

La console "Centre d'administration Active Directory"

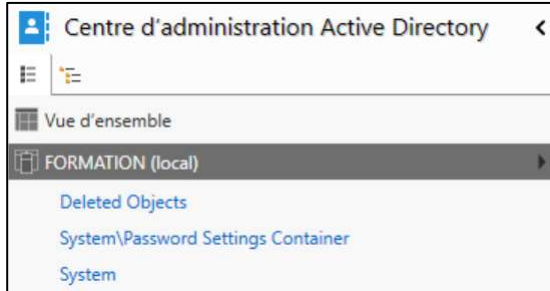
Le nom français de la console est "Centre d'administration Active Directory" mais dans le cours je vais utiliser l'abréviation anglaise (ADAC).

Le nom anglais de la console est "Active Directory Administrative Center" et l'abréviation est (ADAC).

La console ADAC offre des options qui ne sont pas disponibles dans la console "Utilisateurs et ordinateurs Active Directory".

DSAC.EXE est l'exécutable pour ouvrir la console ADAC.

En sélectionnant "FORMATION (local)"



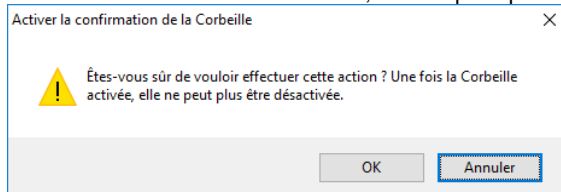
Activation de la corbeille "Active Directory"

"Activer la Corbeille..."

important: Pour activer la Corbeille, le niveau fonctionnel doit être au minimum "Serveur 2012".

note: La Corbeille va contenir des objets de l'Active Directory.

note: Une fois la Corbeille activée, elle ne peut plus être désactivée.

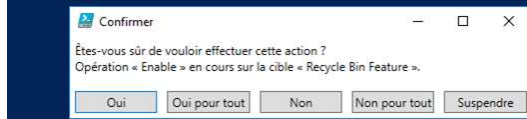


Il est possible d'activer la corbeille par programmation PowerShell.

Cette commande doit s'exécuter sur le contrôleur de domaine

```
Enable-ADOptionalFeature -Identity "Recycle Bin Feature" `
    -Scope Domain `
    -Target "FORMATION.LOCAL" `
    -Server SEVEUR1
```

AVERTISSEMENT : L'activation de « Recycle Bin Feature » sur « DC=FORMATION,DC=LOCAL » est une action irréversible ! Vous ne pourrez pas désactiver « Recycle Bin Feature » sur « DC=FORMATION,DC=LOCAL » si vous continuez.



Supprimer et récupérer un utilisateur supprimé

Vous devez supprimer l'utilisateur "John.Doe".

```
Remove-ADUser -Identity "John.Doe" `
    -Confirm:$false
```

Avant de récupérer des utilisateurs qui sont supprimés, vous devez vérifier avec une commande s'il y a plus d'un utilisateur qui répond aux critères.

Cette commande liste les utilisateurs qui sont supprimés dont le SamAccountName est "John.Doe".

```
Get-ADObject -Filter 'SamAccountName -eq "John.Doe" -AND Deleted -eq $true' `
    -IncludeDeletedObjects
```

Cette commande récupère l'utilisateur à son emplacement d'origine

```
Get-ADObject -Filter 'SamAccountName -eq "John.Doe" -AND Deleted -eq $true' `
    -IncludeDeletedObjects | Restore-ADObject
```

Cette commande récupère l'utilisateur dans un emplacement différent

```
$path = "CN=Users,DC=FORMATION,DC=LOCAL"
```

```
Get-ADObject -Filter 'SamAccountName -eq "John.Doe" -AND Deleted -eq $true' `
    -IncludeDeletedObjects | Restore-ADObject -TargetPath $path
```

Si vous avez plusieurs utilisateurs supprimés qui ont le même SamAccountName, vous devez vérifier la date de suppression du compte en affichant la propriété **Modified**.

Cette commande affiche les utilisateurs qui sont supprimés dont le SamAccountName est "John.Doe"

en affichant la date de suppression

```
Get-ADObject -Filter 'SamAccountName -eq "John.Doe" -AND Deleted -eq $true' `
    -Properties Modified `
    -IncludeDeletedObjects
```

Cette commande affiche les utilisateurs qui sont supprimés dont le SamAccountName est "John.Doe"

en affichant la date de suppression et la date de suppression la plus récente est en première position

```
Get-ADObject -Filter 'SamAccountName -eq "John.Doe" -AND Deleted -eq $true' `
    -Properties Modified `
    -IncludeDeletedObjects | Sort-Object Modified -Descending
```

Cette commande affiche seulement l'utilisateur qui est supprimé dont le SamAccountName est "John.Doe"

dont la date de suppression est la plus récente

```
Get-ADObject -Filter 'SamAccountName -eq "EMP100" -AND Deleted -eq $true' `
    -Properties Modified `
    -IncludeDeletedObjects | `
    Sort-Object Modified -Descending | `
    Select-Object -First 1
```

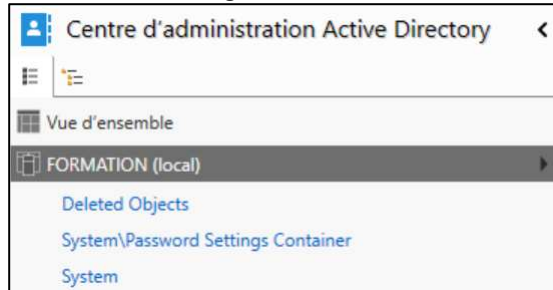
Cette commande récupère l'utilisateur à son emplacement d'origine en vérifiant la date de suppression

```
Get-ADObject -Filter 'SamAccountName -eq "John.Doe" -AND
    Deleted -eq $true -AND
    Modified -eq "2023-04-19 13:28:21"' `
    -Properties Modified `
    -IncludeDeletedObjects | Restore-ADObject
```

Stratégie de mot de passe affinée (Fine-Grained Password Policies)

Les propriétés de "**Password Settings Container**" permettent de configurer des stratégies différentes de mot de passe selon les utilisateurs ou les groupes de sécurité globaux.

"**Password Settings Container**" est sous "**FORMATION (local) / System**"



Historique de Windows PowerShell

En sélectionnant le bouton "Afficher tout", le code PowerShell sera disponible lorsque vous aurez effectué une modification à l'Active Directory à condition d'avoir utilisé la console ADAC.

Informations supplémentaires sur les GPO

Objectifs

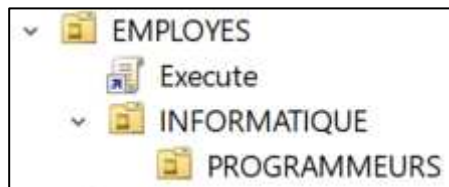
- Comprendre l'implication du blocage de l'héritage
- Comprendre la différence entre "Appliqué" et "Lien activé"

Étape 1 - Création et test d'un objet de stratégie de groupe

Si l'unité d'organisation "EMPLOYES" est directement sous le domaine "FORMATION.LOCAL".

Si l'utilisateur EMP100 est dans l'unité d'organisation "EMPLOYES".

Si l'utilisateur PROG100 est dans l'unité d'organisation "PROGRAMMEURS".



Si la stratégie "Execute" est liée à l'unité d'organisation "EMPLOYES" et la section "Ordinateur" est désactivée.

En supposant que les paramètres de la stratégie "Execute" sont les suivants:

Configuration utilisateur / Stratégies / Modèles d'administration / Panneau de configuration

"Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC"

- Activé

Configuration utilisateur / Stratégies / Modèles d'administration / Système

"Ne pas exécuter les applications Windows spécifiées"

- calc.exe
- win32calc.exe

Si l'utilisateur **EMP100** ouvre une session

- **EMP100 n'a pas d'accès au panneau de configuration**
- **EMP100 n'a pas d'accès à la calculatrice**

Si l'utilisateur **PROG100** ouvre une session

- **PROG100 n'a pas d'accès au panneau de configuration**
- **PROG100 n'a pas d'accès à la calculatrice**

C'est le comportement normal de l'application des GPO.

Étape 2 - L'option "Bloquer l'héritage"

L'option "**Bloquer l'héritage**" est dans le menu contextuel d'une unité d'organisation.



Un point d'exclamation blanc dans un rond bleu nous indique que l'option "**Bloquer l'héritage**" est activée.

Si l'utilisateur **EMP100** ouvre une session

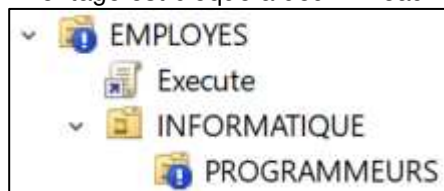
- **EMP100 n'a pas d'accès au panneau de configuration**
 - **EMP100 n'a pas d'accès à la calculatrice**
-

Si l'utilisateur **PROG100** ouvre une session

- **PROG100 n'a pas d'accès au panneau de configuration**
 - **PROG100 n'a pas d'accès à la calculatrice**
-

Le blocage de l'héritage n'a aucun effet sur la GPO qui est liée directement à "EMPLOYES".

L'héritage est bloqué à deux niveaux.



Si l'utilisateur **EMP100** ouvre une session

- **EMP100 n'a pas d'accès au panneau de configuration**
- **EMP100 n'a pas d'accès à la calculatrice**

Si l'utilisateur **PROG100** ouvre une session

- **PROG100 a accès au panneau de configuration**
- **PROG100 a accès à la calculatrice**

La GPO "Execute" ne s'applique pas sur les utilisateurs de l'unité d'organisation "PROGRAMMEURS".

Le blocage empêche l'application des GPO qui sont au-dessus d'une UO mais pas à celles qui sont liées directement à une UO.

En pratique, il faut éviter d'utiliser le blocage des GPO.

Si vous avez besoin d'utiliser l'option "Bloquer l'héritage", vous devez revoir la conception de vos GPO et de vos unités d'organisation.

Avant de continuer

Laisser le blocage d'héritage sur la UO "EMPLOYES"

Laisser le blocage d'héritage sur la UO "PROGRAMMEURS"

Étape 3 - L'option "Appliqué"

L'option "**Appliqué**" est dans le menu contextuel du lien d'une GPO.



Un cadenas nous indique que l'option "**Appliqué**" est activée.

L'option "**Bloquer l'héritage**" doit être active pour voir l'effet de l'option "**Appliqué**".

Si l'utilisateur **EMP100** ouvre une session

- **EMP100 n'a pas d'accès au panneau de configuration**
- **EMP100 n'a pas d'accès à la calculatrice**

Si l'utilisateur **PROG100** ouvre une session

- **PROG100 n'a pas d'accès au panneau de configuration**
- **PROG100 n'a pas d'accès à la calculatrice**

L'option "Appliqué" a priorité sur l'option "Bloquer l'héritage".

IMPORTANT: Il ne faut pas confondre l'option "Appliqué" et "Lien activé".



En français	En anglais
Appliqué	Enforced
Lien activé	Link Enabled

En pratique, il faut éviter d'utiliser l'option "Appliqué".

Si vous avez besoin d'utiliser l'option "Appliqué", vous devez revoir la conception de vos GPO et de vos unités d'organisation.

Stratégies pour le navigateur "Google Chrome"

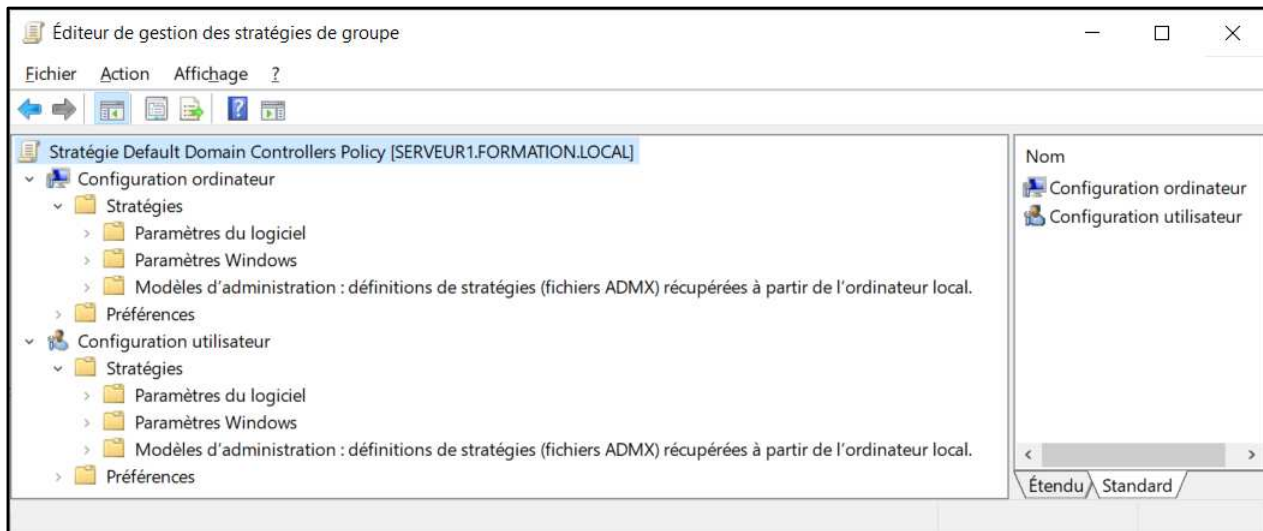
Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectif

- Création du "Magasin central"
- Ajout des fichiers ADMX et ADML pour le navigateur "Google Chrome"

L'utilisation d'un magasin central permet d'utiliser les mêmes fichiers ADMX et ADML sur l'ensemble des contrôleurs de domaine quelle que soit la version de Windows Server. Le magasin central permet de centraliser les modèles d'administration dans le répertoire SYSVOL.

Avant la création du "Magasin central", les stratégies dans "Modèles d'administration" sont récupérées à partir de l'ordinateur local.



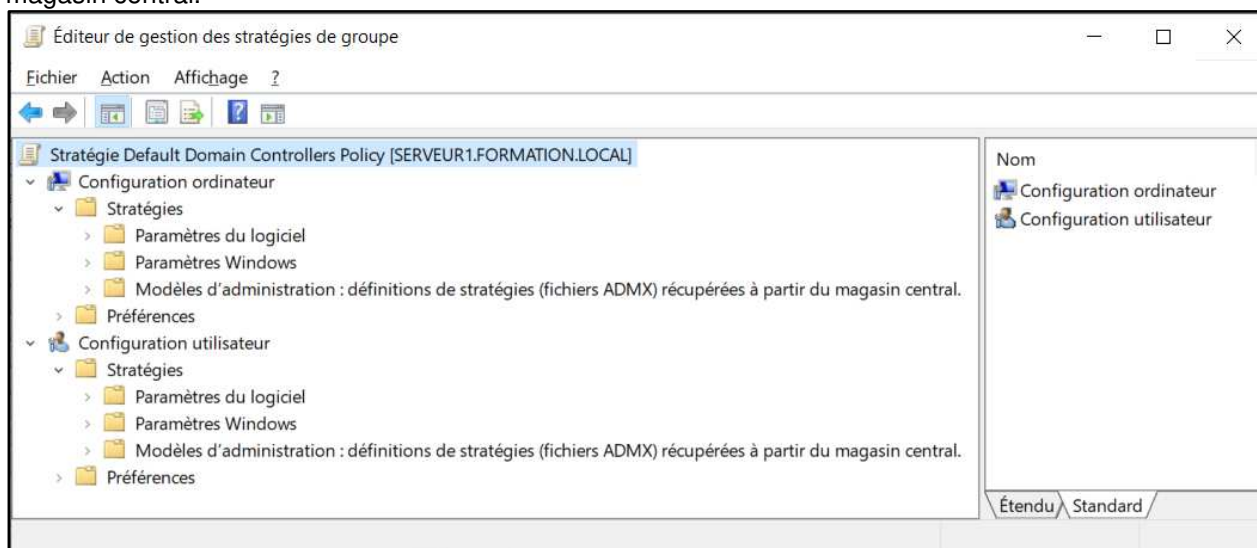
Étape 1 - Création du "Magasin central"

Copier le dossier "\\SERVEUR1\C\$\Windows\PolicyDefinitions" dans le dossier
"\\formation.local\SYSVOL\formation.local\Policies"

Pour éviter les erreurs, vous pouvez utiliser la commande suivante:

```
xcopy \\SERVEUR1\C$\Windows\PolicyDefinitions  
\\formation.local\SYSVOL\formation.local\Policies\PolicyDefinitions\ /S
```

Après la création du "Magasin central", les stratégies dans "Modèles d'administration" sont récupérées à partir du magasin central.



Étape 2 - Copier les fichiers ADMX et ADML de "Chrome" dans le magasin central

Le fichier **policy_templates.zip** est disponible sur le site "Chrome enterprise"

<https://chromeenterprise.google/download>

The screenshot shows the 'Manage and configure Chrome' page. At the top, there are three tabs: 'Windows', 'Mac', and 'Management'. The 'Management' tab is selected. Below the tabs, the heading 'Manage and configure Chrome' is followed by the text 'Manage hundreds of policies and updates centrally from the cloud with Chrome Browser Cloud Management.' A 'Sign up' button is visible. Below this, there are two sections: 'Policy templates' and 'Update management templates'. The 'Policy templates' section has a dropdown menu showing 'Chrome ADM/ADMX templates'. The 'Update management templates' section has a dropdown menu showing 'Google Updater ADM template update'. Below each dropdown is an 'Accept and download' button with a download icon. At the bottom, a disclaimer states: 'By downloading Chrome, you agree to the Google Terms of Service and Chrome ChromeOS Additional Terms of Service'.

Extraire le contenu du fichier **policy_templates.zip** dans un dossier.

Vous devez récupérer les fichiers suivants

..\windows\admx\chrome.admx
..\windows\admx\google.admx
..\windows\admx\fr-FR\chrome.adml
..\windows\admx\fr-FR\google.adml

Copier les fichiers "..\windows\admx\chrome.admx" et "..\windows\admx\google.admx"
dans le dossier

\\formation.local\SYSVOL\formation.local\Policies\PolicyDefinitions\

Copier les fichiers "..\windows\admx\fr-FR\chrome.adml" et "..\windows\admx\fr-FR\google.adml"
dans le dossier

\\formation.local\SYSVOL\formation.local\Policies\PolicyDefinitions\fr-FR\

Étape 3 - Création d'une GPO pour "Google Chrome"

Créer la stratégie "**U_EMPLOYES_Google_Chrome**" et la lier à votre unité d'organisation "**EMPLOYES**"

Désactiver la section "Ordinateur" de votre stratégie

Les paramètres de la GPO serviront à configurer les pages d'accueil du navigateur "Google Chrome".

On doit activer le paramètre de stratégie "**Action au démarrage**" qui est sous:

Configuration utilisateur / Modèles d'administration / Google / Google Chrome / Démarrage, page d'accueil et page Nouvel onglet

On doit sélectionner l'action au démarrage "**Ouvrir une liste d'URL**".

On doit activer le paramètre de stratégie "**URL à ouvrir au démarrage**" qui est sous:

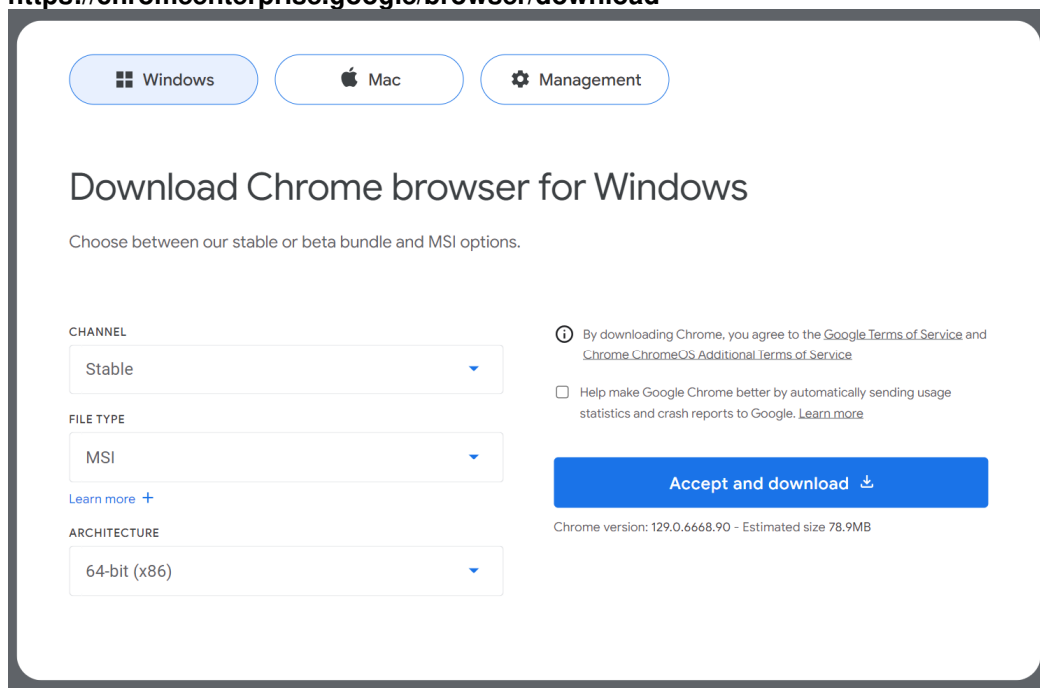
Configuration utilisateur / Modèles d'administration / Google / Google Chrome / Démarrage, page d'accueil et page Nouvel onglet

On doit inscrire une liste de site web que l'on désire ouvrir au démarrage de Chrome.

Étape 4 - Vérifier l'application de la GPO pour le navigateur "Google Chrome"

Vous devez installer le navigateur "Google Chrome" sur le SERVEUR2.

Le fichier googlechromestandaloneenterprise64.msi est disponible sur le site suivant dans la section "Windows"
<https://chromeenterprise.google/browser/download>



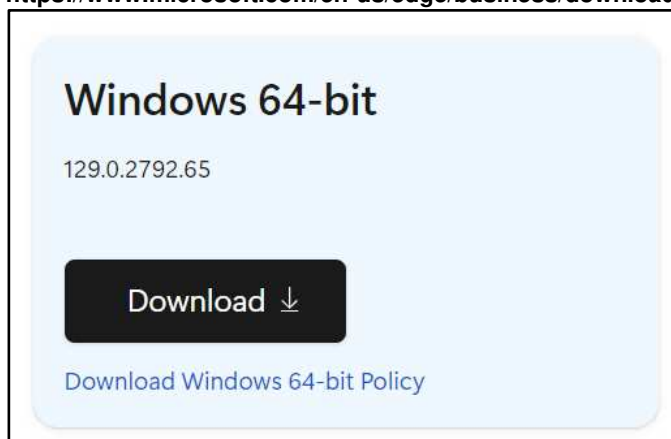
- 1) Fermer la session de l'utilisateur "FORMATION\TECH"
- 2) Ouvrir une session avec un des utilisateurs EMP01 à EMP32
- 3) Vérifier l'application des GPO pour le navigateur "Google Chrome".

ANNEXE

Voici des programmes que vous pouvez contrôler avec des fichiers AMDX et ADML.

Voici le lien pour récupérer les fichiers ADMX et ADML pour "**Edge Chromium**".

<https://www.microsoft.com/en-us/edge/business/download>



Voici le lien pour récupérer les fichiers ADMX et ADML pour

"Microsoft 365 Apps for enterprise - Office LTSC 2024 - Office LTSC 2021 - Office 2019 - Office 216".

