

# RÔLES FSMO

---

WINDOWS SERVER 2016



# EN QUOI LES RÔLES FSMO SONT-ILS IMPORTANTS POUR LES ADMINISTRATEURS SYSTÈMES ?

---

- Afin de répondre à cette problématique, nous allons donc voir les différentes interactions entre ces rôles de maitre d'opérations de l'Active Directory.
- Avant de commencer, il faut savoir que ces derniers sont utilisés pour par exemple des tâches de migration de serveurs : une entreprise dispose d'une multitude de serveurs fonctionnant sous Windows Server 2012 et Windows Server 2012 R2 et souhaite migrer vers des serveurs sous Windows 2016 suivant certains besoins.

# FSMO (FLEXIBLE SINGLE MASTER OPERATION)

---

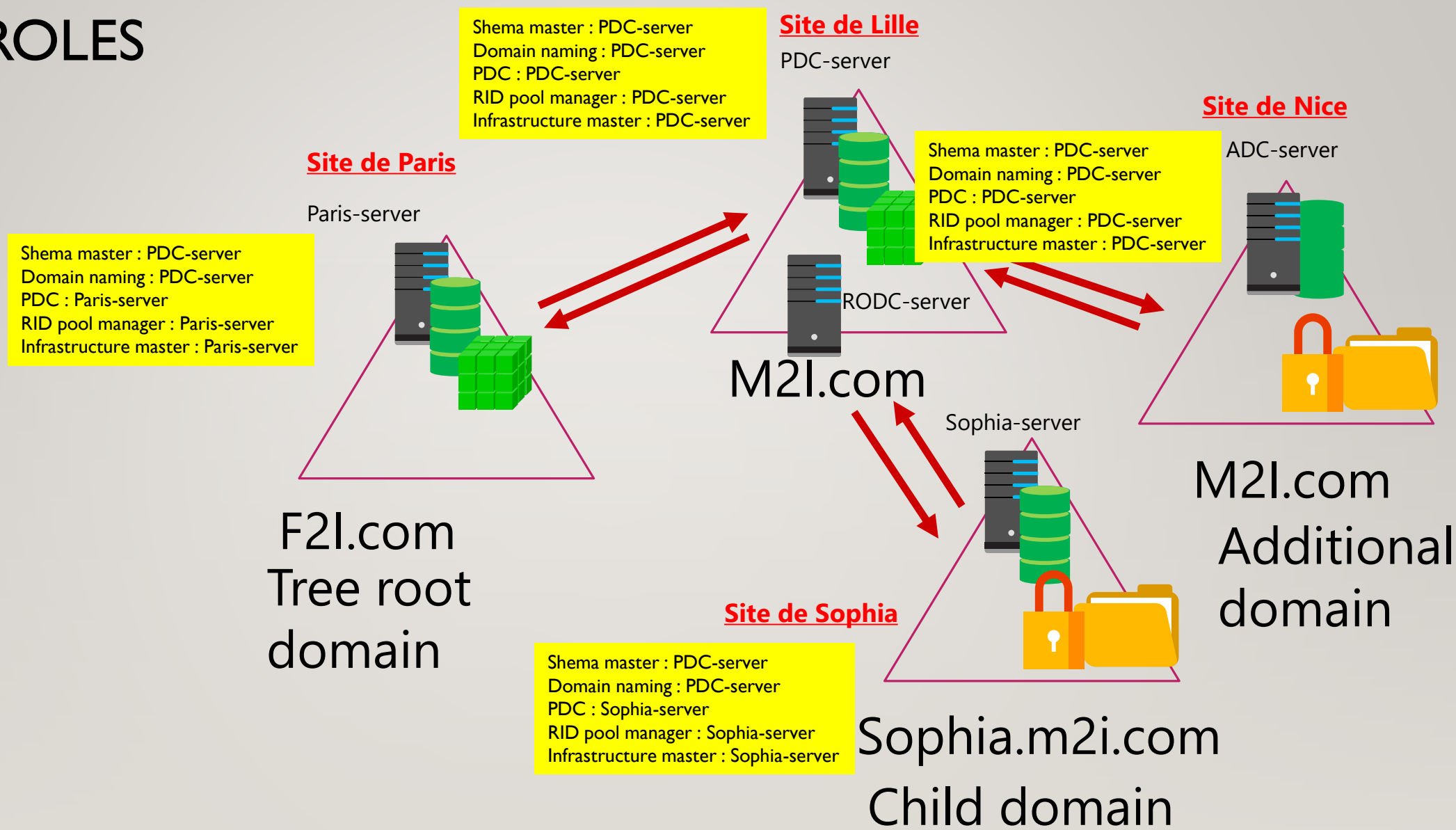
## **Les rôles situés à la racine de la forêt :**

- ✓ Maître de schéma (SM)
- ✓ Maître d'attribution de noms de domaines (DNM)

## **Les rôles situés à la racine de chaque domaine :**

- ✓ Maître d'infrastructure (IM)
- ✓ Maître des ID relatifs (RID)
- ✓ Emulateur du contrôleur principal de domaine (PDC)

# FSMO ROLES



# MAÎTRE DE SCHÉMA (SCHEMA MASTER)

---

- Appelé également Maître d'opération, il gère l'ensemble des mises à jour et modifications du schéma.
- Il assure également les répliquations sur l'ensemble des contrôleurs de domaines.
- Il ne peut y avoir **qu'un seul Maître de schéma par forêt** et les modifications ne seront effectuées qu'avec le groupe « Administrateurs du schéma ».
- Au niveau du domaine racine de la forêt, il doit être placé avec le Maître d'attribution des noms de domaine et également avec le PDC.
- S'il n'est pas disponible, aucune modification sur le schéma ne pourra être appliquée ultérieurement.



