Windows Server

Administration Windows Server 2012

Chapitre 2:Présentation des services de domaine Active Directory

AIT MOULAY

Vue d'ensemble du chapitre

- Vue d'ensemble d'AD DS.
- Vue d'ensemble des contrôleurs de domaine.
- Installation d'un contrôleur de domaine.

Partie 1 : Vue d'ensemble d'AD DS

- Vue d'ensemble d'AD DS
- Que sont les domaines AD DS ?
- Que sont les unités d'organisation ?
- Qu'est-ce qu'une forêt AD DS ?
- Qu'est-ce que le schéma AD DS ?

Vue d'ensemble d'AD DS

- La base de données AD DS stocke des informations sur l'identité de l'utilisateur, les ordinateurs, les groupes, les services et les ressources.
- Les contrôleurs de domaine AD DS hébergent également le service qui authentifie les comptes d'utilisateur et d'ordinateur quand ils se connectent au domaine.
- AD DS constitue le principal moyen vous permettant de configurer et gérer les comptes d'utilisateur et d'ordinateur dans votre réseau.

Vue d'ensemble d'AD DS

AD DS se compose à la fois de composants physiques et logiques

Composants physiques

- Magasin de données
- Contrôleurs de domaine
- Serveur de catalogue global
- Contrôleur de domaine en lecture seule

Composants logiques

- Partitions
- Schéma
- Domaines
- Arborescences de domaines
- Forêts
- Sites
- Unités d'organisation

Vue d'ensemble d'AD DS

- Les informations relatives à AD DS sont stockées dans un fichier unique sur le disque dur de chaque contrôleur de domaine. Le tableau suivant répertorie quelques composants physiques et où ils sont stockés.

Composant physique	Description
Contrôleurs de domaine	Contiennent des copies de la base de données AD DS.
Magasin de données	Fichier sur chaque contrôleur de domaine qui stocke les informations AD DS.
Serveurs de catalogue global	Hébergent le catalogue global, lequel est une copie partielle, en lecture seule, de tous les objets dans la forêt. Un catalogue global accélère les recherches d'objets susceptibles d'être stockés sur des contrôleurs de domaine d'un domaine différent de la forêt.
Contrôleurs de domaine en lecture seule (RODC)	Installation spéciale d'AD DS dans une forme en lecture seule. Elle est souvent utilisée dans les filiales où la sécurité et l'assistance informatique sont souvent moins avancées que dans les centres d'affaires principaux.

Vue d'ensemble d'AD DS

- Les composants logiques AD DS sont des structures utilisées pour l'implémentation d'une conception Active Directory appropriée à une organisation. Le tableau suivant décrit certains types de structures logiques qu'une base de données Active Directory peut contenir.