<https://www.microsoft.com/en-us/download/office.aspx>

note: vous devez rechercher "**Administrative Template files**"

Administrative Template files (ADMX/ADML) for Microsoft Office

This download includes the Group Policy Administrative Template files (ADMX/ADML) for Microsoft 365 Apps for enterprise, Office LTSC 2024, Office LTSC 2021, Office 2019, and Office 2016 and also includes the OPAX/OPAL files for the Office Customization Tool (OCT) for Office 2016.

Important! Selecting a language below will dynamically change the complete page content to that language.

Select language

English ▼

Download

Filtres WMI

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectif

- Utiliser des stratégies avec filtres WMI (Windows Management Instrumentation)
- Les filtres WMI font partie des outils de ciblage de la console GPMC.

Les filtres WMI permettent de cibler les postes clients ou les utilisateurs d'une stratégie de groupe avec précision. Avec un filtre WMI, il est possible d'appliquer des "GPO Utilisateurs" sur des ordinateurs en spécifiant une requête WMI afin de sélectionner un ou plusieurs ordinateurs.

Il est possible de filtrer l'application d'une stratégie en supprimant "**Utilisateurs authentifiés**" dans la section "**Filtrage de sécurité**" et d'ajouter seulement les utilisateurs, les ordinateurs ou les groupes visés par la stratégie.

C'est une solution trop compliquée, voir l'annexe à la fin du fichier.

Le plus simple est de configurer le filtrage WMI.

Filtre SERVEUR2

Étendue Détails Paramètres Délégation État

Liaisons

Afficher les liaisons à cet emplacement : FORMATION.LOCAL

Les sites, domaines et unités d'organisation suivants sont liés à cet objet GPO :

Emplacement	Appliqué	Lien activé	Chemin d'accès
-------------	----------	-------------	----------------

Filtrage de sécurité

Les paramètres dans ce GPO s'appliquent uniquement aux groupes, utilisateurs et ordinateurs suivants :

Nom

Utilisateurs authentifiés

Ajouter... Supprimer Propriétés

Filtrage WMI

Cet objet de stratégie de groupe est lié au filtre WMI suivant :

<aucun> Ouvrir



Le fichier "**C53 - PowerShell - WMI - CIM.docx**" contient des exemples de code WMI.

Les filtres WMI sont basés sur le langage WQL (WMI Query Language) qui est très proche du langage de programmation SQL (Structured Query Language).

Étape 1 - Mise en place

Les unités d'organisations et les utilisateurs de l'unité d'organisation FORMATION doivent exister.

Vous devez supprimer le lien de la GPO "Bouclage_Fichiers" qui est sur l'unité d'organisation "FICHIERS".

Code PowerShell pour ajouter un ordinateur

```
New-ADComputer -Name SERVEUR3 `
-Path "OU=WEB,OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL"
```

Étape 2 - Création des filtres WMI

- 1) Créer une requête WMI pour sélectionner le serveur SERVEUR2

Nom de la requête WMI: **SERVEUR2**

```
select * from Win32_ComputerSystem where Name = "SERVEUR2"
```

- 2) Créer une requête WMI pour sélectionner le serveur SERVEUR3

Nom de la requête WMI: **SERVEUR3**

note: cette requête vérifie exactement le nom du serveur

```
select * from Win32_ComputerSystem where Name = "SERVEUR3"
```

- 3) Créer une requête WMI pour sélectionner les deux serveurs: SERVEUR2 et SERVEUR3

Nom de la requête WMI: **SERVEUR2 et SERVEUR3**

note: cette requête vérifie exactement le nom des deux serveurs

```
select * from Win32_ComputerSystem where ((Name = "SERVEUR2") OR (Name = "SERVEUR3"))
```

- 4) Créer une requête WMI pour sélectionner les ordinateurs dont le nom débute par SERVEUR

Nom de la requête WMI: **SERVEUR***

note: cette requête vérifie si le nom débute par SERVEUR

```
select * from Win32_ComputerSystem where Name LIKE "SERVEUR%"
```

Voici comment vérifier une requête WMI dans PowerShell

```
Get-CimInstance -Query 'une requête WMI'
```

Exemple

```
$req = 'select * from Win32_ComputerSystem where Name = "SERVEUR2"'
```

```
Get-CimInstance -Query $req | Format-Table -AutoSize
```

Étape 3 - Création d'un objet de stratégie de groupe

Vous devez trouver un fichier JPG qui servira de fond d'écran et qui sera déposé dans le partage
\\formation.local\netlogon.
Le nom du fichier sera "Fond_UO_Programmeurs.jpg".

Créer la stratégie "U_Programmeurs_filtre" qui sera liée à l'unité d'organisation
OU=PROGRAMMEURS,OU=INFORMATIQUE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL

Désactiver la section "Ordinateur" de la stratégie

Modifier la stratégie "U_Programmeurs_filtre" en paramétrant ce qui suit:

Paramètres pour l'utilisateur

Configuration utilisateur / Stratégies / Modèles d'administration / Bureau / Bureau

"Papier peint du Bureau"

- Activé
Nom du papier peint = \\formation.local\netlogon\Fond_UO_Programmeurs.jpg
Style du papier peint = Remplir

Filtrage WMI

Vous devez lier la requête WMI "SERVEUR2" à la GPO "U_Programmeurs_Filtre"

Étape 4 – Test sur le SERVEUR2

Ouvrir une session avec l'utilisateur **EMP11** ou **EMP12**

- Vérifier que le fond d'écran qui est spécifié dans le paramètre de la stratégie "U_Programmeurs_filtre" s'applique
- Fermer la session

Étape 5 - Modification du filtrage WMI sur la GPO "U_Programmeurs_filtre"

Vous devez lier la requête WMI "SERVEUR3" à la GPO "U_Programmeurs_Filtre"

Étape 6 – Test sur le SERVEUR2

Ouvrir une session avec l'utilisateur **EMP11** ou **EMP12**

- Vérifier que le fond d'écran qui est spécifié dans le paramètre de la stratégie "U_Programmeurs_filtre" ne s'applique pas
- Fermer la session

Étape 7 - Modélisation

Il est possible de générer un rapport de modélisation même si le SERVEUR3 n'existe pas physiquement.

Dans la console "Gestion de stratégie de groupe"

- Section "Modélisation de stratégie de groupe"
Dans le menu contextuel, vous devez sélectionner "Assistant Modélisation de stratégie de groupe..."

Les configurations à effectuer dans l'Assistant de modélisation de stratégie de groupe

- Sélection du contrôleur de domaine
Vous devez sélectionner l'option "Tout contrôleur de domaine exécutant ..."
- Sélection d'ordinateurs et d'utilisateurs

Assistant Modélisation de stratégie de groupe

Sélection d'ordinateurs et d'utilisateurs

Vous pouvez afficher les paramètres de stratégie pour un utilisateur sélectionné (ou pour un conteneur comportant les informations de l'utilisateur) et pour un ordinateur sélectionné (ou pour un conteneur comportant les informations de l'ordinateur).

Exemple de nom de conteneur : CN=Users,DC=FORMATION,DC=LOCAL
Exemple d'utilisateur ou d'ordinateur : FORMATION\Administrateur

Simuler des paramètres de stratégie pour :

Informations sur l'utilisateur

☐ Conteneur : Parcourir...

☒ Utilisateur : FORMATION\EMP11 Parcourir...

Informations sur l'ordinateur

☐ Conteneur : Parcourir...

☒ Ordinateur : FORMATION\SERVEUR3 Parcourir...

☒ Se rendre à la dernière page de cet Assistant sans recueillir de données supplémentaires

< Précédent Suivant > Annuler

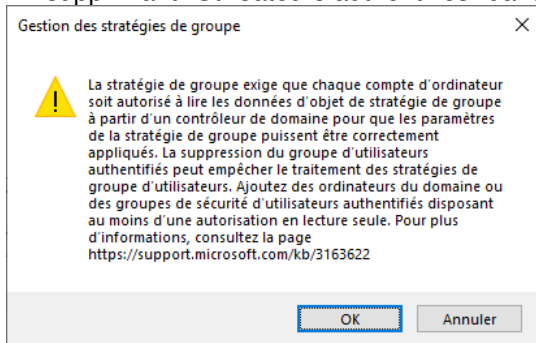
Cocher l'option "**Se rendre à la dernière page de cet Assistant ...**"

Le rapport de la modélisation montre que le fond d'écran qui est spécifié dans le paramètre de la stratégie "**U_Programmeurs_filtre**" s'applique.

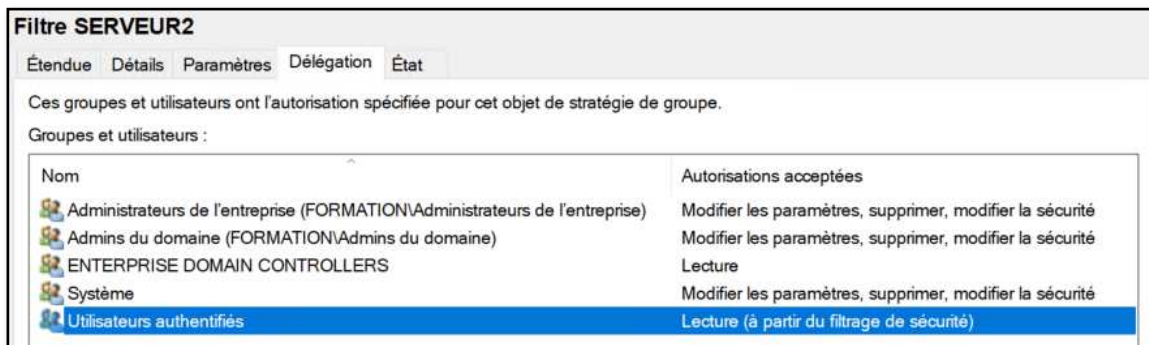
ANNEXE

C'est possible de supprimer "Utilisateurs authentifiés" dans la section "Filtrage de sécurité" et d'ajouter seulement les utilisateurs, les ordinateurs ou les groupes visés par la stratégie. **C'est une solution trop compliquée.**

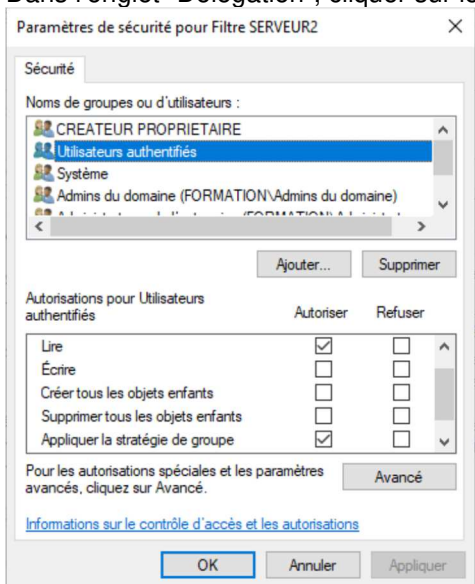
En supprimant "Utilisateurs authentifiés" dans la section "Filtrage de sécurité", il y a un message qui s'affiche.



L'onglet "Délégation" affiche les autorisations.



Dans l'onglet "Délégation", cliquer sur le bouton "Avancé..." et sélectionner "**Utilisateurs authentifiés**".



Par exemple, si vous voulez que la stratégie s'applique seulement à l'utilisateur EMP11.

Il faut ajouter l'utilisateur "**EMP11**".

Les autorisations pour "**EMP11**" seront:

- **Lire**
- **Appliquer la stratégie de groupe**

Il faut **obligatoirement** ajouter le groupe "**Ordinateurs du domaine**".

Les autorisations minimales pour "**Ordinateurs du domaine**" seront

- **Lire**
-

Pour revenir au comportement normal de la stratégie, vous devez défaire vos modifications

- Ajouter "**Utilisateurs authentifiés**"
note: vérifier que les autorisations "**Lire**" et "**Appliquer la stratégie de groupe**" sont cochées
- Supprimer l'utilisateur **EMP11**
- Supprimer le groupe "**Ordinateurs du domaine**"

Cette méthode de filtrage est à éviter.

Stratégies ORDINATEUR

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectif

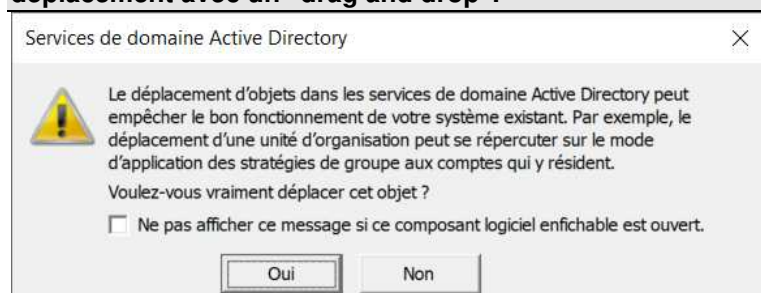
- Introduction aux stratégies "Ordinateur"

Étape 1 - Mise en place

Déplacer l'ordinateur SERVEUR2 dans l'unité d'organisation

OU=FICHIERS,OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL

Lors du déplacement de l'ordinateur SERVEUR2 un message va s'afficher à l'écran si vous effectuez le déplacement avec un "drag and drop".



Étape 2 - Création d'une stratégie ordinateur

Créer la stratégie "C_Serveurs_Fichiers" liée à votre unité d'organisation "FICHIERS".

Désactiver la section "Utilisateur" de votre stratégie

Modifier votre stratégie "C_Serveurs_Fichiers" en paramétrant ce qui suit:

Paramètres pour l'ordinateur

Configuration ordinateur / Stratégies /

Paramètres Windows / Paramètres de sécurité / Stratégies locales / Options de sécurité

"Accès réseau: ne pas autoriser le stockage de mots de passe et d'informations d'identification pour l'authentification du réseau"

- Activé

"Ouverture de session interactive: titre du message pour les utilisateurs essayant de se connecter"

- Le titre sera: "Message important"

"Ouverture de session interactive: contenu du message pour les utilisateurs essayant de se connecter"

- Le contenu du message sera: "Le serveur ne sera pas accessible à partir de 23:00."

Configuration ordinateur / Stratégies /

Modèles d'administration / Système / Ouverture de session

"Afficher l'animation à la première connexion"

- Désactivé

Étape 3 - Création d'une stratégie ordinateur

Créer la stratégie "C_Serveurs_Fichiers_Administrateurs" liée à votre unité d'organisation "FICHIERS".

Désactiver la section "Utilisateur" de votre stratégie

Modifier votre stratégie "C_Serveurs_Fichiers_Administrateurs" en paramétrant ce qui suit:

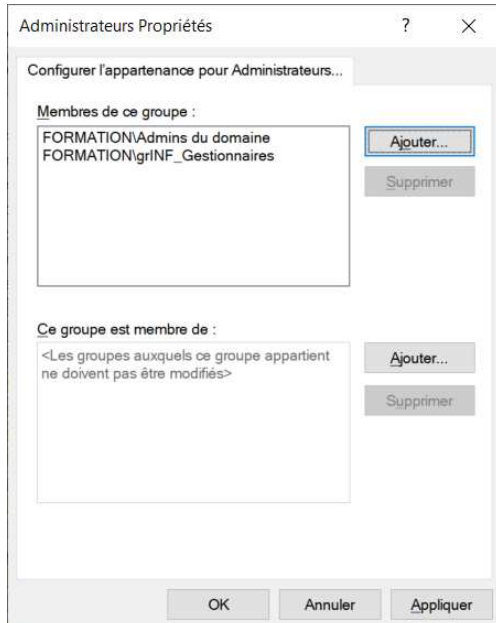
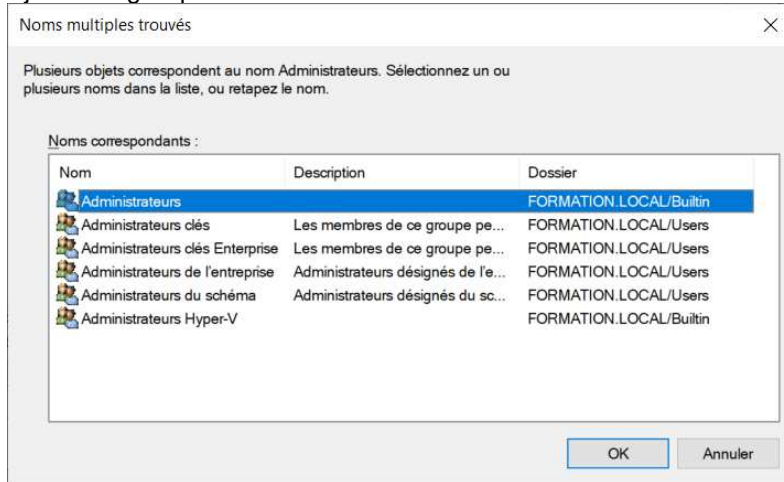
Paramètres pour l'ordinateur

Configuration ordinateur / Stratégies /

Paramètres Windows / Paramètres de sécurité / Groupes restreints

Dans le menu contextuel de "Groupes restreints" choisir l'option "Ajouter un groupe..."

- Ajouter le groupe "Administrateurs"



Ajouter le groupe "FORMATION\Admins du domaine" dans la section "Membres de ce groupe".

Ajouter le groupe "FORMATION\grINF_Gestionnaires" dans la section "Membres de ce groupe"

Étape 4 - Test

Ouvrir une "Invite de commandes" en tant qu'administrateur et exécuter la commande "**gpupdate.exe /force**".

Fermer la session de FORMATION\TECH sur le SERVEUR2.

Vous devez ouvrir une session avec **EMP09** ou **EMP10**.

- Vérifier l'application de la stratégie "**C_Serveurs_Fichiers**"
Un message s'affiche avant de s'authentifier au serveur.
- Vérifier l'application de la stratégie "**C_Serveurs_Fichiers Administrateurs**"
Ouvrir une fenêtre cmd.exe et exécuter la commande suivante "**whoami /groups**"
Dans la liste des groupes, vous allez voir que **EMP09** ou **EMP10** est membre du groupe **BUILTIN\Administrateurs**

Vous devez vous déconnecter de la session **EMP09** ou **EMP10**.

IMPORTANT: il n'y a que les membres des groupes **grINF_Gestionnaires** et "**FORMATION\Admins du domaine**" qui auront des autorisations **Administrateurs** sur le serveur SERVEUR2.

Étape 5 - TRAITEMENT PAR BOUCLAGE

Le traitement par bouclage permet d'appliquer des paramètres utilisateurs dans une unité d'organisation qui contient des ordinateurs.

Il existe deux modes pour le traitement par bouclage.

- **"Remplacer"** indique que les paramètres utilisateur définis dans la stratégie de groupe de "traitement par bouclage" remplacent les paramètres utilisateur normalement appliqués à l'utilisateur.
- **"Fusionner"** indique que les paramètres utilisateur définis dans la stratégie de groupe de "traitement par bouclage" et les paramètres utilisateur normalement appliqués à l'utilisateur se combinent.
Si les paramètres entrent en conflit, les paramètres utilisateur dans la stratégie de groupe de "traitement par bouclage" prévalent sur les paramètres normalement appliqués à l'utilisateur.

Cette solution est souvent appliquée pour des lecteurs réseaux et des imprimantes.

Créer la GPO "**Bouclage_Fichiers**" liée à votre unité d'organisation "FICHIERS".

Paramètres pour l'ordinateur

Configuration ordinateur / Stratégies /
Modèles d'administration / Système / Stratégie de groupe

"Configurer le mode de traitement par bouclage de la stratégie de groupe utilisateur"

- Activé le paramètre et choisir le mode **Remplacer**.

Paramètres pour l'utilisateur

Configuration utilisateur / Stratégies /
Modèles d'administration / Bureau / Bureau

Vous devez trouver un fichier JPG qui servira de fond d'écran et qui sera déposé dans le partage NETLOGON.
Vous devez donner un nom significatif au fichier, par exemple "serveur2.jpg".

"Papier peint du Bureau"

- Activé
Nom du papier peint = \\formation.local\netlogon\serveur2.jpg
Style du papier peint = Remplir

**Je vous recommande de vérifier que le chemin pour le papier peint est valide.
Si le fond d'écran est complètement noir lorsque la GPO s'applique c'est parce que le chemin pour le papier peint n'est pas valide.**

La section "Configuration ordinateur" et la section "Configuration utilisateur" sont activées.

Bouclage_Fichiers

Étendue

Détails

Paramètres

Délégation

Configuration ordinateur (activée)

masquer

Stratégies

masquer

Modèles d'administration

masquer

Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

Système/ Stratégie de groupe

masquer

Stratégie

Paramètre

Commentaire

Configurer le mode de traitement par bouclage de la stratégie de groupe utilisateur

Activé

Mode :

Remplacer

Configuration utilisateur (activée)

masquer

Stratégies

masquer

Modèles d'administration

masquer

Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

Bureau/ Bureau

masquer

Stratégie

Paramètre

Commentaire

Papier peint du Bureau

Activé

Nom du papier peint :

Exemple : avec un chemin local : C:\windows\web\wallpaper\home.jpg

Exemple : avec un chemin UNC : \\Server\Share\Corp.jpg

Style du papier peint :

\\formation.local\netlogon\serveur2.jpg

Ajuster

Tester l'application de la GPO "Bouclage_Fichiers" avec le mode "Remplacer".

Les paramètres utilisateur définis dans la stratégie de groupe de "traitement par bouclage" remplacent les paramètres utilisateur normalement appliqués à l'utilisateur.

Après l'ouverture d'une session:

Le papier peint du Bureau s'affiche avec l'image serveur2.jpg.

"Bouclage_Fichiers"

Dans la GPO "**Bouclage_Fichiers**" changé le mode pour "**Fusionner**".

La section "Configuration ordinateur" et la section "Configuration utilisateur" sont activées.

Bouclage_Fichiers

Étendue Détails Paramètres Délégation

Configuration ordinateur (activée) masquer

Stratégies masquer

Modèles d'administration masquer

Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

Système/ Stratégie de groupe masquer

Stratégie	Paramètre	Commentaire
Configurer le mode de traitement par bouclage de la stratégie de groupe utilisateur	Activé	
Mode :	Fusionner	

Configuration utilisateur (activée) masquer

Stratégies masquer

Modèles d'administration masquer

Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

Bureau/ Bureau masquer

Stratégie	Paramètre	Commentaire
Papier peint du Bureau	Activé	
Nom du papier peint :	\\formation.local\netlogon\serveur2.jpg	
Exemple : avec un chemin local :	C:\windows\web\wallpaper\home.jpg	
Exemple : avec un chemin UNC :	\\Server\Share\Corp.jpg	
Style du papier peint :	Ajuster	

Tester l'application de la GPO "**Bouclage_Fichiers**" avec le mode "**Fusionner**".

Les paramètres utilisateur définis dans la stratégie de groupe de "traitement par bouclage" et les paramètres utilisateur normalement appliqués à l'utilisateur se combinent.

Si les paramètres entrent en conflit, les paramètres utilisateur dans la stratégie de groupe de "traitement par bouclage" prévalent sur les paramètres normalement appliqués à l'utilisateur.

Après l'ouverture d'une session:

Le papier peint du Bureau s'affiche avec l'image serveur2.jpg.

L'écran de veille spécifique est "bubbles.scr".

...

Les bulles de l'écran de veille sont métalliques

...

"Bouclage_Fichiers"

"U_EMPLOYES"

"PU_EMPLOYES"

ANNEXE 1

Pour votre information, les fichiers pour l'image de l'écran de verrouillage et d'ouverture de session pour les ordinateurs du CVM sont dans le dossier **\\reseau.cvm\NETLOGON\CapsuleInfo**

Le dossier contient plusieurs fichiers JPG, mais celui qui est utilisé par défaut a un nom particulier.
\\reseau.cvm\NETLOGON\CapsuleInfo\CVMFondEcranActif.jpg

**Configuration ordinateur / Stratégies /
Modèles d'administration / Panneau de configuration / Personnalisation**

"Forcer une image de l'écran de verrouillage et d'ouverture de session par défaut spécifique"

- Activé
Chemin d'accès de l'image de l'écran de verrouillage = \\formation.local\netlogon\Logo_Corpo.jpg

Cocher l'option "Désactiver les faits fantaisistes, conseils, astuces et plus encore sur l'écran de verrouillage"

ANNEXE 2

Cette GPO pourrait être liée à l'unité d'organisation "**SERVEURS**".

