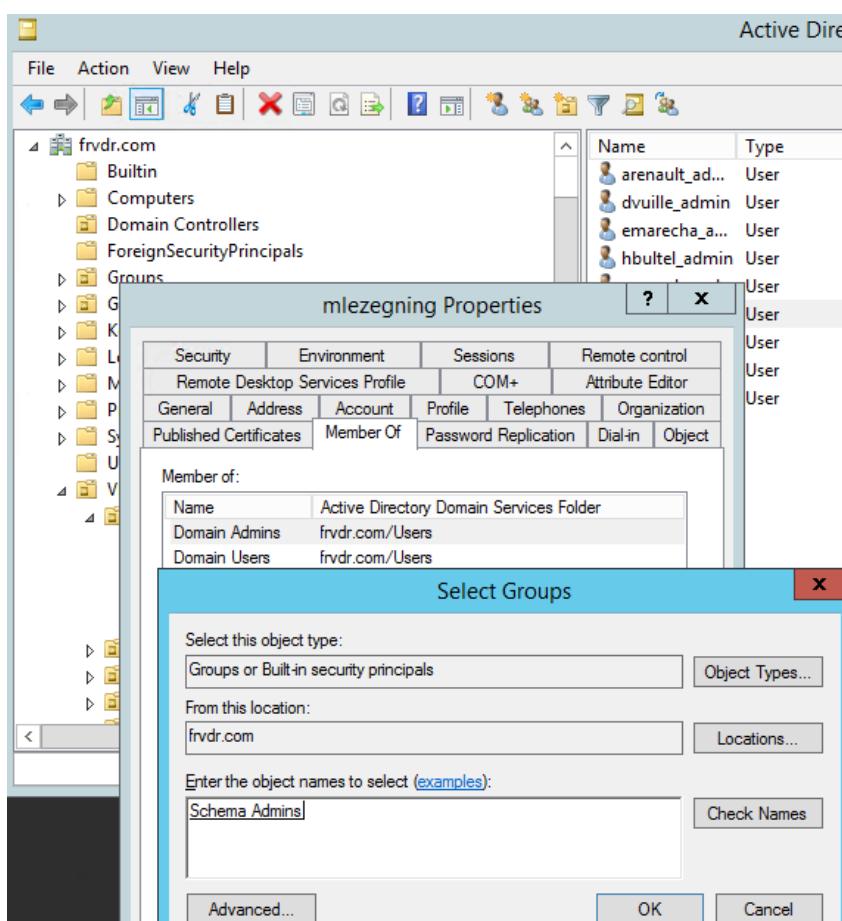
6. STANDARD OPERATING PROCEDURE

6.1 Téléchargement et Installation

C	N/A	Item	Description
<input type="checkbox"/>	<input type="checkbox"/>	6.1.1	<p>Création de l'OU Desktop et GPO Test_LAPS</p>  <p>The screenshot shows the Windows Group Policy Management console. A 'New GPO' dialog box is in the foreground, prompting for a name ('Test_LAPS') and a source starter GPO ('(none)'). In the background, the 'test_desktop' container is selected in the navigation pane under 'FRVDR - Computers - Disable Root Certificates Update'. The right-hand pane displays the 'Linked Group Policy Objects' for this container, showing one entry: 'Link Order 1 GPO Test_LAPS'.</p>

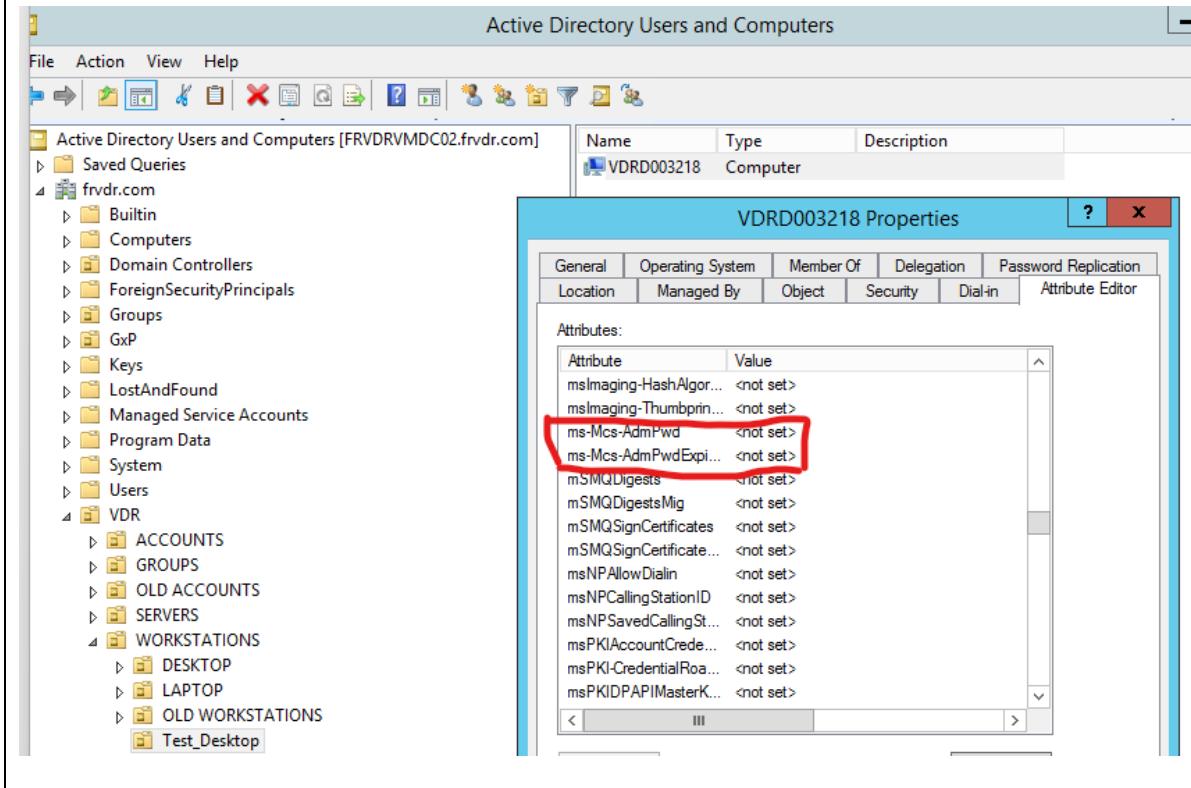
C	N/A	Item	Description																				
<input type="checkbox"/>	<input type="checkbox"/>	6.1.2	<ul style="list-style-type: none">• Télécharger LAPS.X64.msi (https://www.microsoft.com/en-us/download/details.aspx?id=46899 Conversation Microsoft Teams)  <table border="1"><thead><tr><th>Name</th><th>Date modified</th><th>Type</th><th>Size</th></tr></thead><tbody><tr><td>LAPS.x64</td><td>29/01/2026 11:39</td><td>Windows Installer ...</td><td>1 092 KB</td></tr><tr><td>LAPS_Datasheet</td><td>29/01/2026 11:39</td><td>Office Open XML ...</td><td>102 KB</td></tr><tr><td>LAPS_OperationsGuide</td><td>29/01/2026 11:38</td><td>Office Open XML ...</td><td>627 KB</td></tr><tr><td>LAPS_TechnicalSpecification</td><td>29/01/2026 11:39</td><td>Office Open XML ...</td><td>71 KB</td></tr></tbody></table>	Name	Date modified	Type	Size	LAPS.x64	29/01/2026 11:39	Windows Installer ...	1 092 KB	LAPS_Datasheet	29/01/2026 11:39	Office Open XML ...	102 KB	LAPS_OperationsGuide	29/01/2026 11:38	Office Open XML ...	627 KB	LAPS_TechnicalSpecification	29/01/2026 11:39	Office Open XML ...	71 KB
Name	Date modified	Type	Size																				
LAPS.x64	29/01/2026 11:39	Windows Installer ...	1 092 KB																				
LAPS_Datasheet	29/01/2026 11:39	Office Open XML ...	102 KB																				
LAPS_OperationsGuide	29/01/2026 11:38	Office Open XML ...	627 KB																				
LAPS_TechnicalSpecification	29/01/2026 11:39	Office Open XML ...	71 KB																				