# MAÎTRE D'ATTRIBUTION DES NOMS DOMAINE (DOMAIN NAMING MASTER)

---

- Il contrôle les ajouts et suppressions de domaines dans la forêt.
- Il est également en charge de la création et/ou suppression de relations avec les domaines externes.
- Enfin, il gère aussi les objets qui servent à établir le lien entre les différentes partitions et le domaine.
- Ces derniers sont stockés dans la partition de Configuration.
- Le rôle doit être placé avec le Maître de schéma et avec le PDC.
- S'il n'est pas disponible, aucun ajout ou suppression de domaine ne sera possible.
- En conséquence, un serveur de secours avec une réplication directe de maître à partenaire est nécessaire.

LILLE-Windows Server MC... x ADC Server x CHILD server x forest x Windows 10 x64 x Windows Server 2016 (4) x tree x

Gestionnaire de serveur

Domaines et approbations Active Directory

Fichier Action Affichage ?

Domaines et approbations Active D

> m2i.com

Nom	Type	Actions
m2i.com	domainDNS	Domaines et approbations ... Autres actions

**Maître d'opérations**

Le maître des opérations d'attribution de noms du domaine s'assure que les noms du domaine sont uniques. Seul un contrôleur de domaine Active Directory dans l'entreprise peut jouer ce rôle.

Maître des opérations d'attribution de noms de domaine :

PDC.m2i.com

Cliquez sur Modifier pour transférer le rôle principal d'attribution de noms de domaine vers l'ordinateur ci-dessous. **Modifier...**

PDC.m2i.com

Fermer

Activer Windows					10:13:59
Accédez aux paramètres pour activer Windows.					10:13:59
PDC	7023	Erreur	Microsoft-Windows-Service Control Manager	Système	03/04/2020 10:13:59
PDC	7023	Erreur	Microsoft-Windows-Service Control Manager	Système	03/04/2020 10:08:59

# MAÎTRE D'INFRASTRUCTURE (INFRASTRUCTURE MASTER)

---

- Il maintient à jour les références d'objets entre les différents domaines.
- Si un utilisateur d'un domaine X est ajouté dans un groupe d'un domaine Y, il sera responsable de répliquer cette référence sur l'ensemble du domaine Y.
- Il ne peut y avoir **qu'un seul Maître d'infrastructure** par domaine.
- Il met à jour des références d'objets à partir d'informations situées sur les Global Catalog d'autres Domain Controller de la forêt.
- S'il n'est pas disponible, l'appartenance et la traduction d'objets ne pourront plus être effectuées.



LILLE-Windows Server MC... x ADC Server x CHILD server x forest x Windows 10 x64 x Windows Server 2016 (4) x tree x

Gestionnaire de serveur

Gestionnaire de serveur ▸ Serveur local

Tableau de bord

**Serveur local**

Tous les serveurs

AD DS

DNS

Services de fichiers et d... ▸

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Utilisateurs et ordinateurs Active Directory

Requêtes enregistrées

m2i.com

Built-in

Nom Type Description

Built-in builtinDomain

Délégation de contrôle...

Rechercher...

Changer de domaine...

Changer de contrôleur de domaine...

Augmenter le niveau fonctionnel du domaine...

**Maîtres d'opérations...**

Nouveau >

Toutes les tâches >

Affichage >

Actualiser

Exporter la liste...

Propriétés

Aide

Maîtres d'opérations de domaine

LILLE-Windows Server MC... x ADC Server x CHILD server x forest x Windows 10 x64 x Windows Server 2016 (4) x tree x

Gestionnaire de serveur

Gestionnaire de serveur ▸ Serveur local

Gérer Outils Afficher Aide

Tableau de bord

Serveur local

Tous les serveurs

AD DS

DNS

Services de fichiers et d... ▸

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage

Utilisateurs et ordinateurs Active Directory

Requêtes enregistrées

m2i.com

Builtin

Computers

Domain Controllers

ForeignSecurityPrinci

IT-dep

Managed Service Acc

Users

Maître d'opérations

RID CDP Infrastructure

Le maître d'infrastructure assure la cohérence des objets pour les opérations interdomaines. Seul un serveur du domaine joue ce rôle.

Maître d'opérations :

PDC.m2i.com

Pour transférer le rôle de maître d'opérations à l'ordinateur suivant, cliquez sur Modifier.

Modifier...

