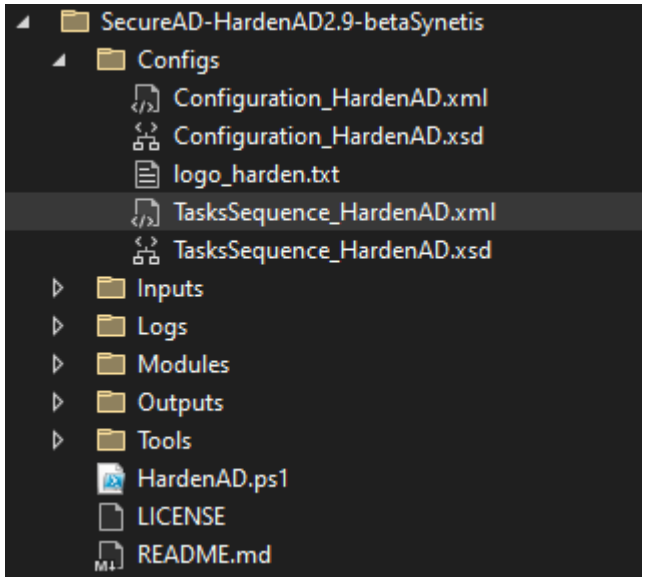
Harden – Déploiement et personnalisation du modèle

SOMMAIRE

- Introduction
- Personnalisation des paramètres
- Les séquences de déploiement
- Les autres fichiers
- Exécution Harden AD

Introduction

Le fichier xml



- Le fichier xml permet de venir personnaliser le modèle Harden AD, avec les informations utiles à son futur déploiement
- Il est composé de 2 gros blocs qui divisent le côté paramètres et le côté séquence de déploiement
- Chacun de ces blocs se compose de modules en lien avec les séquences

Le bloc paramètre

```
<Settings>
  <!-- ########################################################################################################################################## -->
  <!-- Revision: 2022/07/08 - contact@hardenad.net                                                                                              -->
  <!-- ########################################################################################################################################## -->
  <OrganizationalUnits>...</OrganizationalUnits>

  <!-- ########################################################################################################################################## -->
  <!-- NEW SECTION (2022/07)                                                                                                                    -->
  <!-- This section push delegation ACL to designated OU                                                                                        -->
  <!-- ########################################################################################################################################## -->
  <DelegationACEs>...</DelegationACEs>

  <!-- ########################################################################################################################################## -->
  <!-- NEW SECTION (2022/07)                                                                                                                    -->
  <!-- This section create a reference table to be used through the scripts                                                                     -->
  <!-- For now, only the GPO parts use this dynamic logic to fillup the migration and the preference table.                                    -->
  <!--    > WellKnownID..: used to replace a dynamic pattern in a name (group, user, path, gpo, ...)                                           -->
  <!--    > Keyword......: used to shorten a word in a name (group, user, path, gpo, ...), helping in avoiding too long name in AD            -->
  <!-- ########################################################################################################################################## -->
  <Translation>...</Translation>

  <GroupPolicies>...</GroupPolicies>

  <Accounts>...</Accounts>

  <Groups>...</Groups>

  <DefaultMembers>...</DefaultMembers>

  <TaskSchedules BaseDir="C:\_ADM\TasksSc">...</TaskSchedules>

  <LocalAdminPasswordSolution>...</LocalAdminPasswordSolution>
```

Ce bloc ce compose des paramètres pour la création des éléments suivants :

- OUs
- Délégation
- Translation
- GPOs
- Comptes
- Groupes
- Membres par défaut aux groupes
- Taches planifiées
- LAPS

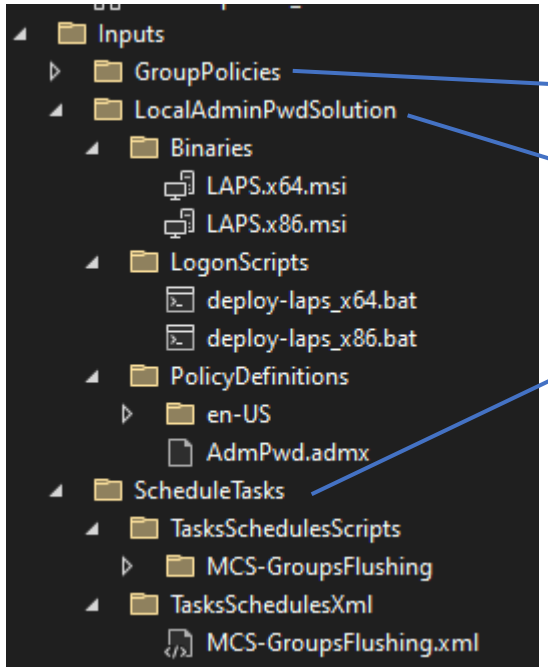
Le bloc séquence

Le bloc des séquences contient les appels des fonctions (contenus dans les modules) pour appliquer le modèle.

Nous pouvons ici commenter certain bloc pour ne pas les appliquer.

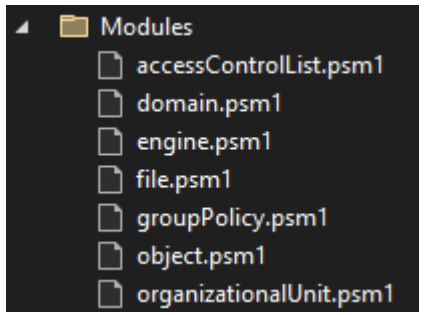
Les autres fichiers

Nous avons d'autres fichiers utile au déploiement



Dans le dossier « Inputs », nous trouverons :

- Le dossier contenant les GPOs à déployer
- Le dossier avec les configurations LAPS
- Le dossier contenant les taches planifiées à déployer



Dans le dossier « Modules », nous trouverons les fichiers contenant les fonctions à importer en module au script de déploiement du modèle HARDEN AD

Personnalisation paramètres

OUs

```
<OrganizationalUnits>
  <!-- The section <ouTree> handle the base model for OU creation.                                                    -->
  <!-- When calling the function [Set-OUTree], you need to add as parameter the "OU class" name of the tree structure you want to add.   -->
  <!-- This could also be used to manage new OU generation.                                                          -->
  <ouTree>
    <!-- CLASS: HardenAD_ADMIN                                                                                       -->
    <!-- This class generate an OU tree used for administration purpose in a tiering model. This is the English Edtiion.   -->
    <OU Class="HardenAD_ADMIN" Name="Administration" Description="Privileged acco">...</OU>

    <!-- CLASS: HardenAD_PROD-T0                                                                                     -->
    <!-- This class generate an OU tree used for administration purpose in a tiering model. This is the English Edtiion.   -->
    <OU Class="HardenAD_PROD-T" Name="Harden - Tier 0" Description="Tier 0 resource">...</OU>

    <!-- CLASS: HardenAD_PROD-T1and2                                                                                 -->
    <!-- This class generate an OU tree used for administration purpose in a tiering model. This is the English Edtiion.   -->
    <OU Class="HardenAD_PROD-T" Name="Harden - Tier 1" Description="Tier 1 and Tier">...</OU>

    <!-- CLASS: HardenAD_PROD-LEGACY                                                                                 -->
    <!-- This class generate an OU tree used for administration purpose in a tiering model. This is the English Edtiion.   -->
    <OU Class="HardenAD_PROD-L" Name="Harden - Tier L" Description="Legacy resource">...</OU>

    <!-- CLASS: PROVISIONNING-EN                                                                                     -->
    <!-- This class generate an OU tree used for provisioning objects in a default location. This is the English Edition.  -->
    <OU Class="PROVISIONNING-E" Name="Provisioning" Description="New objects pro">...</OU>
  </ouTree>
</OrganizationalUnits>
```

Dans ce bloc, nous pouvons personnaliser les noms des OUs qui seront créées.

Pour le renommage des ou faire un remplacer ligne par lignes car certain balise système ont besoin du mot administration.