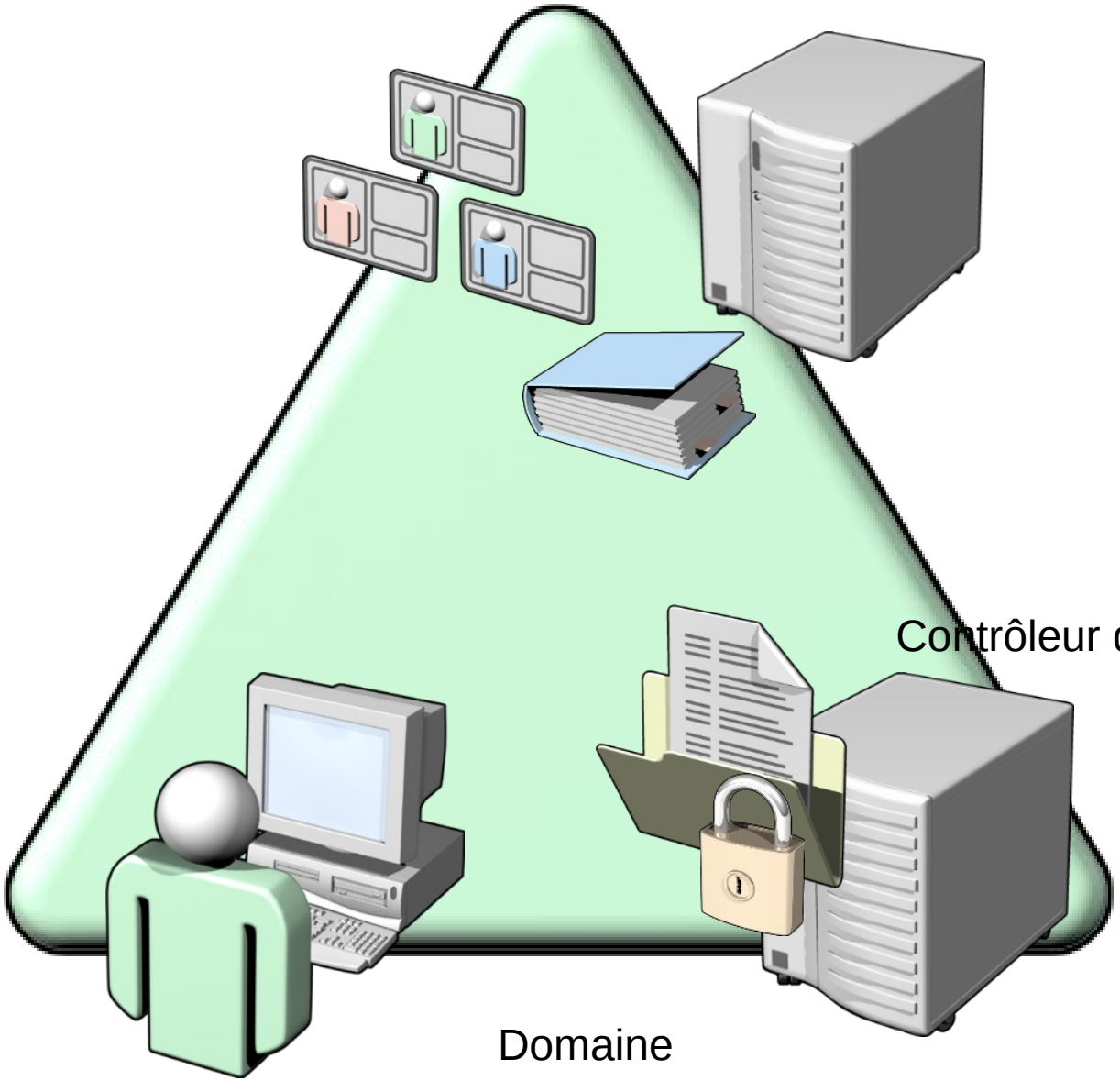
Vue d'ensemble d'AD DS

Composant logique	Description
Partition	Une section de la base de données AD DS. Bien que la base de données soit un seul fichier nommé NTDS.DIT, elle est affichée, gérée et répliquée comme si elle était composée de sections ou d'instances distinctes. Celles-ci sont appelées partitions ou encore contextes d'appellation.
Schéma	Définit la liste des types d'objets et d'attributs que tous les objets dans AD DS peuvent avoir.
Domaine	Limite d'administration logique pour les utilisateurs et les ordinateurs.
Arborescence de domaine	Collection des domaines qui partagent un domaine racine commun et un espace de noms DNS (Domain Name System).
Forêt	Collection des domaines qui partagent un service AD DS commun.
Site	Collection d'utilisateurs, de groupes et d'ordinateurs, tels qu'ils sont définis par leurs emplacements physiques. Les sites sont utiles dans des tâches d'administration de la planification telles que la réplication des modifications apportées à la base de données AD DS.
Unité d'organisation	Les unités d'organisation (OU) sont des conteneurs dans AD DS qui fournissent une infrastructure pour déléguer des droits d'administration et pour lier des objets de stratégie de groupe (GPO).

Que sont les domaines AD DS ?