		6.1.3	<ul style="list-style-type: none">Ensuite, vous devez installer tous les outils d'administration (comme sur l'image ci-dessous) et vous pouvez désélectionner l'entrée "AdmPwd GPO Extension" car elle n'est pas utile sur le contrôle de domaine  
--	--	-------	--

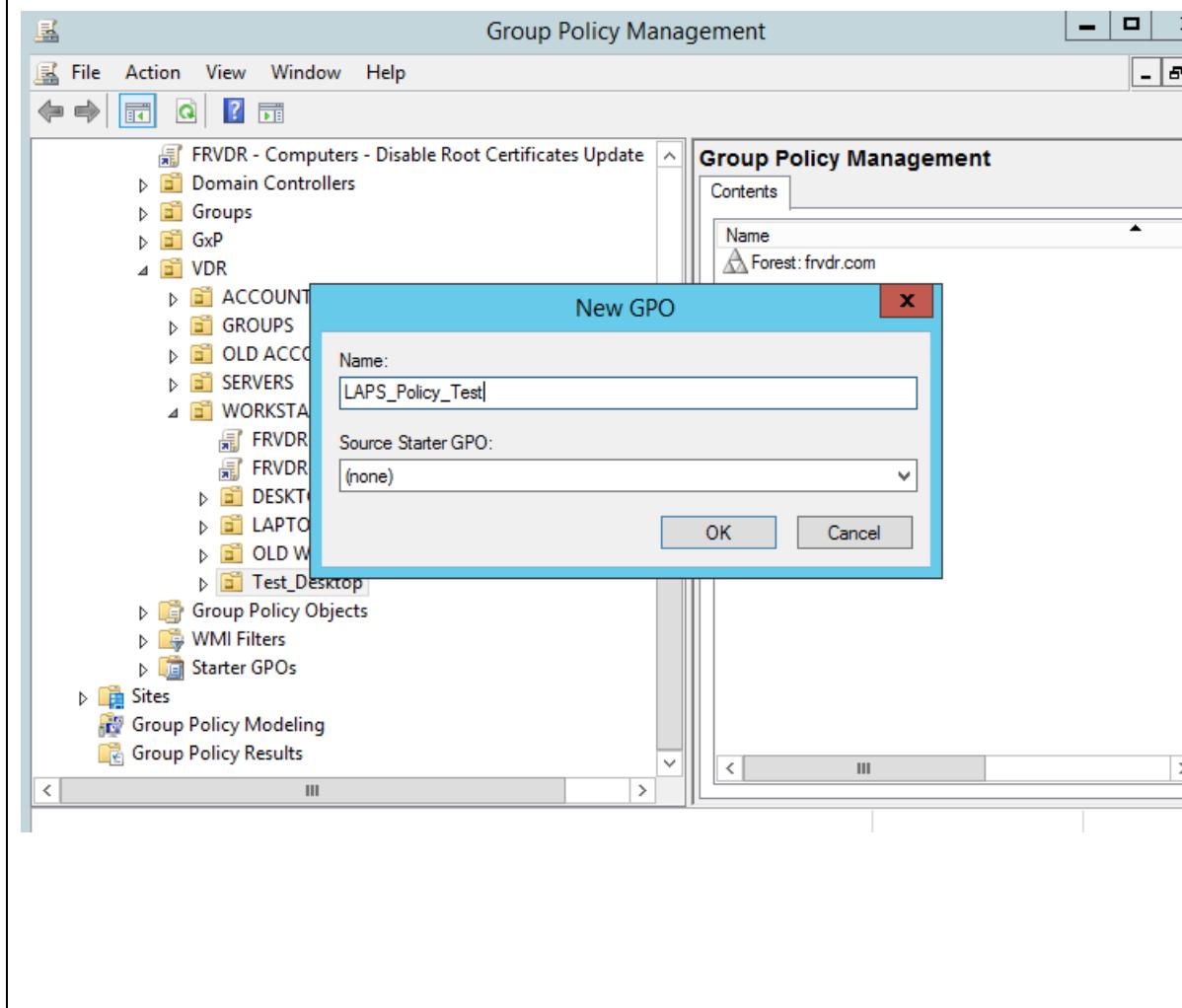
C	N/A	Item	Description
<input type="checkbox"/>	<input type="checkbox"/>	6.1.4	<p>Préparation de l'AD pour LAPS</p> <p>Mettre à jour le schéma Active Directory</p> <pre>PS C:\Users\mlezege..._admin> Update-AdmPwdADSschema Update-AdmPwdADSschema : The user has insufficient access rights. At line:1 char:1 + Update-AdmPwdADSschema + ~~~~~~ + CategoryInfo : NotSpecified: (:) [Update-AdmPwdADSschema], DirectoryOperationException + FullyQualifiedErrorId : System.DirectoryServices.Protocols.DirectoryOperationException,AdmPwd.PS.UpdateAdSchem...</pre> <p>PS C:\Users\mlezege..._admin> _</p> <ul style="list-style-type: none"> Vu que je ne suis pas membre du groupe Schema Admin je n'ai pas pu exécuter la commande j'ai me rajouter dans le groupe 

C	N/A	Item	Description
<input type="checkbox"/>	<input type="checkbox"/>	6.1.5	<ul style="list-style-type: none">Exécutez la commande suivante pour importer le module PowerShell de LAPS <p>Ensuite, exécuter la commande ci-dessous pour mettre à jour le schéma AD</p> <pre>PS C:\Users\mlezeegning_admin> Import-Module AdmPwd.ps PS C:\Users\mlezeegning_admin> Update-AdmPwdADSchema Operation DistinguishedName Status ----- AddSchemaAttribute cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration,DC=f... Success AddSchemaAttribute cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=frvdr,DC=com Success ModifySchemaClass cn=computer,CN=Schema,CN=Configuration,DC=frvdr,DC=com Success PS C:\Users\mlezeegning_admin> _</pre> <p># Autoriser les postes de l'OU à écrire leur mot de passe</p> <pre>PS C:\Users\mlezeegning_admin> Set-AdmPwdComputerSelfPermission -OrgUnit "OU=Test/Desktop,OU=WORKSTATIONS,OU=VDR,DC=frvdr,DC=com" Name DistinguishedName Status ----- Test/Desktop OU=Test/Desktop,OU=WORKSTATIONS,OU=VDR,DC=frvdr,DC=com Delegated PS C:\Users\mlezeegning_admin> _</pre>