Exemple d'une GPO "C_powershell"

La section utilisateur doit être désactivée sur la GPO, onglet "Détails", paramètre "État GPO".

**Configuration ordinateur / Stratégies /
Modèles d'administration / Composants Windows / Windows PowerShell**

- Activer l'exécution des scripts
note: configurer la valeur de ce paramètre à "Autoriser tous les scripts"

ANNEXE 3

Cette GPO pourrait être liée à l'unité d'organisation "**ORDINATEURS_CLIENTS**".

Exemple d'une GPO "C_arret_systeme"

La section utilisateur doit être désactivée sur la GPO, onglet "Détails", paramètre "État GPO".

**Configuration ordinateur / Stratégies /
Paramètres Windows / Paramètres de sécurité / Stratégies locales / Options de sécurité**

- Arrêt: permet au système d'être arrêté sans avoir à se connecter
note: configurer la valeur de ce paramètre à Activé

ANNEXE 4

Cette GPO pourrait être liée à l'unité d'organisation "**SERVEURS**".

Exemple d'une GPO "**C_securite**"

La section utilisateur doit être désactivée sur la GPO, onglet "Détails", paramètre "État GPO".

Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies locales / Options de sécurité

- Ouverture de session interactive: ne pas afficher le nom du dernier utilisateur connecté
note: configurer la valeur de ce paramètre à Activé
- Ouvertures de sessions interactives: nombre d'ouverture de sessions précédentes réalisées en utilisant la cache (lorsqu'aucun contrôleur de domaine n'est disponible)
note: configurer la valeur de ce paramètre à 0

ANNEXE 5

Cette GPO pourrait être liée à l'unité d'organisation "**SERVEURS**".

Exemple d'une GPO "**C_divers**"

La section utilisateur doit être désactivée sur la GPO, onglet "Détails", paramètre "État GPO".

Configuration ordinateur / Stratégies / Modèles d'administration / Composants Windows / Options d'ouverture de session Windows

- Afficher les informations sur les ouvertures de session précédentes au cours d'une ouverture de session utilisateur
note: configurer la valeur de ce paramètre à Activé

Configuration ordinateur / Stratégies / Modèles d'administration / Système

- Afficher le moniteur d'évènements de mise hors tension
note: configurer la valeur de ce paramètre à Désactivé

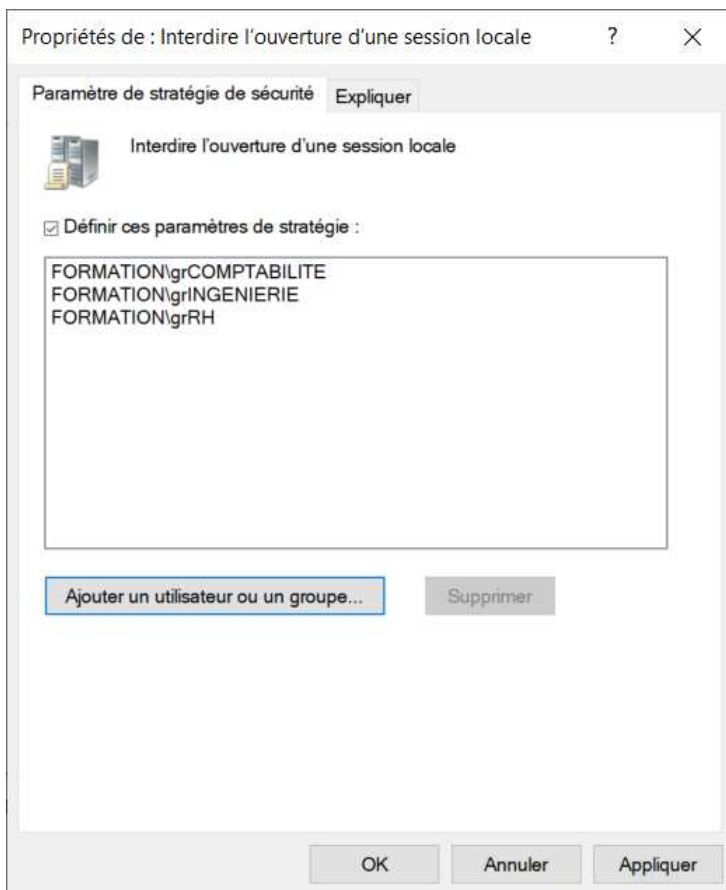
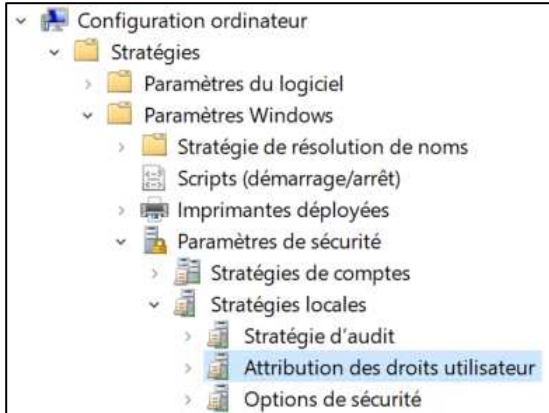
Configuration ordinateur / Stratégies / Modèles d'administration / Système / Ouverture de session

- Toujours attendre le réseau lors du démarrage de l'ordinateur et de l'ouverture de session
note: configurer la valeur de ce paramètre à Activé

ANNEXE 6

Voici comment refuser l'accès à des utilisateurs d'ouvrir une session locale sur des ordinateurs qui sont dans une unité d'organisation.

Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies locales / Attribution des droits utilisateur



Si la GPO est liée à l'unité d'organisation SERVEURS, il sera impossible aux utilisateurs des trois groupes d'ouvrir une session locale sur les ordinateurs qui sont dans l'unité d'organisation SERVEURS.
"OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL"

Préférences UTILISATEUR

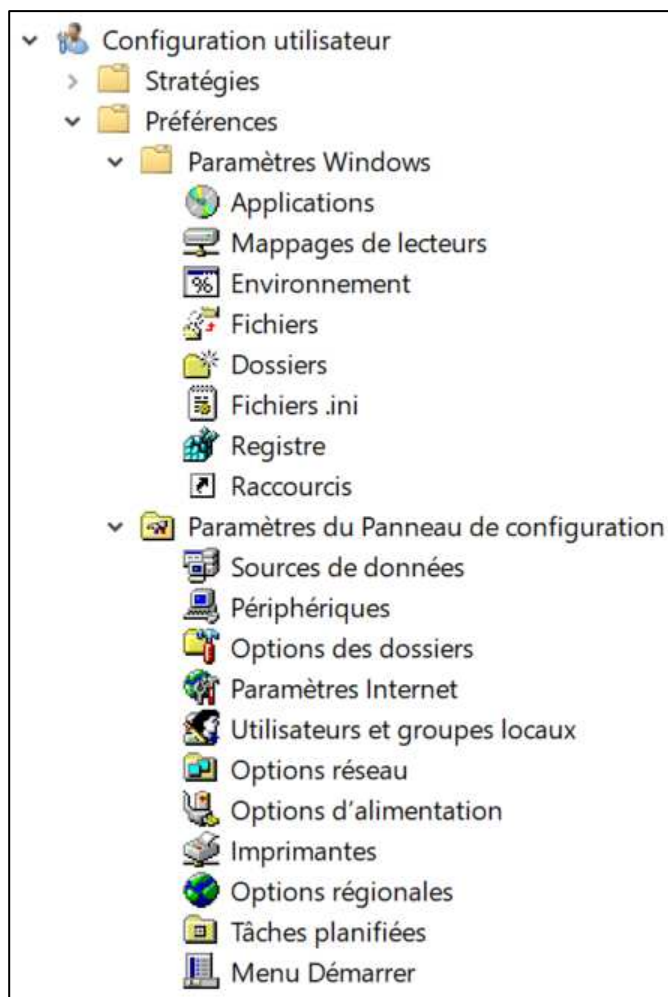
Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectif

- Introduction aux préférences "Utilisateur"

IMPORTANT: sous aucun prétexte les stratégies suivantes ne peuvent être détruites ou modifiées

- Default Domain Controllers Policy
- Default Domain Policy



Les utilisateurs peuvent modifier les configurations qui sont configurées par des préférences.
Les préférences ne sont pas supprimées quand la GPO n'est plus appliquée.

Lors de la création d'une préférence, nous devons choisir entre Créer, Remplacer, Mettre à jour, Supprimer

Créer

Permet de créer un nouveau paramètre de préférence pour l'utilisateur ou l'ordinateur.

Remplacer













Permet de remplacer et de recréer un paramètre de préférence pour l'utilisateur ou l'ordinateur.

Mettre à jour

Permet de modifier un paramètre de préférence existant pour l'utilisateur ou l'ordinateur.

Supprimer

Permet de supprimer un paramètre de préférence existant pour un utilisateur ou un ordinateur.

Créer	Un triangle vert est présent.	<table><tr><td>Nom</td><td>Action</td></tr><tr><td> R:</td><td>Créer</td></tr></table>	Nom	Action	 R:	Créer
Nom	Action					
 R:	Créer					
Remplacer	Un triangle rouge est présent.	<table><tr><td>Nom</td><td>Action</td></tr><tr><td> R:</td><td>Remplacer</td></tr></table>	Nom	Action	 R:	Remplacer
Nom	Action					
 R:	Remplacer					
Mettre à jour	Un triangle jaune est présent.	<table><tr><td>Nom</td><td>Action</td></tr><tr><td> R:</td><td>Mettre à jour</td></tr></table>	Nom	Action	 R:	Mettre à jour
Nom	Action					
 R:	Mettre à jour					
Supprimer	Un X rouge est présent.	<table><tr><td>Nom</td><td>Action</td></tr><tr><td> R:</td><td>Supprimer</td></tr></table>	Nom	Action	 R:	Supprimer
Nom	Action					
 R:	Supprimer					

Création d'une GPO avec des préférences au niveau de la UO EMPLOYES

Créer la GPO "PU_EMPLOYES" et la lier à votre unité d'organisation "EMPLOYES"

Désactiver la section "Configuration ordinateur".

Toutes les options se trouvent dans la section "Configuration utilisateur / Préférences"

Configuration utilisateur / Préférences / Paramètres Windows / Mappages de lecteurs

Lier la lettre "R:" au partage "\\formation.local\netlogon".

- **Mappages de lecteurs**

dans le menu contextuel de la fenêtre blanche, sélectionner "Nouveau / Lecteur mappé"

Propriétés de : R:

Général Commun

Action : Mettre à jour

Emplacement : \\formation.local\netlogon

Reconnecter : ☐ Libeller en tant que :

Lettre de lecteur

☐ Utiliser le premier disponible, en commençant à : ☐ Utiliser : R

Se connecter en tant que (facultatif)

Nom d'utilisateur : Mot de passe : Confirmer le mot de passe

Masquer/Afficher ce lecteur

☒ Aucune modification ☐ Masquer ce lecteur ☐ Afficher ce lecteur

Masquer/Afficher tous les lecteurs

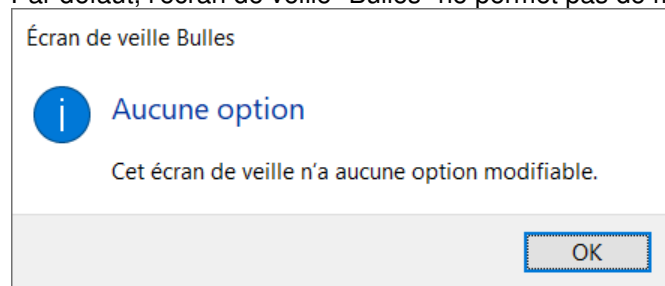
☒ Aucune modification ☐ Masquer tous les lecteurs ☐ Afficher tous les lecteurs

OK Annuler Appliquer Aide

- Action: Mette à jour
- Emplacement: \\formation.local\netlogon
- Utiliser: R
- Cliquer sur le bouton Appliquer
- Cliquer sur le bouton OK

Configuration utilisateur / Préférences / Paramètres Windows / Registre

Par défaut, l'écran de veille "Bulles" ne permet pas de modifier le comportement des bulles.



En modifiant le registre Windows, il est possible de modifier l'aspect des bulles pour l'écran de veille "Bulles".

- **Registre**

dans le menu contextuel de la fenêtre blanche, sélectionner "Nouveau / Élément Registre"

- Action: Mettre à jour
- Ruche: HKEY_CURRENT_USER
- Chemin d'accès de la clé: Software\Microsoft\Windows\CurrentVersion\Screensavers\Bubbles
- Nom de valeur: MaterialGlass
- Type de valeur: REG_DWORD
- Données de valeur: 0
- Cliquer sur le bouton Appliquer
- Cliquer sur le bouton OK

MaterialGlass

- 0 pour afficher des bulles métalliques
- 1 pour afficher des bulles transparentes

Configuration utilisateur / Préférences / Paramètres Windows / Raccourcis

Créer un raccourci sur le Bureau vers NCPA.CPL

- **Raccourcis**

dans le menu contextuel de la fenêtre blanche, sélectionner "Nouveau / Raccourci"

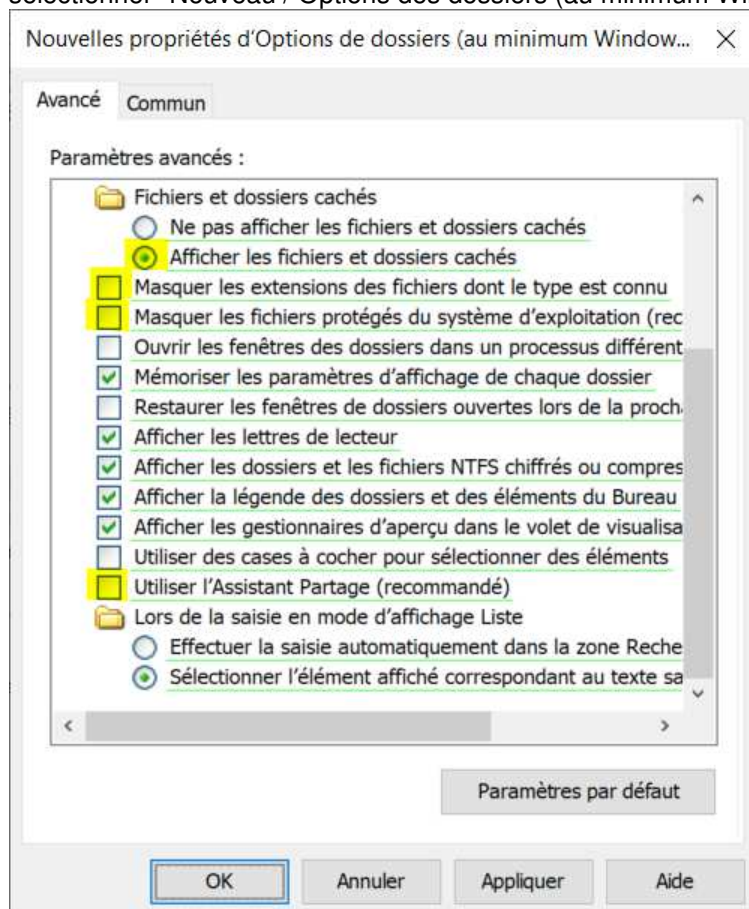
- Action: Mettre à jour
- Nom: Connexions réseau
- Type de cible: Objet du système de fichiers
- Emplacement: Bureau
- Chemin d'accès cible: c:\windows\system32\ncpa.cpl
- Chemin d'accès du fichier d'icône: c:\windows\system32\netshell.dll
- Index de l'icône: 0
- Cliquer sur le bouton Appliquer
- Cliquer sur le bouton OK

Configuration utilisateur / Préférences / Paramètres du Panneau de configuration / Options des dossiers

Configurer les options de dossiers qui permettront

● Options des dossiers

dans le menu contextuel de la fenêtre blanche,
sélectionner "Nouveau / Options des dossiers (au minimum Windows Vista)"



- ACTIVÉ Afficher les fichiers et dossiers cachés
- DÉSACTIVÉ Masquer les extensions des fichiers dont le type est connu
- DÉSACTIVÉ Masques les fichiers protégés du système d'exploitation (recommandé)
- DÉSACTIVÉ Utiliser l'assistant de Partage (recommandé)
- Cliquer sur le bouton Appliquer
- Cliquer sur le bouton OK

Création d'une GPO de préférences au niveau de la UO INFORMATIQUE

Créer une GPO "**PU_INFORMATIQUE_CIBLAGE_EMP09_EMP20**" et la lier à votre unité d'organisation "**INFORMATIQUE**".

Désactiver la section "Configuration ordinateur".



Toutes les options se trouvent dans la section "Configuration utilisateur / Préférences"

Configuration utilisateur / Préférences / Paramètres Windows / Environnement

Créer une variable d'environnement pour l'utilisateur EMP09.

Créer une variable d'environnement pour l'utilisateur EMP20.

Créer une variable d'environnement pour les utilisateurs.

Nom	Action	Valeur	Utilisateur	Ordre
 V09	Remplacer	EMP09	Oui	1
 V20	Remplacer	EMP20	Oui	2
 DIRCMD	Remplacer	/a/o	Oui	3

- **Environnement**

dans le menu contextuel de la fenêtre blanche, sélectionner "Nouveau / Variable d'environnement"

- Action: Remplacer
- Onglet Général
 - ❖ Variable utilisateur
 - ❖ Nom: V09
 - ❖ Valeur: EMP09
- Onglet Commun
 - ❖ Cocher "Supprimer l'élément lorsqu'il n'est plus appliqué"
 - ❖ Ciblage au niveau de l'élément: **EMP09**
- Cliquer sur le bouton Appliquer
- Cliquer sur le bouton OK

dans le menu contextuel de la fenêtre blanche, sélectionner "Nouveau / Variable d'environnement"

- Action: Remplacer
- Onglet Général
 - ❖ Variable utilisateur
 - ❖ Nom: V20
 - ❖ Valeur: EMP20
- Onglet Commun
 - ❖ Cocher "Supprimer l'élément lorsqu'il n'est plus appliqué"
 - ❖ Ciblage au niveau de l'élément: **EMP20**
- Cliquer sur le bouton Appliquer
- Cliquer sur le bouton OK

dans le menu contextuel de la fenêtre blanche, sélectionner "Nouveau / Variable d'environnement"

- Action: Remplacer
 - ❖ Variable utilisateur
 - ❖ Nom: DIRCMD
 - ❖ Valeur: /a/o
- Onglet Commun
 - ❖ Cocher "Supprimer l'élément lorsqu'il n'est plus appliqué"
- Cliquer sur le bouton Appliquer
- Cliquer sur le bouton OK

Validation

Sur le SERVEUR2

Ouvrir une session avec l'utilisateur **EMP07**

- Vérifier l'application des paramètres des préférences qui sont dans les deux GPO
"PU_EMPLOYES"
"PU_INFORMATIQUE_CIBLAGE_EMP09_EMP20"
- Fermer la session

Ouvrir une session avec l'utilisateur **EMP09**

- Vérifier l'application des paramètres des préférences qui sont dans les deux GPO
"PU_EMPLOYES"
"PU_INFORMATIQUE_CIBLAGE_EMP09_EMP20"
- Fermer la session

Ouvrir une session avec l'utilisateur **EMP20**

- Vérifier l'application des paramètres des préférences qui sont dans les deux GPO
"PU_EMPLOYES"
"PU_INFORMATIQUE_CIBLAGE_EMP09_EMP20"
- Fermer la session

Tableau résumé

Paramètres des préférences de la GPO "PU_EMPLOYES"	EMP07	EMP09	EMP20
Le lecteur R: est mappé vers \\formation.local\netlogon	OUI	OUI	OUI
Écran de veille "Bulles" et les bulles sont opaques	OUI	OUI	OUI
Présence du raccourci vers NCPA.CPL sur le Bureau	OUI	OUI	OUI
Les quatre options des dossiers sont présentes	OUI	OUI	OUI

Paramètres des préférences de la GPO "PU_INFORMATIQUE_CIBLAGE_EMP09_EMP20"	EMP07	EMP09	EMP20
Présence des variables d'environnement: V09 V20 DIRCMD	NON NON OUI	OUI NON OUI	NON OUI OUI

L'utilisateur EMP07 est dans l'unité d'organisation suivante:

OU=ANALYSTES,OU=INFORMATIQUE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL

L'utilisateur EMP09 est dans l'unité d'organisation suivante:

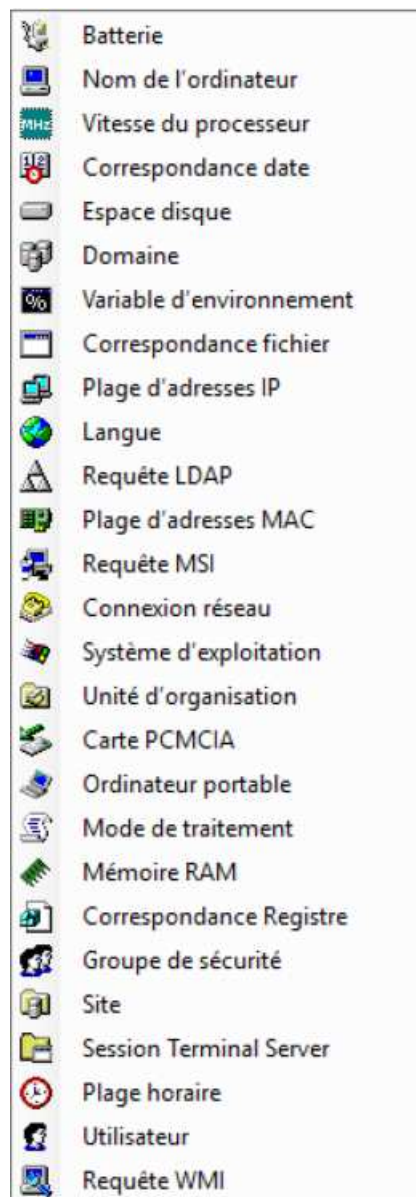
OU=GESTIONNAIRES,OU=INFORMATIQUE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL

L'utilisateur EMP20 est dans l'unité d'organisation suivante:

OU=TECHNICIENS_RESEAU,OU=INFORMATIQUE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL

ANNEXE

Voici les différents critères qui sont disponibles pour le ciblage.



ANNEXE

Commande qui permet de démarrer l'écran de veille "**Bulles**" avec une commande.