- Un domaine AD DS est un regroupement logique d'objets (utilisateur, ordinateur et groupe), créé pour des raisons de gestion et de sécurité.
- Tous ces objets sont enregistrés dans la base de données AD DS et une copie de cette base de donnée est enregistrée sur chaque contrôleur de domaine dans le domaine AD DS.
- Le domaine AD DS est également une limite de réplication c’est à dire lorsque des changements sont apportés à n'importe quel objet du domaine, ces changements sont répliqués automatiquement sur tous les autres contrôleurs de domaine du domaine.
- Un domaine AD DS est un centre d'administration. Il contient un compte Administrateur et un groupe Administrateurs du domaine ; chacun a le contrôle total sur chaque objet du domaine. leur plage de contrôle est toutefois limitée au domaine.
- Le domaine AD DS fournit un centre d'authentification. Tous les comptes d'utilisateur et comptes d'ordinateur dans le domaine sont stockés dans la base de données du domaine, et les utilisateurs et les ordinateurs doivent se connecter à un contrôleur de domaine pour s'authentifier.

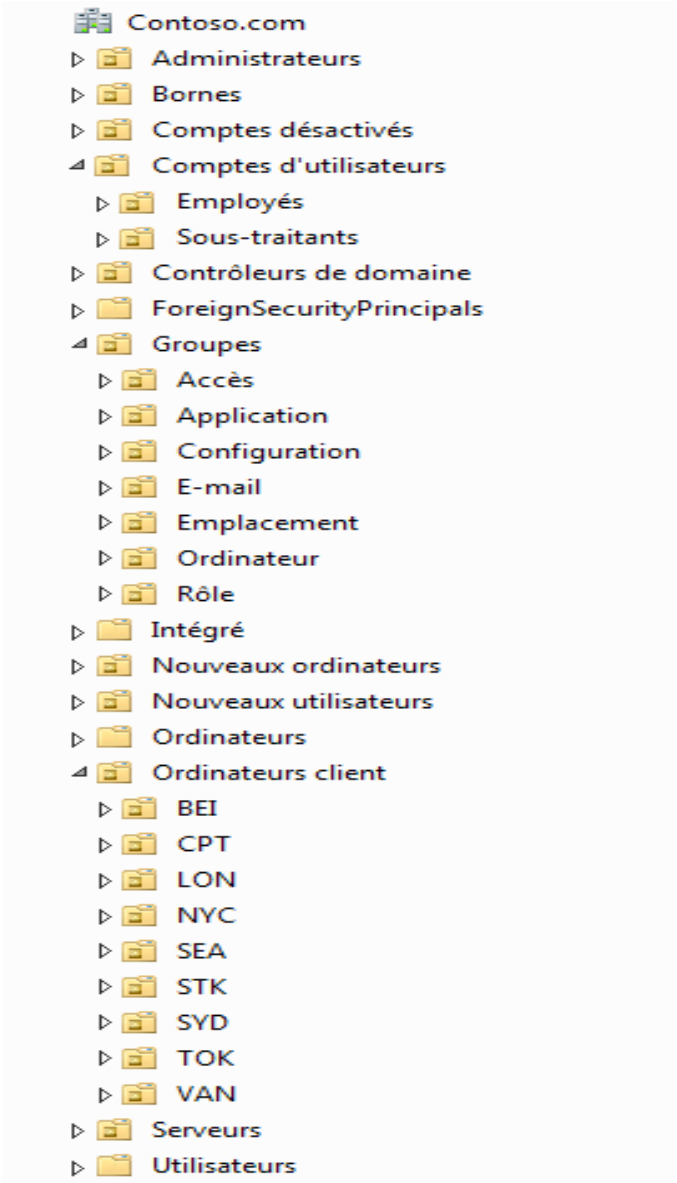
Que sont les domaines AD DS ?



Que sont les unités d'organisation ?