PDC.m2i.com

Fermer Annuler

Nom du serveur	ID	Gravité	Source	Journal	Date et heure
PDC	8198	Erreur	Microsoft-Windows-Security-SPP	Application	03/04/2020 10:25:14
PDC	5719	Erreur	NETLOGON	Système	03/04/2020 10:15:03
PDC	7023	Erreur	Microsoft-Windows-Service Control Manager	Système	03/04/2020 10:13:59

Explorateur de fichiers

# MAITRE RID (RID MASTER)

---

- Il est chargé d'attribuer à chaque objet Active Directory (utilisateur, groupe, ordinateur, etc) un identifiant unique de sécurité (SID).
- Il est structuré de la façon suivante :
  - Un numéro de révision
  - Un identificateur de sécurité du domaine (domaine SID)
  - Un RID (Relative Identifier)
- Lorsque cette plage est épuisée, une demande est effectuée auprès du RID afin de le renouveler.
- Il ne peut y avoir qu'un seul Maître RID par domaine.
- Il doit être placé de préférence avec le PDC.
- Et s'il n'est pas disponible, les pools RID ne seront plus alloués au DC

LILLE-Windows Server MC... x ADC Server x CHILD server x forest x Windows 10 x64 x Windows Server 2016 (4) x tree x

Gestionnaire de serveur

Gestionnaire de serveur ▸ Serveur local

Gérer Outils Afficher Aide

Tableau de bord

Serveur local

Tous les serveurs

AD DS

DNS

Services de fichiers et d... ▸

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage

Utilisateurs et ordinateurs Active Directory

Requêtes enregistrées

m2i.com

Builtin

Computers

Domain Controllers

ForeignSecurityPrinci

IT-dep

Managed Service Acc

Users

Maître d'opérations

RID CDP Infrastructure

Le maître d'opérations gère l'allocation des pools RID aux autres contrôleurs de domaine. Seul un serveur du domaine joue ce rôle.

Maître d'opérations :

PDC.m2i.com

Pour transférer le rôle de maître d'opérations à l'ordinateur suivant, cliquez sur Modifier.

Modifier...

PDC.m2i.com

Fermer Annuler

Nom du serveur	ID	Gravité	Source	Journal	Date et heure
PDC	8198	Erreur	Microsoft-Windows-Security-SPP	Application	03/04/2020 10:25:14
PDC	5719	Erreur	NETLOGON	Système	03/04/2020 10:15:03
PDC	7023	Erreur	Microsoft-Windows-Service Control Manager	Système	03/04/2020 10:13:59

Internet Explorer

# LE PDC EMULATOR

---

- Il est chargé de la réplication des mots de passe.
- Il agit aussi comme un serveur de temps, car il assure la synchronisation des horloges clientes avec les différents contrôleurs de domaine.
- Le service de temps est utilisé dans le cadre de l'authentification Kerberos qui nécessite un horodatage des paquets d'authentification.
- Il a un rôle vital et a un réel impact sur les performances d'une infrastructure Active Directory.
- Une défaillance de ce rôle peut entraîner :
  - Un arrêt de la réplication pour les domaines.
  - L'impossibilité de verrouiller les comptes utilisateurs.
  - Une éventuelle perte de synchronisation entre les DC.
  - Des problèmes d'authentification Kerberos.
  - Des problèmes pour changer/appliquer les GPO.





Tableau de bord

Serveur local

Tous les serveurs

AD DS

DNS

Services de fichiers et d...

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage

Utilisateurs et ordinateurs Active Directory

Requêtes enregistrées

m2i.com

Builtin

Computers

Domain Controllers

ForeignSecurityPrinci

IT-dep

Managed Service Acc

Users

Maître d'opérations

RID

CDP

Infrastructure

Le maître d'opérations émule les fonctions d'un contrôleur de domaine principal pour les clients antérieurs à Windows 2000. Seul un serveur du domaine joue ce rôle.

Maître d'opérations :

PDC.m2i.com

Pour transférer le rôle de maître d'opérations à l'ordinateur suivant, cliquez sur Modifier.

Modifier...

PDC.m2i.com

Fermer

Annuler

ÉVÉ

Tous

Nom du serveur

ID

Gravité

Source

Journal

Date et heure

PDC

8198

Erreur

Microsoft-Windows-Security-SPP

Application

03/04/2020 10:25:14

PDC

5719

Erreur

NETLOGON

Système

03/04/2020 10:15:03

PDC

7023

Erreur

Microsoft-Windows-Service Control Manager

Système

03/04/2020 10:13:59

# Gestionnaire de serveur - Tous les serveurs

- Tableau de bord
- Serveur local
- Tous les serveurs**
- AD DS
- DNS
- Services de fichiers et d...