C:\Windows\System32\Bubbles.scr /s

Stratégies "Utilisateur"

Ce laboratoire doit être fait individuellement sur le SERVEUR2

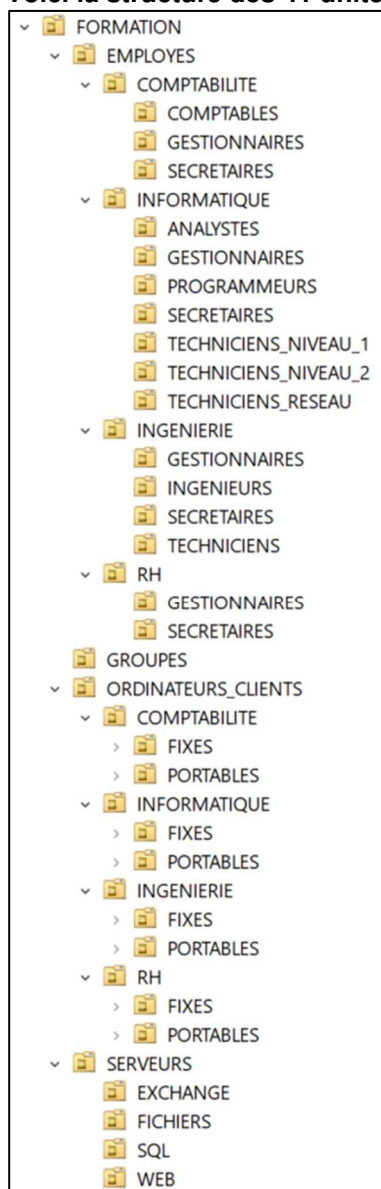
Objectifs

- Introduction aux stratégies "Utilisateur"
- Utiliser la modélisation et les rapports résultants

Étape 1 - Mise en place

Les unités d'organisations et les utilisateurs de l'unité d'organisation FORMATION doivent exister.

Voici la structure des 41 unités d'organisation



IMPORTANT: sous aucun prétexte les stratégies suivantes ne peuvent être détruites ou modifiées

- Default Domain Controllers Policy
- Default Domain Policy

Étape 2 - Création d'un objet de stratégie de groupe

Créer la stratégie "**U_EMPLOYES**" et la lier à votre unité d'organisation "**EMPLOYES**".

Désactiver la section "Ordinateur" de votre stratégie

Modifier votre stratégie "U_EMPLOYES" en paramétrant ce qui suit:

Configuration utilisateur / Stratégies / Modèles d'administration / Bureau / Bureau

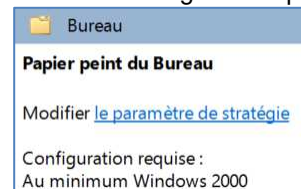
"Papier peint du Bureau"

- Activé
Nom du papier peint = \\formation.local\netlogon\Logo_Corpo.jpg
Style du papier peint = Remplir

Vous devez trouver un fichier JPG qui servira de fond d'écran et qui sera déposé dans le partage NETLOGON. Vous devez donner un nom significatif au fichier, par exemple "Logo_Corpo.jpg".

**Je vous recommande de vérifier que le chemin pour le papier peint est valide.
Si le fond d'écran est complètement noir lorsque la GPO s'applique c'est parce que le chemin pour le papier peint n'est pas valide.**

Avant de configurer un paramètre pour une GPO, vous devez vérifier la configuration requise.

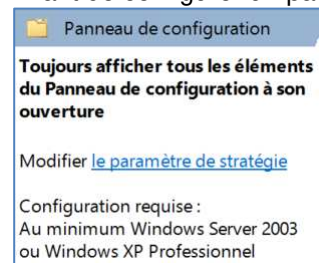


Configuration utilisateur / Stratégies / Modèles d'administration / Panneau de configuration

"Toujours afficher tous les éléments du Panneau de configuration à son ouverture"

- Activé

Avant de configurer un paramètre pour une GPO, vous devez vérifier la configuration requise.



Configuration utilisateur / Stratégies / Modèles d'administration / Panneau de configuration / Personnalisation

"Forcer un écran de veille spécifique"

- Activé
Nom du fichier exécutable de l'écran de veille: bubbles.scr

Avant de configurer un paramètre pour une GPO, vous devez vérifier la configuration requise.

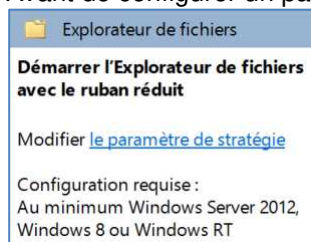


Configuration utilisateur / Stratégies / Modèles d'administration / Composants Windows / Explorateur de fichiers

"Démarrer l'Explorateur de fichiers avec le ruban réduit"

- Activé
Sélectionner: "Ne jamais ouvrir de nouvelles fenêtres de l'Explorateur de fichiers avec le ruban réduit"

Avant de configurer un paramètre pour une GPO, vous devez vérifier la configuration requise.



Étape 3 - Validation

Sur le SERVEUR2

Ouvrir une session avec un des utilisateurs de l'unité d'organisation FORMATION

note: le nom des utilisateurs varie de **EMP01** à **EMP32**

- Vérifier l'application de chaque paramètre de votre stratégie "U_EMPLOYES"
- Fermer la session

Tableau résumé

Paramètres	EMP01 à EMP32 Répondre par Oui ou NON
Papier peint utilise le fichier Logo_Corpo.jpg	OUI
Affichage du panneau de configuration (pas en catégorie)	OUI
Écran de veille est "Bulles"	OUI
Explorateur de fichiers ouvre sans le ruban réduit	OUI

Étape 4 - Modélisation

Dans la console "Gestion de stratégie de groupe"

- Section "Modélisation de stratégie de groupe"
- Menu contextuel
Vous devez sélectionner "Assistant Modélisation de stratégie de groupe..."

Les configurations générales à effectuer dans l'Assistant de modélisation de stratégie de groupe

- Sélection du contrôleur de domaine
Vous devez sélectionner l'option "Tout contrôleur de domaine exécutant ..."
- Sélection d'ordinateurs et d'utilisateurs
 - Sélectionner "Utilisateur"
Parcourir pour sélectionner l'utilisateur visé par la modélisation
 - Sélectionner "Ordinateur"
Parcourir pour sélectionner le serveur virtuel 2
 - Cocher l'option "Se rendre à la dernière page de cet Assistant ..."

Lorsque le rapport s'affiche, il est possible de l'enregistrer dans un fichier HTML.

Étape 5 - Jeu de stratégies résultant

Sur votre serveur virtuel 2

Ouvrir une session avec un des utilisateurs de l'unité d'organisation FORMATION

note: le nom des utilisateurs varie de **EMP01** à **EMP32**

Exécuter la commande suivante: RSOP.MSC

Le refus sur la section Ordinateur est normal étant donné que les utilisateurs de l'unité d'organisation FORMATION ne sont pas membres du groupe "Administrateurs".

RSOP.MSC affiche le jeu de stratégies résultant dans une fenêtre.

RSOP.MSC ne permet pas de sauvegarder le résultat dans un fichier.

Exécuter la commande suivante dans une invite de commandes (ne pas exécuter en tant qu'administrateur)

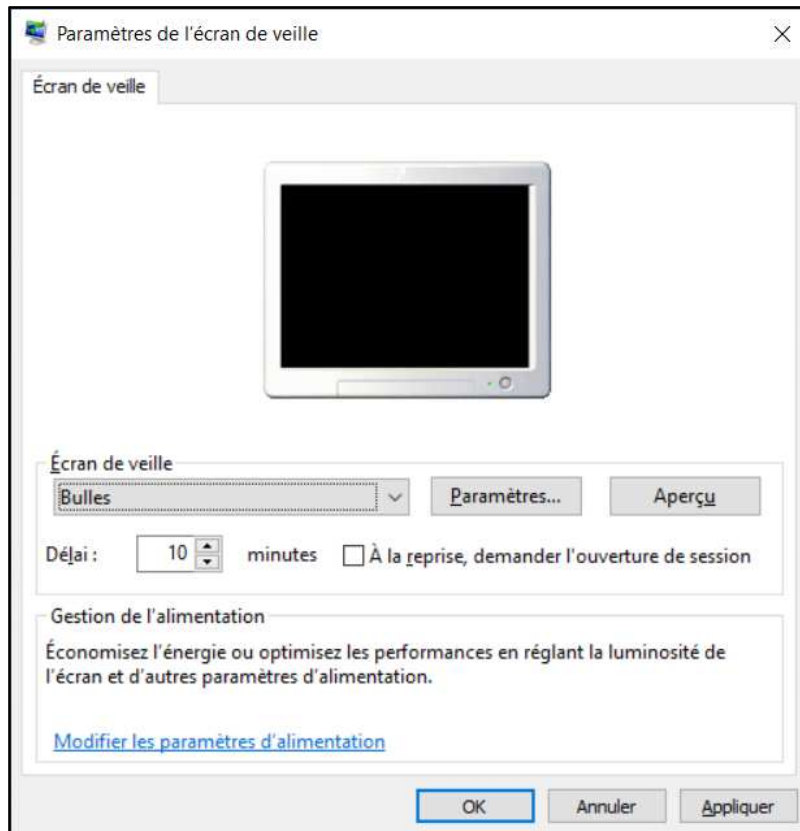
- **gpresult.exe /SCOPE USER /H C:_outils\rapport_EMPxx.html /F**
Consulter le fichier C:_outils\rapport_EMPxx.html

Fermer cette session

La commande gpresult.exe permet de sauvegarder le résultat dans un fichier HTML.

ANNEXE

Comment ouvrir la console "**Paramètres de l'écran de veille**" avec une commande.
control.exe desk.cpl,screensaver,@screensaver



GPO au niveau du domaine

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectifs

- Créer une GPO au niveau du domaine

IMPORTANT: sous aucun prétexte les stratégies suivantes ne peuvent être détruites ou modifiées

- Default Domain Controllers Policy
- Default Domain Policy

Lorsqu'on configure des paramètres de sécurité au niveau du domaine c'est pour améliorer la sécurité.

Les stratégies de mot de passe, les stratégies de verrouillage du compte et les stratégies Kerberos doivent être configurées au niveau du domaine.

Création d'une GPO au niveau du domaine

Exemple d'une GPO "C_Domaine_Mot de passe"

La section utilisateur doit être désactivée sur la GPO, onglet "Détails", paramètre "État GPO".




**Configuration ordinateur / Stratégies /
Paramètres Windows / Paramètres de sécurité / Stratégies de comptes / Stratégie de mot de passe**

- Longueur minimale du mot de passe
note: configurer la valeur de ce paramètre à 9 caractères

**Configuration ordinateur / Stratégies /
Paramètres Windows / Paramètres de sécurité / Stratégies de comptes / Stratégie de verrouillage du compte**

- Seuil de verrouillage du compte
note: configurer la valeur de ce paramètre à 5

Les deux autres paramètres sont configurés automatiquement à 30 minutes.

Stratégie	Paramètres de stratégie
 Durée de verrouillage des comptes	30 minutes
 Réinitialiser le compteur de verrouillages du compte après	30 minutes
 Seuil de verrouillage du compte	5 tentatives d'ouvertures de session non valides

**Configuration ordinateur / Stratégies /
Paramètres Windows / Paramètres de sécurité / Stratégies locales / Options de sécurité**

- Ouverture de session interactive: prévenir l'utilisateur qu'il doit changer son mot de passe avant qu'il n'expire
note: configurer la valeur de ce paramètre à 7 jours

Dans la console de gestion des GPO

- Lier la GPO "C_Domaine_Mot de passe" au niveau du domaine
- Dans "**Ordre des liens**"

Vous devez associer le plus petit chiffre (le chiffre 1) à la GPO "**C_Domaine_Mot de passe**"
Plus le chiffre est petit, plus grande est la priorité d'exécution de la GPO.

FORMATION.LOCAL					
État					
Objets de stratégie de groupe liés					
Héritage de stratégie de groupe					
Délégation					
Ordre des liens	Objet de stratégie de groupe	Appliqué	Lien activé	État GPO	
1	C_Domaine_Mot de passe	Non	Oui	Paramètres de configuration utilisateurs désactivés	
2	Default Domain Policy	Non	Oui	Activé	

La commande "**net accounts**" permet d'afficher des informations pour les stratégies de mot de passe et les stratégies de verrouillage du compte.

```
C:\Windows\system32\cmd.exe

E:\>whoami
formation\emp09

E:\>net accounts
Fermeture forcée de la session après expiration ? :          Jamais
Durée de vie minimale du mot de passe (jours) :             1
Durée de vie maximale du mot de passe (jours) :             42
Longueur minimale du mot de passe :                          9
Nombre de mots de passe antérieurs à conserver :             24
Seuil de verrouillage :                                       5
Durée du verrouillage (min) :                                  30
Fenêtre d'observation du verrouillage (min) :                 30
Rôle de l'ordinateur :                                         SERVEUR
La commande s'est terminée correctement.

E:\>
```

Voici les informations pour les stratégies de mot de passe et les stratégies de verrouillage du compte pour le domaine **RESEAUCEVM**.

```
Invite de commandes

X:\>echo %USERDOMAIN%
RESEAUCEVM

X:\>net accounts
Fermeture forcée de la session après expiration ? :          Jamais
Durée de vie minimale du mot de passe (jours) :              0
Durée de vie maximale du mot de passe (jours) :             42
Longueur minimale du mot de passe :                           6
Nombre de mots de passe antérieurs à conserver :              1
Seuil de verrouillage :                                       5
Durée du verrouillage (min) :                                  5
Fenêtre d'observation du verrouillage (min) :                  5
Rôle de l'ordinateur :                                         STATION
La commande s'est terminée correctement.

X:\>
```

Modélisation

Dans la console "Gestion de stratégie de groupe"

- Section "Modélisation de stratégie de groupe"
Dans le menu contextuel, vous devez sélectionner "Assistant Modélisation de stratégie de groupe..."

Les configurations à effectuer dans l'Assistant de modélisation de stratégie de groupe

- Sélection du contrôleur de domaine
Vous devez sélectionner l'option "Tout contrôleur de domaine exécutant ..."
- Sélection d'ordinateurs et d'utilisateurs

Assistant Modélisation de stratégie de groupe

Sélection d'ordinateurs et d'utilisateurs

Vous pouvez afficher les paramètres de stratégie pour un utilisateur sélectionné (ou pour un conteneur comportant les informations de l'utilisateur) et pour un ordinateur sélectionné (ou pour un conteneur comportant les informations de l'ordinateur).

Exemple de nom de conteneur : CN=Users,DC=FORMATION,DC=LOCAL
Exemple d'utilisateur ou d'ordinateur : FORMATION\Administrateur

Simuler des paramètres de stratégie pour :

Informations sur l'utilisateur

☐ Conteneur : Parcourir...

☒ Utilisateur : FORMATION\TECH Parcourir...

Informations sur l'ordinateur

☐ Conteneur : Parcourir...

☒ Ordinateur : FORMATION\SERVEUR2 Parcourir...

☒ Se rendre à la dernière page de cet Assistant sans recueillir de données supplémentaires

< Précédent Suivant > Annuler

Cocher l'option "**Se rendre à la dernière page de cet Assistant ...**"

Lorsque le rapport s'affiche, il est possible de l'enregistrer dans un fichier HTML.

"Default Domain Policy" et "Default Domain Controllers Policy"

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectifs

- Installer la console "Gestion des stratégies de groupe" sur le SERVEUR2
- Utiliser la console "Gestion des stratégies de groupe"
- Se familiariser avec les objets de stratégie "Default Domain Policy" et "Default Domain Controllers Policy"

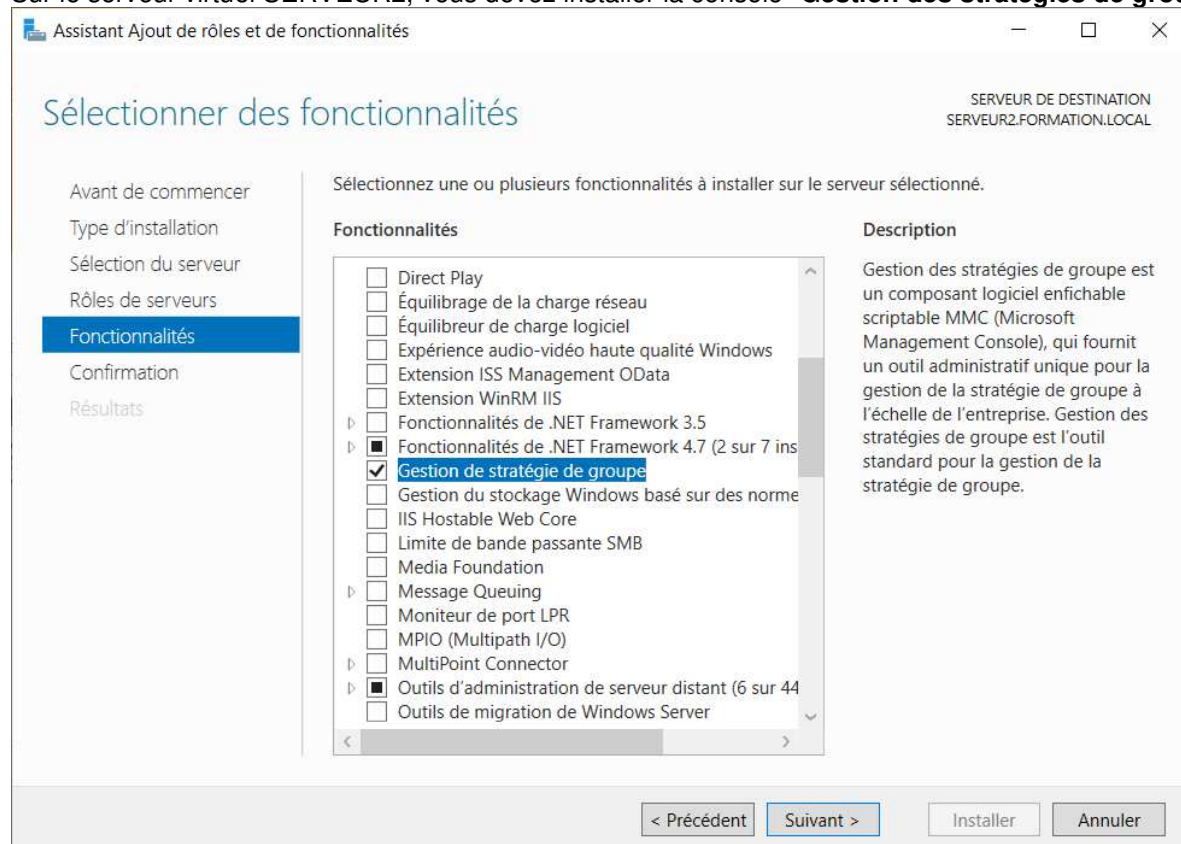
IMPORTANT: sous aucun prétexte les stratégies suivantes ne peuvent être détruites ou modifiées

- Default Domain Controllers Policy
- Default Domain Policy

La console "Gestion des stratégies de groupe"

La console "**Gestion des stratégies de groupe**" est présente par défaut sur le SERVEUR1 parce que c'est le contrôleur de domaine.

Sur le serveur virtuel SERVEUR2, vous devez installer la console "**Gestion des stratégies de groupe**".



Informations sur la GPO "Default Domain Policy"

Aucun paramètre n'est défini dans la section "Configuration utilisateur" de la GPO "Default Domain Policy".

Default Domain Policy

Étendue Détails Paramètres Délégation État

Default Domain Policy
Données recueillies le : 2024-06-04 15:13:09

Général afficher tout

Détails masquer

Liaisons afficher

Filtrage de sécurité afficher

Délégation afficher

Configuration ordinateur (activée) masquer

Stratégies masquer

Paramètres Windows masquer

Paramètres de sécurité afficher

Configuration utilisateur (activée) masquer

Aucun paramètre n'est défini.

Les paramètres de la GPO "Default Domain Policy" s'appliquent sur toutes les OU du domaine.

Ce n'est pas une bonne idée de modifier les paramètres des la GPO "Default Domain Policy".

Ce n'est pas une bonne idée de configurer des GPO au niveau du domaine parce que les paramètres s'appliquent sur toutes les OU du domaine incluant l'untié d'organisation "Domain Controllers".

Informations sur la GPO "Default Domain Controllers Policy"

Aucun paramètre n'est défini dans la section "Configuration utilisateur" de la GPO "Default Domain Controllers Policy".

Default Domain Controllers Policy

Étendue Détails Paramètres Délégation État

Default Domain Controllers Policy
Données recueillies le : 2024-06-04 15:06:42

Général afficher tout

Détails masquer

Liaisons afficher

Filtrage de sécurité afficher

Délégation afficher

Configuration ordinateur (activée) masquer

Stratégies masquer

Paramètres Windows masquer

Paramètres de sécurité afficher

Configuration utilisateur (activée) masquer

Aucun paramètre n'est défini.

Ce n'est pas une bonne idée de modifier les paramètres des la GPO "Default Domain Controllers Policy".

Étape 1a - La GPO "Default Domain Policy"

Les paramètres d'une GPO sont visibles dans l'onglet "**Paramètres**".



Vous pouvez créer un rapport HTM de la GPO "**Default Domain Policy**" dans le dossier E:_GPO_RAPPORTS.

- Vous devez sélectionner la GPO "**Default Domain Policy**" et dans le menu contextuel sélectionner "**Enregistrer le rapport...**".

L'avantage d'un fichier HTM par rapport à l'onglet "**Paramètres**", c'est que vous pouvez effectuer une recherche et vous pouvez l'imprimer.

Étape 1b – Les paramètres de la GPO "Default Domain Policy"

Voici les paramètres de la GPO "Default Domain Policy".

Configuration ordinateur (activée)

Stratégies

Paramètres Windows

Paramètres de sécurité

Stratégies de comptes/ Stratégie de mot de passe

Stratégie	Paramètre
Antériorité maximale du mot de passe	42 jours
Antériorité minimale du mot de passe	1 jours
Appliquer l'historique des mots de passe	24 mots de passe mémorisés
Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé
Le mot de passe doit respecter des exigences de complexité	Activé
Longueur minimale du mot de passe	7 caractères

Stratégies de comptes/ Stratégie de verrouillage du compte

Stratégie	Paramètre
Seuil de verrouillage de comptes	0 tentative d'ouverture de session non valides

Stratégies de comptes/ Stratégie Kerberos

Stratégie	Paramètre
Appliquer les restrictions pour l'ouverture de session	Activé
Durée de vie maximale du ticket d'utilisateur	10 heures
Durée de vie maximale du ticket de service	600 minutes
Durée de vie maximale pour le renouvellement du ticket utilisateur	7 jours
Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur	5 minutes

Stratégies locales/ Options de sécurité

Accès réseau

Stratégie	Paramètre
Accès réseau : permet la traduction de noms/ SID anonymes	Désactivé

Sécurité réseau

Stratégie	Paramètre
Sécurité réseau : ne pas stocker de valeurs de hachage de niveau LAN Manager sur la prochaine modification de mot de passe	Activé
Sécurité réseau : forcer la fermeture de session quand les horaires de connexion expirent	Désactivé

Stratégies de clé publique/ Système de fichiers de chiffrement

Certificats

Émise à	Délivré par	Date d'expiration	Rôles prévus
Administrateur	Administrateur	2123-08-10 19:49:04	Récupération de fichiers

Pour obtenir plus d'informations sur les paramètres, exécutez l'Éditeur d'objet de stratégie de groupe locale.








Les stratégies de mot de passe, les stratégies de verrouillage du compte et les stratégies Kerberos sont définies pour l'ensemble du domaine dans Active Directory.

En utilisant la console "**Gestion des stratégies de groupe**" sélectionner la GPO "**Default Domain Policy**"

- Vous devez choisir "**Modifier...**" dans le menu contextuel.
- Vous devez sélectionner le paramètre.
note: vous devez vous déplacer jusqu'à l'emplacement du paramètre recherché
- Vous devez afficher les propriétés du paramètre et cliquer sur l'onglet "**Expliquer**".

Voici la section que vous devez consulter pour répondre aux prochaines questions.