- Une unité d'organisation (OU) est un objet conteneur dans un domaine, que vous pouvez utiliser pour regrouper des utilisateurs, des groupes, des ordinateurs et d'autres objets. Vous pouvez créer des unités d'organisation pour deux raisons :
  - Pour configurer des objets contenus dans l'unité d'organisation et appliquer des stratégies de groupe.
  - Pour déléguer le contrôle administratif d'objets présents dans l'unité d'organisation à d’autres utilisateurs.

Que sont les unités d'organisation ?

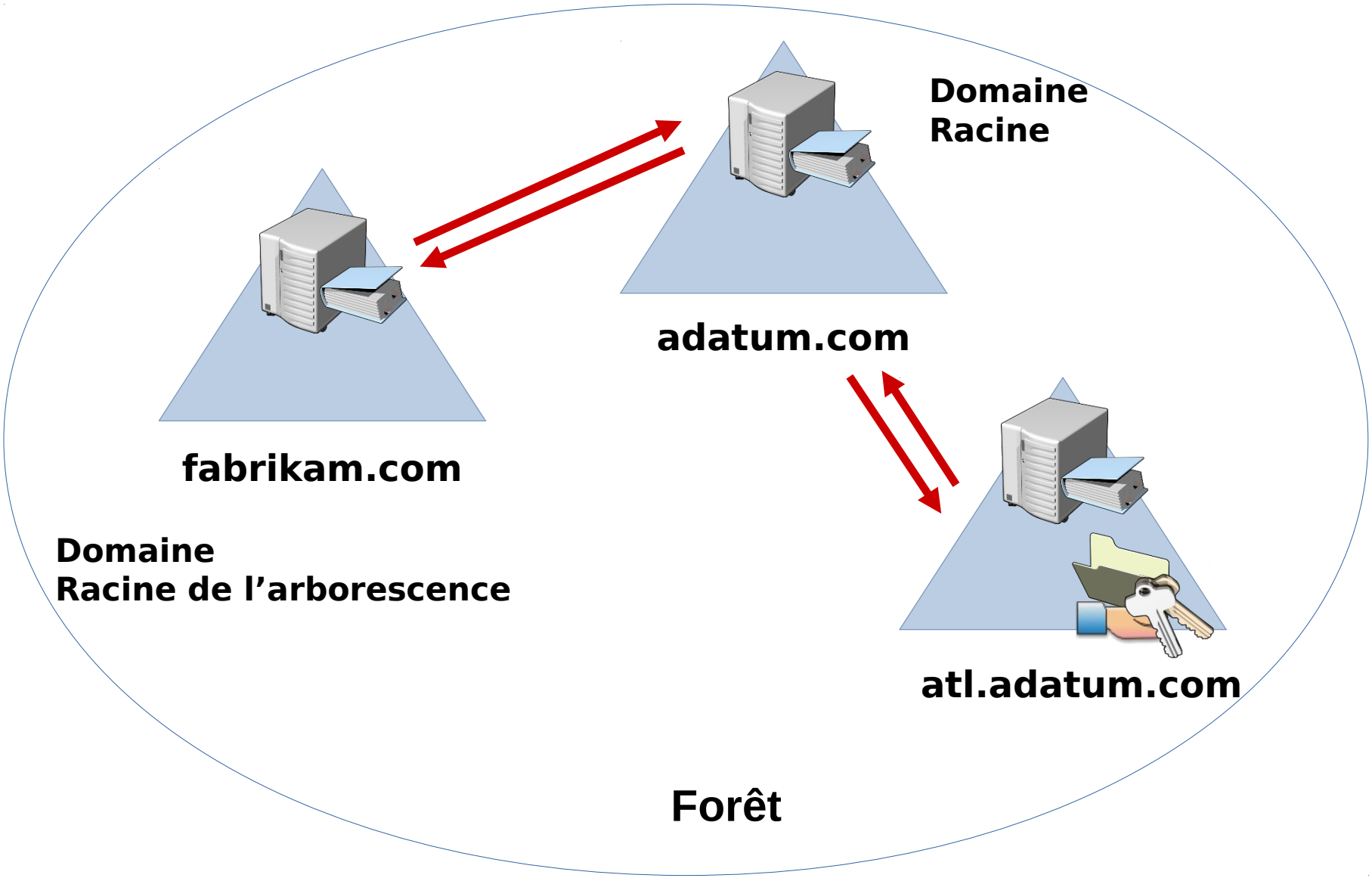


- Vous pouvez utiliser des unités d'organisation pour représenter les structures hiérarchiques et logiques au sein de votre organisation.
- Par exemple, vous pouvez créer des unités d'organisation qui représentent les différents services de votre organisation, les régions géographiques de votre organisation ou une combinaison des services et des régions géographiques.

Qu'est-ce qu'une forêt AD DS ?

- Une forêt est une collection d'une ou plusieurs arborescences de domaines.
- Le premier domaine qui est créé dans la forêt est appelé le domaine racine de la forêt.
- Le domaine racine de la forêt contient quelques objets qui n'existent pas dans d'autres domaines de la forêt.
  - Par exemple, le domaine racine de la forêt contient deux rôles de contrôleur de domaine spéciaux, le contrôleur de schéma et le maître d'opérations des noms de domaine.
  - Le domaine racine contient aussi le groupe Administrateurs de l'entreprise et le groupe Administrateurs du schéma. Le groupe Administrateurs de l'entreprise a le contrôle total sur chaque domaine de la forêt.
- La forêt AD DS est une limite de sécurité. Ceci signifie que, par défaut, aucun utilisateur provenant de l'extérieur de la forêt ne peut accéder à une ressource située à l'intérieur de la forêt.
- La forêt AD DS est également la limite de réplication pour les partitions de configuration et de schéma dans la base de données AD DS. Ceci signifie que tous les contrôleurs de domaine de la forêt doivent partager le même schéma