- Si l'on ouvre la console "Utilisateurs et ordinateurs Active Directory" et que l'on regarde les propriétés d'un ordinateur membre du domaine, on peut voir la présence des deux nouveaux attributs. Voici un exemple



Créer et lier GPO Test/Desktop



Configurer les paramètres LAPS

Une fois la GPO créée, vous devez la paramétrer pour qu'elle s'applique à vos machines

1. Faites un **clic droit** sur votre nouvelle GPO LAPS_Policy_Test et choisissez **Edit**.

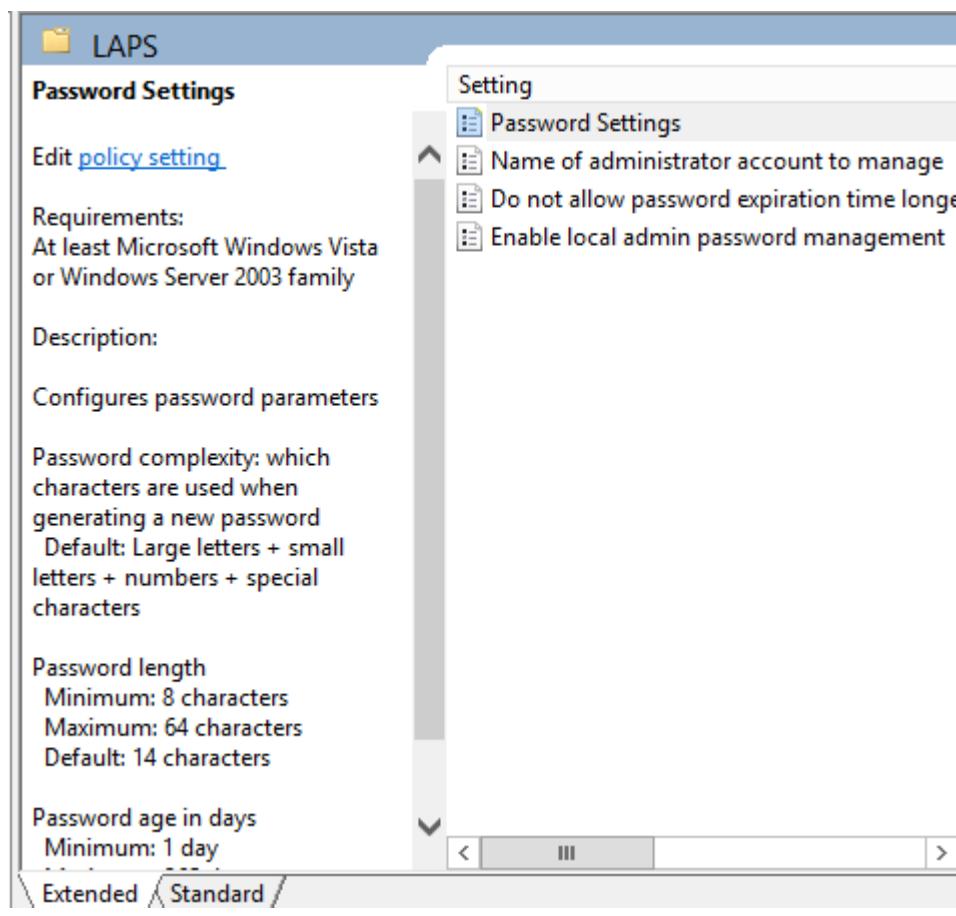
2. Allez dans le chemin suivant :

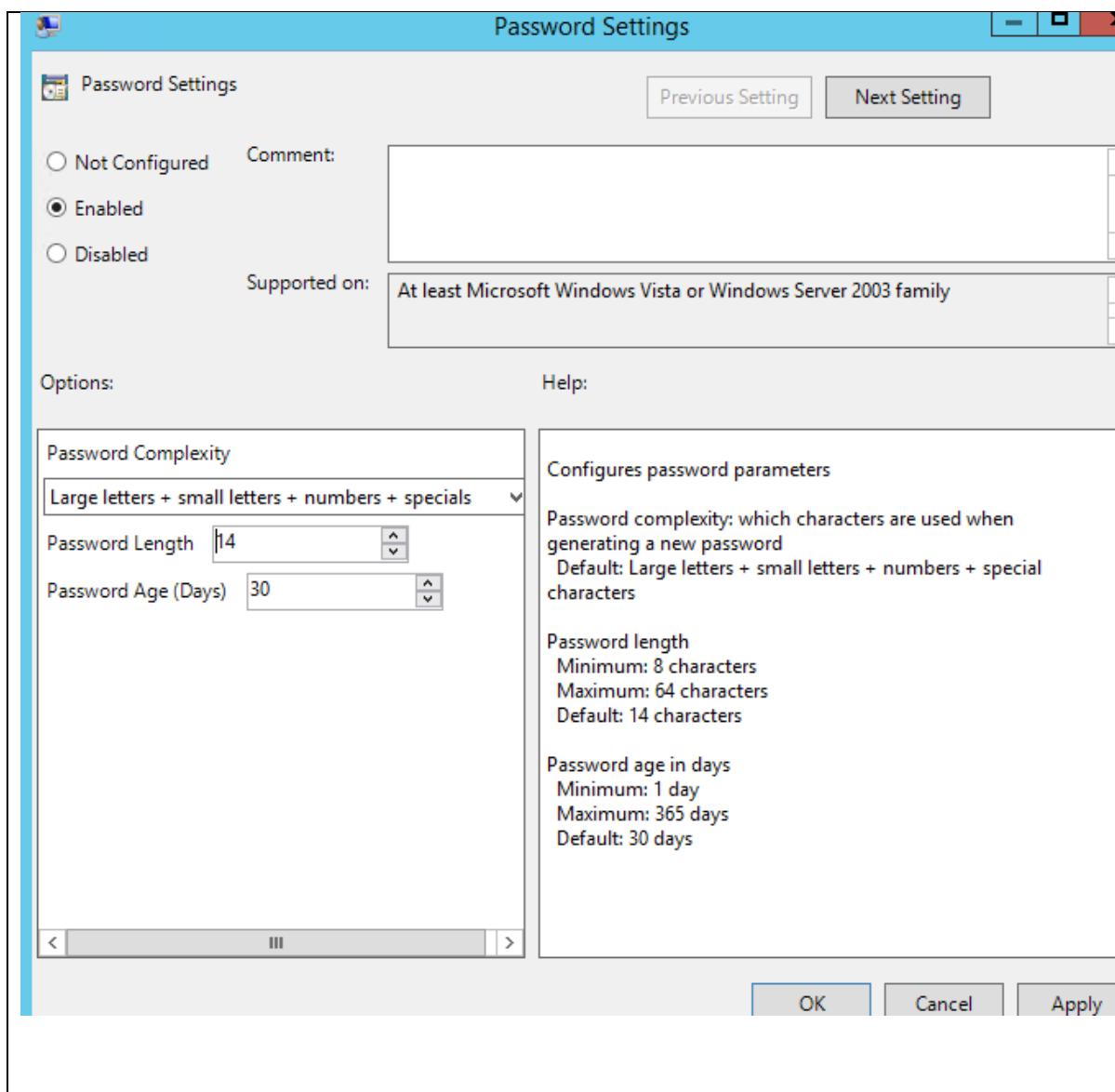
Computer Configuration > Policies > Administrative Templates > LAPS.

