# Contexte

Lorsqu’un contrôleur de domaine n'a pas été actif ou n'a pas répliqué ses données depuis un certain temps, cela peut indiquer que ce contrôleur de domaine n’est plus opérationnel ou utilisé.

# Conséquences

Décommissionner des contrôleurs de domaine inactifs permet d’éviter les scénarios suivants :

* **Accès aux identifiants** : Les contrôleurs de domaine inactifs peuvent ne pas bénéficier des mises à jour de sécurité régulières ou des correctifs de vulnérabilité.
* **Élévation de privilèges** : Les contrôleurs de domaine inactifs peuvent ne pas bénéficier des mises à jour de sécurité régulières ou des correctifs de vulnérabilité.

## Chaine de cyberattaques

Décommissionner des contrôleurs de domaine inactifs permet d’éviter l’accomplissement des étapes suivantes d’une chaine de cyberattaques :

* **Exploitation** : Une faille de sécurité dans un contrôleur de domaine inactif, donc non mis à jour, pourrait permettre à un attaquant d'exécuter un code malveillant, de compromettre des comptes d'administration ou d'obtenir des informations d'identification sensibles stockées.

# Détection

Les commandes PowerShell suivantes permettent de lister les contrôleurs de domaine inactifs depuis au moins 45 jours :

#  
# Importer le module Active Directory

#

Import-Module ActiveDirectory  
  
#

# Définir le nombre de jours après lesquels un contrôleur de domaine est considéré comme inactif

#  
$inactiveDaysThreshold = 45

#  
# Obtenir la date actuelle

#

$currentDate = Get-Date

#  
# Obtenir tous les contrôleurs de domaine

#

$domainControllers = Get-ADDomainController -Filter \*

#  
# Créer une liste pour stocker les contrôleurs de domaine inactifs

#

$inactiveDomainControllers = @()

#

# Parcourir chaque contrôleur de domaine pour vérifier son statut d'activité

#

foreach ($dc in $domainControllers) {

#

# Obtenir la date de la dernière synchronisation de l'AD pour le contrôleur de domaine  
 #

$lastSync = (Get-ADReplicationPartnerMetadata -Target $dc.HostName -Scope Server).LastReplicationSuccess

#

# Calculer le nombre de jours depuis la dernière synchronization  
 #  
 $daysSinceLastSync = ($currentDate - $lastSync).Days

#  
 # Vérifier si le nombre de jours dépasse le seuil d'inactivité

#  
 if ($daysSinceLastSync -gt $inactiveDaysThreshold) {

#

# Ajouter le contrôleur de domaine dans la liste des controleurs de domain inactifs

#

$inactiveDomainControllers += $dc

}

}

#

# Afficher la liste des contrôleurs de domaine inactifs

#  
if ($inactiveDomainControllers.Count -gt 0) {

$inactiveDomainControllers | Format-Table -AutoSize

}

La liste de contrôleurs de domaine inactifs doit être vide.

# Correction

Si le contrôleur de domaine est inactif car il n’est pas utilisé, alors celui-ci peut être supprimé en suivant la procédure suivante :

## Prérequis

* Si le contrôleur de domaine sert de serveur de catalogue global, *global catalog* en anglais, le supprimer sans s'assurer qu'un autre contrôleur de domaine remplit ce rôle peut perturber la capacité des utilisateurs à se connecter et à accéder aux ressources dans des environnements multi-domaines. Il faut donc s’assurer que le rôle de catalogue global est transféré à un autre contrôleur de domaine.
* Si des applications ou services dépendent de ce contrôleur de domaine pour l'authentification ou les services d'annuaire. Une décommission soudaine pourrait perturber ces services. Il faut donc reconfigurer les applications et services afin qu’ils s’appuient sur un autre contrôleur de domaine pour l’authentification et les services d’annuaire.
* Si le contrôleur de domaine sert également de serveur DNS ou DHCP, il faut que ces services soient déplacés ou répliqués vers d'autres serveurs.

## Procédure

Les commandes PowerShell suivantes permettent de décommissionner un contrôleur de domaine :

#  
# Importer le module Active Directory

#

Import-Module ActiveDirectory  
  
#  
# Nom du contrôleur de domaine à décommissionner

#  
$domainControllerToDemote = "NomDuDCÀDécommissionner"  
  
#  
# Nom du contrôleur de domaine à qui transférer les rôles FSMO du contrôleur de domaine à décommissionner

#  
$domainControllerToPromote = "NomDuDCÀCommissionner"  
  
#  
# Nom de la zone DNS dans laquelle supprimer l’enregistrement du contrôleur de domaine à décommissionner  
#  
$DNSZoneName = "NomDeLaZoneDNS"

#  
# Récupérer le contrôleur de domaine grâce à son nom

#  
$dc = Get-ADDomainController -Identity $domainControllerToDemote -ErrorAction SilentlyContinue

#  
# Vérifier que le serveur spécifié est un contrôleur de domaine  
#  
if (-not $dc) {

Write-Host "The server $domainControllerToDemote is not a domain controlleur or cannot be found."

exit

}

#  
# Lister les rôles FSMO à transférer

#  
$fsmoRoles = "SchemaMaster", "DomainNamingMaster", "PDCEmulator", "RIDMaster", "InfrastructureMaster"

#  
# Parcourir chaque rôle FSMO à transférer  
#

foreach ($role in $fsmoRoles) {  
 #  
 # Récupérer le contrôleur de domaine ayant le rôle actuel  
 #

$currentRoleHolder = Get-ADDomainController -Filter { OperationsMasterRole -eq $role }  
  
 #  
 # Si le contrôleur de domaine ayant le rôle actuel est le contrôleur de domaine à décommissionner  
 #  
 if ($currentRoleHolder.Name -eq $domainControllerToDemote) {  
 #  
 # Transférer le rôle actuel au contrôleur de domaine à commissionner  
 #

Move-ADDirectoryServerOperationMasterRole -Identity $domainControllerToPromote -OperationMasterRole $role

}

}

#

# Décommissionner le contrôleur de domaine  
#

Uninstall-ADDSDomainController -DemoteOperationMasterRole -RemoveApplicationPartitions -Force -Target $domainControllerToDemote

#  
# Supprimer les métadonnées du contrôleur de domaine

#

Remove-ADDomainController -Identity $domainControllerToDemote -MetadataCleanup

#

# Supprimer l'objet ordinateur du contrôleur de domaine

#

Remove-ADComputer -Identity $domainControllerToDemote

#

# Supprimer les enregistrements DNS associés au contrôleur de domaine  
#

Remove-DnsServerResourceRecord -ZoneName $DNSZoneName -Name $domainControllerToDemote -RRType "A" -Force

Documentation :

* <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/demoting-domain-controllers-and-domains--level-200->

# Vérification

Pour vérifier la bonne correction de l’anomalie, il est possible de d’exécuter à nouveau la partie "Détection" et de constater qu’aucun contrôleur de domaine n’est listé.