## SERVEURS

Tous les serveurs | 3 au total

Filtrer		
Nom du serveur	Adresse IPv4	Facilité de gestion
ADC	10.0.0.2	En ligne - Compteurs de performance
PDC	10.0.0.1,10.0.0.30	En ligne - Compteurs de performance
SHOPHIA	-	Erreur de résolution de cible Kerberos

## ÉVÉNEMENTS

Tous les événements | 196 au total

Filtrer			
Nom du serveur	ID	Gravité	Source
			Microsoft-Windows-Security-SPF
			NETLOGON
			Microsoft-Windows-Service Con
			Microsoft-Windows-Service Con
			Microsoft-Windows-Service Con
			Microsoft-Windows-Service Con
			Microsoft-Windows-Security-SPF

Gérer Outils Afficher Aide

- Configuration du système
- Défragmenter et optimiser les lecteurs
- Diagnostic de mémoire Windows
- DNS
- Domaines et approbations Active Directory
- Gestion de l'impression
- Gestion de l'ordinateur
- Gestion des stratégies de groupe
- Informations système
- Initiateur iSCSI
- Modification ADSI
- Module Active Directory pour Windows PowerShell
- Moniteur de ressources
- Nettoyage de disque
- Observateur d'événements
- Pare-feu Windows avec fonctions avancées de sécurité
- Planificateur de tâches
- Sauvegarde Windows Server
- Services
- Services de composants
- Services Microsoft Azure
- Sites et services Active Directory
- Sources de données ODBC (32 bits)
- Sources de données ODBC (64 bits)
- Stratégie de sécurité locale
- Utilisateurs et ordinateurs Active Directory
- Windows PowerShell**
- Windows PowerShell (x86)
- Windows PowerShell ISE

```
Administrateur : Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Tous droits réservés.

PS C:\Users\Administrateur.WIN-LQVAPSHNH4B>
PS C:\Users\Administrateur.WIN-LQVAPSHNH4B>
PS C:\Users\Administrateur.WIN-LQVAPSHNH4B>
PS C:\Users\Administrateur.WIN-LQVAPSHNH4B>
PS C:\Users\Administrateur.WIN-LQVAPSHNH4B>
PS C:\Users\Administrateur.WIN-LQVAPSHNH4B>
PS C:\Users\Administrateur.WIN-LQVAPSHNH4B> hostname
PS C:\Users\Administrateur.WIN-LQVAPSHNH4B> netdom query fsmo
Contrôleur de schéma          PDC.m2i.com
Maître des noms de domaine   PDC.m2i.com
Contrôleur domaine princip. PDC.m2i.com
Gestionnaire du pool RID      PDC.m2i.com
Maître d'infrastructure     PDC.m2i.com
L'opération s'est bien déroulée.

PS C:\Users\Administrateur.WIN-LQVAPSHNH4B> dcdiag

Diagnostic du serveur d'annuaire

Exécution de l'installation initiale :
  Tentative de recherche de serveur associé...
  Serveur associé : PDC
  * Forêt AD identifiée.
  Collecte des informations initiales terminée.

Exécution des tests initiaux nécessaires

  Test du serveur : Lille\PDC
  Démarrage du test : Connectivity
  ..... Le test Connectivity
  de PDC a réussi

Exécution des tests principaux

  Test du serveur : Lille\PDC
  Démarrage du test : Advertising
  ..... Le test Advertising
  de PDC a réussi
  Démarrage du test : FrsEvent
  ..... Le test FrsEvent
  de PDC a réussi
  Démarrage du test : DFSREvent
  Erreurs ou avertissements détectés au cours des dernières 24 heures après le partage de SYSVOL. Des problèmes
  liés à l'échec de la réplication SYSVOL peuvent provoquer des problèmes de stratégie de groupe.
```

Tableau de bord  
Serveur local  
Tous les serveurs  
AD DS  
DNS  
Services de fichiers