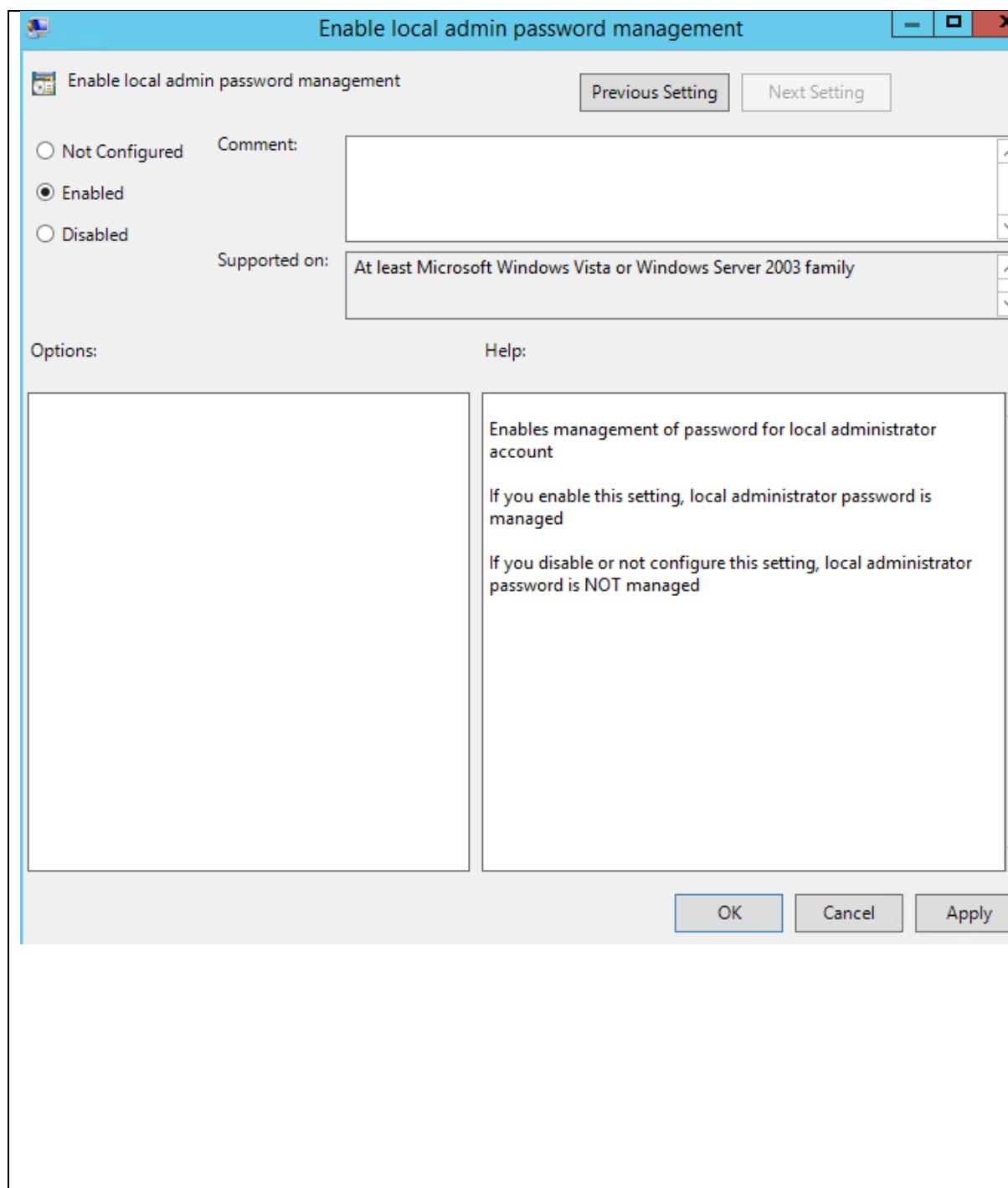
3. Configurez au minimum ces deux paramètres :

Password Settings : Définissez la complexité et la durée de validité (ex : 14 jours).

Enable local admin password management : Mettez ce paramètre sur **Enabled**.