Délégations

```
<DelegationACEs>
  <!-- Administration -->
  <!-- Delegation for L-S-T1-DELEG_Group - Create and Delete (administration) -->
  <ACL Trustee="L-S-T1-DELEG_Group - Create and Delete (administration)" Right="CreateChild, DeleteChild" RightType="Allow" Inheritance="All"         InheritedObjects=""      ObjectType="group" TargetDN="OU=Groups Tier 1,OU=Administration,ROOTDN"/>
  <ACL Trustee="L-S-T1-DELEG_Group - Create and Delete (administration)" Right="GenericAll"             RightType="Allow" Inheritance="Descendents" InheritedObjects="Group" ObjectType=""      TargetDN="OU=Groups Tier 1,OU=Administration,ROOTDN"/>
  <ACL Trustee="L-S-T1-DELEG_Group - Create and Delete (administration)" Right="CreateChild, DeleteChild" RightType="Allow" Inheritance="All"         InheritedObjects=""      ObjectType="group" TargetDN="OU=Groups Tier Legacy,OU=Administration,ROOTDN"/>
  <ACL Trustee="L-S-T1-DELEG_Group - Create and Delete (administration)" Right="GenericAll"             RightType="Allow" Inheritance="Descendents" InheritedObjects="Group" ObjectType=""      TargetDN="OU=Groups Tier Legacy,OU=Administration,ROOTDN"/>
  <!-- Delegation for L-S-T2-DELEG_Group - Create and Delete (administration) -->
  <ACL Trustee="L-S-T2-DELEG_Group - Create and Delete (administration)" Right="CreateChild, DeleteChild" RightType="Allow" Inheritance="All"         InheritedObjects=""      ObjectType="group" TargetDN="OU=Groups Tier 2,OU=Administration,ROOTDN"/>
  <ACL Trustee="L-S-T2-DELEG_Group - Create and Delete (administration)" Right="GenericAll"             RightType="Allow" Inheritance="Descendents" InheritedObjects="Group" ObjectType=""      TargetDN="OU=Groups Tier 2,OU=Administration,ROOTDN"/>
  <!-- Delegation for L-S-T1-DELEG_User - Create and Delete (administration) -->
  <ACL Trustee="L-S-T1-DELEG_User - Create and Delete (administration)" Right="CreateChild, DeleteChild" RightType="Allow" Inheritance="All"         InheritedObjects=""      ObjectType="user"  TargetDN="OU=Users Tier 1,OU=Administration,ROOTDN"/>
  <ACL Trustee="L-S-T1-DELEG_User - Create and Delete (administration)" Right="GenericAll"             RightType="Allow" Inheritance="Descendents" InheritedObjects="user"  ObjectType=""      TargetDN="OU=Users Tier 1,OU=Administration,ROOTDN"/>
  <ACL Trustee="L-S-T1-DELEG_User - Create and Delete (administration)" Right="CreateChild, DeleteChild" RightType="Allow" Inheritance="All"         InheritedObjects=""      ObjectType="user"  TargetDN="OU=Users Tier Legacy,OU=Administration,ROOTDN"/>
  <ACL Trustee="L-S-T1-DELEG_User - Create and Delete (administration)" Right="GenericAll"             RightType="Allow" Inheritance="Descendents" InheritedObjects="user"  ObjectType=""      TargetDN="OU=Users Tier Legacy,OU=Administration,ROOTDN"/>
  <!-- Delegation for L-S-T1-DELEG_User - Create and Delete (administration) -->
  <ACL Trustee="L-S-T2-DELEG_User - Create and Delete (administration)" Right="CreateChild, DeleteChild" RightType="Allow" Inheritance="All"         InheritedObjects=""      ObjectType="user"  TargetDN="OU=Users Tier 2,OU=Administration,ROOTDN"/>
  <ACL Trustee="L-S-T2-DELEG_User - Create and Delete (administration)" Right="GenericAll"             RightType="Allow" Inheritance="Descendents" InheritedObjects="user"  ObjectType=""      TargetDN="OU=Users Tier 2,OU=Administration,ROOTDN"/>
  <!-- Production -->
  <!-- Delegation for L-S-T1-DELEG_Computer - Create and Delete -->
  <ACL Trustee="L-S-T1-DELEG_Computer - Create and Delete" Right="CreateChild, DeleteChild" RightType="Allow" Inheritance="All"         InheritedObjects=""         ObjectType="computer" TargetDN="OU=Servers,OU=Harden - Tier 1 and 2,ROOTDN"/>
  <ACL Trustee="L-S-T1-DELEG_Computer - Create and Delete" Right="GenericAll"             RightType="Allow" Inheritance="Descendents" InheritedObjects="computer" ObjectType=""         TargetDN="OU=Servers,OU=Harden - Tier 1 and 2,ROOTDN"/>
  <ACL Trustee="L-S-T1-DELEG_Computer - Create and Delete" Right="CreateChild, DeleteChild" RightType="Allow" Inheritance="All"         InheritedObjects=""         ObjectType="computer" TargetDN="OU=Servers,OU=Harden - Tier Legacy,ROOTDN"/>
  <ACL Trustee="L-S-T1-DELEG_Computer - Create and Delete" Right="GenericAll"             RightType="Allow" Inheritance="Descendents" InheritedObjects="computer" ObjectType=""         TargetDN="OU=Servers,OU=Harden - Tier Legacy,ROOTDN"/>
  <!-- Delegation for L-S-T1-DELEG_User - Create and Delete -->
  <ACL Trustee="L-S-T1-DELEG_User - Create and Delete" Right="CreateChild, DeleteChild" RightType="Allow" Inheritance="All"         InheritedObjects=""     ObjectType="user" TargetDN="OU=Services,OU=Harden - Tier 1 and 2,ROOTDN"/>
  <ACL Trustee="L-S-T1-DELEG_User - Create and Delete" Right="GenericAll"             RightType="Allow" Inheritance="Descendents" InheritedObjects="user" ObjectType=""     TargetDN="OU=Services,OU=Harden - Tier 1 and 2,ROOTDN"/>
  <ACL Trustee="L-S-T1-DELEG_User - Create and Delete" Right="CreateChild, DeleteChild" RightType="Allow" Inheritance="All"         InheritedObjects=""     ObjectType="user" TargetDN="OU=Services,OU=Harden - Tier Legacy,ROOTDN"/>
  <ACL Trustee="L-S-T1-DELEG_User - Create and Delete" Right="GenericAll"             RightType="Allow" Inheritance="Descendents" InheritedObjects="user" ObjectType=""     TargetDN="OU=Services,OU=Harden - Tier Legacy,ROOTDN"/>
  <!-- Delegation for L-S-T2-DELEG_Computer - Create and Delete -->
  <ACL Trustee="L-S-T2-DELEG_Computer - Create and Delete" Right="CreateChild, DeleteChild" RightType="Allow" Inheritance="All"         InheritedObjects=""         ObjectType="computer" TargetDN="OU=Workstations,OU=Harden - Tier 1 and 2,ROOTDN"/>
  <ACL Trustee="L-S-T2-DELEG_Computer - Create and Delete" Right="GenericAll"             RightType="Allow" Inheritance="Descendents" InheritedObjects="computer" ObjectType=""         TargetDN="OU=Workstations,OU=Harden - Tier 1 and 2,ROOTDN"/>
  <ACL Trustee="L-S-T2-DELEG_Computer - Create and Delete" Right="CreateChild, DeleteChild" RightType="Allow" Inheritance="All"         InheritedObjects=""         ObjectType="computer" TargetDN="OU=Workstations,OU=Harden - Tier Legacy,ROOTDN"/>
  <ACL Trustee="L-S-T2-DELEG_Computer - Create and Delete" Right="GenericAll"             RightType="Allow" Inheritance="Descendents" InheritedObjects="computer" ObjectType=""         TargetDN="OU=Workstations,OU=Harden - Tier Legacy,ROOTDN"/>
  <!-- Delegation for L-S-T1-DELEG_Group - Create and Delete -->
  <ACL Trustee="L-S-T1-DELEG_Group - Create and Delete" Right="CreateChild, DeleteChild" RightType="Allow" Inheritance="All"         InheritedObjects=""      ObjectType="group" TargetDN="OU=Groups,OU=Harden - Tier 1 and 2,ROOTDN"/>
  <ACL Trustee="L-S-T1-DELEG_Group - Create and Delete" Right="GenericAll"             RightType="Allow" Inheritance="Descendents" InheritedObjects="group" ObjectType=""      TargetDN="OU=Groups,OU=Harden - Tier 1 and 2,ROOTDN"/>
  <ACL Trustee="L-S-T1-DELEG_Group - Create and Delete" Right="CreateChild, DeleteChild" RightType="Allow" Inheritance="All"         InheritedObjects=""      ObjectType="group" TargetDN="OU=Groups,OU=Harden - Tier Legacy,ROOTDN"/>
  <ACL Trustee="L-S-T1-DELEG_Group - Create and Delete" Right="GenericAll"             RightType="Allow" Inheritance="Descendents" InheritedObjects="group" ObjectType=""      TargetDN="OU=Groups,OU=Harden - Tier Legacy,ROOTDN"/>
  <!-- Delegation for L-S-T2-DELEG_contact - Create and Delete -->
  <ACL Trustee="L-S-T2-DELEG_Contact - Create and Delete" Right="CreateChild, DeleteChild" RightType="Allow" Inheritance="All"         InheritedObjects=""        ObjectType="contact" TargetDN="OU=contacts,OU=Harden - Tier 1 and 2,ROOTDN"/>
  <ACL Trustee="L-S-T2-DELEG_Contact - Create and Delete" Right="GenericAll"             RightType="Allow" Inheritance="Descendents" InheritedObjects="contact" ObjectType=""        TargetDN="OU=Contacts,OU=Harden - Tier 1 and 2,ROOTDN"/>
  <ACL Trustee="L-S-T2-DELEG_Contact - Create and Delete" Right="CreateChild, DeleteChild" RightType="Allow" Inheritance="All"         InheritedObjects=""        ObjectType="contact" TargetDN="OU=Contacts,OU=Harden - Tier Legacy,ROOTDN"/>
  <ACL Trustee="L-S-T2-DELEG_Contact - Create and Delete" Right="GenericAll"             RightType="Allow" Inheritance="Descendents" InheritedObjects="contact" ObjectType=""        TargetDN="OU=Contacts,OU=Harden - Tier Legacy,ROOTDN"/>
  <!-- Delegation for L-S-T2-DELEG_User - Create and Delete -->
  <ACL Trustee="L-S-T2-DELEG_User - Create and Delete" Right="CreateChild, DeleteChild" RightType="Allow" Inheritance="All"         InheritedObjects=""     ObjectType="user" TargetDN="OU=Users,OU=Harden - Tier 1 and 2,ROOTDN"/>
  <ACL Trustee="L-S-T2-DELEG_User - Create and Delete" Right="GenericAll"             RightType="Allow" Inheritance="Descendents" InheritedObjects="user" ObjectType=""     TargetDN="OU=Users,OU=Harden - Tier 1 and 2,ROOTDN"/>
  <ACL Trustee="L-S-T2-DELEG_User - Create and Delete" Right="CreateChild, DeleteChild" RightType="Allow" Inheritance="All"         InheritedObjects=""     ObjectType="user" TargetDN="OU=Users,OU=Harden - Tier Legacy,ROOTDN"/>
  <ACL Trustee="L-S-T2-DELEG_User - Create and Delete" Right="GenericAll"             RightType="Allow" Inheritance="Descendents" InheritedObjects="user" ObjectType=""     TargetDN="OU=Users,OU=Harden - Tier Legacy,ROOTDN"/>
  <!-- Delegation for L-S-T2-DELEG_Group - Manage Membership -->
  <ACL Trustee="L-S-T2-DELEG_Group - Manage Membership" Right="ReadProperty, WriteProperty" RightType="Allow" Inheritance="Descendents" InheritedObjects="group" ObjectType="" TargetDN="OU=Groups,OU=Harden - Tier 1 and 2,ROOTDN"/>
  <ACL Trustee="L-S-T2-DELEG_Group - Manage Membership" Right="ReadProperty, WriteProperty" RightType="Allow" Inheritance="Descendents" InheritedObjects="group" ObjectType="" TargetDN="OU=Groups,OU=Harden - Tier Legacy,ROOTDN"/>
</DelegationACEs>
```