- Par défaut, tous les domaines d'une forêt approuvent automatiquement les autres domaines de la forêt. Ceci facilite l'activation de l'accès à des ressources telles que des partages de fichiers et des sites Web pour tous les utilisateurs dans une forêt, indépendamment du domaine dans lequel le compte d'utilisateur est situé.

Qu'est-ce qu'une forêt AD DS ?



Qu'est-ce que le schéma AD DS ?

- Le schéma AD DS est le composant AD DS qui définit tous les types d'objet et attributs qu'AD DS utilise pour stocker des données.
- AD DS utilise des objets comme unités de stockage. Tous les types d'objet sont définis dans le schéma. Chaque fois que l'annuaire traite des données, il interroge le schéma pour obtenir une définition d'objet appropriée
- Dans AD DS, le schéma définit les éléments suivants :
  - les objets qui sont utilisés pour stocker des données dans l'annuaire ;
  - les règles qui définissent quels types d'objet vous pouvez créer, quels attributs doivent être définis (obligatoire) quand vous créez l'objet et quels attributs sont facultatifs ;
  - la structure et le contenu de l'annuaire lui-même.

Qu'est-ce que le schéma AD DS ?

- Vous pouvez utiliser un compte qui est un membre des administrateurs de schéma pour modifier les composants de schéma
- Les types des objets qui sont définis dans le schéma comprennent **l'utilisateur, l'ordinateur, le groupe et le site**.
- Parmi les nombreux attributs sont compris les suivants : **location, accountExpires, buildingName, company, manager et displayName.**
- Le contrôleur de schéma est un contrôleur de domaine à partir du quel on peut modifier le schéma.
- Tout changement qui est apporté au schéma est répliqué sur chaque contrôleur de domaine de la forêt à partir du titulaire du rôle contrôleur de schéma.

Partie 2 : Vue d'ensemble des contrôleurs de domaine

- Qu'est-ce qu'un contrôleur de domaine ?
- Qu'est-ce que le catalogue global ?
- Que sont les maîtres d'opérations ?