Configuration ordinateur / Stratégies /
Paramètres Windows / Paramètres de sécurité / Stratégies de comptes / Stratégie de mot de passe

Stratégie	Paramètres de stratégie
 Audit de la longueur minimale du mot de passe	Non défini
 Conserver l'historique des mots de passe	24 mots de passe mémorisés
 Durée de vie maximale du mot de passe	42 jours
 Durée de vie minimale du mot de passe	1 jours
 Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé
 Le mot de passe doit respecter des exigences de complexité	Activé
 Longueur minimale du mot de passe	7 caractère(s)

"**Antériorité maximale du mot de passe**"

42 jours

Quelle est la valeur recommandée pour le paramètre "**Durée de vie maximale du mot de passe**" ?

un délai entre 30 et 90 jours

réponse: _____

Quelle est la valeur maximale pour le paramètre "**Durée de vie maximale du mot de passe**" ?

999 jours

réponse: _____

"**Antériorité minimale du mot de passe**"

1 jours

Que signifie le paramètre "**Durée de vie minimale du mot de passe**" ?

Le nombre de jours avant qu'un utilisateur puisse changer son mot de passe.

réponse: _____

Quelle est la valeur par défaut sur les contrôleurs de domaine ?

1 jours

réponse: _____

Quelle est la valeur par défaut sur les serveurs autonomes ?

0 jours

réponse: _____

Remarque : par défaut, les ordinateurs membres adoptent la configuration de leur contrôleur de domaine.

Appliquer l'historique des mots de passe

24 mots de passe mémorisés

Quelle est la valeur par défaut sur les contrôleurs de domaine ?

24

réponse: _____

Quelle est la valeur par défaut sur les serveurs autonomes ?

0

réponse: _____

Remarque : par défaut, les ordinateurs membres suivent la configuration de leur contrôleur de domaine.

Le mot de passe doit respecter des exigences de complexité

Activé

Quelle est la valeur par défaut sur les contrôleurs de domaine ?

Activé

réponse: _____

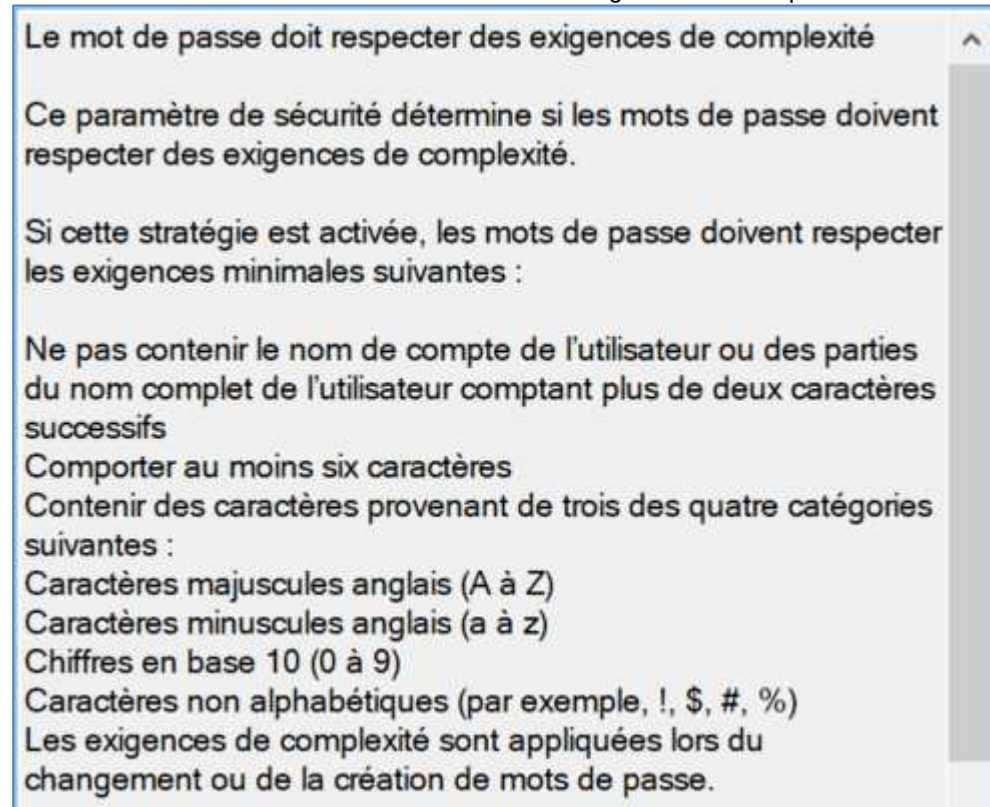
Quelle est la valeur par défaut sur les serveurs autonomes ?

Désactivé

réponse: _____

Remarque : par défaut, les ordinateurs membres adoptent la configuration de leur contrôleur de domaine.

Voici les recommandations de Microsoft sur les exigences de complexité.



The screenshot shows the 'Le mot de passe doit respecter des exigences de complexité' (The password must meet complexity requirements) setting in Windows Security. The setting is currently 'Activé' (On). The text explains that this security parameter determines if passwords must meet complexity requirements. If this strategy is activated, passwords must meet the following minimum requirements:

- Ne pas contenir le nom de compte de l'utilisateur ou des parties du nom complet de l'utilisateur comptant plus de deux caractères successifs
- Comporter au moins six caractères
- Contenir des caractères provenant de trois des quatre catégories suivantes :
 - Caractères majuscules anglais (A à Z)
 - Caractères minuscules anglais (a à z)
 - Chiffres en base 10 (0 à 9)
 - Caractères non alphabétiques (par exemple, !, \$, #, %)

Les exigences de complexité sont appliquées lors du changement ou de la création de mots de passe.

Longueur minimale du mot de passe

7 caractères

Quelle est la valeur par défaut sur les contrôleurs de domaine ?

7

réponse: _____

Quelle est la valeur par défaut sur les serveurs autonomes ?

0

réponse: _____

Remarque : par défaut, les ordinateurs membres adoptent la configuration de leur contrôleur de domaine.

Quelle est la plus grande longueur minimale pour les mots de passe ?




14 caractères

réponse: _____

Voici la section que vous devez consulter pour répondre à la prochaine question.

Configuration ordinateur / Stratégies /

Paramètres Windows / Paramètres de sécurité / Stratégies de comptes / Stratégie de verrouillage du compte

Stratégie	Paramètres de stratégie
 Durée de verrouillage des comptes	Non défini
 Réinitialiser le compteur de verrouillages du compte après	Non défini
 Seuil de verrouillage du compte	0 tentatives d'ouvertures de session non valides

Seuil de verrouillage de comptes

0 tentative d'ouverture de session non valides

Que signifie la valeur 0 pour ce paramètre ?

La valeur 0 signifie que le compte ne se sera jamais verrouillé.

réponse: _____

Quelle est la plus grande valeur pour le seuil de verrouillage de comptes ?

999






réponse: _____

Le paramètre "Seuil de verrouillage de comptes" dans une GPO fonctionne seulement si la GPO est liée au domaine en raison de la manière dont les stratégies de verrouillage de compte sont appliquées dans Active Directory.

Si vous définissez ces paramètres dans une GPO liée à une OU, les contrôleurs de domaine ne prendront pas en compte ces paramètres pour la gestion des tentatives de connexion et du verrouillage des comptes.

Voici l'explication d'un paramètre important de cette GPO.

**Configuration ordinateur / Stratégies /
Paramètres Windows / Paramètres de sécurité / Stratégies de comptes / Stratégie Kerberos**

Stratégie	Paramètres de stratégie
 Appliquer les restrictions pour l'ouverture de session	Activé
 Durée de vie maximale du ticket de service	600 minutes
 Durée de vie maximale du ticket utilisateur	10 minutes
 Durée de vie maximale pour le renouvellement du ticket utilisateur	7 minutes
 Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur	5 minutes

"Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur" 5 minutes

Pour permettre le bon fonctionnement des horodatages, les horloges du client et du contrôleur de domaine doivent être aussi synchronisées que possible. En d'autres termes, les deux ordinateurs doivent être réglés aux mêmes date et heure. **Ce paramètre accepte une marge d'erreur de 5 minutes.**

C'est un paramètre important de l'Active Directory.

Étape 2a - La GPO "Default Domain Controllers Policy"

Les paramètres d'une GPO sont visibles dans l'onglet "Paramètres".



Vous pouvez créer un rapport HTM de la GPO "Default Domain Controllers Policy" dans le dossier E:_GPO_RAPPORTS.

- Vous devez sélectionner la GPO "Default Domain Controllers Policy" et dans le menu contextuel sélectionner "Enregistrer le rapport...".

L'avantage d'un fichier HTM par rapport à l'onglet "Paramètres", c'est que vous pouvez effectuer une recherche et vous pouvez l'imprimer.

Étape 2b – Les paramètres de la GPO "Default Domain Controllers Policy"

Voici les paramètres de la GPO "Default Domain Controllers Policy".

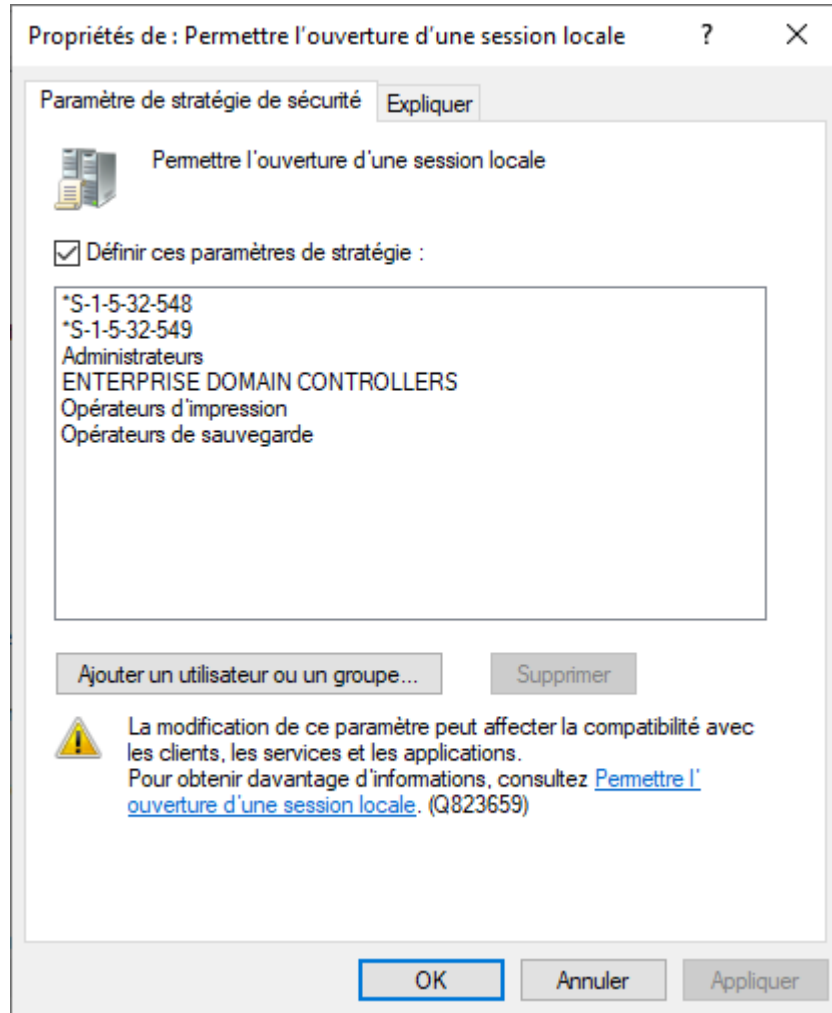
Configuration ordinateur (activée)		masquer
Stratégies		masquer
Paramètres Windows		masquer
Paramètres de sécurité		masquer
Stratégies locales/ Attribution des droits utilisateur		masquer
Stratégie	Paramètre	
Accéder à cet ordinateur à partir du réseau	BUILTIN\Accès compatible pré-Windows 2000, AUTORITE NT\ENTREPRISE DOMAIN CONTROLLERS, AUTORITE NT\Utilisateurs authentifiés, BUILTIN\Administrateurs, Tout le monde	
Ajouter des stations de travail au domaine	AUTORITE NT\Utilisateurs authentifiés	
Ajuster les quotas de mémoire pour un processus	BUILTIN\Administrateurs, AUTORITE NT\SERVICE RÉSEAU, AUTORITE NT\SERVICE LOCAL	
Arrêter le système	BUILTIN\Opérateurs d'impression, BUILTIN\Opérateurs de serveur, BUILTIN\Opérateurs de sauvegarde, BUILTIN\Administrateurs	
Augmenter la priorité de planification	Window Manager\Window Manager Group, BUILTIN\Administrateurs	
Charger et décharger les pilotes de périphériques	BUILTIN\Opérateurs d'impression, BUILTIN\Administrateurs	
Contourner la vérification de parcours	BUILTIN\Accès compatible pré-Windows 2000, AUTORITE NT\Utilisateurs authentifiés, BUILTIN\Administrateurs, AUTORITE NT\SERVICE RÉSEAU, AUTORITE NT\SERVICE LOCAL, Tout le monde	
Créer un fichier d'échange	BUILTIN\Administrateurs	
Déboguer les programmes	BUILTIN\Administrateurs	
Forcer l'arrêt à partir d'un système distant	BUILTIN\Opérateurs de serveur, BUILTIN\Administrateurs	
Générer des audits de sécurité	AUTORITE NT\SERVICE RÉSEAU, AUTORITE NT\SERVICE LOCAL	
Gérer le journal d'audit et de sécurité	BUILTIN\Administrateurs	
Modifier l'heure système	BUILTIN\Opérateurs de serveur, BUILTIN\Administrateurs, AUTORITE NT\SERVICE LOCAL	
Modifier les valeurs de l'environnement du microprogramme	BUILTIN\Administrateurs	
Ouvrir une session en tant que tâche	BUILTIN\Utilisateurs du journal de performances, BUILTIN\Opérateurs de sauvegarde, BUILTIN\Administrateurs	
Performance système du profil	NT SERVICE\Wd\WebHost, BUILTIN\Administrateurs	
Permettre à l'ordinateur et aux comptes d'utilisateurs d'être approuvés pour la délégation	BUILTIN\Administrateurs	
Permettre l'ouverture d'une session locale	AUTORITE NT\ENTREPRISE DOMAIN CONTROLLERS, BUILTIN\Opérateurs d'impression, BUILTIN\Opérateurs de serveur, BUILTIN\Opérateurs de compte, BUILTIN\Opérateurs de sauvegarde, BUILTIN\Administrateurs	
Prendre possession de fichiers ou d'autres objets	BUILTIN\Administrateurs	
Processus unique du profil	BUILTIN\Administrateurs	
Remplacer un jeton de niveau processus	AUTORITE NT\SERVICE RÉSEAU, AUTORITE NT\SERVICE LOCAL	
Restaurer les fichiers et les répertoires	BUILTIN\Opérateurs de serveur, BUILTIN\Opérateurs de sauvegarde, BUILTIN\Administrateurs	
Retirer l'ordinateur de la station d'accueil	BUILTIN\Administrateurs	
Sauvegarder les fichiers et les répertoires	BUILTIN\Opérateurs de serveur, BUILTIN\Opérateurs de sauvegarde, BUILTIN\Administrateurs	

Les paramètres de la section "Attribution des droits utilisateur" servent à déterminer **qui peut faire quoi**.

Voici l'explication d'un paramètre important de cette GPO.

**Configuration ordinateur / Stratégies /
Paramètres Windows / Paramètres de sécurité / Stratégies locales / Attribution des droits utilisateur**

Permettre l'ouverture d'une session locale



Les utilisateurs du domaine ne peuvent pas se connecter sur le "Contrôleur de domaine".

C'est un paramètre important de l'Active Directory.

"Default Domain Policy" et "Default Domain Controllers Policy"

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectifs

- Installer la console "Gestion des stratégies de groupe" sur le SERVEUR2
- Utiliser la console "Gestion des stratégies de groupe"
- Se familiariser avec les objets de stratégie "Default Domain Policy" et "Default Domain Controllers Policy"

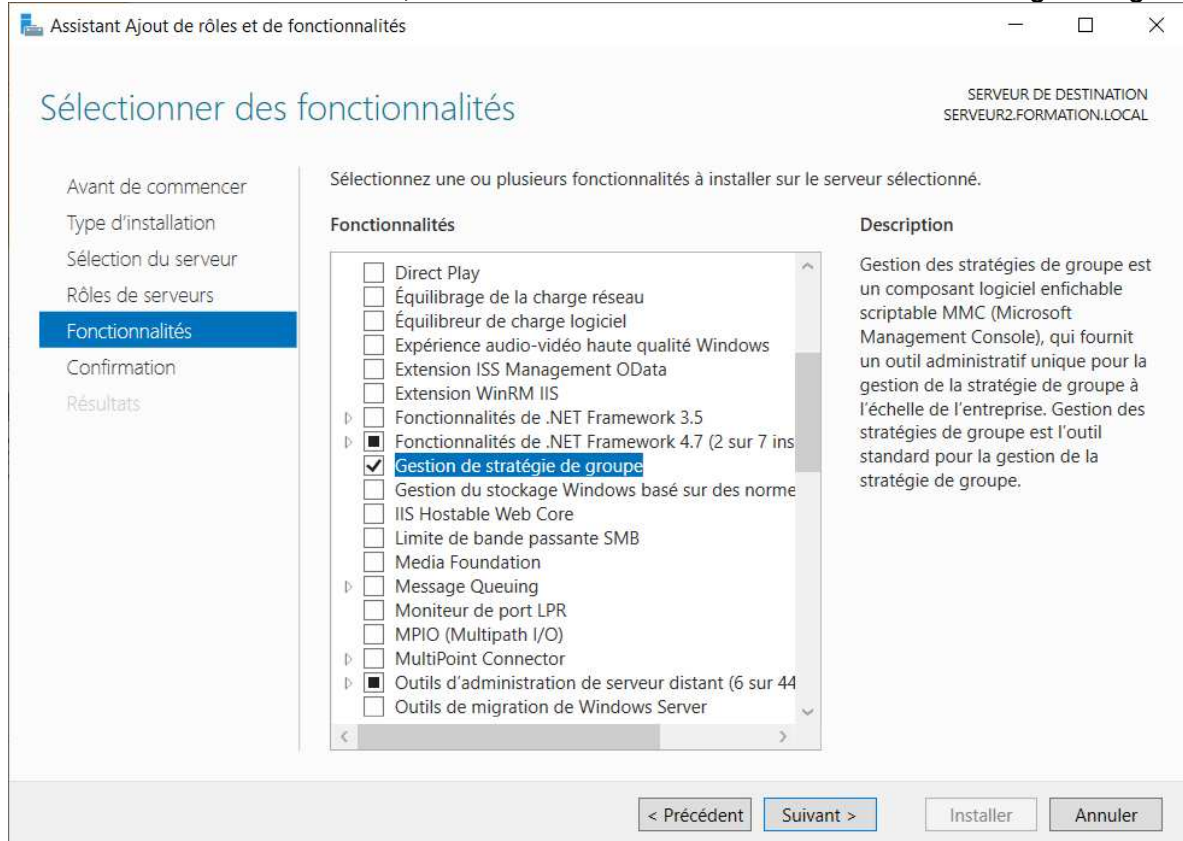
IMPORTANT: sous aucun prétexte les stratégies suivantes ne peuvent être détruites ou modifiées

- Default Domain Controllers Policy
- Default Domain Policy

La console "Gestion des stratégies de groupe"

La console "**Gestion des stratégies de groupe**" est présente par défaut sur le SERVEUR1 parce que c'est le contrôleur de domaine.

Sur le serveur virtuel SERVEUR2, vous devez installer la console "**Gestion des stratégies de groupe**".



Informations sur la GPO "Default Domain Policy"

Aucun paramètre n'est défini dans la section "Configuration utilisateur" de la GPO "Default Domain Policy".

Default Domain Policy

Étendue Détails Paramètres Délégation État

Default Domain Policy
Données recueillies le : 2024-06-04 15:13:09

Général masquer

Détails afficher

Liaisons afficher

Filtrage de sécurité afficher

Délégation afficher

Configuration ordinateur (activée) masquer

Stratégies masquer

Paramètres Windows masquer

Paramètres de sécurité afficher

Configuration utilisateur (activée) masquer

Aucun paramètre n'est défini.

Les paramètres de la GPO "Default Domain Policy" s'appliquent sur toutes les OU du domaine.

Ce n'est pas une bonne idée de modifier les paramètres des la GPO "Default Domain Policy".

Ce n'est pas une bonne idée de configurer des GPO au niveau du domaine parce que les paramètres s'appliquent sur toutes les OU du domaine incluant l'untié d'organisation "Domain Controllers".

Informations sur la GPO "Default Domain Controllers Policy"

Aucun paramètre n'est défini dans la section "Configuration utilisateur" de la GPO "Default Domain Controllers Policy".

Default Domain Controllers Policy

Étendue Détails Paramètres Délégation État

Default Domain Controllers Policy
Données recueillies le : 2024-06-04 15:06:42

Général masquer

Détails afficher

Liaisons afficher

Filtrage de sécurité afficher

Délégation afficher

Configuration ordinateur (activée) masquer

Stratégies masquer

Paramètres Windows masquer

Paramètres de sécurité afficher

Configuration utilisateur (activée) masquer

Aucun paramètre n'est défini.

Ce n'est pas une bonne idée de modifier les paramètres de la GPO "Default Domain Controllers Policy".

Étape 1a - La GPO "Default Domain Policy"

Les paramètres d'une GPO sont visibles dans l'onglet "**Paramètres**".



Vous pouvez créer un rapport HTM de la GPO "**Default Domain Policy**" dans le dossier E:_GPO_RAPPORTS.

- Vous devez sélectionner la GPO "**Default Domain Policy**" et dans le menu contextuel sélectionner "**Enregistrer le rapport...**".

L'avantage d'un fichier HTM par rapport à l'onglet "**Paramètres**", c'est que vous pouvez effectuer une recherche et vous pouvez l'imprimer.

Étape 1b – Les paramètres de la GPO "Default Domain Policy"

Voici les paramètres de la GPO "Default Domain Policy".

Configuration ordinateur (activée)

Stratégies

Paramètres Windows

Paramètres de sécurité

Stratégies de comptes/ Stratégie de mot de passe

Stratégie	Paramètre
Antériorité maximale du mot de passe	42 jours
Antériorité minimale du mot de passe	1 jours
Appliquer l'historique des mots de passe	24 mots de passe mémorisés
Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé
Le mot de passe doit respecter des exigences de complexité	Activé
Longueur minimale du mot de passe	7 caractères

Stratégies de comptes/ Stratégie de verrouillage du compte

Stratégie	Paramètre
Seuil de verrouillage de comptes	0 tentative d'ouverture de session non valides

Stratégies de comptes/ Stratégie Kerberos

Stratégie	Paramètre
Appliquer les restrictions pour l'ouverture de session	Activé
Durée de vie maximale du ticket d'utilisateur	10 heures
Durée de vie maximale du ticket de service	600 minutes
Durée de vie maximale pour le renouvellement du ticket utilisateur	7 jours
Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur	5 minutes

Stratégies locales/ Options de sécurité

Accès réseau

Stratégie	Paramètre
Accès réseau : permet la traduction de noms/ SID anonymes	Désactivé

Sécurité réseau

Stratégie	Paramètre
Sécurité réseau : ne pas stocker de valeurs de hachage de niveau LAN Manager sur la prochaine modification de mot de passe	Activé
Sécurité réseau : forcer la fermeture de session quand les horaires de connexion expirent	Désactivé

Stratégies de clé publique/ Système de fichiers de chiffrement

Certificats

Émise à	Délivré par	Date d'expiration	Rôles prévus
Administrateur	Administrateur	2123-08-10 19:49:04	Récupération de fichiers

Pour obtenir plus d'informations sur les paramètres, exécutez l'Éditeur d'objet de stratégie de groupe locale.








Les stratégies de mot de passe, les stratégies de verrouillage du compte et les stratégies Kerberos sont définies pour l'ensemble du domaine dans Active Directory.