Dans ce bloc, nous retrouvons les délégations de droits données sur les différentes ressources de l'AD

Paramètres de translation

```
<Translation>
  <wellKnownID objectClass="text"  translateFrom="%AuthenticatedUsers%"          translateTo="Authenticated Users"/>
  <wellKnownID objectClass="text"  translateFrom="%Administrators%"              translateTo="Administrators"/>
  <wellKnownID objectClass="text"  translateFrom="%domain%"                      translateTo="FORMATION99"/>
  <wellKnownID objectClass="text"  translateFrom="%domaindns%"                   translateTo="formation99.lan"/>
  <wellKnownID objectClass="text"  translateFrom="%RemoteDesktopUsers%"          translateTo="Remote Desktop Users"/>
  <wellKnownID objectClass="text"  translateFrom="%RootDN%"                      translateTo="DC=formation99,DC=lan"/>
  <wellKnownID objectClass="text"  translateFrom="%Users%"                       translateTo="Users"/>
  <wellKnownID objectClass="group" translateFrom="%t0-managers%"                 translateTo="G-S-T0_Managers"/>
  <wellKnownID objectClass="group" translateFrom="%t0-localAdmin-servers%"       translateTo="L-S-T0_LocalAdmins_Servers"/>
  <wellKnownID objectClass="group" translateFrom="%t0-localAdmin-workstations%"  translateTo="L-S-T0_LocalAdmins_Workstations"/>
  <wellKnownID objectClass="group" translateFrom="%t1-managers%"                 translateTo="G-S-T1_Managers"/>
  <wellKnownID objectClass="group" translateFrom="%t1-administrators%"           translateTo="G-S-T1_Administrators"/>
  <wellKnownID objectClass="group" translateFrom="%t1-operators%"                translateTo="G-S-T1_Operators"/>
  <wellKnownID objectClass="group" translateFrom="%t1-localAdmin-servers%"       translateTo="L-S-T1_LocalAdmins_Servers"/>
  <wellKnownID objectClass="group" translateFrom="%t2-managers%"                 translateTo="G-S-T2_Managers"/>
  <wellKnownID objectClass="group" translateFrom="%t2-administrators%"           translateTo="G-S-T2_Administrators"/>
  <wellKnownID objectClass="group" translateFrom="%t2-operators%"                translateTo="G-S-T2_Operators"/>
  <wellKnownID objectClass="group" translateFrom="%t2-localAdmin-workstations%"  translateTo="L-S-T2_LocalAdmins_Workstations"/>
  <wellKnownID objectClass="group" translateFrom="%tl-operators%"                translateTo="G-S-TL_Operators"/>
  <wellKnownID objectClass="group" translateFrom="%tl-localAdmin-servers%"       translateTo="L-S-TL_LocalAdmins_Servers"/>
  <wellKnownID objectClass="group" translateFrom="%tl-localAdmin-workstations%"  translateTo="L-S-TL_LocalAdmins_Workstations"/>
  <wellKnownID objectClass="group" translateFrom="%T1-LAPS-PasswordReset%"       translateTo="L-S-T1-DELEG_LAPS_PwdReset"/>
  <wellKnownID objectClass="group" translateFrom="%T1-LAPS-PasswordReader%"      translateTo="L-S-T1-DELEG_LAPS_PwdRead"/>
  <wellKnownID objectClass="group" translateFrom="%T2-LAPS-PasswordReset%"       translateTo="L-S-T2-DELEG_LAPS_PwdReset"/>
  <wellKnownID objectClass="group" translateFrom="%T2-LAPS-PasswordReader%"      translateTo="L-S-T2-DELEG_LAPS_PwdRead"/>
  <wellKnownID objectClass="group" translateFrom="%Prefix%"                      translateTo="L-S"/>
  <wellKnownID objectClass="group" translateFrom="%Groups_Computers%"            translateTo="localAdmins_%computername%"/>

  <Keyword LongName="servers"        ShortenName="Srv"/>
  <Keyword LongName="server"         ShortenName="Srv"/>
  <Keyword LongName="workstations"   ShortenName="Wks"/>
  <Keyword LongName="workstation"    ShortenName="Wks"/>
  <Keyword LongName="services"       ShortenName="Svc"/>
  <Keyword LongName="service"        ShortenName="Svc"/>
  <Keyword LongName="accounts"       ShortenName="Acct"/>
  <Keyword LongName="account"        ShortenName="Acct"/>
  <Keyword LongName="passwords"      ShortenName="Pwd"/>
  <Keyword LongName="password"       ShortenName="Pwd"/>
  <Keyword LongName="Firewalls"      ShortenName="Fwl"/>
  <Keyword LongName="Firewall"       ShortenName="Fwl"/>
  <Keyword LongName="security"       ShortenName="Secu"/>
  <Keyword LongName="local"          ShortenName="Loc"/>
  <Keyword LongName="administrators" ShortenName="Adm"/>
  <Keyword LongName="administrator"  ShortenName="Adm"/>
  <Keyword LongName="Operators"      ShortenName="Ope"/>
  <Keyword LongName="Operator"       ShortenName="Ope"/>
  <Keyword LongName="Managers"       ShortenName="Mgr"/>
  <Keyword LongName="Manager"        ShortenName="Mgr"/>
</Translation>
```

Dans ce bloc, nous retrouvons les translation qu'il faut configurer afin de faciliter le déploiement personnalisé

Il faut **impérativement** changer 3 points sur les lignes :

- %domain% = nom du domaine
- %domaindns% = nom FQDN du domaine
- %RootDN% = chemin du domaine

D'autres points peuvent être personnalisés, comme :