Administrateur : Windows PowerShell

```
PS C:\Users\Administrateur.WIN-LQVAPSHNH48>
PS C:\Users\Administrateur.WIN-LQVAPSHNH48>
PS C:\Users\Administrateur.WIN-LQVAPSHNH48>
PS C:\Users\Administrateur.WIN-LQVAPSHNH48>
PS C:\Users\Administrateur.WIN-LQVAPSHNH48> ntdsutil
C:\Windows\system32\ntdsutil.exe: roles
fsmo maintenance: ?

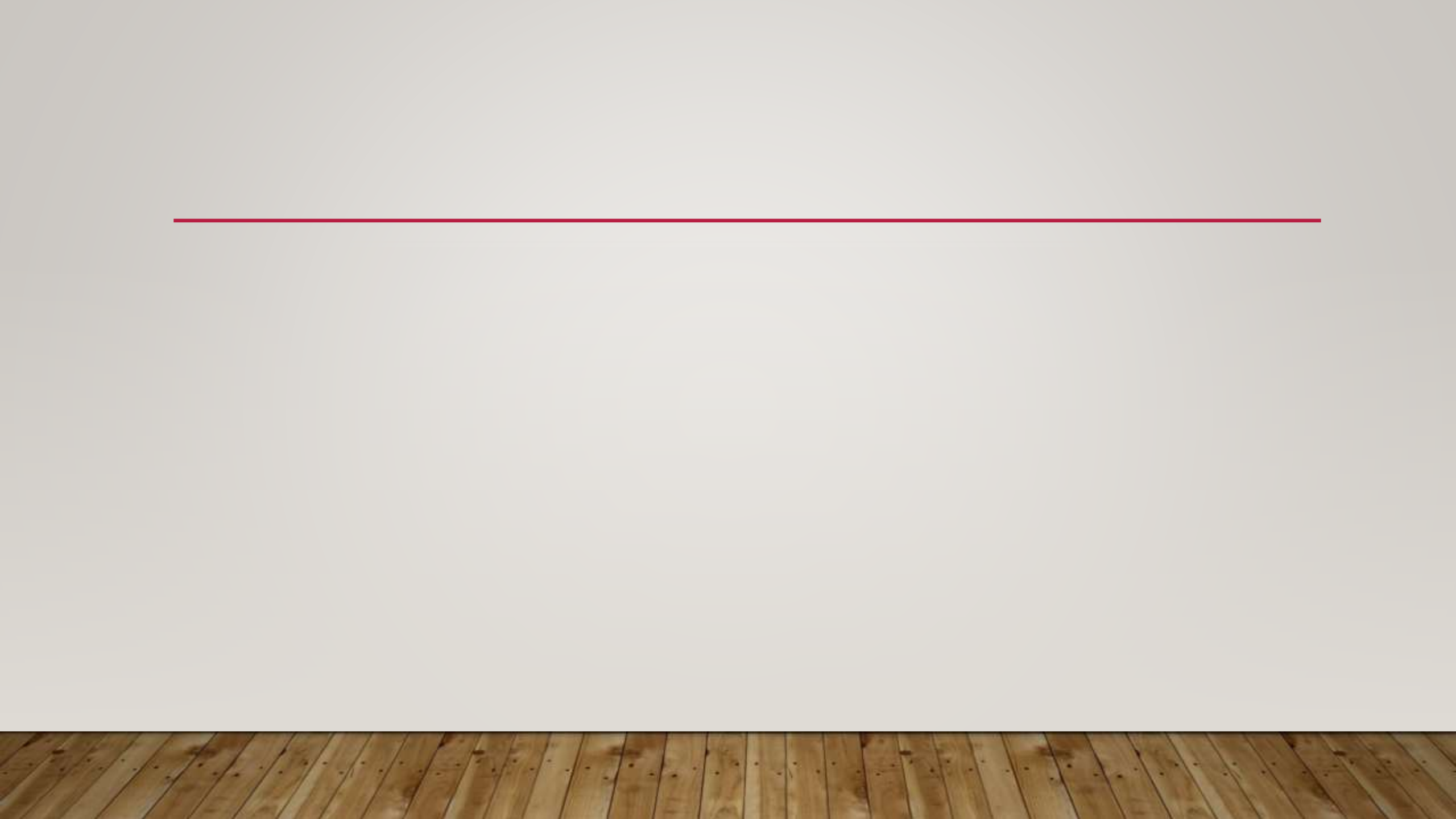
?
Connections
Help
Quit
Seize infrastructure master
Seize naming master
Seize PDC
Seize RID master
Seize schema master
Select operation target
Transfer infrastructure master
Transfer naming master
Transfer PDC
Transfer RID master
Transfer schema master

- Afficher ces informations d'aide
- Connexion à un contrôleur de domaine spécifique
- Afficher ces informations d'aide
- Revenir au menu précédent
- Remplace le rôle d'infrastructure sur le serveur connecté
- Remplace le rôle de maître d'attribution de noms sur le serveur connecté
- Remplace le rôle PDC sur le serveur connecté
- Remplace le rôle RID sur le serveur connecté
- Remplace le rôle de schéma sur le serveur connecté
- Sélection des sites, serveurs, domaines, rôles et contextes de nommage
- Faire du serveur connecté le maître d'infrastructure
- Faire du serveur connecté le maître d'attribution de noms
- Désigne le serveur connecté comme PDC
- Faire du serveur connecté le maître RID
- Faire du serveur connecté le maître de schéma

fsmo maintenance: _
```

Activer Windows  
Accédez aux paramètres pour activer Windows.