En utilisant la console "**Gestion des stratégies de groupe**" sélectionner la GPO "**Default Domain Policy**"

- Vous devez choisir "**Modifier...**" dans le menu contextuel.
- Vous devez sélectionner le paramètre.
note: vous devez vous déplacer jusqu'à l'emplacement du paramètre recherché
- Vous devez afficher les propriétés du paramètre et cliquer sur l'onglet "**Expliquer**".

Voici la section que vous devez consulter pour répondre aux prochaines questions.

Configuration ordinateur / Stratégies /
Paramètres Windows / Paramètres de sécurité / Stratégies de comptes / Stratégie de mot de passe

Stratégie	Paramètres de stratégie
 Audit de la longueur minimale du mot de passe	Non défini
 Conserver l'historique des mots de passe	24 mots de passe mémorisés
 Durée de vie maximale du mot de passe	42 jours
 Durée de vie minimale du mot de passe	1 jours
 Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé
 Le mot de passe doit respecter des exigences de complexité	Activé
 Longueur minimale du mot de passe	7 caractère(s)

"Antériorité maximale du mot de passe" 42 jours

Quelle est la valeur recommandée pour le paramètre "**Durée de vie maximale du mot de passe**" ?

réponse: _____

Quelle est la valeur maximale pour le paramètre "**Durée de vie maximale du mot de passe**" ?

réponse: _____

"Antériorité minimale du mot de passe" 1 jours

Que signifie le paramètre "**Durée de vie minimale du mot de passe**" ?

réponse: _____

Quelle est la valeur par défaut sur les contrôleurs de domaine ?

réponse: _____

Quelle est la valeur par défaut sur les serveurs autonomes ?

réponse: _____

Remarque : par défaut, les ordinateurs membres adoptent la configuration de leur contrôleur de domaine.

Appliquer l'historique des mots de passe

24 mots de passe mémorisés

Quelle est la valeur par défaut sur les contrôleurs de domaine ?

réponse: _____

Quelle est la valeur par défaut sur les serveurs autonomes ?

réponse: _____

Remarque : par défaut, les ordinateurs membres suivent la configuration de leur contrôleur de domaine.

Le mot de passe doit respecter des exigences de complexité

Activé

Quelle est la valeur par défaut sur les contrôleurs de domaine ?

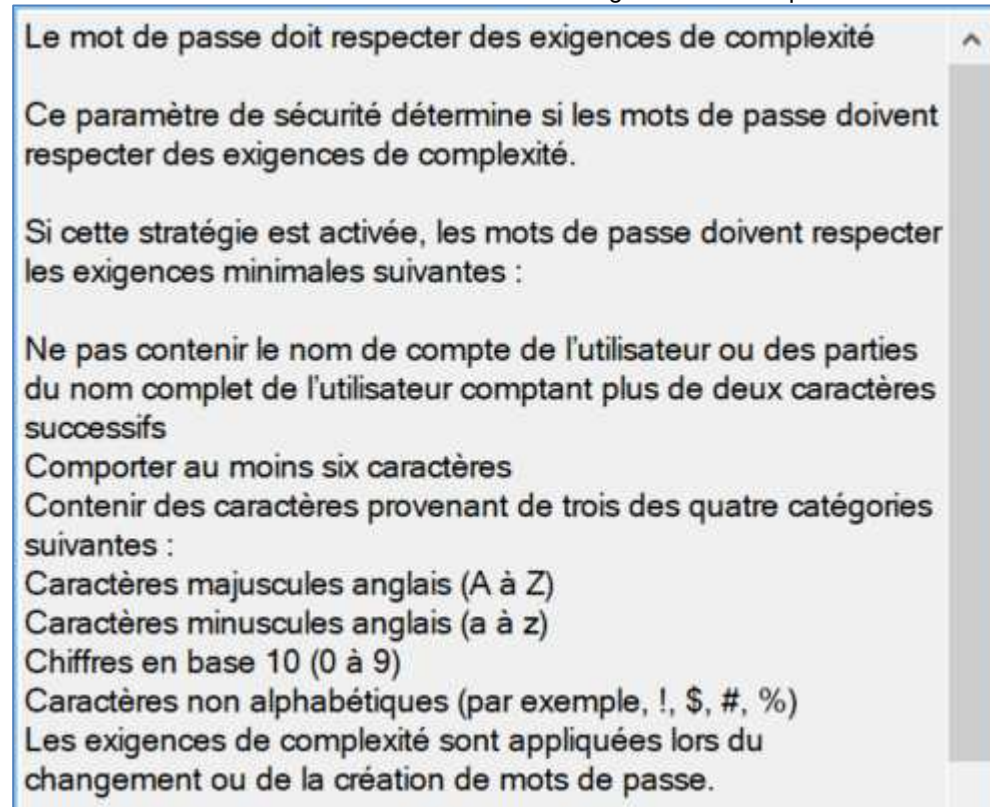
réponse: _____

Quelle est la valeur par défaut sur les serveurs autonomes ?

réponse: _____

Remarque : par défaut, les ordinateurs membres adoptent la configuration de leur contrôleur de domaine.

Voici les recommandations de Microsoft sur les exigences de complexité.



The screenshot shows a Windows Security notification window titled "Le mot de passe doit respecter des exigences de complexité". The text inside explains that this security parameter determines if passwords must meet complexity requirements. It lists the minimum requirements when the strategy is active: passwords must not contain the user's account name or full name (more than two consecutive characters), must be at least six characters long, and must contain characters from three of the four categories: English uppercase letters (A-Z), English lowercase letters (a-z), base 10 digits (0-9), and non-alphabetic characters (e.g., !, \$, #, %). It concludes by stating that these requirements are applied during password changes or creation.

Le mot de passe doit respecter des exigences de complexité

Ce paramètre de sécurité détermine si les mots de passe doivent respecter des exigences de complexité.

Si cette stratégie est activée, les mots de passe doivent respecter les exigences minimales suivantes :

- Ne pas contenir le nom de compte de l'utilisateur ou des parties du nom complet de l'utilisateur comptant plus de deux caractères successifs
- Comporter au moins six caractères
- Contenir des caractères provenant de trois des quatre catégories suivantes :
- Caractères majuscules anglais (A à Z)
- Caractères minuscules anglais (a à z)
- Chiffres en base 10 (0 à 9)
- Caractères non alphabétiques (par exemple, !, \$, #, %)

Les exigences de complexité sont appliquées lors du changement ou de la création de mots de passe.

Longueur minimale du mot de passe

7 caractères

Quelle est la valeur par défaut sur les contrôleurs de domaine ?

réponse: _____

Quelle est la valeur par défaut sur les serveurs autonomes ?

réponse: _____


Remarque : par défaut, les ordinateurs membres adoptent la configuration de leur contrôleur de domaine.

Quelle est la plus grande longueur minimale pour les mots de passe ?

réponse: _____

Voici la section que vous devez consulter pour répondre à la prochaine question.

Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies de comptes / Stratégie de verrouillage du compte

Stratégie	Paramètres de stratégie
 Durée de verrouillage des comptes	Non défini
 Réinitialiser le compteur de verrouillages du compte après	Non défini
 Seuil de verrouillage du compte	0 tentatives d'ouvertures de session non valides

Seuil de verrouillage de comptes

0 tentative d'ouverture de session non valides

Que signifie la valeur 0 pour ce paramètre ?

réponse: _____

Quelle est la plus grande valeur pour le seuil de verrouillage de comptes ?






réponse: _____

Le paramètre "Seuil de verrouillage de comptes" dans une GPO fonctionne seulement si la GPO est liée au domaine en raison de la manière dont les stratégies de verrouillage de compte sont appliquées dans Active Directory.

Si vous définissez ces paramètres dans une GPO liée à une OU, les contrôleurs de domaine ne prendront pas en compte ces paramètres pour la gestion des tentatives de connexion et du verrouillage des comptes.

Voici l'explication d'un paramètre important de cette GPO.

**Configuration ordinateur / Stratégies /
Paramètres Windows / Paramètres de sécurité / Stratégies de comptes / Stratégie Kerberos**

Stratégie	Paramètres de stratégie
 Appliquer les restrictions pour l'ouverture de session	Activé
 Durée de vie maximale du ticket de service	600 minutes
 Durée de vie maximale du ticket utilisateur	10 minutes
 Durée de vie maximale pour le renouvellement du ticket utilisateur	7 minutes
 Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur	5 minutes

"Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur" 5 minutes

Pour permettre le bon fonctionnement des horodatages, les horloges du client et du contrôleur de domaine doivent être aussi synchronisées que possible. En d'autres termes, les deux ordinateurs doivent être réglés aux mêmes date et heure. **Ce paramètre accepte une marge d'erreur de 5 minutes.**

C'est un paramètre important de l'Active Directory.

Étape 2a - La GPO "Default Domain Controllers Policy"

Les paramètres d'une GPO sont visibles dans l'onglet "Paramètres".



Vous pouvez créer un rapport HTM de la GPO "Default Domain Controllers Policy" dans le dossier E:_GPO_RAPPORTS.

- Vous devez sélectionner la GPO "Default Domain Controllers Policy" et dans le menu contextuel sélectionner "Enregistrer le rapport...".

L'avantage d'un fichier HTM par rapport à l'onglet "Paramètres", c'est que vous pouvez effectuer une recherche et vous pouvez l'imprimer.

Étape 2b – Les paramètres de la GPO "Default Domain Controllers Policy"

Voici les paramètres de la GPO "Default Domain Controllers Policy".

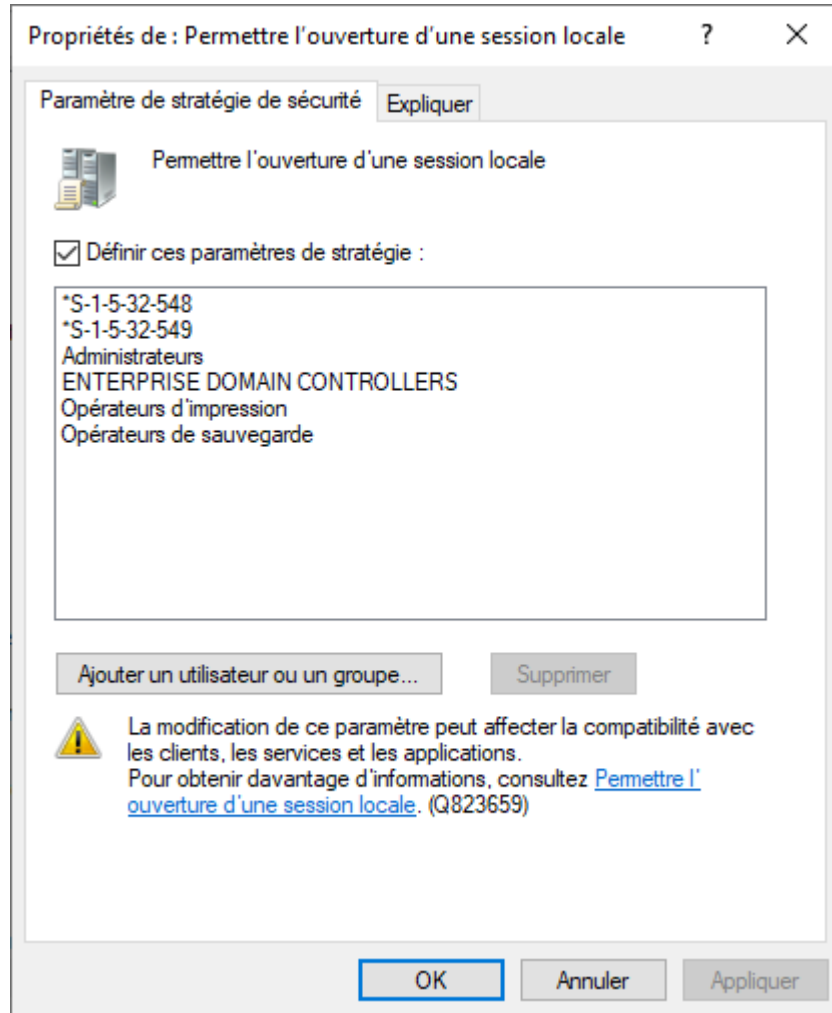
Configuration ordinateur (activée)		masquer
Stratégies		masquer
Paramètres Windows		masquer
Paramètres de sécurité		masquer
Stratégies locales/ Attribution des droits utilisateur		masquer
Stratégie	Paramètre	
Accéder à cet ordinateur à partir du réseau	BUILTIN\Accès compatible pré-Windows 2000, AUTORITE NT\ENTERPRISE DOMAIN CONTROLLERS, AUTORITE NT\Utilisateurs authentifiés, BUILTIN\Administrateurs, Tout le monde	
Ajouter des stations de travail au domaine	AUTORITE NT\Utilisateurs authentifiés	
Ajuster les quotas de mémoire pour un processus	BUILTIN\Administrateurs, AUTORITE NT\SERVICE RÉSEAU, AUTORITE NT\SERVICE LOCAL	
Arrêter le système	BUILTIN\Opérateurs d'impression, BUILTIN\Opérateurs de serveur, BUILTIN\Opérateurs de sauvegarde, BUILTIN\Administrateurs	
Augmenter la priorité de planification	Window Manager\Window Manager Group, BUILTIN\Administrateurs	
Charger et décharger les pilotes de périphériques	BUILTIN\Opérateurs d'impression, BUILTIN\Administrateurs	
Contourner la vérification de parcours	BUILTIN\Accès compatible pré-Windows 2000, AUTORITE NT\Utilisateurs authentifiés, BUILTIN\Administrateurs, AUTORITE NT\SERVICE RÉSEAU, AUTORITE NT\SERVICE LOCAL, Tout le monde	
Créer un fichier d'échange	BUILTIN\Administrateurs	
Déboguer les programmes	BUILTIN\Administrateurs	
Forcer l'arrêt à partir d'un système distant	BUILTIN\Opérateurs de serveur, BUILTIN\Administrateurs	
Générer des audits de sécurité	AUTORITE NT\SERVICE RÉSEAU, AUTORITE NT\SERVICE LOCAL	
Gérer le journal d'audit et de sécurité	BUILTIN\Administrateurs	
Modifier l'heure système	BUILTIN\Opérateurs de serveur, BUILTIN\Administrateurs, AUTORITE NT\SERVICE LOCAL	
Modifier les valeurs de l'environnement du microprogramme	BUILTIN\Administrateurs	
Ouvrir une session en tant que tâche	BUILTIN\Utilisateurs du journal de performances, BUILTIN\Opérateurs de sauvegarde, BUILTIN\Administrateurs	
Performance système du profil	NT SERVICE\Wd\WebHost, BUILTIN\Administrateurs	
Permettre à l'ordinateur et aux comptes d'utilisateurs d'être approuvés pour la délégation	BUILTIN\Administrateurs	
Permettre l'ouverture d'une session locale	AUTORITE NT\ENTERPRISE DOMAIN CONTROLLERS, BUILTIN\Opérateurs d'impression, BUILTIN\Opérateurs de serveur, BUILTIN\Opérateurs de compte, BUILTIN\Opérateurs de sauvegarde, BUILTIN\Administrateurs	
Prendre possession de fichiers ou d'autres objets	BUILTIN\Administrateurs	
Processus unique du profil	BUILTIN\Administrateurs	
Remplacer un jeton de niveau processus	AUTORITE NT\SERVICE RÉSEAU, AUTORITE NT\SERVICE LOCAL	
Restaurer les fichiers et les répertoires	BUILTIN\Opérateurs de serveur, BUILTIN\Opérateurs de sauvegarde, BUILTIN\Administrateurs	
Retirer l'ordinateur de la station d'accueil	BUILTIN\Administrateurs	
Sauvegarder les fichiers et les répertoires	BUILTIN\Opérateurs de serveur, BUILTIN\Opérateurs de sauvegarde, BUILTIN\Administrateurs	

Les paramètres de la section "Attribution des droits utilisateur" servent à déterminer qui peut faire quoi.

Voici l'explication d'un paramètre important de cette GPO.

**Configuration ordinateur / Stratégies /
Paramètres Windows / Paramètres de sécurité / Stratégies locales / Attribution des droits utilisateur**

Permettre l'ouverture d'une session locale



Les utilisateurs du domaine ne peuvent pas se connecter sur le "Contrôleur de domaine".

C'est un paramètre important de l'Active Directory.

Stratégie de groupe locale avec Windows

Le service "Client de stratégie de groupe" (gpsvc) est responsable de l'application des paramètres configurés par les administrateurs pour les ordinateurs et pour les utilisateurs.

Les fichiers ADMX et ADML

- les fichiers ADMX sont dans le dossier c:\windows\PolicyDefinitions
les fichiers ADMX sont basés sur un format XML
- les fichiers ADML sont dans le dossier c:\windows\PolicyDefinitions\fr-FR
les fichiers ADML sont des fichiers spécifiques à la langue

On peut ajouter des fichiers ADMX et ADML supplémentaires.

Microsoft distribue des fichiers ADMX et ADML "**Microsoft Office**"

"Administrative Template files (ADMX/ADML) for Microsoft 365 Apps for enterprise/Office LTSC 2021/Office 2019/Office 2016 and the Office Customization Tool for Office 2016"

- admintemplates_x64_5452-1000_en-us.exe
- office2016grouppolicyandocsettings.xlsx

Microsoft distribue des fichiers ADMX et ADML pour "**Edge Chromium**".

- MicrosoftEdgePolicyTemplates.zip

Microsoft distribue des fichiers ADMX et ADML pour "**PowerToys**".

- GroupPolicyObjectsFiles-0.82.1.zip

Google distribue des fichiers ADMX et ADML pour "**Chrome**".

- policy_templates.zip

Lien entre stratégie de groupe locale et le registre

La "Stratégie de groupe locale" permet de configurer des restrictions pour l'utilisation de Windows en spécifiant des paramètres à appliquer à l'ordinateur ou à l'utilisateur.

Lorsqu'on configure un paramètre de la stratégie de groupe locale on modifie une clé de registre.

Les clés du registre pour la "Configuration utilisateur":

- HKEY_CURRENT_USER\Software\Policies
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies

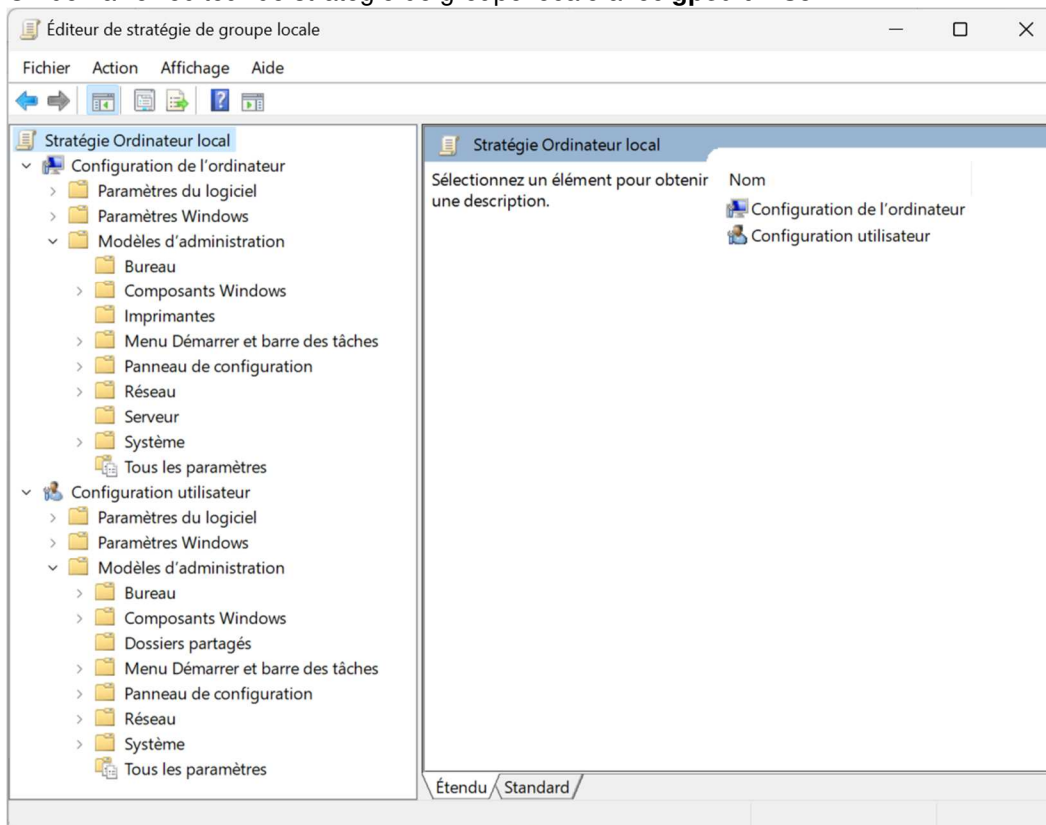
Les clés du registre pour la "Configuration ordinateur":

- HKEY_LOCAL_MACHINE\Software\Policies
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies

"Windows Serveur 2019" et "Windows 10" permettent de configurer environ 4500 stratégies.

Les paramètres qui sont dans les Stratégies ne peuvent pas être modifiés par l'utilisateur.

On démarre l'éditeur de stratégie de groupe locale avec **gpedit.msc**.



Configuration ordinateur / Stratégies / Modèles d'administration / **Tous les paramètres**
Configuration utilisateur / Stratégies / Modèles d'administration / **Tous les paramètres**

GPEDIT.MSC et la "Configuration ordinateur"

- Lorsque l'on configure la partie "**Configuration ordinateur**", elle s'applique que si la GPO est liée à une OU contenant des ordinateurs.
- **Les paramètres de la stratégie de l'ordinateur sont appliqués lors du démarrage du poste et mis à jour aux 90 minutes avec un décalage aléatoire compris entre 0 et 30 minutes sur les postes clients mais aux 5 minutes sur le contrôleur de domaine.**

Les fichiers POL pour la configuration ordinateur

- %ALLUSERSPROFILE%\ntuser.pol
- %windir%\system32\GroupPolicy\Machine\Registry.pol

GPEDIT.MSC et la "Configuration utilisateur"

- Lorsque l'on configure la partie "**Configuration utilisateur**", elle s'applique que si la GPO est liée à une OU contenant des utilisateurs.
- **Les paramètres de la stratégie utilisateur sont appliqués à l'ouverture d'une session et mis à jour aux 90 minutes avec un décalage aléatoire compris entre 0 et 30 minutes sur les postes clients mais aux 5 minutes sur le contrôleur de domaine.**

Les fichiers POL de la configuration utilisateur

- %USERPROFILE%\ntuser.pol
- %windir%\system32\GroupPolicy\User\Registry.pol

Les outils avec une interface graphique

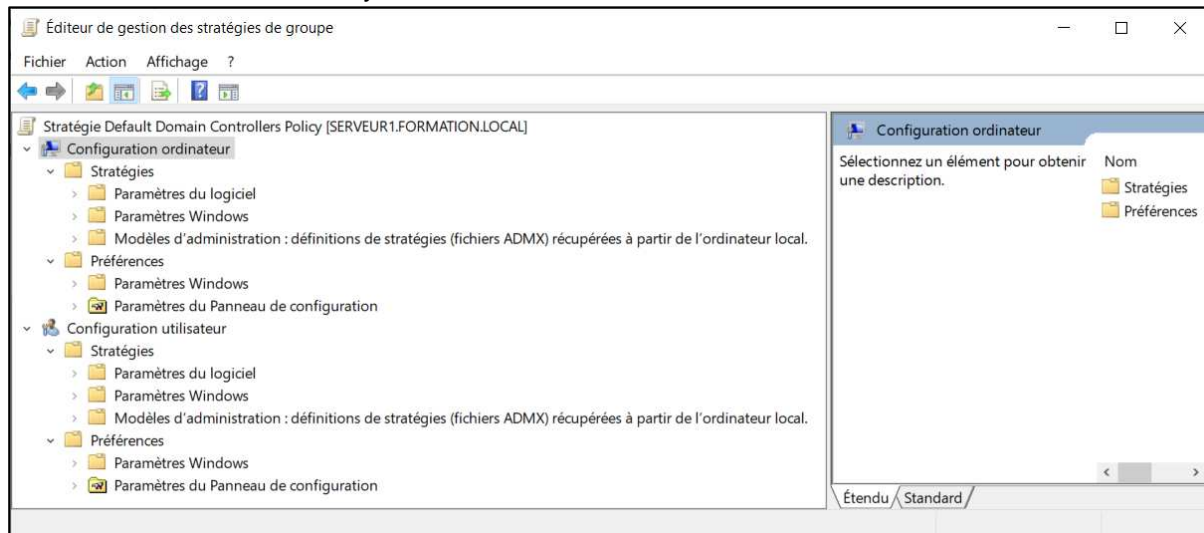
- **gpedit.msc** est l'éditeur de stratégie de groupe locale
- **rsop.msc**
Cet outil affiche le jeu de stratégies résultant (RSoP).
Cet outil ne permet pas de sauvegarder le résultat.
RSOP (Resultant Set of Policy)

Les programmes sans interface graphique

- **gpresult.exe**
Cet outil de ligne de commande affiche le jeu de stratégies résultant (RSoP).
Cet outil permet de sauvegarder le résultat de la commande dans un fichier HTML.
 - **gpupdate.exe**
Cet outil met à jour les paramètres de stratégie de groupe.
-

Les GPO dans un domaine

Les stratégies de groupe permettent une gestion centralisée des ordinateurs et des utilisateurs dans un environnement Active Directory.