Qu'est-ce qu'un contrôleur de domaine ?

- Un contrôleur de domaine est un serveur configuré pour stocker une copie de la base de données d'annuaire AD DS (NTDS.DIT) et une copie du dossier SYSVOL.
- Tous les contrôleurs de domaine, à l'exception des contrôleurs de domaine en lecture seule, stockent une copie en lecture/écriture de NTDS.DIT et du dossier SYSVOL.
- NTDS.DIT est la base de données elle-même et le dossier SYSVOL contient tous les paramètres de modèle des objets GPO.
- Il est possible d'initier des modifications de la base de données AD DS sur n'importe quel contrôleur de domaine d'un domaine, à l'exception des contrôleurs de domaine en lecture seule. Le service de réplication AD DS synchronise alors les modifications et les mises à jour de la base de données AD DS sur tous les autres contrôleurs de domaine du domaine.
- Les dossiers SYSVOL sont répliqués par le service de réplication de fichiers (FRS) ou par la réplication DFS (Distributed File System) plus récente.

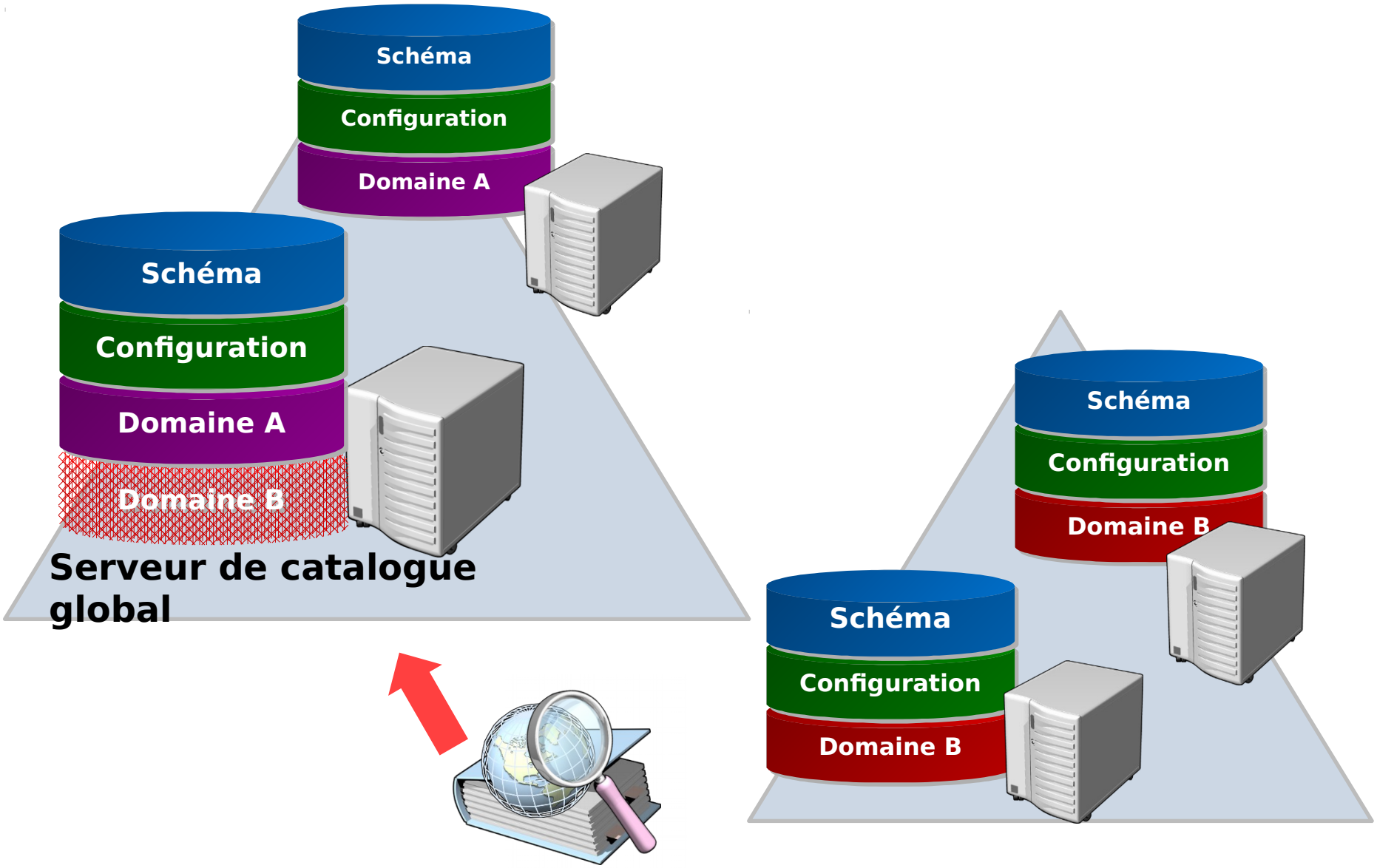
Qu'est-ce qu'un contrôleur de domaine ?