- %Prefix%
- %Groups_Computers%
- …

GPOs

```
<GroupPolicies>
  <!-- ############################################################################################################################################ -->
  <!-- The <WmiFilter> section allows the script to import MOF files to the Group Policy WMI Filters Container.                                    -->
  <!-- Once a WMI Filter has been imported, it could be attached to a GPO through this script with te <GpoFilter> reference.                      -->
  <!-- All MOF files to import must be located in .\Inputs\GroupPolicies\WmiFilters.                                                              -->
  <!-- Name refers to the display name, as shown in the GUI. Source refers to the source mof file to import.                                      -->
  <!-- ############################################################################################################################################ -->
  <WmiFilters>
    <Filter Name="Windows_X64_Only"                    Source="Windows_X64_Only.mof"                    />
    <Filter Name="Windows_X86_Only"                    Source="Windows_X86_Only.mof"                    />
    <Filter Name="Windows_Server_Only"                 Source="Windows_Server_Only.mof"                 />
    <Filter Name="Windows_Server_2016_And_Newer_Only"  Source="Windows_Server_2016_And_Newer_Only.mof"  />
    <Filter Name="Windows_Server_2012_R2_And_Older_Only" Source="Windows_Server_2012_R2_And_Older_Only.mof"/>
    <Filter Name="Windows_Server_2012_And_Newer_Only"  Source="Windows_Server_2012_And_Newer_Only.mof"  />
    <Filter Name="Windows_Server_2008_R2_And_Older_Only" Source="Windows_Server_2008_R2_And_Older_Only.mof"/>
    <Filter Name="Windows_Client_Only"                 Source="Windows_Client_Only.mof"                 />
    <Filter Name="Windows_10_And_Newer_Only"           Source="Windows_10_And_Newer_Only.mof"           />
    <Filter Name="Windows_8.1_And_Older_Only"          Source="Windows_8.1_And_Older_Only.mof"          />
  </WmiFilters>
```

```
<!-- GPO GROUP SETTINGS: used to generate APPLY and DENY Group Name. Use %tier% to mark the Tier localization in the new name          -->
<!--   > GpoName..: define the group name for applying or denying a group                                                              -->
<GlobalGpoSettings GroupName="G-S-%tier%-GPO_%GpoName%_%mode%" Tier0="T0" Tier1="T1" Tier2="T2">
  <GpoTier0 OU="OU=GPO,OU=Groups Tier 0,OU=Administration,%rootDN%"/>
  <GpoTier1 OU="OU=GPO,OU=Groups Tier 1,OU=Administration,%rootDN%"/>
  <GpoTier2 OU="OU=GPO,OU=Groups Tier 2,OU=Administration,%rootDN%"/>
</GlobalGpoSettings>
```

```
<!-- TEMPLATE
  <GPO BackupID="{9A9AD00F-56D9-476C-9D65-CEAD0FB31B4F}"  Validation="Yes" Name="display name" Description="gpo description">
    <GpoFilter>WmiFilterName</GpoFilter>
    <GpoLink Path="RootDN" Enabled="No" Enforced="No"/>
</GPO>
  -->
  <GPO BackupID="{50BCE76B-CE52-4024-A118-6592D4D6C76D}" Validation="Yes" Name="HAD_Activate_NLA_for_RDP_All" Description="GPO to enable NLA for RDP access">
      <GpoMode Mode="BOTH" Tier="Tier0"/>
      <GpoLink Path="RootDN" Enabled="Yes" Enforced="Yes"/>
</GPO>
  <GPO BackupID="{A69848CE-0866-4B9F-8E2C-E8F747FFE643}" Validation="Yes" Name="HAD_Activate_RDP_All" Description="GPO to enable RDP">
      <GpoMode Mode="BOTH" Tier="Tier0"/>
      <GpoLink Path="RootDN" Enabled="Yes" Enforced="Yes"/>
</GPO>
  <GPO BackupID="{483EF314-0049-4E87-AAE4-2F7BD57880D5}" Validation="Yes" Name="HAD_Auto-Update_S1_Thu_0h_Srv" Description="GPO to update servers">
      <GpoMode Mode="BOTH" Tier="Tier0"/>
  <GpoFilter WMI="Windows_Server_Only"/>
      <GpoLink Path="RootDN" Enabled="Yes" Enforced="Yes"/>
</GPO>
```

Dans ce bloc, nous retrouvons la configuration des GPOs, il est divisé en 3 sous blocs :

- Un premier sous bloc configure les différents filtre WMI
- Le second sous bloc permet de personnaliser le nommage des groupes d'application ou non des GPOs
- Le dernier sous bloc liste les GPOs qui seront déployées.

Vous pouvez commenter le bloc de GPO afin de ne pas la déployer

Utilisateurs (Administration)

```
<Accounts>
  <!-- ########################################################################################################################################## -->
  <!-- The <Account> Section list all user identities to be generated by the script.                                                            -->
  <!-- The script first check if the account is already present in the domain (if so, nothing is done), and if not, it will generatae it.      -->
  <!-- The newly created user is then stored with its random password in a keepass file (.\Outputs\HardenAD.kbdx).                             -->
  <!-- Each account is provided with the following input:                                                                                       -->
  <!--   > GivenName.....: the given name of the account                                                                                        -->
  <!--   > Surname.......: the surname of the account                                                                                           -->
  <!--   > sAMAccountName: the sAMAccountName of the account                                                                                    -->
  <!--   > displayName...: the name displayed by the GUI                                                                                        -->
  <!--   > Description...: the description of the account                                                                                       -->
  <!--   > Path..........: the distingsuihedName of the OU containing the account. you can use ROOTDN to refer to the domain DN               -->
  <!-- ########################################################################################################################################## -->
  <!-- Tier 0 accounts - Manager -->
  <User DisplayName="Admin HARDEN (T0M)" Surname="HARDEN" samAccountName="T0M-AHARDEN" GivenName="Admin" Description="Admin HARDEN (Tier 0 Manager)" Path="OU=Users Tier 0,OU=Administration,ROOTDN"/>

  <!-- Tier 1 accounts - Managers -->

  <!-- Tier 1 accounts - Administrators -->

  <!-- Tier 1 accounts - Operators -->

  <!-- Tier 2 accounts - Managers -->

  <!-- Tier 2 accounts - Administrators -->

  <!-- Tier 2 accounts - Operators -->

  <!-- Tier Legacy accounts - Operators -->
</Accounts>
```

Dans ce bloc, nous retrouvons les utilisateurs qui seront créés afin de leurs attribuer des rôles d'administration.

Il sera créé avec un nommage explicit, et placé dans l'OU user du tier de l'OU Administration.

Les mots de passe seront stockés dans le fichier Keepass configurer avec le mot de passe stocké dans le fichier de module « file.psm1 »

Groupes

```
<Groups>
  <!-- ############################################################################################################################################ -->
  <!-- The <Groups> Section list all group identities to be generated by the script.                                                              -->
  <!-- The script first check if the group is already present in the domain (if so, nothing is done), and if not, it will generatae it.          -->
  <!-- Each group is provided with the following input:                                                                                           -->
  <!--   > Name..........: the name of the group, also its display name and sAMAccountName                                                       -->
  <!--   > Description...: the description of the group                                                                                          -->
  <!--   > Scope.........: domainLocal, Local, Global or Universal                                                                               -->
  <!--   > Category......: security or distribution                                                                                              -->
  <!--                                                                                                                                           -->
  <!-- In a second time, all groups are populated with the <member> input.                                                                        -->
  <!--   > sAMAccountName: the sAMAccountName of the target member.                                                                              -->
  <!-- ############################################################################################################################################ -->
  <!-- #### TIER 0 #### -->
  <Group name="G-S-T0_Managers" Category="Security" Scope="Global" Description="Members of this group can see and manage all the Active Directory objects" Path="OU=Groups Tier 0,OU=Administration,ROOTDN">
    <Member samAccountName="T0M-AHARDEN"/>
  </Group>

  <Group name="L-S-T0_LocalAdmins_Servers" Category="Security" Scope="domainLocal" Description="Members of this group will become member of the builtin\administrators group" Path="OU=Local Admins,OU=Groups Tier 0,OU=Administration,ROOTDN">
  </Group>
  <Group name="L-S-T0_LocalAdmins_Workstations" Category="Security" Scope="domainLocal" Description="Members of this group will become member of the builtin\administrators group" Path="OU=Local Admins,OU=Groups Tier 0,OU=Administration,ROOTDN">
  </Group>

  <!-- #### TIER 1 #### -->
  <Group name="G-S-T1_Managers" Category="Security" Scope="Global" Description="Members of this group can manage all Tier 1 ressources, including T1 admin users and groups" Path="OU=Groups Tier 1,OU=Administration,ROOTDN">
  </Group>

  <Group name="G-S-T1_Administrators" Category="Security" Scope="Global" Description="Members of this group can manage all Tier 1 ressources, excluding T1 admin users and groups" Path="OU=Groups Tier 1,OU=Administration,ROOTDN">
  </Group>

  <Group name="G-S-T1_Operators" Category="Security" Scope="Global" Description="Members of this group can operate on Tier 1 resources (login)" Path="OU=Groups Tier 1,OU=Administration,ROOTDN">
  </Group>

  <Group name="L-S-T1-DELEG_Group - Manage Membership" Category="Security" Scope="domainLocal" Description="Members of this group can add and remove members of tier 1 groups within productions OUs" Path="OU=Deleg,OU=Groups Tier 1,OU=Administration,ROOTDN">
  </Group>

  <Group name="L-S-T1-DELEG_Group - Create and Delete" Category="Security" Scope="domainLocal" Description="Members of this group can create, update and delete groups within productions OUs (Tier 1 and 2)" Path="OU=Deleg,OU=Groups Tier 1,OU=Administration,ROOTDN">
    <Member samAccountName="G-S-T1_Administrators"/>
    <Member samAccountName="G-S-T1_Managers"/>
  </Group>
```

Dans ce bloc, nous retrouvons la liste de tous les groupes qui seront créés dans le cadre du tiering.
Nous retrouverons les groupes de délégation, ainsi que les groupe de tier.

C’est également ici que nous pourrons automatiquement ajouter des utilisateurs dans les groupes avant le déploiement.