Dans un domaine, un administrateur peut configurer des Stratégies et des Préférences.

Les paramètres qui sont dans les Préférence peuvent être modifiés par l'utilisateur.

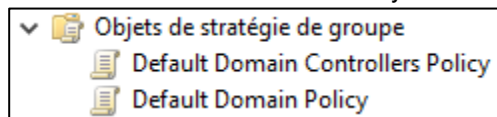
Une GPO peut être liée

- à une OU → on la voit sous la OU
- à plusieurs OU → on la voit sous chaque OU
- à aucune OU → on la voit seulement dans la section OSG (Objets de stratégie de groupe)

Les GPO sont emmagasinées dans SYSVOL.

Dans un domaine, il existe deux GPO par défaut:

- Default Domain Policy
- Default Domain Controllers Policy



Pour une question de performance, Microsoft limite à 999 le nombre de GPO qui peuvent être appliquées à un ordinateur ou à un utilisateur.

Documentation sur l'ordre d'exécution des GPO

L'ordre d'exécution des GPO respecte la formule LSDOU.

- L pour "Local"
- S pour "Site"
- D pour "Domain"
- OU pour "Organizational Unit"

exemples

- Il est possible de gérer l'accès aux périphériques amovibles (USB, CD-RW, DVD-RW, ...) si on modifie un des nombreux paramètres dans

Configuration ordinateur / Stratégies /
Modèles d'administration / Système / Accès au stockage amovible

Exemples de paramètres intéressants

Disques amovibles: refuser l'accès en écriture
Disques amovibles: refuser l'accès en exécution
Disques amovibles: refuser l'accès en lecture

- Il est possible de modifier plusieurs paramètres pour gérer les stratégies de groupe.

Configuration ordinateur / Stratégies /
Modèles d'administration / Système / Stratégie de groupe

Exemples de paramètres intéressants

Définir l'intervalle d'actualisation de la stratégie de groupe pour les contrôleurs de domaine
Définir l'intervalle d'actualisation de la stratégie de groupe pour les ordinateurs
Désactiver le jeu de stratégie résultant
Désactiver le traitement des objets de stratégie de groupe locaux

Configuration utilisateur / Stratégies /
Modèles d'administration / Système / Stratégie de groupe

Exemples de paramètres intéressants

Définir l'intervalle d'actualisation de la stratégie de groupe pour les utilisateurs
Déterminer si les utilisateurs interactifs peuvent générer des données de jeu de stratégie résultant

Les bonnes pratiques pour la gestion des GPO

- 1) Ne modifiez pas les stratégies "**Default Domain Policy**" et "**Default Domain Controller Policy**".
- 2) Votre structure Active Directory doit faciliter l'application des stratégies.
La conception d'UO a une incidence sur le déploiement des stratégies de groupe.
Il est important de ne pas mélanger les utilisateurs et les ordinateurs dans une même UO.
Ne gardez pas les utilisateurs et les ordinateurs dans les conteneurs "**Users**" et "**Computers**".
- 3) Vous devez donner des noms significatifs à vos stratégies.

Les stratégies qui s'appliquent à des utilisateurs	U nom_de_la_GPO
Les stratégies qui s'appliquent à des ordinateurs	C nom_de_la_GPO
Les préférences qui s'appliquent à des utilisateurs	PU nom_de_la_GPO
Les préférences qui s'appliquent à des ordinateurs	PC nom_de_la_GPO
- 4) Il est recommandé d'ajouter des commentaires à vos stratégies.
- 5) Vous devez éviter de créer des stratégies au niveau du domaine.
Parce que les stratégies s'appliquent à tous les utilisateurs et à tous les ordinateurs du domaine.
- 6) Il est préférable de créer plusieurs petites stratégies qui ont des paramètres communs.
 - mot de passe
 - sécurité
 - ...
- 7) Vous devez éviter de configurer le même paramètre dans des GPO différentes.
- 8) Pour augmenter la vitesse d'application des stratégies
Il faut désactiver les paramètres de configuration ordinateurs si la stratégie n'a aucun paramètre dans la section "**Configuration ordinateur**".

État GPO :	Paramètres de configuration ordinateurs désact
Commentaire :	Activé Paramètres de configuration ordinateurs désact Paramètres de configuration utilisateurs désact Tous les paramètres désactivés

Il faut désactiver les paramètres de configuration utilisateurs si la stratégie n'a aucun paramètre dans la section "**Configuration utilisateur**".

État GPO :	Paramètres de configuration utilisateurs désa
Commentaire :	Activé Paramètres de configuration ordinateurs désact Paramètres de configuration utilisateurs désact Tous les paramètres désactivés

La sauvegarde et la restauration des GPO

Ce laboratoire doit être fait individuellement sur le SEVEUR2

Objectif

- Apprendre à lire le contenu du fichier manifest.xml
- Sauvegarder et restaurer des GPO dans un domaine

Mise en place

Vous devez créer les dossiers E:_GPO_BACKUP et E:_GPO_BACKUP_PS.

Créer une sauvegarde des GPO en utilisant PowerShell

La commande pour sauvegarder la GPO "C_DisableRDP"

- Emplacement: le dossier E:_GPO_BACKUP_PS
note: le dossier utilisé pour les backups doit obligatoirement exister
- Description: "La GPO désactive le Bureau à distance"

```
Backup-GPO -Name "C_DisableRDP" `
            -Path E:\_GPO_BACKUP_PS `
            -Comment "La GPO désactive le Bureau à distance"
```

Créer une sauvegarde des GPO en utilisant la console

Vous devez créer une copie de sécurité de la GPO "C_Serveurs_Fichiers" dans le dossier E:_GPO_BACKUP.

- Dans le menu contextuel de la GPO "C_Serveurs_Fichiers"
 - Vous devez sélectionner l'option "Sauvegarder..."

Supprimer une GPO et la récupérer dans la sauvegarde en utilisant la console

Vous devez supprimer la GPO "C_Serveurs_Fichiers".

- Dans le menu contextuel de "Objets de stratégie de groupe"
 - Vous devez sélectionner l'option "Gérer les sauvegardes..."

Vous devez restaurer la GPO "C_Serveurs_Fichiers".

Vous devez lier la GPO "C_Serveurs_Fichiers" à l'unité d'organisation

"OU=FICHIERS,OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL".

Informations sur la structure du fichier manifest.xml

Quand on effectue une sauvegarde de nos stratégies de groupe, à la racine de notre dossier un fichier "**manifest.xml**" est créé.

Ce fichier a la structure suivante:

- Backups
 - BackupInst
 - ❖ GPOGuid
 - ❖ GPODomain
 - ❖ GPODomainGuid
 - ❖ GPODomainController
 - ❖ BackupTime
 - ❖ ID
 - ❖ Comment
 - ❖ GPODisplayName

Pour exécuter le cmdlet Import-GPO, nous avons besoin du contenu de la balise "**GPODisplayName**" ou de la balise "**ID**".

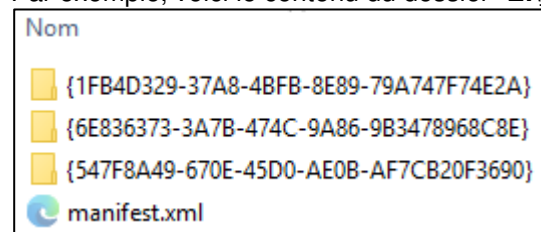
Avant de commencer, vous devez sauvegarder les GPO suivantes dans le dossier "**E:_GPO_BACKUP\UTILISATEURS**".

- PU_EMPLOYES
- PU_INFORMATIQUE_CIBLAGE_EMP09_EMP20
- U_EMPLOYES

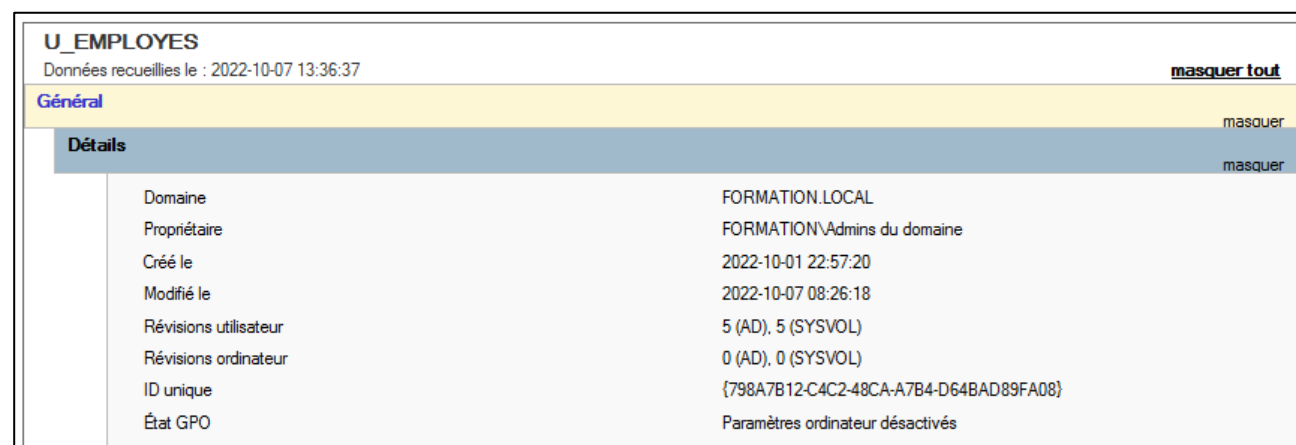
Informations

La sauvegarde des GPO génère un fichier manifest.xml et des dossiers dont le nom ne correspond pas au nom des stratégies.

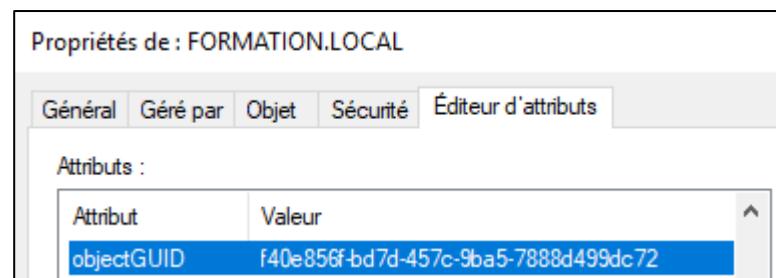
Par exemple, voici le contenu du dossier "E:\GPO_BACKUP\UTILISATEURS".



Le nom de chaque dossier correspond à la balise "ID" du fichier manifest.xml.



La valeur de "ID unique" correspond à la balise "GPOGuid" du fichier manifest.xml.



La valeur de l'attribut "objectGUID" du domaine correspond à la balise "GPODomainGuid" du fichier manifest.xml.

Voici un script PowerShell qui va lire le contenu d'un fichier "manifest.xml" et afficher toutes les informations des stratégies qui sont dans le dossier de la sauvegarde.

```
# Le chemin complet du fichier MANIFEST.XML
$xmlPath = 'E:\_GPO_BACKUP\UTILISATEURS\manifest.xml'

$xml = [xml](Get-Content -Path $xmlPath -Encoding UTF8)
$xmlExpanded = $xml.DocumentElement.BackupInst

Write-Host $("-" * 80) -ForegroundColor Cyan

foreach ($item in $xmlExpanded)
{
    "GPOGuid           = " + $item.GPOGuid.InnerText
    "GPODomain         = " + $item.GPODomain.InnerText
    "GPODomainGuid     = " + $item.GPODomainGuid.InnerText
    "GPODomainController = " + $item.GPODomainController.InnerText
    "BackupTime        = " + $item.BackupTime.InnerText
    "ID                = " + $item.ID.InnerText
    "Comment           = " + $item.Comment.InnerText
    "GPODisplayName    = " + $item.GPODisplayName.InnerText

    Write-Host $("-" * 80) -ForegroundColor Cyan
}
```

```
-----
GPOGuid           = {AD1087E6-426F-4982-8045-1063C4F5069F}
GPODomain         = FORMATION.LOCAL
GPODomainGuid     = {f40e856f-bd7d-457c-9ba5-7888d499dc72}
GPODomainController = SERVEUR1.FORMATION.LOCAL
BackupTime        = 2022-10-17T16:30:27
ID                = {6E836373-3A7B-474C-9A86-9B3478968C8E}
Comment           = Version 2
GPODisplayName    = U_EMPLOYES
-----
GPOGuid           = {652AB980-1E74-4E67-A173-92BE27EA206B}
GPODomain         = FORMATION.LOCAL
GPODomainGuid     = {f40e856f-bd7d-457c-9ba5-7888d499dc72}
GPODomainController = SERVEUR1.FORMATION.LOCAL
BackupTime        = 2022-10-02T03:48:51
ID                = {1FB4D329-37A8-48FB-8E89-79A747F74E2A}
Comment           = PU_INFORMATIQUE_CIBLAGE_EMP09_EMP20
GPODisplayName    = PU_INFORMATIQUE_CIBLAGE_EMP09_EMP20
-----
GPOGuid           = {D826A6C3-19A9-4645-9121-17EC495A09FE}
GPODomain         = FORMATION.LOCAL
GPODomainGuid     = {f40e856f-bd7d-457c-9ba5-7888d499dc72}
GPODomainController = SERVEUR1.FORMATION.LOCAL
BackupTime        = 2022-10-02T03:48:36
ID                = {547F8A49-670E-45D0-AE0B-AF7CB20F3690}
Comment           = PU_EMPLOYES
GPODisplayName    = PU_EMPLOYES
-----
```

Restauration d'une GPO par programmation PowerShell

Il existe deux cmdlets pour importer des GPO: Import-GPO ou Restore-GPO.

Import-GPO

- Import-GPO permet de restaurer une GPO en utilisant un nom différent de l'original.
- La restauration d'une GPO peut se faire dans un domaine ou une forêt différente de la sauvegarde qui a été faite et n'a pas besoin d'exister.

Restore-GPO

- Restore-GPO permet de restaurer une ou plusieurs GPO dans un domaine à condition que les GPO proviennent du même domaine.
- Si le domaine original n'est pas disponible ou si la GPO n'existe plus dans le domaine alors le cmdlet génère une erreur.

Il est préférable d'utiliser Import-GPO.

Exemples en utilisant le nom de la GPO qui est dans la balise "GPODisplayName".

```
# Importation de la GPO si elle n'existe plus.  
# Dans ce cas, le paramètre -CreateIfNeeded est obligatoire.  
Import-GPO -BackupGpoName "U_EMPLOYES" `
    -Path "E:\_GPO_BACKUP\UTILISATEURS" `
    -TargetName "U_EMPLOYES" `
    -CreateIfNeeded  
  
# Importation de la GPO si elle existe.  
# Dans ce cas, le paramètre -CreateIfNeeded n'est pas obligatoire.  
Import-GPO -BackupGpoName "U_EMPLOYES" `
    -Path "E:\_GPO_BACKUP\UTILISATEURS" `
    -TargetName "U_EMPLOYES"
```

Exemples en utilisant la valeur qui est dans la balise "ID".

```
# Importation de la GPO si elle n'existe plus.  
# Dans ce cas, le paramètre -CreateIfNeeded est obligatoire.  
Import-GPO -BackupId 6E836373-3A7B-474C-9A86-9B3478968C8E `
    -Path "E:\_GPO_BACKUP\UTILISATEURS" `
    -TargetName "U_EMPLOYES" `
    -CreateIfNeeded  
  
# Importation de la GPO si elle existe.  
# Dans ce cas, le paramètre -CreateIfNeeded n'est pas obligatoire.  
Import-GPO -BackupId 6E836373-3A7B-474C-9A86-9B3478968C8E `
    -Path "E:\_GPO_BACKUP\UTILISATEURS" `
    -TargetName "U_EMPLOYES"
```

GPO avec PowerShell

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectifs

- Utiliser plusieurs cmdlets relatifs aux stratégies de groupe.

Le lien entre une stratégie et la base de registre

La configuration d'un paramètre de stratégie de groupe modifie une clé de registre.

Les clés de registre pour la section "**Configuration utilisateur**"

- HKEY_CURRENT_USER\Software\Policies
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies

Les clés de registre pour la section "**Configuration ordinateur**"

- HKEY_LOCAL_MACHINE\Software\Policies
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies

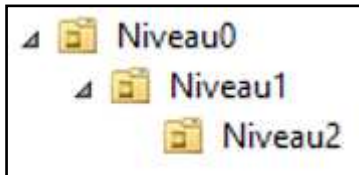
Le fichier "**Windows11andWindowsServer2019PolicySettings--23H2.xlsx**" contient les clés de registre qui sont sous "**Configuration ordinateur \ Stratégies \ Modèles d'administration**" et "**Configuration utilisateur \ Stratégies \ Modèles d'administration**".

Étape 1 - Mise en place

Connectez-vous sur votre serveur virtuel "SERVEURV2" avec l'utilisateur "FORMATION\TECH"

Créer des unités d'organisation

- Sous votre domaine créer la structure d'unités d'organisation suivante.



Pour la création des unités d'organisation, vous pouvez utiliser la console "Utilisateurs et ordinateurs Active Directory" ou la programmation PowerShell.

Vous devez créer le dossier E:_RAPPORTS.

L'annexe à la fin du document contient la liste complète des cmdlets du module GroupPolicy.

Étape 2 - Gestion des objets de stratégie de groupe (GPO)

Vous allez utiliser PowerShell pour gérer les objets de stratégie de groupe:

Création par la console "Gestion de stratégie de groupe"

Ouvrir la console "Gestion de stratégie de groupe"

Créer un objet

- Dans la section "Objets de stratégie de groupe" créer l'objet GPO "gpoA"

Créer un objet et le lier

- Dans la section "Objets de stratégie de groupe" créer l'objet GPO "gpoB"
- Dans l'unité Niveau2 lier l'objet GPO "gpoB"

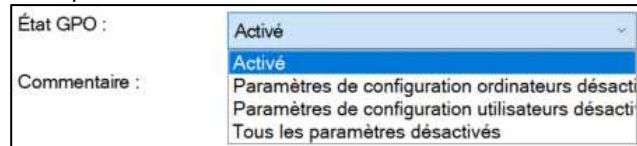
Créer deux objets et lier directement dans les unités

- Directement dans l'unité "Niveau0" créer l'objet GPO "gpoC"
- Directement dans l'unité Niveau1 créer l'objet GPO "gpoD"

La commande pour créer un objet GPO dont le nom est "gpo1"

New-GPO -Name "gpo1"

Il est possible de modifier l'état d'une GPO en modifiant la propriété "GpoStatus".



```
(Get-GPO -Name "gpo1").GpoStatus = "AllSettingsEnabled"  
(Get-GPO -Name "gpo1").GpoStatus = "ComputerSettingsDisabled"  
(Get-GPO -Name "gpo1").GpoStatus = "UserSettingsDisabled"  
(Get-GPO -Name "gpo1").GpoStatus = "AllSettingsDisabled"
```

La commande pour afficher la valeur de "GpoStatus" de l'objet GPO "gpo1"

(Get-GPO -Name gpo1).GpoStatus

La commande pour modifier le commentaire de l'objet GPO "gpo1"

(Get-GPO -Name "gpo1").Description = "La GPO gpo1 n'est pas liée à une OU."

La commande pour afficher le commentaire de l'objet GPO "gpo1"

(Get-GPO -Name gpo1).Description

La commande pour créer un objet GPO et configurer un commentaire.

New-GPO -Name "gpo2" `
-Comment "gpo2 est liée à la OU Niveau0"

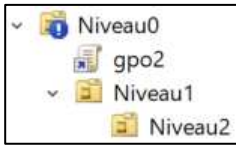
La commande pour lier l'objet GPO "gpo2" à l'unité d'organisation "Niveau0"

New-GPLink -Name "gpo2" `
-Target "ou=Niveau0,dc=formation,dc=local"

Étape 3 - Bloquer l'héritage sur une unité d'organisation

La commande pour bloquer l'héritage sur une OU

```
Set-GPinheritance -Target "ou=niveau0,dc=formation,dc=local" `
                  -IsBlocked Yes
```



La commande pour ne pas bloquer l'héritage sur une OU

```
Set-GPinheritance -Target "ou=niveau0,dc=formation,dc=local" `
                  -IsBlocked No
```

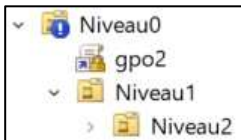
Étape 4 - "Appliqué" une GPO

IMPORTANT: Il ne faut pas confondre l'option "Appliqué" et "Lien activé".



En français	En anglais
Appliqué	Enforced
Lien activé	Link Enabled

```
Set-GPLink -Name gpo2 `
            -Target "ou=niveau0,dc=formation,dc=local" `
            -Enforced Yes
```



Le paramètre **-Enforced** existe également dans **New-GPLink**.

Étape 5 - Changer l'ordre d'application d'une GPO

La commande qui place une GPO en position 1 donc la plus haute priorité.

```
Set-GPLink -Name "gpo2" `
            -Target "OU=niveau0,DC=formation,DC=local" `
            -Order 1
```

Le paramètre **-Order** existe également dans **New-GPLink**.

Étape 6 - Suppression d'objets de stratégie de groupe (GPO) et de liaison

Supprimer le lien d'une GPO sur une unité d'organisation

La commande pour supprimer le lien "gpoB" qui est sur l'unité d'organisation "Niveau2" sans confirmation

```
Remove-GPlink -Name "gpoB" `
    -Target "ou=Niveau2, ou=Niveau1, ou=Niveau0, dc=formation, dc=local" `
    -Confirm:$false
```

Supprimer une GPO

La commande pour supprimer l'objet GPO "gpoB" sans confirmation

```
Remove-GPO -Name gpoB `
    -Confirm:$false
```

Étape 7a - Créer une GPO et configurer les paramètres avec les clés de registre

```
(Get-Command -Module GroupPolicy -Name *GPRegistryValue).Name
```

```
Get-GPRegistryValue  
Remove-GPRegistryValue  
Set-GPRegistryValue
```

Il est possible de désactiver le "Bureau à distance" à l'aide d'une clé de registre qui est une GPO.