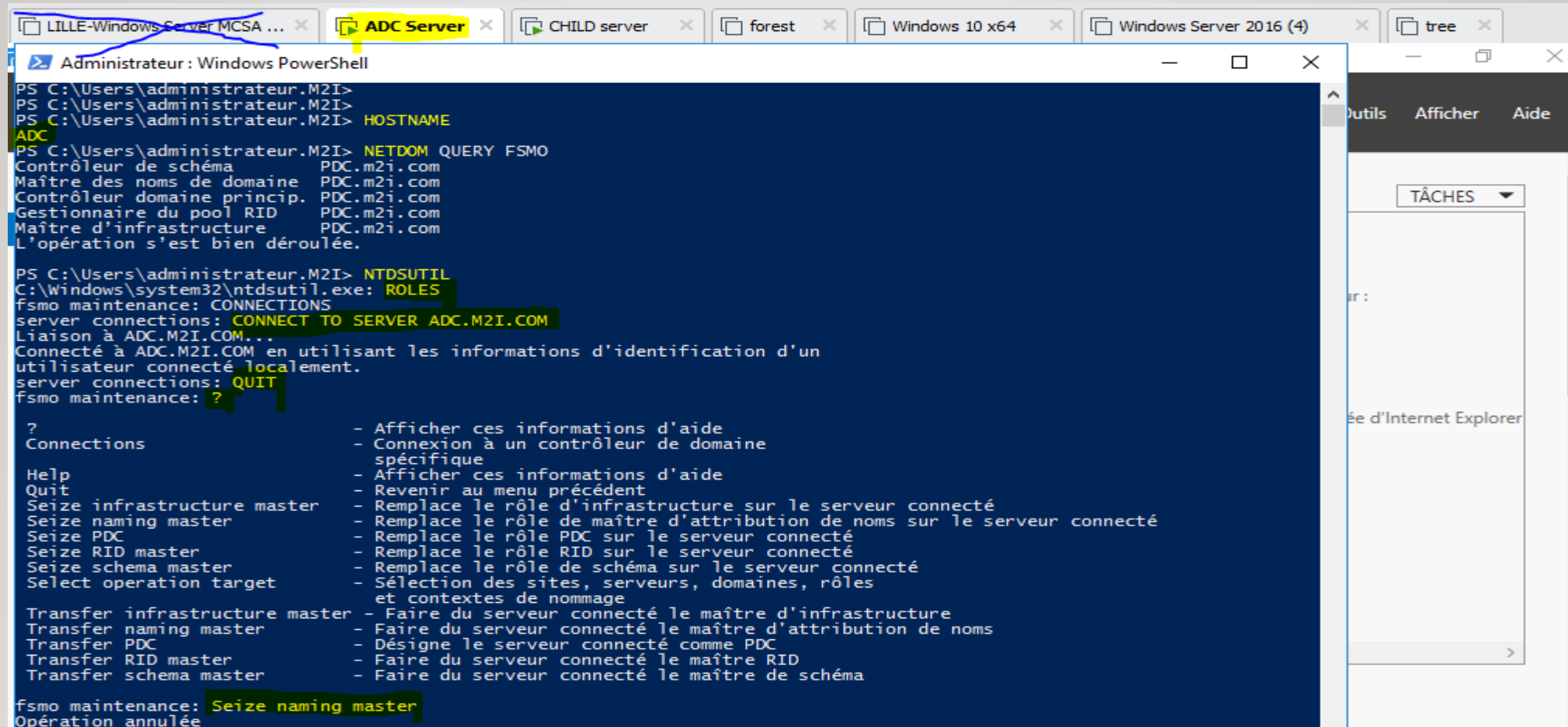
Explorateur de fichiers





# ETUDE DE CAS :

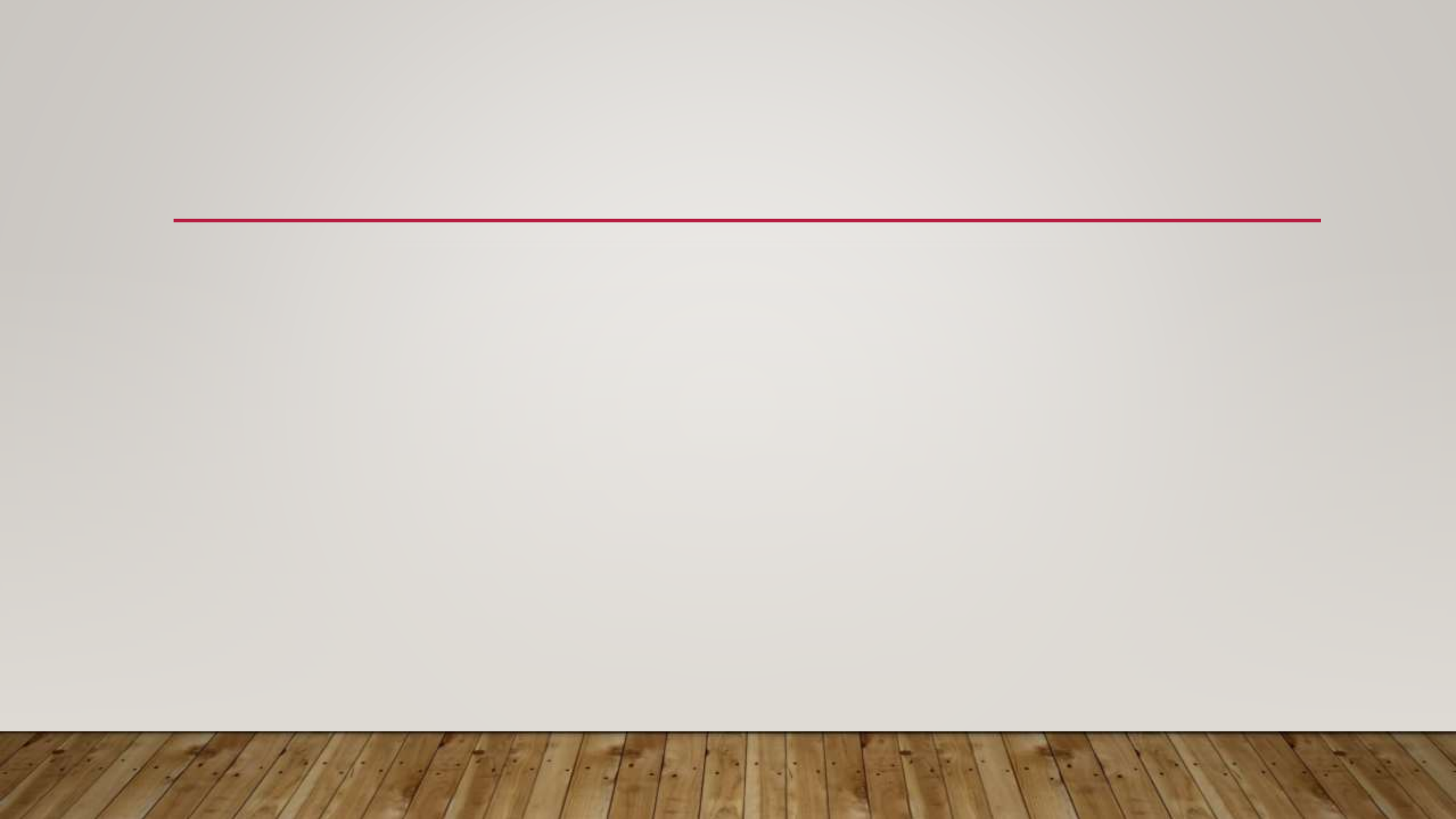
PDC SERVER EST CRACHER ET ON VEUT TRANSFERER LES ROLES (SN) ET (DNM)