Attribution groupe Manager T0

```
<DefaultMembers>
  <!-- ############################################################################################################################################################ -->
  <!-- The <DefaultMembers> Section list strictely allowed members of a specified group.                                                                            -->
  <!-- When the script call the function "Reset-GroupMembership", the function will use this data to leave only mandatory identity.                                -->
  <!--   > Member: either a SID or a sAMAccountName. Use %domainSID% to dynamically replace it by the domain SID.                                                   -->
  <!-- ############################################################################################################################################################ -->
  <!-- Builtin\Administrators -->
  <Group Target="S-1-5-32-544">
    <Member>%DomainSID%-500</Member>
    <Member>%DomainSID%-512</Member>
    <Member>%DomainSID%-519</Member>
  </Group>
  <!-- Domain Admins -->
  <Group Target="%DomainSID%-512">
    <Member>%DomainSID%-500</Member>
  </Group>
  <!-- Enterprise Admins -->
  <Group Target="%DomainSID%-519">
    <Member>%t0-Managers%</Member>
  </Group>
  <!-- Protected Users -->
  <Group Target="%DomainSID%-525">
    <Member>%t0-managers%</Member>
  </Group>
</DefaultMembers>
```

Dans ce bloc, nous voyons l'intégration du groupe %t0-managers% dans les 3 groupes suivant :

- %DomainSID%-512 = Domain_Admins
- %DomainSID%-519 = Enterprise_Admins
- %DomainSID%-525 = Protected_Users

C'est 3 groupes sont ensuite ajoutés au groupe S-1-5-32-544 qui correspond au groupe Administrateurs

Taches planifiées

```
<TaskSchedules BaseDir="C:\_ADM\TasksSchedulesScripts">
  <!-- ############################################################################################################################################ -->
  <!-- the <TaskSchedules> section define the sched. tasks to add to the running system and is called by the function New-ScheduleTasks.          -->
  <!-- The following parameters are expected:                                                                                                     -->
  <!--   > Name......: The scheduled tasks name, as shown in the GUI.                                                                            -->
  <!--   > Xml.......: The xml file containing a backup of the new scheduled tasks and located in .\Inputs\ScheduleTasks\TasksSchedulesXml       -->
  <!--   > SchedCmd..: The executable to be used. It will replace the %command% in the xml file.                                                 -->
  <!--   > SchedArg..: The arguments line to pass to the executable. If a script is specified, it should present in                              -->
  <!--                 .\Inputs\ScheduleTasks\TasksSchedulesScripts                                                                             -->
  <!--   > SchedDir..: The effective path context when the schedule is run - use %BaseDir% to refer to the directory value speciefied in          -->
  <!--                 the "BaseDir" parameters of the section <TaskSchedules> (this one, yup).                                                 -->
  <!--   > SchedDsc..: The description field for this task.                                                                                       -->
  <!--   > SchedPth..: The folder name where the task will be stored in the Tasks Scheduler console.                                             -->
  <!-- ############################################################################################################################################ -->
  <!-- flushing Sensible groups with MCS-GroupsFlushing.ps1 -->
  <SchedTask Name="MCS - Sensitive Groups Flushing" Xml="MCS-GroupsFlushing.xml">
    <SchedCmd>powershell.exe</SchedCmd>
    <SchedArg>-windowstyle hidden -file .\MCS-GroupsFlushing.ps1</SchedArg>
    <SchedDir>%BaseDir%\MCS-GroupsFlushing</SchedDir>
    <SchedDsc>Flush highly sensitive groups (see MCS-GroupsScheduling.csv for details)</SchedDsc>
    <SchedPth>HardenAD</SchedPth>
  </SchedTask>
</TaskSchedules>
```

Dans ce bloc, nous retrouvons la partie qui permet de créer les taches planifiées.

LAPS

```
<LocalAdminPasswordSolution>
  <!-- ############################################################################################################################################################ -->
  <!-- The <LocalAdminPasswordSolution> is used to setup LAPS over an existing domain.                                                                            -->
    <!-- By default, the model delegate permission to Tier 1 for servers and Tier 2 for workstations. All others are handled by Dom admins.  -->
  <!--                                                                                                                                                            -->
  <!-- SelfPermission: Add Write Permission to ms-Mcs-AdmPwdExiprationTime and ms-Mcs-AdmPwd attribute to SELF (i.e. the computer object). -->
    <!-- PasswordReader: Offer the ability to read ms-Mcs-AdmPwd which contains the local user password                                                            -->
    <!-- PasswordReset.: Offer the ability to read and write ms-Mcs-AdmPwdExiprationTime and ms-Mcs-AdmPwd attribute                                             -->
    <!--                                                                                                                                                          -->
    <!-- The script now handles dynamic group mapping and will look at the <Translation> section of this document.                                                -->
    <!--                                                                                                                                                          -->
    <!-- <AdmPwdSelfPermission>:                                                                                                                                  -->
  <!--    Target: target OU distinguished name with computer objects. use "RootDN" to dynamically specify the domain distanguished name.   -->
  <!--                                                                                                                                                            -->
  <!-- <AdmPwdPasswordreader>:                                                                                                                                    -->
  <!--    Target: target OU distinguished name with computer objects. use "RootDN" to dynamically specify the domain distanguished name.   -->
  <!--    Id....: Specific the group sAMAccountName to be granted with the password read permission on the target OU.                      -->
  <!--                                                                                                                                                            -->
  <!-- <AdmPwdPasswordreset>:                                                                                                                                     -->
  <!--    Target: target OU distinguished name with computer objects. use "RootDN" to dynamically specify the domain distanguished name.   -->
  <!--    Id....: Specific the group sAMAccountName to be granted with the password reset permission on the target OU.                     -->
  <!-- ############################################################################################################################################################ -->
  <AdmPwdSelfPermission Target="OU=Servers,OU=Harden - Tier Legacy,%RootDN%"/>
  <AdmPwdSelfPermission Target="OU=Servers,OU=Harden - Tier 1 and 2,%RootDN%"/>
    <AdmPwdSelfPermission Target="OU=Workstations,OU=Harden - Tier Legacy,%RootDN%"/>
    <AdmPwdSelfPermission Target="OU=Workstations,OU=Harden - Tier 1 and 2,%RootDN%"/>
    <AdmPwdSelfPermission Target="OU=PAW Tier 0,OU=Administration,%RootDN%"/>
    <AdmPwdSelfPermission Target="OU=PAW Tier 1,OU=Administration,%RootDN%"/>
    <AdmPwdSelfPermission Target="OU=PAW Tier 2,OU=Administration,%RootDN%"/>
    <AdmPwdSelfPermission Target="OU=PAW Tier Legacy,OU=Administration,%RootDN%"/>

    <AdmPwdPasswordReader Target="OU=Servers,OU=Harden - Tier Legacy,%RootDN%"       Id="%domain%\%T1-LAPS-PasswordReader%"/>
  <AdmPwdPasswordReader Target="OU=Servers,OU=Harden - Tier 1 and 2,%RootDN%"      Id="%domain%\%T1-LAPS-PasswordReader%"/>
  <AdmPwdPasswordReader Target="OU=Workstations,OU=Harden - Tier Legacy,%RootDN%"  Id="%domain%\%T2-LAPS-PasswordReader%"/>
  <AdmPwdPasswordReader Target="OU=Workstations,OU=Harden - Tier 1 and 2,%RootDN%" Id="%domain%\%T2-LAPS-PasswordReader%"/>

    <AdmPwdPasswordReset  Target="OU=Servers,OU=Harden - Tier Legacy,%RootDN%"       Id="%domain%\%T1-LAPS-PasswordReset%"/>
  <AdmPwdPasswordReset  Target="OU=Servers,OU=Harden - Tier 1 and 2,%RootDN%"      Id="%domain%\%T1-LAPS-PasswordReset%"/>
  <AdmPwdPasswordReset  Target="OU=Workstations,OU=Harden - Tier Legacy,%RootDN%"  Id="%domain%\%T2-LAPS-PasswordReset%"/>
  <AdmPwdPasswordReset  Target="OU=Workstations,OU=Harden - Tier 1 and 2,%RootDN%" Id="%domain%\%T2-LAPS-PasswordReset%"/>
</LocalAdminPasswordSolution>
```

Dans ce bloc, nous retrouvons la partie de configuration des permissions d'accès à LAPS

Séquences de déploiement

Séquence 1/4

```
 <!-- Upgrade Domain Functional Level
<Id Number="005" Name="Upgrade Domain Functional Level">
  <CallingFunction>Set-ADFunctionalLevel</CallingFunction>
  <!--Parameter: Specify Upgrade is applied to Domain (and not Forest)
  <UseParameters>Domain</UseParameters>
  <!--Parameter: Target Functional Level. Possibe values: "2008R2","2012","2012R2","2016","Last"
  <UseParameters>Last</UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>Upgrade `(DomainFunctionalLevel` </TaskDescription>
</Id>

<!-- Upgrade Forest Functional Level
<Id Number="006" Name="Upgrade Forest Functional Level">
  <CallingFunction>Set-ADFunctionalLevel</CallingFunction>
  <!--Parameter: Specify Upgrade is applied to Domain (and not Forest)
  <UseParameters>Forest</UseParameters>
  <!--Parameter: Target Functional Level. Possibe values: "2008R2","2012","2012R2","2016","Last"
  <UseParameters>Last</UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>Upgrade `(ForestFunctionalLevel` </TaskDescription>
</Id>

<!-- SET MS-DS-MACHINEACCOUNTQUOTA TO 0
<Id Number="010" Name="Restrict computer junction to the domain">
  <CallingFunction>Set-msDSMachineAccountQuota</CallingFunction>
  <!--Parameter: new ms-DS-MachineAccountQuota value
  <UseParameters>0</UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>set `(msDSMachineAccountQuota` to `(0` to restrict domain junction</TaskDescription>
</Id>

<!-- ENABLE THE AD RECYCLE BIN
<Id Number="020" Name="Activate Active Directory Recycle Bin">
  <CallingFunction>Set-ADRecycleBin</CallingFunction>
  <UseParameters></UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>activate the `(AD Recycle Bin` optional feature</TaskDescription>
</Id>

<!-- CONFIGURE ALL AD SITE LINKS WITH THE NOTIFY OPTIONS
<Id Number="030" Name="Set Notify on every Site Links">
  <CallingFunction>Set-SiteLinkNotify</CallingFunction>
  <UseParameters></UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>set `(notify` on every `(Site Links</TaskDescription>
</Id>

<!-- ACTIVATE THE GPO CENTRAL STORE
<Id Number="040" Name="Set GPO Central Store">
  <CallingFunction>Set-GpoCentralStore</CallingFunction>
  <UseParameters></UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>set `(GPO Central Store` and update `{adm` and `{admx` files</TaskDescription>
</Id>
```

Bloc séquence pour promouvoir le domaine dans la dernière version de mode natif le plus haut possible

Bloc séquence pour promouvoir la forêt dans la dernière version de mode natif le plus haut possible

Bloc séquence pour mise en place ???