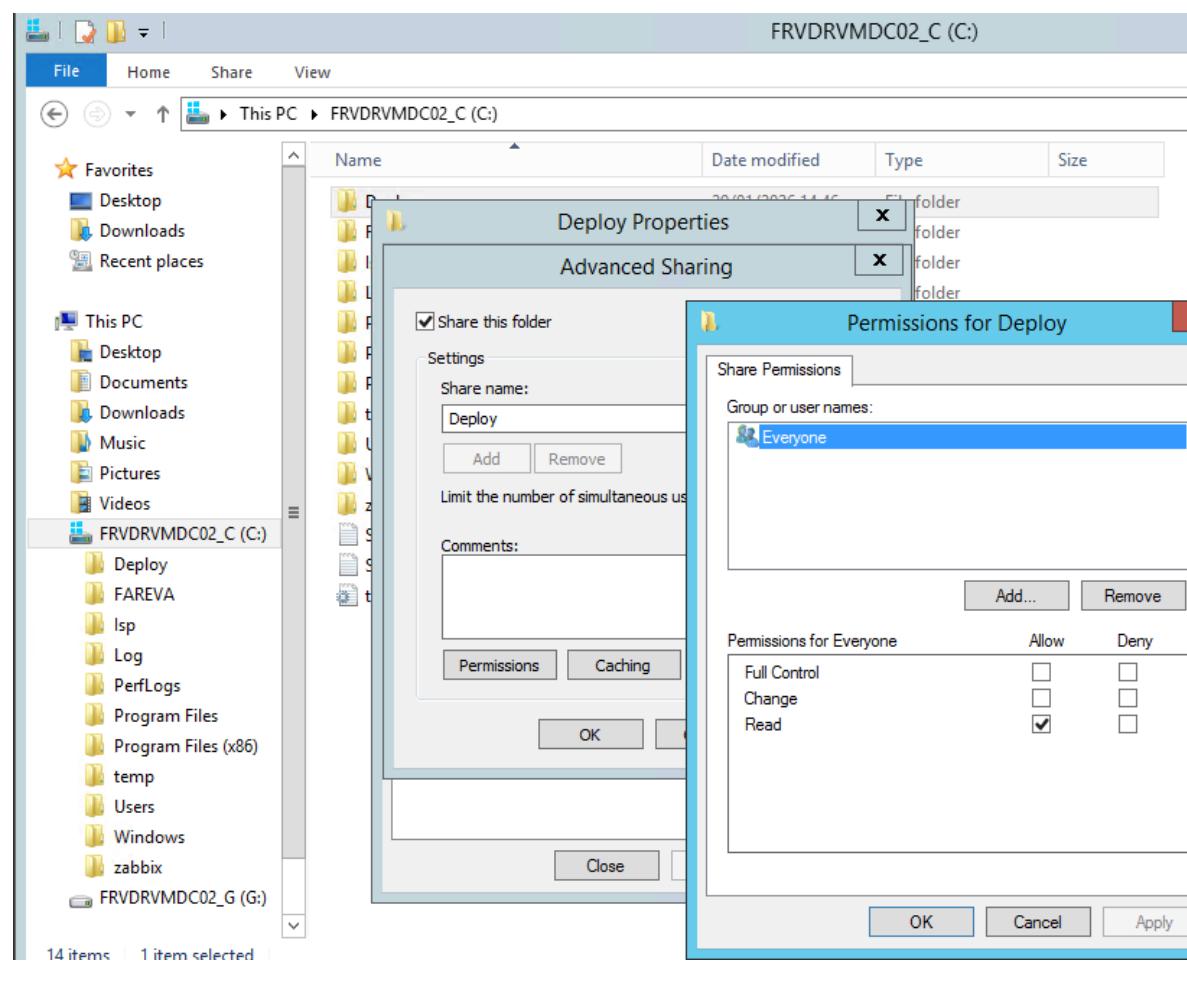
Déploiement sur le Client

Créer le dossier et placer le fichier

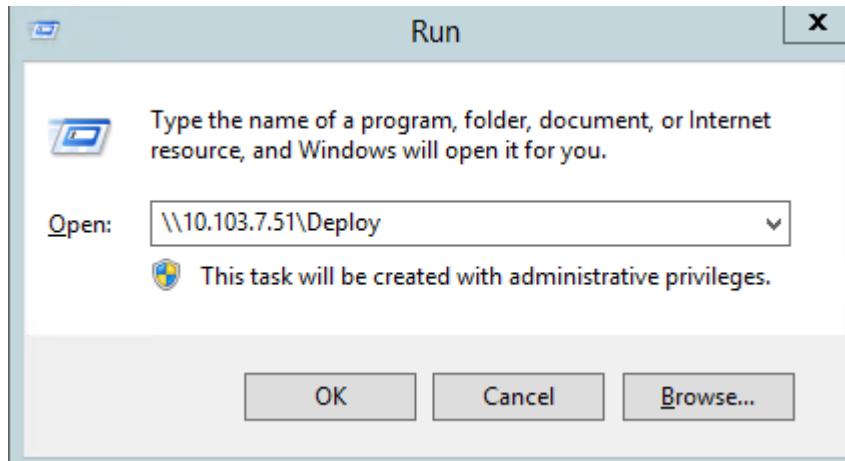
- Ouvrez l'explorateur de fichiers sur votre serveur (FRVDRMDC02).
- Créez un dossier à la racine d'un disque (par exemple C:\Deploy).
- Copiez le fichier **LAPS.x64.msi** à l'intérieur de ce dossier.

Partager le dossier (Droits de Partage)

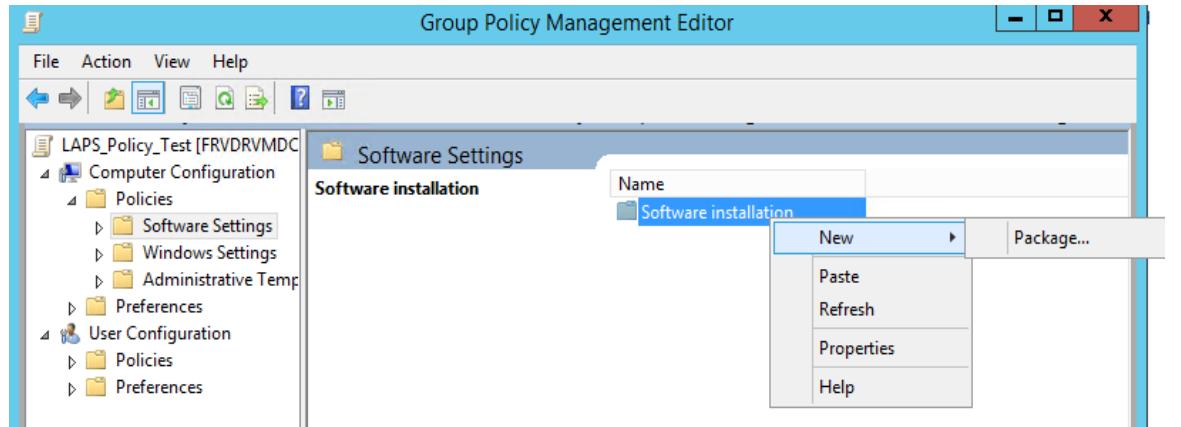
- Faites un **clic droit** sur le dossier C:\Deploy > **Properties** (Propriétés).
- Allez dans l'onglet **Sharing** (Partage) et cliquez sur **Advanced Sharing...** (Partage avancé).
- Cochez **Share this folder**.
- Cliquez sur le bouton **Permissions**.
- Cliquez sur **Add...**, tapez Domain Computers (Ordinateurs du domaine) et validez.
- Vérifiez que la case **Read** (Lecture) est cochée pour ce groupe->Validez