La clé de registre est dans le fichier "Windows11andWindowsServer2019PolicySettings--23H2.xlsx".

```
$pol = New-GPO -Name "C_DisableRDP" -Comment "Désactive RDP"  
$pol.GpoStatus = "UserSettingsDisabled"
```

```
# Si la valeur est 0 alors l'accès au Bureau à distance est "Activé".  
# Si la valeur est 1 alors l'accès au Bureau à distance est "Désactivé".
```

Première syntaxe

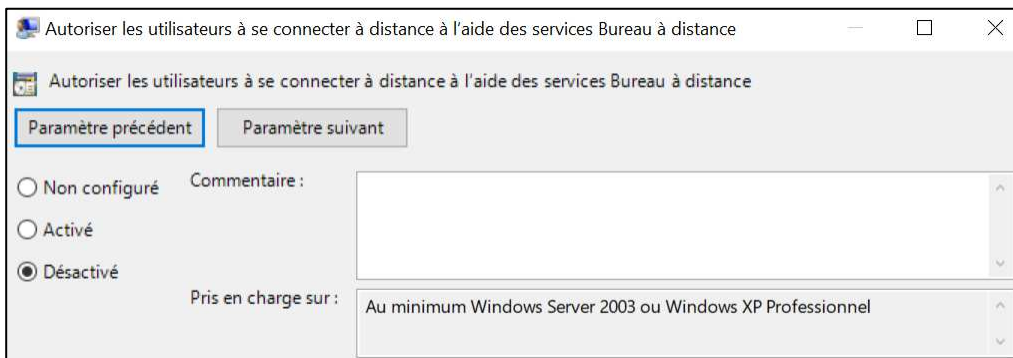
```
Set-GPRegistryValue `
    -Name "C_DisableRDP" `
    -Key "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" `
    -ValueName "fDenyTSConnections" `
    -Type DWord `
    -Value 1
```

Deuxième syntaxe

Utilisation d'une "hash table" pour passer les paramètres

```
$HT1= @{  
    Name      = "C_DisableRDP"  
    Key       = "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services"  
    ValueName = "fDenyTSConnections"  
    Type      = "DWord"  
    Value     = 1  
}
```

```
Set-GPRegistryValue @HT1
```



Configuration ordinateur (activée)	
Stratégies	
Modèles d'administration	
Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.	
Composants Windows/ Services Bureau à distance/ Hôte de la session Bureau à distance/ Connexions	
Stratégie	Paramètre
Autoriser les utilisateurs à se connecter à distance à l'aide des services Bureau à distance	Désactivé
Configuration utilisateur (désactivée)	
Aucun paramètre n'est défini.	

Nous voulons que le paramètre de la GPO soit "Non configuré".

Première syntaxe

```
Set-GPRegistryValue `
    -Name "C_DisableRDP" `
    -Key "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" `
    -Disable
```

Deuxième syntaxe

Utilisation d'une "hash table" pour passer les paramètres

```
$HT2= @{
    Name      = "C_DisableRDP"
    Key       = "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services"
    Disable   = $true
}
```

```
Set-GPRegistryValue @HT2
```

The screenshot shows the Group Policy Editor window for the policy 'Autoriser les utilisateurs à se connecter à distance à l'aide des services Bureau à distance'. The policy is currently set to 'Non configuré' (Not configured), which is selected with a radio button. There are also options for 'Activé' (Enabled) and 'Désactivé' (Disabled). A 'Commentaire' (Comment) field is present but empty. Below the radio buttons, it says 'Pris en charge sur : Au minimum Windows Server 2003 ou Windows XP Professionnel' (Supported on: At least Windows Server 2003 or Windows XP Professional). Navigation buttons 'Paramètre précédent' (Previous parameter) and 'Paramètre suivant' (Next parameter) are visible at the top.

Configuration ordinateur (activée)	
	Aucun paramètre n'est défini.
Configuration utilisateur (désactivée)	
	Aucun paramètre n'est défini.

Étape 7b - Créer une préférence et configurer les paramètres avec les clés du registre

(Get-Command -Module GroupPolicy -Name *GPPrefRegistryValue).Name

Get-GPPrefRegistryValue
Remove-GPPrefRegistryValue
Set-GPPrefRegistryValue

Il est possible de désactiver le "Bureau à distance" à l'aide d'une clé de registre qui n'est pas une GPO.

Pour cet exemple, nous utiliserons une préférence pour modifier une clé de registre.

```
$pol = New-GPO -Name "PC_DisableRDP" -Comment "Désactive RDP"  
$Pol.GpoStatus = "UserSettingsDisabled"  
  
# Configuration d'une préférence "Ordinateur"  
Set-GPPrefRegistryValue `   
    -Name "PC_DisableRDP" `   
    -Key "HKLM\System\CurrentControlSet\Control\Terminal Server" `   
    -ValueName fDenyTSConnections `   
    -Type Dword `   
    -Value 1 `   
    -Context Computer `   
    -Action Update
```

Configuration ordinateur (activée)	
Préférences	
Paramètres Windows	
Registre	
fDenyTSConnections (ordre : 1)	
Général	
Action	Mettre à jour
Propriétés	
Ruche	HKEY_LOCAL_MACHINE
Chemin d'accès à la clé	System\CurrentControlSet\Control\Terminal Server
Nom de la valeur	fDenyTSConnections
Type de la valeur	REG_DWORD
Données de la valeur	0x1 (1)
Commun	
Options	
Interrompre le traitement des éléments sur cette extension si une erreur se produit sur cet élément	Non
Supprimer cet élément lorsqu'il n'est plus appliqué	Non
Appliquer une fois et ne pas réappliquer	Non
Configuration utilisateur (désactivée)	
Aucun paramètre n'est défini.	

Nous voulons supprimer la préférence "PC_DisableRDP".

```
Remove-GPPrefRegistryValue `
    -Name "PC_DisableRDP" `
    -Key "HKLM\System\CurrentControlSet\Control\Terminal Server" `
    -Context Computer
```

Configuration ordinateur (activée)	
	Aucun paramètre n'est défini.
Configuration utilisateur (désactivée)	
	Aucun paramètre n'est défini.

Étape 8 - Mise à jour des GPO

Invoke-GPUUpdate est l'équivalent de "gpupdate.exe".

```
# Mise à jour des GPO pour les utilisateurs et les ordinateurs  
# sur l'ordinateur local  
Invoke-GPUUpdate -Force
```

```
# Mise à jour des GPO pour les utilisateurs et les ordinateurs  
# sur un ordinateur distant  
Invoke-GPUUpdate -Computer "SERVEUR2" \  
                -Force
```

```
# Mise à jour des GPO pour les utilisateurs  
# sur un ordinateur distant  
Invoke-GPUUpdate -Computer "SERVEUR2" \  
                -Target "User" \  
                -Force
```

Étape 9 - Sauvegarder la résultante des stratégies

Get-GPResultantSetOfPolicy est l'équivalent de "gpresult.exe".

```
# Jeu de stratégie résultant sur l'ordinateur local  
Get-GPResultantSetOfPolicy -ReportType Xml \  
                          -Path "e:\_rapports\UserAndComputer.xml"
```

```
# Jeu de stratégie résultant sur un ordinateur distant  
Get-GPResultantSetOfPolicy -ReportType Xml \  
                          -Path "e:\_rapports\SERVEUR2_UserAndComputer.xml" \  
                          -Computer "SERVEUR2"
```

Étape 10 - Création d'un rapport HTML par programmation PowerShell

La commande pour créer un rapport HTML pour l'objet "C_DisableRDP"

```
Get-GPOReport -Name "C_DisableRDP" \  
              -ReportType HTML \  
              -Path e:\_rapports\C_DisableRDP.html
```

ANNEXE

Voici la liste des CMDLETS du module GroupPolicy.

```
PS E:\_OUTILS> (Get-Command -Module GroupPolicy).Name
Get-GPPPermissions
Set-GPPPermissions
Backup-GPO
Copy-GPO
Get-GPInheritance
Get-GPO
Get-GPOReport
Get-GPPPermission
Get-GPPrefRegistryValue
Get-GPRegistryValue
Get-GPResultantSetOfPolicy
Get-GPStarterGPO
Import-GPO
Invoke-GPUUpdate
New-GPLink
New-GPO
New-GPStarterGPO
Remove-GPLink
Remove-GPO
Remove-GPPrefRegistryValue
Remove-GPRegistryValue
Rename-GPO
Restore-GPO
Set-GPInheritance
Set-GPLink
Set-GPPPermission
Set-GPPrefRegistryValue
Set-GPRegistryValue
```

Voici deux cmdlets du ActiveDirectory.

```
Get-ADDefaultDomainPasswordPolicy
Set-ADDefaultDomainPasswordPolicy
```

Stratégie de mot de passe affinée

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectifs

- La configuration de "**Stratégie de mot de passe affinée**" avec la console "**Centre d'administration Active Directory**".

IMPORTANT: sous aucun prétexte les stratégies suivantes ne peuvent être détruites ou modifiées

- Default Domain Controllers Policy
- Default Domain Policy

Lorsqu'on configure des paramètres de sécurité au niveau du domaine c'est pour améliorer la sécurité.

Les stratégies de mot de passe, les stratégies de verrouillage du compte et les stratégies Kerberos doivent être configurées au niveau du domaine.

Il est possible d'améliorer la sécurité en créant une stratégie de mot de passe affinée.

Stratégie de mot de passe affinée (Fine-Grained Password Policies)

Les stratégies de mot de passe affinées permettent de spécifier plusieurs stratégies de mot de passe au sein d'un même domaine et appliquer des restrictions différentes pour les stratégies de mot de passe et de verrouillage de compte à des ensembles d'utilisateurs différents dans un domaine.

La configuration des stratégies de mot de passe affinée est disponible seulement dans la console "**Centre d'administration Active Directory**".

Les stratégies de mot de passe affinées s'appliquent uniquement à des objets utilisateur et à des groupes de sécurité globaux. Par défaut, seuls les membres du groupe **"Admins du domaine"** peuvent définir des stratégies de mot de passe affinées.

Créer Paramètres de mot de passe : MOT_DE_PASSE_14

Paramètres de mot de passe

S'applique directement à

Nom : * MOT_DE_PASSE_14

Priorité : * 1

☒ Appliquer la longueur minimale du mot de passe

Longueur minimale du mot de passe (caractères) : * 7

☒ Appliquer l'historique des mots de passe

Nombre de mots de passe mémorisés : * 24

☒ Le mot de passe doit respecter des exigences de complexité

☐ Stocker le mot de passe en utilisant un chiffrement réversible

☒ Protéger contre la suppression accidentelle

Description :
Mot de passe de 14 caractères pour les administrateurs de la OU INFORMATIQUE

Options d'âge du mot de passe :

☒ Appliquer l'âge minimal de mot de passe

L'utilisateur ne peut pas changer le mot de passe d'ici à (jou...) * 1

☒ Appliquer l'âge maximal de mot de passe

L'utilisateur doit changer le mot de passe après (jours) : * 42

☒ Appliquer la stratégie de verrouillage des comptes :

Nombre de tentatives de connexion échouées autorisé : * 3

Réinitialiser le nombre de tentatives de connexion échouées a... * 30

Le compte va être verrouillé

☒ Pendant une durée de (mins) : * 30

☐ Jusqu'à ce qu'un administrateur déverrouille manuellement le compte

S'applique directement à

Nom	Courrier
grINF_Gestionnaires	

Ajouter...
Supprimer

Informations supplémentaires...

OK Annuler

« FORMATION (local) » System » Password Settings Container

Centre d'administr...

Vue d'ensemble

FORMATION (local)

...Password Settings Contain...

System

Contrôle d'accès dynamique

Authentification

Recherche globale

Filter

Nom	Priorité	Description	Type
MOT_DE_PASSE_14	1	Mot de passe de 14 caractères pour les administrateurs de la OU INFORMATIQUE	Paramètres de mot de passe

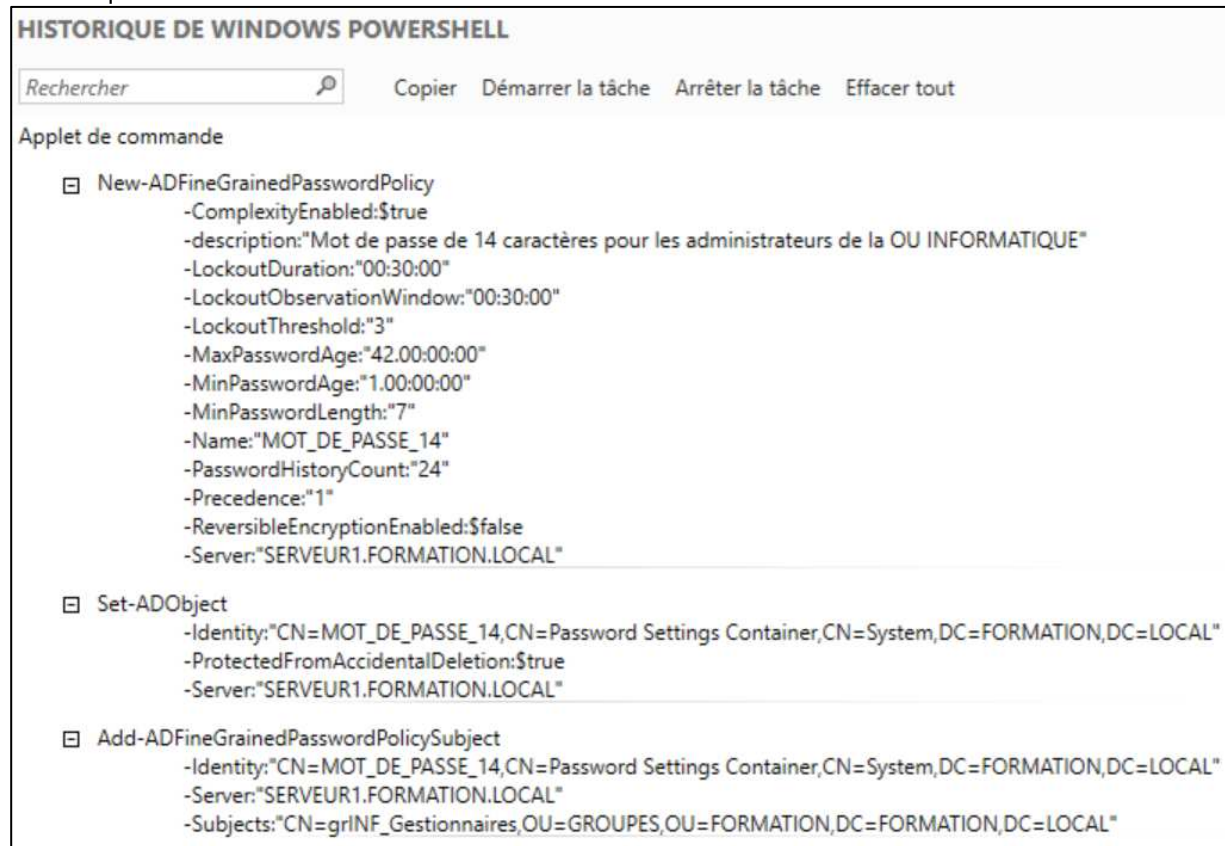
Dans la console UOAD.

Nom	Type	Description
MOT_DE_PASSE_14	msDS-PasswordSettings	Mot de passe de 14 caractères pour les administrateurs de la OU INFORMATIQUE

La console **"Gestion des stratégies de groupe"** ne montre pas **"MOT_DE_PASSE_14"** parce que cette **"Stratégie de mot de passe affinée"** est dans le conteneur **"Password Settings Container"**.

CN=MOT_DE_PASSE_14,CN=Password Settings Container,CN=System,DC=FORMATION,DC=LOCAL

L'historique de Windows PowerShell affiche le code.



Trois commandes PowerShell sont utilisées pour la création d'une stratégie de mot de passe affinée.

Le conteneur "**Password Settings Container**" est visible dans la console UOAD.

```
# Définir le DistinguishedName pour le conteneur "Password Settings Container"
$nom = "CN=Password Settings Container,CN=System,DC=FORMATION,DC=LOCAL"
```

```
# Utiliser Get-ADObject pour afficher le contenu du conteneur
Get-ADObject -Filter * `
    -SearchBase $nom | Format-List Name,DistinguishedName,ObjectClass
```

```
Name           : MOT_DE_PASSE_14
DistinguishedName : CN=MOT_DE_PASSE_14,CN=Password Settings
                  Container,CN=System,DC=FORMATION,DC=LOCAL
ObjectClass      : msDS-PasswordSettings
```

Le contenu de l'attribut **ObjectClass** est **msDS-PasswordSettings**

```
# Définir le DistinguishedName pour le conteneur "Password Settings Container"
$nom = "CN=Password Settings Container,CN=System,DC=FORMATION,DC=LOCAL"
```

```
# Utiliser Get-ADObject pour afficher le contenu du conteneur
```

```
Get-ADObject -Filter * `
    -SearchBase $nom `
    -Properties * | Format-List Name,
                                DistinguishedName,
                                ObjectClass,
                                msDS-LockoutDuration,
                                msDS-LockoutObservationWindow,
                                msDS-LockoutThreshold,
                                msDS-MaximumPasswordAge,
                                msDS-MinimumPasswordAge,
                                msDS-MinimumPasswordLength,
                                msDS-PasswordComplexityEnabled,
                                msDS-PasswordHistoryLength,
                                msDS-PasswordReversibleEncryptionEnabled,
                                msDS-PasswordSettingsPrecedence,
                                msDS-PSOAppliesTo
```

```
Name : MOT_DE_PASSE_14
DistinguishedName : CN=MOT_DE_PASSE_14,CN=Password Settings Container,CN=System,DC=FORMATION,DC=LOCAL
ObjectClass : msDS-PasswordSettings
msDS-LockoutDuration : -18000000000
msDS-LockoutObservationWindow : -18000000000
msDS-LockoutThreshold : 3
msDS-MaximumPasswordAge : -36288000000000
msDS-MinimumPasswordAge : -864000000000
msDS-MinimumPasswordLength : 7
msDS-PasswordComplexityEnabled : True
msDS-PasswordHistoryLength : 24
msDS-PasswordReversibleEncryptionEnabled : False
msDS-PasswordSettingsPrecedence : 1
msDS-PSOAppliesTo : {CN=grINF_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL}
```

msDS-LockoutDuration, msDS-LockoutObservationWindow, msDS-MaximumPasswordAge et msDS-MinimumPasswordAge ont des valeurs négatives.

Par exemple, la valeur **-18000000000** pour la propriété **msDS-LockoutDuration** est déroutante. Cette valeur est exprimée en unités de 100 nanosecondes (ou 0.0000001 secondes). Active Directory utilise ce format pour représenter les durées de temps.

La fonction **Convert-ADTime** convertit les valeurs de 100 nanosecondes en minutes. La formule de conversion est basée sur le fait qu'une minute contient 600,000,000 unités de 100 nanosecondes.

```
function Convert-ADTime
{
    param ([long]$time)

    return ($time / -6000000000)
}
```



```
# Définir le DN pour le conteneur "Password Settings Container"
$nom = "CN=Password Settings Container,CN=System,DC=FORMATION,DC=LOCAL"

# Utiliser Get-ADObject pour afficher le contenu du conteneur
Get-ADObject -Filter * `
    -SearchBase $nom `
    -Properties * | Format-List Name,
                        DistinguishedName,
                        ObjectClass,
    @{Name="LockoutDuration (minutes)";
      Expression={Convert-ADTime $PSItem."msDS-LockoutDuration"}}},
    @{Name="LockoutObservationWindow (minutes)";
      Expression={Convert-ADTime $PSItem."msDS-LockoutObservationWindow"}}},
    msDS-LockoutThreshold,
    @{Name="MaxPasswordAge (minutes)";
      Expression={Convert-ADTime $PSItem."msDS-MaximumPasswordAge"}}},
    @{Name="MinPasswordAge (minutes)";
      Expression={Convert-ADTime $PSItem."msDS-MinimumPasswordAge"}}},
    msDS-MinimumPasswordLength,
    msDS-PasswordComplexityEnabled,
    msDS-PasswordHistoryLength,
    msDS-PasswordReversibleEncryptionEnabled,
    msDS-PasswordSettingsPrecedence,
    msDS-PSOAppliesTo
```

```
Name : MOT_DE_PASSE_14
DistinguishedName : CN=MOT_DE_PASSE_14,CN=Password Settings Container,CN=System,DC=FORMATION,DC=LOCAL
ObjectClass : msDS-PasswordSettings
LockoutDuration (minutes) : 30
LockoutObservationWindow (minutes) : 30
msDS-LockoutThreshold : 3
MaxPasswordAge (minutes) : 60480
MinPasswordAge (minutes) : 1440
msDS-MinimumPasswordLength : 7
msDS-PasswordComplexityEnabled : True
msDS-PasswordHistoryLength : 24
msDS-PasswordReversibleEncryptionEnabled : False
msDS-PasswordSettingsPrecedence : 1
msDS-PSOAppliesTo : {CN=grINF_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL}
```

Les commandes PowerShell pour les stratégies de mot de passe affinée

(Get-Command -Name *FineGrainedPasswordPolicy*).Name

Add-ADFineGrainedPasswordPolicySubject
Get-ADFineGrainedPasswordPolicy
Get-ADFineGrainedPasswordPolicySubject
New-ADFineGrainedPasswordPolicy
Remove-ADFineGrainedPasswordPolicy
Remove-ADFineGrainedPasswordPolicySubject
Set-ADFineGrainedPasswordPolicy

Voici la commande pour afficher un jeu de stratégies résultant pour un utilisateur qui utilise une stratégie de mot de passe affinée.

Get-ADUserResultantPasswordPolicy -Identity EMP09

```
PS E:\PowerShell> Get-ADUserResultantPasswordPolicy -Identity EMP09

AppliesTo                : {CN=grRH_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL,
                           CN=grING_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL,
                           CN=grINF_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL,
                           CN=grCOMP_Gestionnaires,OU=GROUPES,OU=FORMATION,DC=FORMATION,DC=LOCAL}
ComplexityEnabled         : True
DistinguishedName         : CN=MOT_DE_PASSE_14,CN=Password Settings Container,CN=System,DC=FORMATION,DC=LOCAL
LockoutDuration           : 00:30:00
LockoutObservationWindow  : 00:30:00
LockoutThreshold          : 3
MaxPasswordAge            : 30.00:00:00
MinPasswordAge            : 1.00:00:00
MinPasswordLength         : 14
Name                     : MOT_DE_PASSE_14
ObjectClass               : msDS-PasswordSettings
ObjectGUID               : e3e5c5a1-9c17-4a8f-8004-d93aa5a348bc
PasswordHistoryCount      : 24
Precedence               : 1
ReversibleEncryptionEnabled : False
```

Si **Get-ADUserResultantPasswordPolicy** retourne rien, c'est parce que l'utilisateur n'utilise pas de stratégie de mot de passe affinée.

```
PS E:\PowerShell> Get-ADUserResultantPasswordPolicy -Identity EMP08

PS E:\PowerShell>
```

Une stratégie de mot de passe affinée permet de configurer l'historique des mots de passe entre 1 et 1024

Set-ADFineGrainedPasswordPolicy -Identity MOT_DE_PASSE_14 `
-PasswordHistoryCount:"60"

Les commandes pour supprimer une stratégie de mot de passe affinée

Set-ADFineGrainedPasswordPolicy -Identity MOT_DE_PASSE_14 `
-ProtectedFromAccidentalDeletion \$False

Remove-ADFineGrainedPasswordPolicy -Identity MOT_DE_PASSE_14 `
-Confirm