Bloc séquence pour activer la corbeille AD

Bloc séquence pour mise en place ???

Bloc séquence pour activer l’application de GPO

Séquence 2/4

```
<!-- GENERATE NEW ADMINISTRATION ORGANIZATIONAL UNIT
<Id Number="050" Name="Set Administration Organizational Unit">
  <CallingFunction>Set-TreeOU</CallingFunction>
  <!--Parameter: class name from OrganizationalUnits | ouTree in this document
  <UseParameters>HardenAD_ADMIN</UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>set `(Administration` organizational unit</TaskDescription>
</Id>

<!-- GENERATE NEW TIER 0 ORGANIZATIONAL UNIT
<Id Number="051" Name="Set Tier 0 Organizational Unit">
  <CallingFunction>Set-TreeOU</CallingFunction>
  <!--Parameter: class name from OrganizationalUnits | ouTree in this document
  <UseParameters>HardenAD_PROD-T0</UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>set `(Tier 0` organizational unit</TaskDescription>
</Id>

<!-- GENERATE NEW TIER 1 and 2 ORGANIZATIONAL UNIT
<Id Number="052" Name="Set Tier 1 and Tier 2 Organizational Unit">
  <CallingFunction>Set-TreeOU</CallingFunction>
  <!--Parameter: class name from OrganizationalUnits | ouTree in this document
  <UseParameters>HardenAD_PROD-T1and2</UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>set `(Tier 1 and Tier 2 combo` organizational unit</TaskDescription>
</Id>

<!-- GENERATE NEW LEGACY ORGANIZATIONAL UNIT
<Id Number="053" Name="Set Legacy Organizational Unit">
  <CallingFunction>Set-TreeOU</CallingFunction>
  <!--Parameter: class name from OrganizationalUnits | ouTree in this document
  <UseParameters>HardenAD_PROD-LEGACY</UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>set `(Tier Legacy` organizational unit</TaskDescription>
</Id>

<!-- GENERATE NEW DEFAULT OBJECTS LOCATION TREE
<Id Number="060" Name="Set Provisioning Organizational Unit">
  <CallingFunction>Set-TreeOU</CallingFunction>
  <!--Parameter: class name from OrganizationalUnits | ouTree in this document
  <UseParameters>PROVISIONNING-EN</UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>set `(Provisioning` organizational unit</TaskDescription>
</Id>

<!-- RELOCATE NEW USER/GROUP OBJECT LOCATION
<Id Number="070" Name="Default user location on creation">
  <CallingFunction>Set-DefaultObjectLocation</CallingFunction>
  <!--Parameter: user or computer
  <UseParameters>User</UseParameters>
  <!--Parameter: OU distinguishedName. Use RootDN to automatically fill-in the domain name
  <UseParameters>OU=users,OU=provisioning,RootDN</UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>set `(user objects` default location</TaskDescription>
</Id>
```

Bloc séquence pour création de l'OU d'administration

Bloc séquence pour création de l'OU Tier 0

Bloc séquence pour création de l'OU Tier 1 et 2

Bloc séquence pour création de l'OU Tier Legacy

Bloc séquence pour création de l'OU Provisioning

Bloc séquence pour configuration de l'OU par défaut des nouveaux utilisateurs et groupes

Séquence 3/4

```
<!-- RELOCATE NEW COMPUTER OBJECT LOCATION
<Id Number="071" Name="Default computer location on creation">
  <CallingFunction>Set-DefaultObjectLocation</CallingFunction>
  <!--Parameter: user or computer
  <UseParameters>Computer</UseParameters>
  <!--Parameter: OU distinguishedName. Use RootDN to automatically fill-in the domain name
  <UseParameters>OU=computers,OU=provisioning,RootDN</UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>set `(computer objects` default location</TaskDescription>
</Id>

<!-- GENERATE NEW ADMIN ACCOUNTS ON WHICH THE DELEGATION MODEL WILL WORKS
<Id Number="080" Name="Create administration accounts">
  <CallingFunction>New-AdministrationAccounts</CallingFunction>
  <!-- Parameter: KeePass password for the kdbx database
  <UseParameters>H4rd3n@D!!</UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>create `(administration accounts` used by the tier model</TaskDescription>
</Id>

<!-- GENERATE NEW ADMIN GROUPS ON WHICH THE DELEGATION MODEL WILL WORKS
<Id Number="090" Name="Create administration groups">
  <CallingFunction>New-AdministrationGroups</CallingFunction>
  <UseParameters></UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>create `(administration groups` used by the tier model</TaskDescription>
</Id>

<!-- ACEs DEPLOYMENT FOR DELEGATION MODEL
<Id Number="095" Name="Enforce delegation model through ACEs">
  <CallingFunction>Push-DelegationModel</CallingFunction>
  <UseParameters></UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>Enforce `(Delegation ACEs` used by the tier model</TaskDescription>
</Id>

<!-- IMPORT WMI FILTERS
<Id Number="125" Name="Import additional WMI Filters">
  <CallingFunction>Import-WmiFilters</CallingFunction>
  <UseParameters></UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>Import `(WMI filter` to the domain</TaskDescription>
</Id>

<!-- LOC ADM TASK DEPLOYMENT SCRIPT UDATE
<Id Number="127" Name="Update Loca Adm Task deployment scripts">
  <CallingFunction>Set-LocAdmTaskScripts</CallingFunction>
  <UseParameters>SYSVOL\%domaindns%\scripts\LocAdmTask</UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>Update `(LocAdmTask Scripts` to match with the domain name</TaskDescription>
</Id>
```

Bloc séquence pour configuration de l'OU par défaut des nouveaux ordinateurs

Bloc séquence pour création des utilisateurs d'administrations

Bloc séquence pour création des groupes (d'administration et de délégation)

Bloc séquence pour mise en place des droits de délégation sur les ressources de l'AD

Bloc séquence pour importation des filtres WMI pour les GPOs

Bloc séquence pour importer la tache planifiée de création de groupe ordinateurs pour l'administration locale

Séquence 4/4

```
<!-- IMPORT GPOs
<Id Number="130" Name="Import new GPO or update existing ones">
  <CallingFunction>New-GpoObject</CallingFunction>
  <UseParameters></UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>Import or update `(group policy objects` to the domain and link them</TaskDescription>
</Id>

<!-- LAPS SCHEMA UPDATE AND POWERSHELL TOOLING DEPLOYMENT
<!-- Warning: this only works with .Net 4.0 or greater.
<Id Number="134" Name="Update Ad schema for LAPS and deploy PShell tools">
  <CallingFunction>Install-Laps</CallingFunction>
  <!-- Parameter: ForceDcIsSchemaOwner (default) will require that the running system is also the Schema Master owner
  <!--            IgnoreDcIsSchameOwner will remove this requierment (child domain, etc.)
  <UseParameters>ForceDcIsSchemaOwner</UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>Update `(AD Schema` for `[LAPS` and add `(PShell add-on`</TaskDescription>
</Id>

<!-- LAPS PERMISSIONS DEPLOYMENT OVER THE DOMAIN
<Id Number="135" Name="Setup LAPS permissions over the domain">
  <CallingFunction>Set-LapsPermissions</CallingFunction>
  <!-- Parameter: CUSTOM : will teach the script to apply a fine-grained definition (refering to <LocalAdminPasswordSolution>)
  <!--            DEFAULT: will apply permission at the root domain level and leave domain admins as the only allowed users.
  <UseParameters>CUSTOM</UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>Set-up `(LAPS` permissions on the target domain</TaskDescription>
</Id>

<!-- LAPS DEPLOYMENT SCRIPT UDATE
<Id Number="136" Name="Update LAPS deployment scripts">
  <CallingFunction>Set-LapsScripts</CallingFunction>
  <!-- Parameter: use NETLOGON or SYSVOL for a dynamic location. Else enter the UNC Path
  <UseParameters>NETLOGON\LAPS</UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>Update `(LAPS Scripts` to match with the domain name</TaskDescription>
</Id>

<!-- IMPORT SCHEDULE TASKS
<Id Number="140" Name="Import schedule tasks on the running system">
  <CallingFunction>New-ScheduleTasks</CallingFunction>
  <UseParameters></UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>Import new `(schedule tasks` to the `[running system`</TaskDescription>
</Id>

<!-- RESET SENSIBLE GROUPS
<Id Number="150" Name="Reset Group Memberships">
  <CallingFunction>Reset-GroupMembership</CallingFunction>
  <UseParameters></UseParameters>
  <TaskEnabled>Yes</TaskEnabled>
  <TaskDescription>Reset `(groups's membeberships` to the `[trusted list`</TaskDescription>
</Id>-->
```

Bloc séquence pour importer les GPOs

Bloc séquence pour mise en place ???