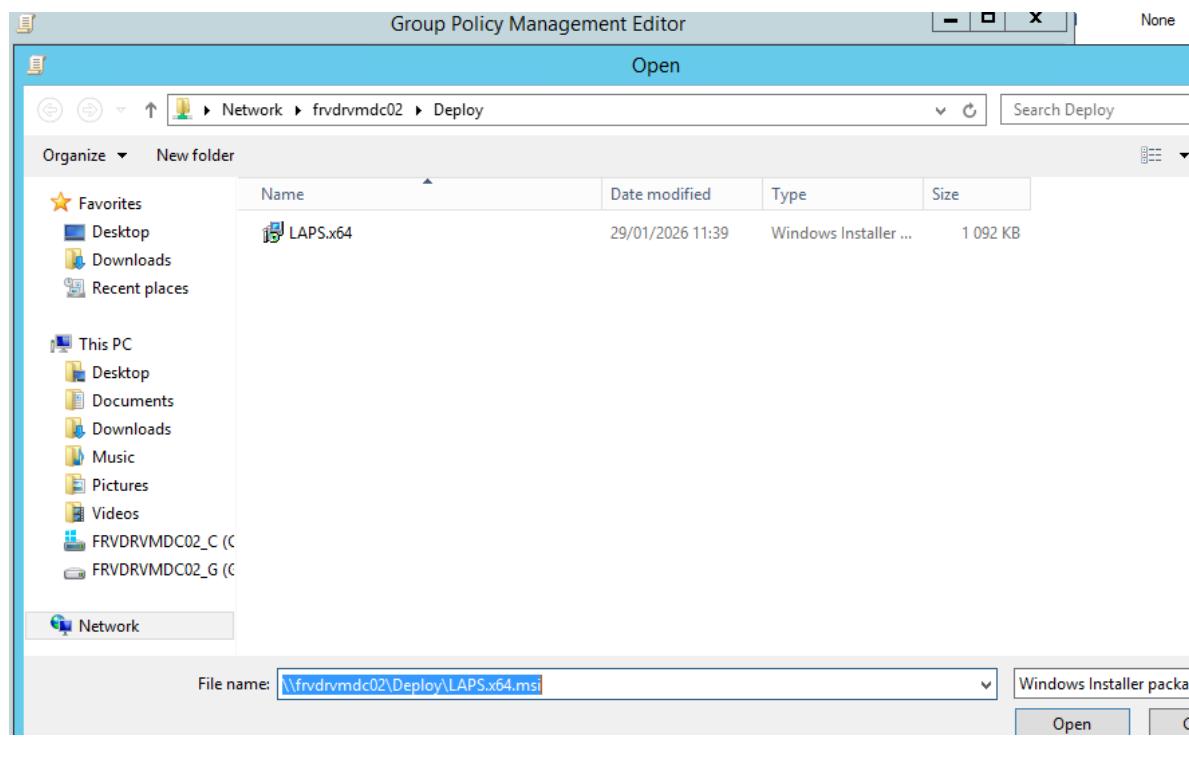
- Sur le serveur on fait W+R et on entrer le chemin soit avec l'IP soit avec le nom de domaine et la fois apparaitre le fichier LAPS.msi

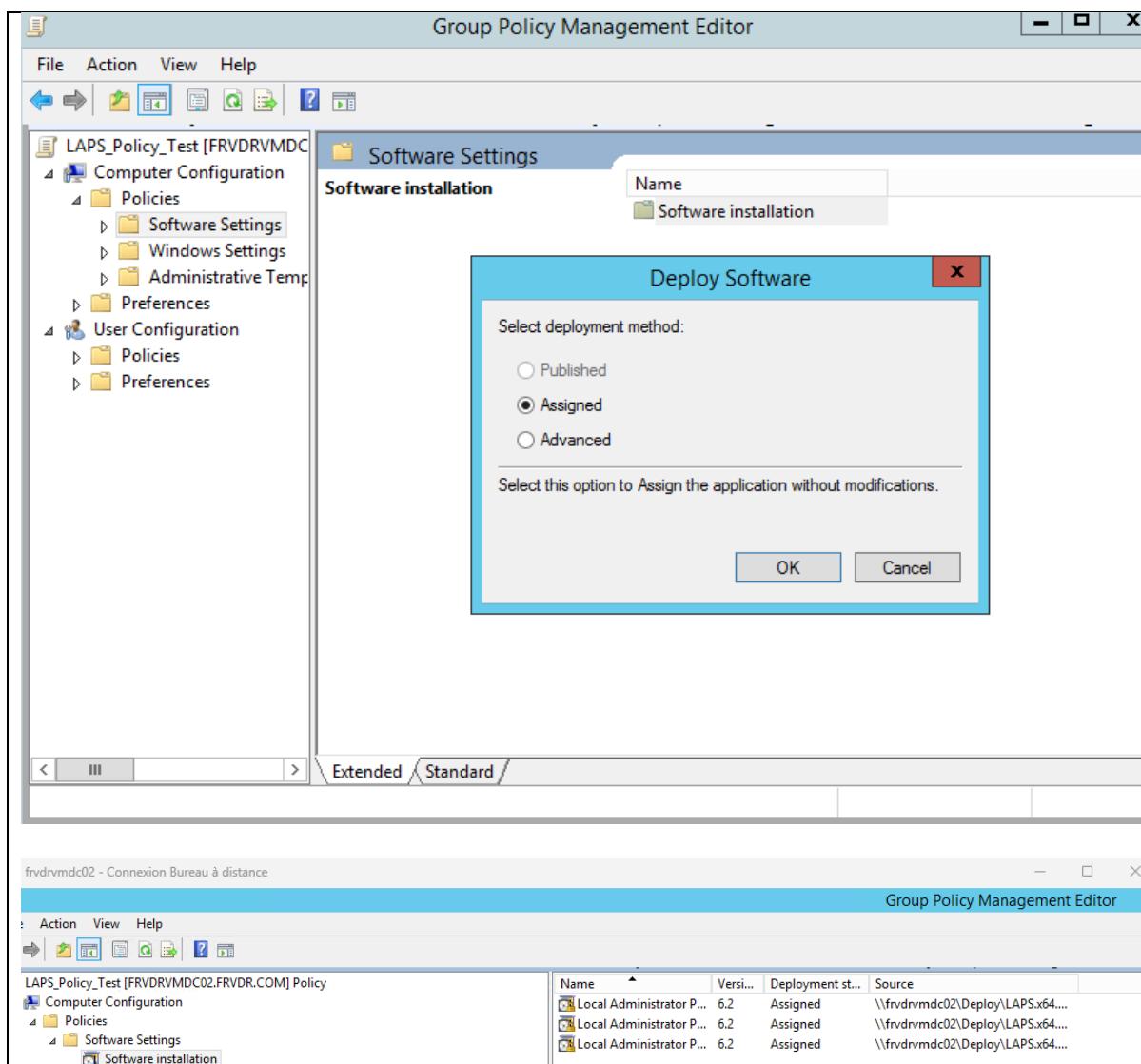


- Ajouter le package d'installation (MSI)