The screenshot shows a Windows PowerShell console window titled "Administrateur : Windows PowerShell". The user is logged in as "administrateur.M2I". The console displays the following commands and output:

```
PS C:\Users\administrateur.M2I>
PS C:\Users\administrateur.M2I>
PS C:\Users\administrateur.M2I> HOSTNAME
ADC
PS C:\Users\administrateur.M2I> NETDOM QUERY FSMO
Contrôleur de schéma PDC.m2i.com
Maître des noms de domaine PDC.m2i.com
Contrôleur domaine princip. PDC.m2i.com
Gestionnaire du pool RID PDC.m2i.com
Maître d'infrastructure PDC.m2i.com
L'opération s'est bien déroulée.
PS C:\Users\administrateur.M2I> NTDSUTIL
C:\Windows\system32\ntdsutil.exe: ROLES
fsmo maintenance: CONNECTIONS
server connections: CONNECT TO SERVER ADC.M2I.COM
Liaison à ADC.M2I.COM...
Connecté à ADC.M2I.COM en utilisant les informations d'identification d'un
utilisateur connecté localement.
server connections: QUIT
fsmo maintenance: ?
?
Connections - Afficher ces informations d'aide
               - Connexion à un contrôleur de domaine
               spécifique
Help          - Afficher ces informations d'aide
Quit         - Revenir au menu précédent
Seize infrastructure master - Remplace le rôle d'infrastructure sur le serveur connecté
Seize naming master      - Remplace le rôle de maître d'attribution de noms sur le serveur connecté
Seize PDC                - Remplace le rôle PDC sur le serveur connecté
Seize RID master         - Remplace le rôle RID sur le serveur connecté
Seize schema master      - Remplace le rôle de schéma sur le serveur connecté
Select operation target  - Sélection des sites, serveurs, domaines, rôles
                        et contextes de nommage
Transfer infrastructure master - Faire du serveur connecté le maître d'infrastructure
Transfer naming master      - Faire du serveur connecté le maître d'attribution de noms
Transfer PDC                - Désigne le serveur connecté comme PDC
Transfer RID master         - Faire du serveur connecté le maître RID
Transfer schema master      - Faire du serveur connecté le maître de schéma
fsmo maintenance: Seize naming master
Opération annulée
```

The background of the PowerShell window is dark blue. The text is white. The user has highlighted the "ADC" output of the HOSTNAME command and the "CONNECT TO SERVER ADC.M2I.COM" command in the NTDSUTIL console. The "Seize naming master" command is also highlighted. The "Opération annulée" (Operation cancelled) message is shown at the bottom.




```
Administrateur : Windows PowerShell
PS C:\Users\administrateur.M2I>
PS C:\Users\administrateur.M2I>
PS C:\Users\administrateur.M2I> HOSTNAME
ADC
PS C:\Users\administrateur.M2I> NETDOM QUERY FSMO
Contrôleur de schéma PDC.m2i.com
Maître des noms de domaine PDC.m2i.com
Contrôleur domaine princip. PDC.m2i.com
Gestionnaire du pool RID PDC.m2i.com
Maître d'infrastructure PDC.m2i.com
L'opération s'est bien déroulée.

PS C:\Users\administrateur.M2I> NTDSUTIL
C:\Windows\system32\ntdsutil.exe: ROLES
fsmo maintenance: CONNECTIONS
server connections: CONNECT TO SERVER ADC.M2I.COM
Liaison à ADC.M2I.COM...
Connecté à ADC.M2I.COM en utilisant les informations d'identification d'un
utilisateur connecté localement.
server connections: QUIT
fsmo maintenance: ?

? - Affich
Connections - Connex
spécif
Help - Affich
Quit - Reven
Seize infrastructure master - Rempla
Seize naming master - Rempla
Seize PDC - Rempla
Seize RID master - Rempla
Seize schema master - Rempla
Select operation target - Sélect
et cor
Transfer infrastructure master - Faire
Transfer naming master - Faire
Transfer PDC - Désign
Transfer RID master - Faire
Transfer schema master - Faire

fsmo maintenance: Seize naming master
Opération annulée
fsmo maintenance: Seize naming master
```