Bloc séquence pour mise en place ???

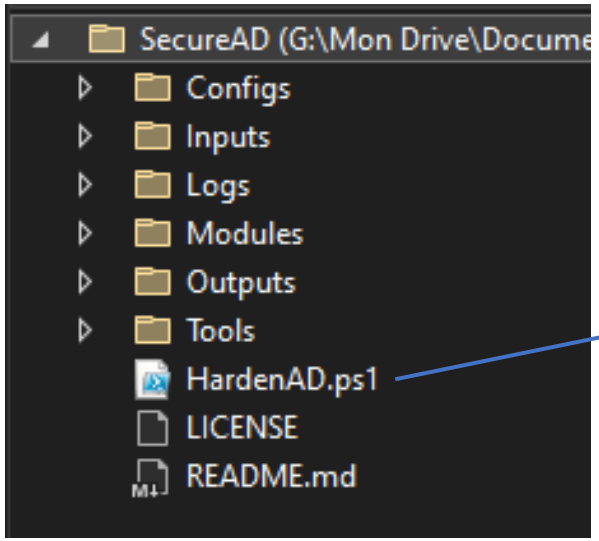
Bloc séquence pour mise en place ???

Bloc séquence pour importer les taches planifiées

Bloc séquence pour vider les groupes d’administration du domaine de leurs membres.
A commenter pour le déploiement

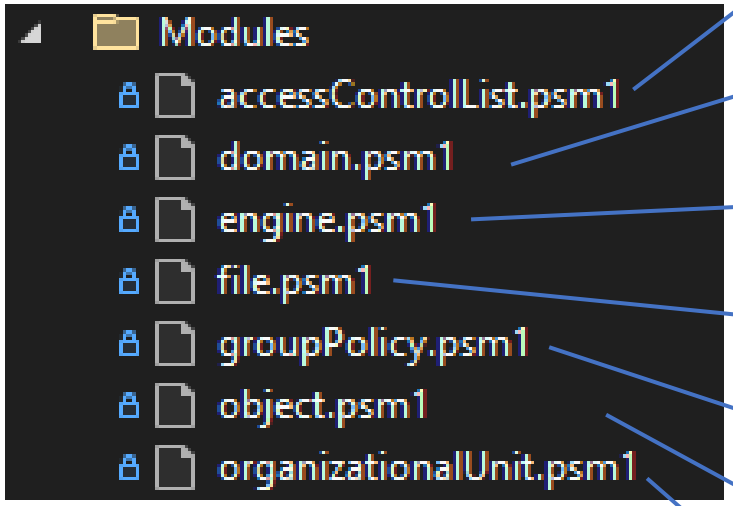
Autres fichiers

Le script de déploiement Harden AD



Ce fichier est le script principal qu'il faut exécuter pour lancer le déploiement d'Harden AD

Les modules



Fichier des modules pour les Acls (délégation de droits, …)

Fichier des modules pour les configurations du domaine (RecycleBin, niveau fonctionnel, …)

Fichier des modules pour les engines (Convertit les .ini en tableau PowerShell)

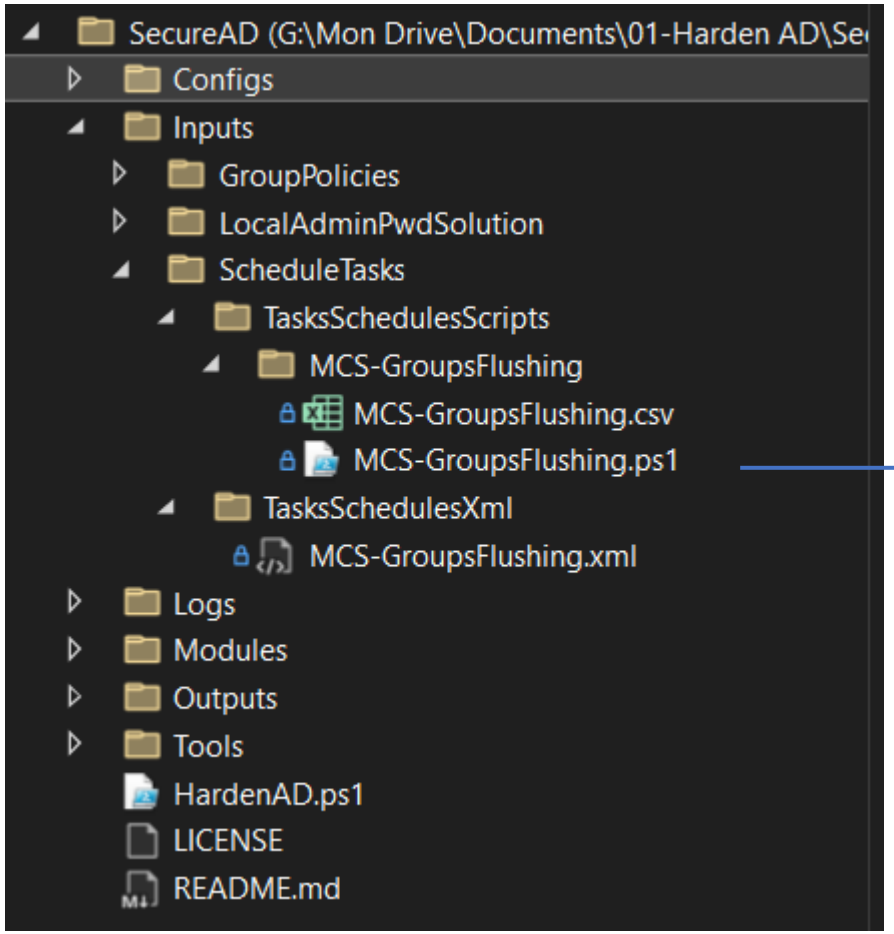
Fichier des modules pour les copies de fichier (Scripts, activation GPO, Tache planifiée, …)

Fichier des modules pour les GPOs (Import filtre WMI, des GPOs, …)

Fichier des modules pour les objets (Utilisateurs, Groupes, …)