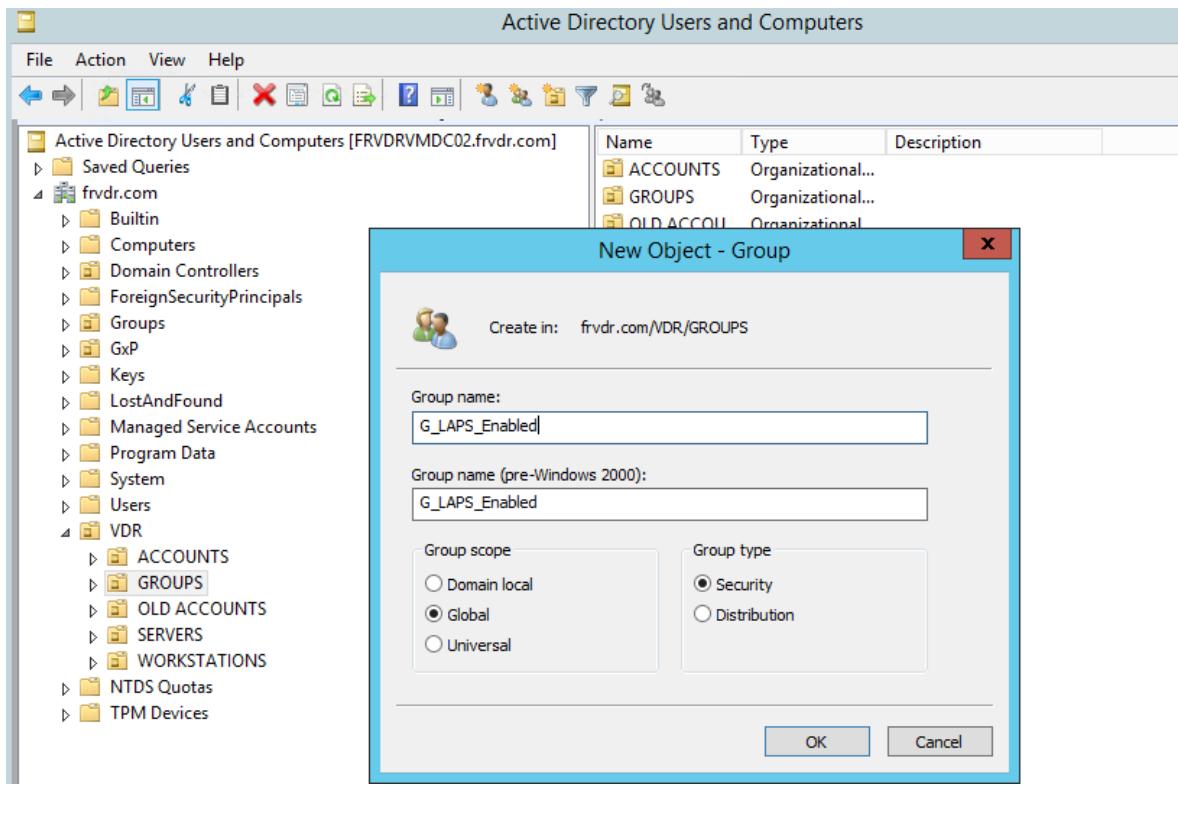


Très important : Dans la barre d'adresse de la fenêtre qui s'ouvre, collez votre chemin réseau : \\frvdrvmdc02\Deploy\LAPS.X64.msi