Boîte de dialogue de confirmation de cessation de rôle

 Voulez-vous vraiment que le serveur « ADC.M2I.COM » prenne le rôle  
domain naming avec la valeur  
ci-dessous ?

CN=NTDS  
Settings,CN=ADC,CN= Servers,CN= Nice,CN= Sites,CN= Configuration,D  
C=m2i,DC=com

```
LILLE-Windows Server MCSA ... x ADC Server x CHILD server x forest x Windows 10 x64 x Windows Server 2016 (4)
Administrateur : Windows PowerShell

Transfer RID master - Faire du serveur connecté le maître RID
Transfer schema master - Faire du serveur connecté le maître de schéma

fsmo maintenance: Seize naming master
Opération annulée
fsmo maintenance: Seize naming master
Tentative de transfert sûr de domain naming FSMO avant la cessation.
Erreur ldap_modify_sW 0x34(52 (Non disponible)).
Le message d'erreur étendue Ldap est 000020AF: SvcErr: DSID-03210494, problem 5002 (UNAVAILABLE), data 5

L'erreur Win32 renvoyée est 0x20af(L'opération FSMO demandée a échoué. Le propriétaire FSMO actuel n'a pas pu être contacté.)
)
Selon le code d'erreur, ceci peut indiquer une erreur Ldap, de connexion ou de transfert de rôle.
Le transfert de domain naming FSMO a échoué, cessation en cours...
Le serveur « ADC.M2I.COM » est informé de 5 rôles
Schéma - CN=NTDS Settings,CN=PDC,CN=Servers,CN=Lille,CN=Sites,CN=Configuration,DC=m2i,DC=com
Maître d'attribution de noms - CN=NTDS Settings,CN=ADC,CN=Servers,CN=Nice,CN=Sites,CN=Configuration,DC=m2i,DC=com
PDC - CN=NTDS Settings,CN=PDC,CN=Servers,CN=Lille,CN=Sites,CN=Configuration,DC=m2i,DC=com
RID - CN=NTDS Settings,CN=PDC,CN=Servers,CN=Lille,CN=Sites,CN=Configuration,DC=m2i,DC=com
Infrastructure - CN=NTDS Settings,CN=PDC,CN=Servers,CN=Lille,CN=Sites,CN=Configuration,DC=m2i,DC=com
fsmo maintenance: Seize schema master
Tentative de transfert sûr de schema FSMO avant la cessation.
Erreur ldap_modify_sW 0x34(52 (Non disponible)).
Le message d'erreur étendue Ldap est 000020AF: SvcErr: DSID-03210494, problem 5002 (UNAVAILABLE), data 5

L'erreur Win32 renvoyée est 0x20af(L'opération FSMO demandée a échoué. Le propriétaire FSMO actuel n'a pas pu être contacté.)
)
Selon le code d'erreur, ceci peut indiquer une erreur Ldap, de connexion ou de transfert de rôle.
Le transfert de schema FSMO a échoué, cessation en cours...
Le serveur « ADC.M2I.COM » est informé de 5 rôles
Schéma - CN=NTDS Settings,CN=ADC,CN=Servers,CN=Nice,CN=Sites,CN=Configuration,DC=m2i,DC=com
Maître d'attribution de noms - CN=NTDS Settings,CN=ADC,CN=Servers,CN=Nice,CN=Sites,CN=Configuration,DC=m2i,DC=com
PDC - CN=NTDS Settings,CN=PDC,CN=Servers,CN=Lille,CN=Sites,CN=Configuration,DC=m2i,DC=com
RID - CN=NTDS Settings,CN=PDC,CN=Servers,CN=Lille,CN=Sites,CN=Configuration,DC=m2i,DC=com
Infrastructure - CN=NTDS Settings,CN=PDC,CN=Servers,CN=Lille,CN=Sites,CN=Configuration,DC=m2i,DC=com
fsmo maintenance: QUIT
C:\Windows\system32\ntdsutil.exe: QUIT
PS C:\Users\administrateur.M2I> NETDOM QUERY FSMO
Contrôleur de schéma ADC.m2i.com
Maître des noms de domaine ADC.m2i.com
Contrôleur domaine princ. PDC.m2i.com
Gestionnaire du pool RID PDC.m2i.com
Maître d'infrastructure PDC.m2i.com
L'opération s'est bien déroulée.

PS C:\Users\administrateur.M2I>
```