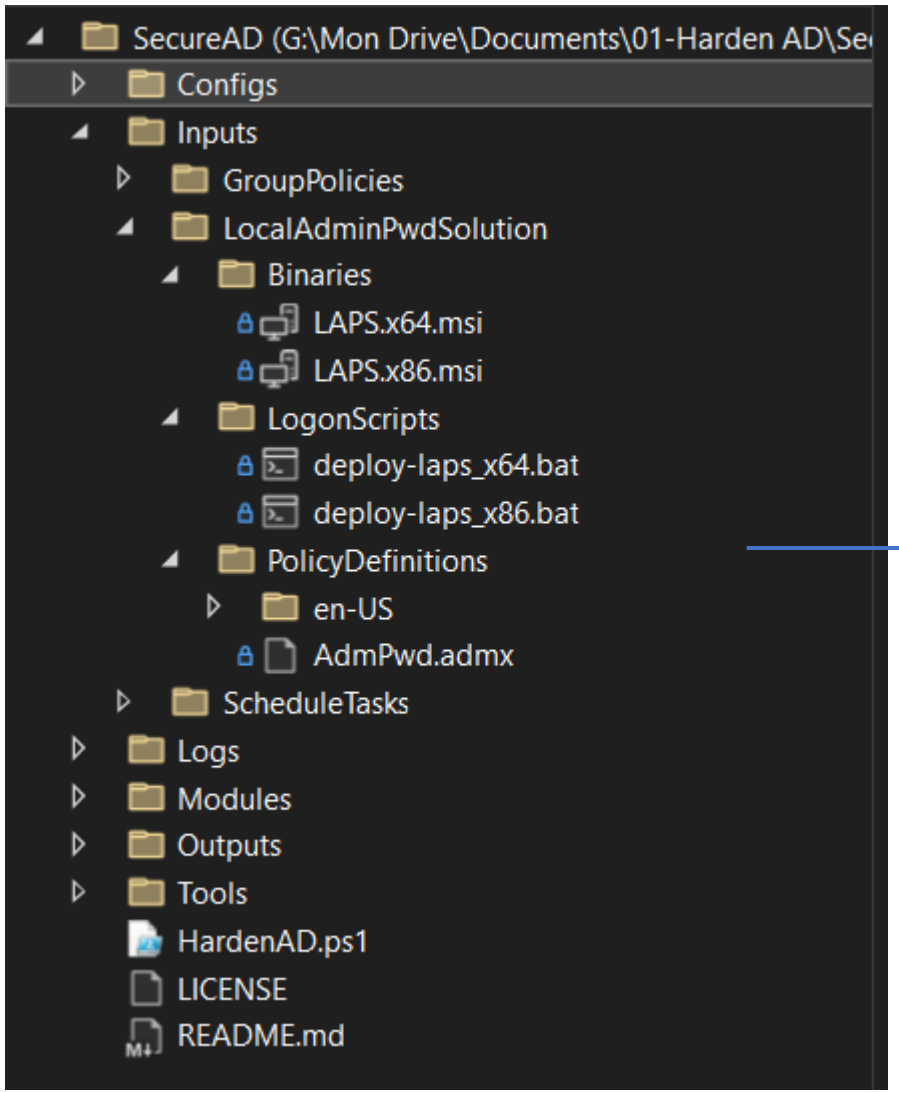
Fichier des modules pour les OUs

Tache planifiée clear groupe administration



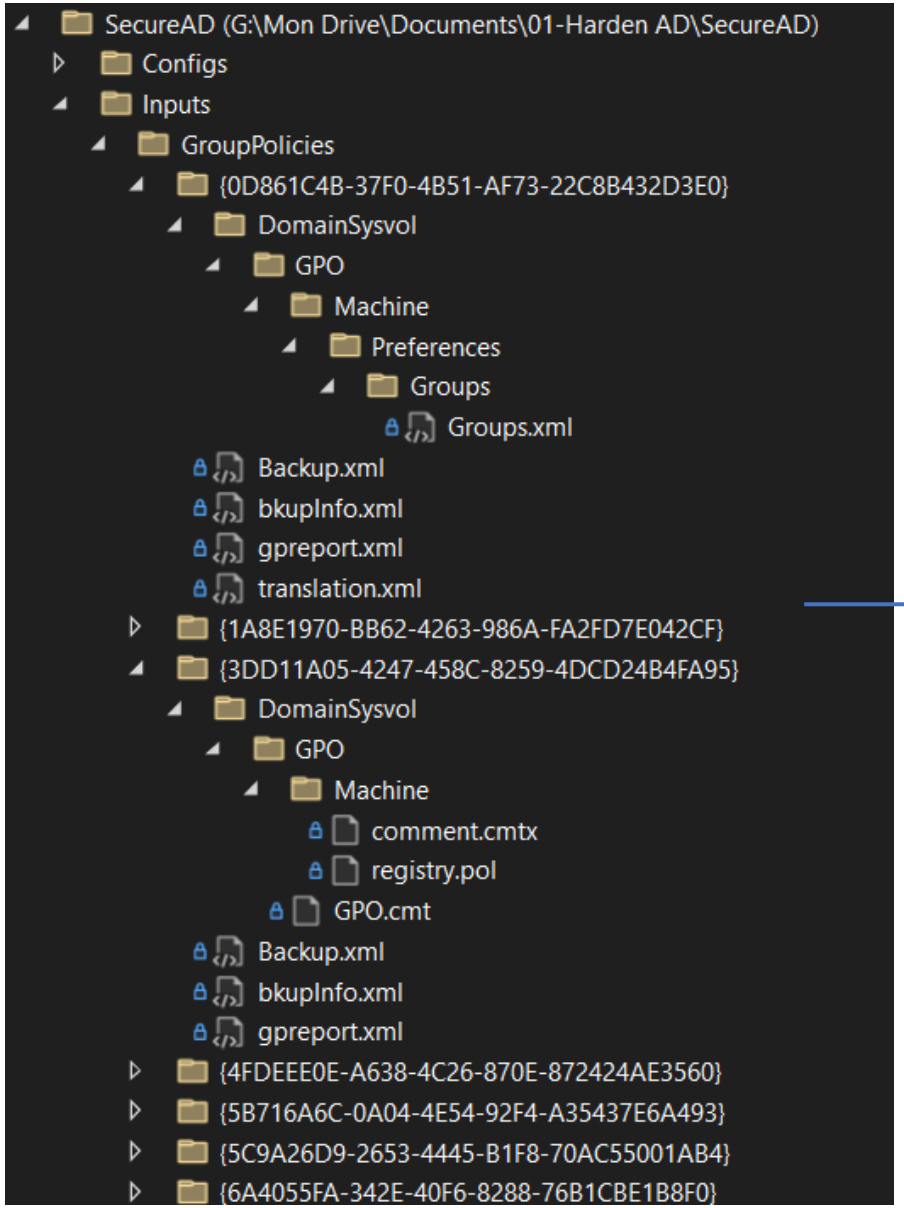
Dans ce dossier, nous retrouvons le script qui permet de vider les d'administration des serveurs et des ordinateurs

LAPS



Nous retrouvons ici les fichier de configuration pour l'outil LAPS

Les GPOs

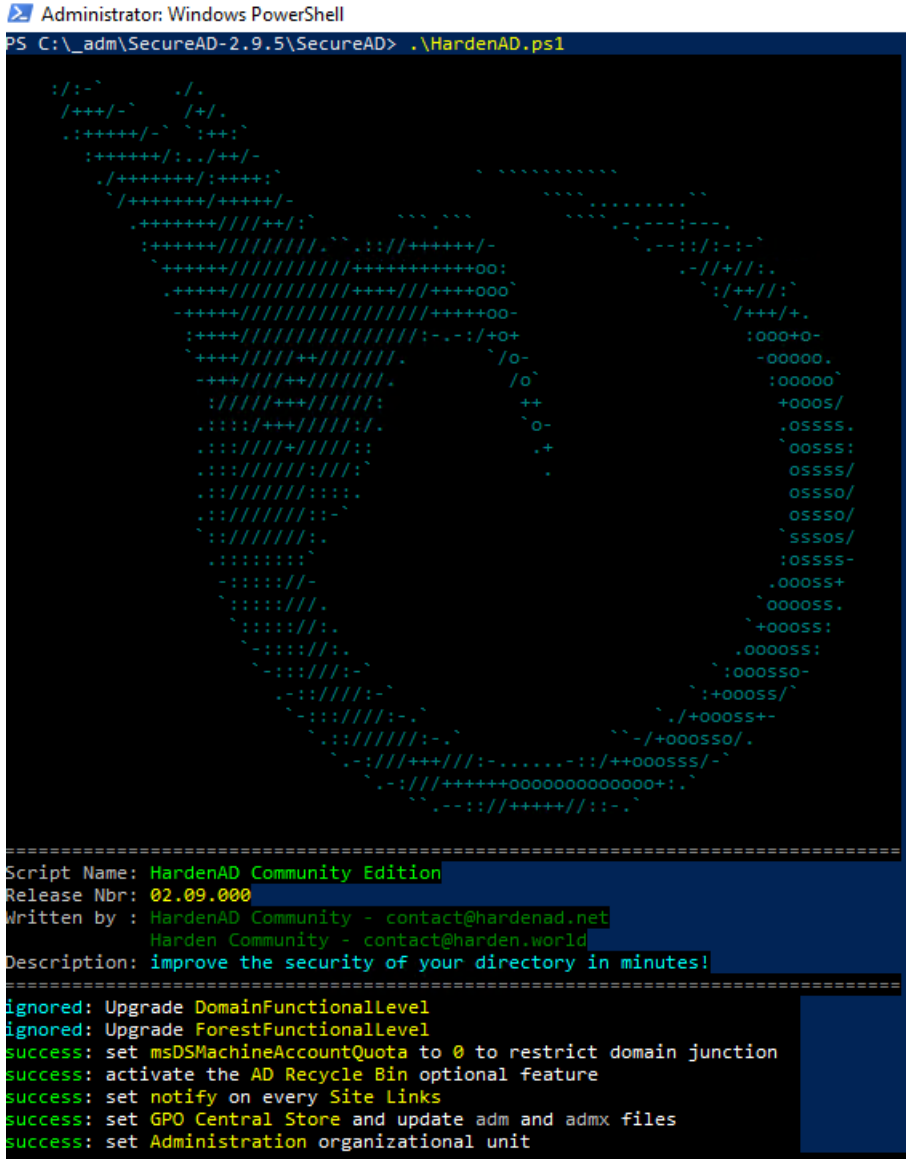


Nous retrouvons ici les dossiers contenant toutes les GPOs.

Dans certaines, nous avons un fichier translation afin de remplacer correctement les informations dans le fichier xml de configuration de la GPO, utiles à son bon fonctionnement.

Exécution Harden AD

Exécution de Harden AD



Faire une sauvegarde complète d'au moins 2 contrôleurs de chacun de vos domaines avec *Windows Server Backup*.

Faire un DCDIAD /V /E et valider le bon fonctionnement de de votre domaine. Lancer ensuite la commande suivante pour vérifier que les rôles FSMO sont disponibles : *NETDOM QUERY FSMO*

Ouvrir une session avec un compte utilisateur membres des groupes *Enterprise Admins* et *Schema Admins*.

Exécuter Harden AD sur le contrôleur domaine avec le rôle *PDC Emulator*.

Exécuter pour cela le script PowerShell *HardenAD.ps1*.

Conclusion

Pour conclure

- Le déploiement Harden peut être entièrement personnalisé.
- Certains paramètres ont des liens avec d'autres. Il est donc très important de modifier le paramètre à tous les niveaux.
- Il faut prendre en considération l'existant afin de configurer le fichier de config correctement afin de ne pas avoir d'erreur.
- Nous pouvons choisir ce que nous déployons, par exemple une seule partie des GPOs, ou la création de plusieurs utilisateurs avec le déploiement, etc. . Afin de gérer au mieux et de ne pas perdre la configuration par défaut d'Harden, il est préférable de commenter les blocs qui ne nous intéressent pas.
- Afin de s'approprier le modèle, plusieurs tests de déploiement pourront être utile.
- Dans le but de ne pas faire d'erreur, un premier déploiement en lab. est toujours judicieux.


?
QUESTIONS

HARDEN AD

Secure your domain in minutes