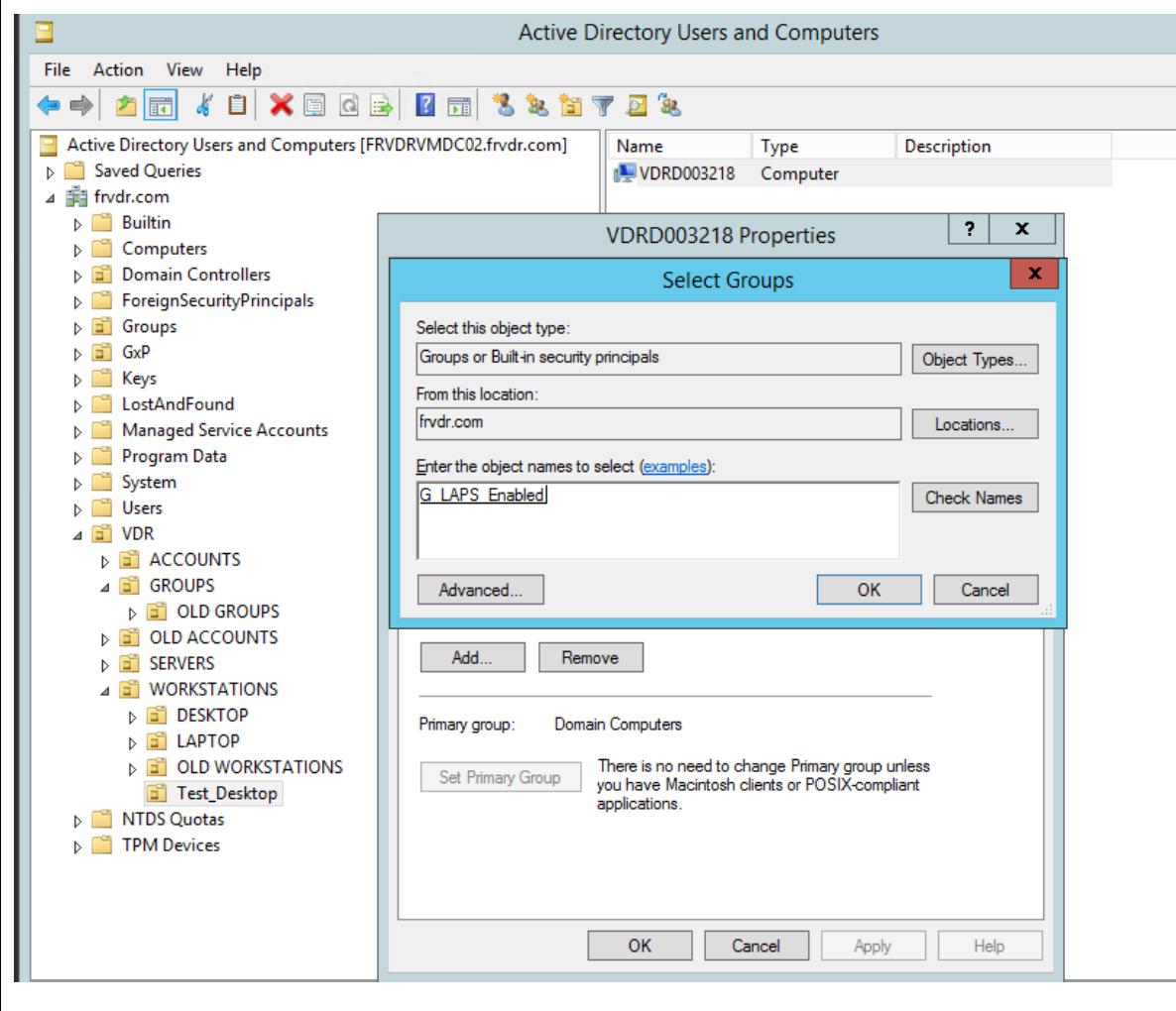




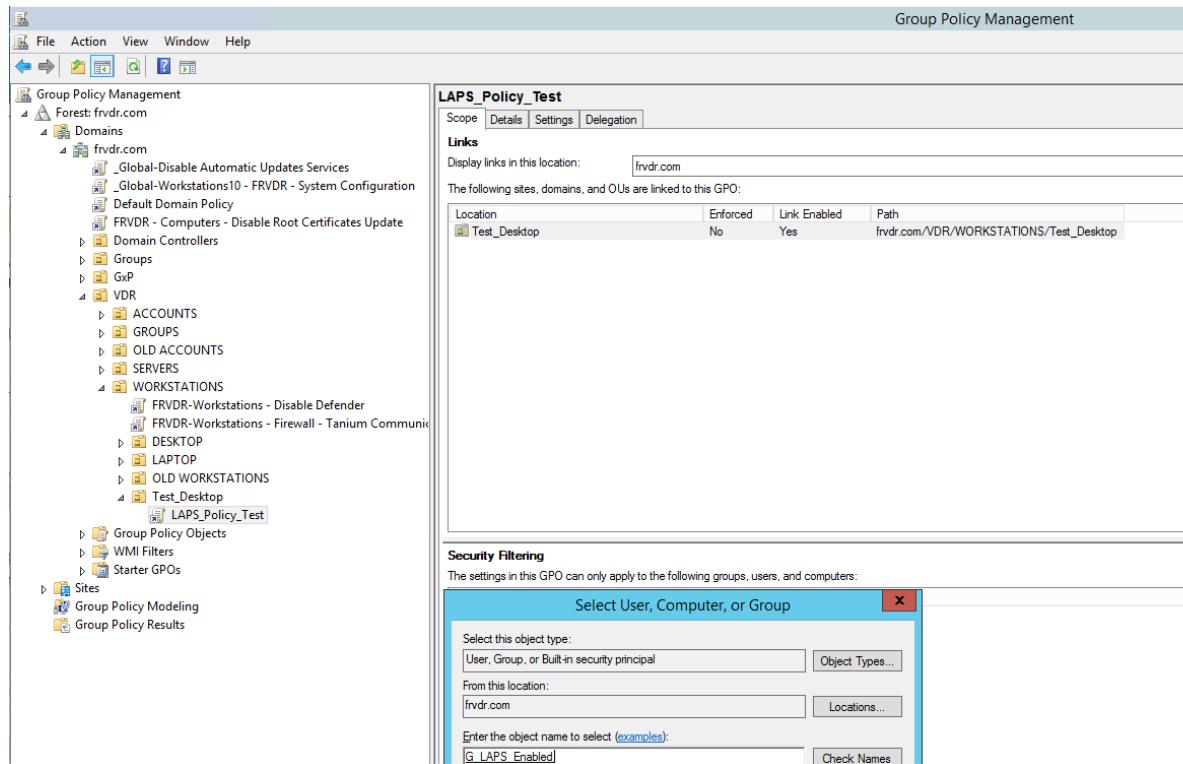
- ❖ Crée un groupe de sécurité : pour Appliquer LAPS par rapport à un groupe de sécurité que si le pc est dans le groupe LAPS qu'il soit déployer et que s'il n'est pas dans le groupe non



- ❖ Ajoute le PC test (ex : Test/Desktop) comme membre de ce groupe.



- ❖ Clique sur la GPO qu'on a créée et chercher Security Filtering et on ajoute le Groupe qu'on a créer
- ❖ Par défaut, il y a "Authenticated Users". Sélectionne et cliquez sur Remove, sinon la GPO s'appliquera à tous les PC de l'OU WORKSTATION



- ❖ Si on retire "Authenticated Users", on doit faire ceci pour que la GPO puisse toujours être lue par les PC

The screenshot shows the Active Directory Group Policy Management console. On the left, the navigation pane displays the forest: rvar.com, under Domains, with frvdr.com selected. The 'WORKSTATIONS' container is expanded, showing subfolders like DESKTOP, LAPTOP, and OLD WORKSTATIONS, along with specific GPOs such as FRVDR-Workstations - Disable Defender and FRVDR-Workstations - Firewall - Tamium Communication. On the right, a 'Select User, Computer, or Group' dialog box is open over a GPO configuration window. The dialog box allows selecting objects from the 'fvdr.com' location, with 'Domain Computers' entered in the search field. The GPO configuration window shows a table of users and groups with their permissions.

Name	Allowed Permissions	Inherited
Domain A...	Edit settings, delete, modif...	No
Enterprise...	Edit settings, delete, modif...	No
ENTERP...	Read	No
G_LAPS_...	Read (from Security Filtering)	No
SYSTEM	Edit settings, delete, modif...	No

- ❖ Gérer le déploiement sans effort

Pour ne pas ajouter les PC un par un manuellement, voici la méthode rapide dans **Active Directory Users and Computers**

- Allez dans l'OU **WORKSTATIONS** (ou ses sous-dossiers DESKTOP, LAPTOP).
- Maintient la touche **Ctrl** et on clique sur tous les ordinateurs qu'on veut activer.
- Fait un **clic droit** sur l'un des PC sélectionnés > **Add to a group**
- Tapez **G_LAPS_Enabled** et validez.

Forcer l'installation sur le PC de test

Comme c'est une installation de logiciel par GPO "Ordinateur", elle ne s'exécutera qu'au démarrage du PC.

- Allez sur le PC client qui se trouve dans l'OU Test/Desktop.
- Ouvrez une invite de commande (CMD) en tant qu'administrateur.
- Tapez : gpupdate /force.
- Si Windows vous demande de redémarrer pour appliquer les paramètres logiciels, tapez-O(OUI) et validez.

Vérifier l'installation sur le client

Après le redémarrage du PC de test, vérifiez que l'agent est bien là :

- Allez dans C:\Program Files\LAPS. Vous devriez y voir un fichier nommé Admpwd.dll.
- Si ce dossier existe, l'agent est prêt à générer un mot de passe.

Le test final dans Active Directory

The screenshot shows the 'Active Directory Users and Computers' window. On the left, the navigation pane lists various Active Directory containers: Saved Queries, frvdr.com (selected), Builtin, Computers, Domain Controllers, ForeignSecurityPrincipals, Groups, GxP, Keys, LostAndFound, Managed Service Accounts, Program Data, System, Users, VDR (selected), ACCOUNTS, GROUPS, OLD ACCOUNTS, SERVERS, WORKSTATIONS (selected), DESKTOP, LAPTOP, OLD WORKSTATIONS, and Test/Desktop (selected). In the center, a table shows one item: Name (VDRD003218), Type (Computer). On the right, the 'VDRD003218 Properties' dialog is open, specifically the 'General' tab. It displays attributes like msExchLabeledURI, msIIS-FTPDir, msIIS-FTPRoot, msImaging-HashAlg..., msImaging-Thumbnin..., ms-Mcs-AdmPwd (set to I2jogLlx), and ms-Mcs-AdmPwdExpire (set to 134167637664101722). The 'Value' column for ms-Mcs-AdmPwd and ms-Mcs-AdmPwdExpire is highlighted with a red box.

- Pour la voir en ligne de commande

```
PS C:\Users\mlezegeing_admin> Get-AdmPwdPassword -ComputerName "VDRD003218"
ComputerName      DistinguishedName          Password          ExpirationTimestamp
-----           -----CN=VDRD003218,OU=Test_Desktop,OU=WORKSTATION... I2jogLlx          28/02/2026 15:49:26
```

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: 30/01/2026
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	

7. CHANGE LOG - JOURNAL DES REVISIONS

Version	Auteur	Description des modifications	Raison / Commentaire
1	Megane Leezgning	Création initiale du MO IT	Installation de LAPS

8. CHANGE LOG – ANNULATION PROCEDURE

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