- les contrôleurs de domaine hébergent plusieurs autres services liés à Active Directory dont:
  - le service d'authentification Kerberos,
  - et le centre de distribution de clés (KDC)
- Meilleures pratiques pour déployer un contrôleur de domaine.
  - **Disponibilité** : Au moins deux contrôleurs de domaine dans un domaine
  - **Sécurité** : Contrôleur de domaine en lecture seule et BitLocker

Qu'est-ce que le catalogue global ?

- Dans un même domaine, la base de données AD DS contient toutes les informations sur chaque objet présent dans ce domaine. Ces informations ne sont pas répliquées en dehors du domaine.
  - Par exemple, une requête pour un objet dans AD DS est dirigée vers l'un des contrôleurs de domaine pour ce domaine. Si la forêt contient plusieurs domaines, cette requête ne fournit aucun résultat pour des objets figurant dans un autre domaine.
- Pour permettre une recherche sur plusieurs domaines, vous pouvez configurer un ou plusieurs contrôleurs de domaine pour stocker une copie du catalogue global.
- Le catalogue global est une base de données distribuée qui contient une représentation pouvant faire l'objet d'une recherche de tous les objets issus de tous les domaines d'une forêt.
- Par défaut, le seul serveur de catalogue global qui est créé est le premier contrôleur de domaine dans le domaine racine de la forêt.

Qu'est-ce que le catalogue global ?



Que sont les maîtres d'opérations ?

- Bien que tous les contrôleurs de domaine soient essentiellement égaux, certaines tâches peuvent être effectuées uniquement en ciblant un contrôleur de domaine particulier.
  - Par exemple, si vous devez ajouter un domaine supplémentaire à la forêt, vous devez être en mesure de vous connecter au maître d'opérations des noms de domaine.
- Les contrôleurs de domaine dotés de ces rôles sont :
  - les maîtres d'opérations ;
  - les rôles de maître unique ;
  - les opérations à maître unique flottant (FSMO).
- Ces rôles sont distribués comme suit :
  - Chaque forêt possède un contrôleur de schéma et un maître d'opérations des noms de domaine.
  - Chaque domaine AD DS possède un maître RID, un maître d'infrastructure et un émulateur de contrôleur de domaine principal (PDC).

Que sont les maîtres d'opérations ?

Maîtres d'opérations de forêt

- Les rôles suivants sont les rôles de maître unique présents dans une forêt :
  - **Maître d'attribution de noms de domaine**. Il s'agit du contrôleur de domaine qui doit être contacté lorsque vous ajoutez ou supprimez un domaine, ou lorsque vous apportez des modifications de nom à des domaines.
  - **Contrôleur de schéma**. Il s'agit du contrôleur de domaine sur lequel toutes les modifications de schéma sont effectuées.

Que sont les maîtres d'opérations ?

Maîtres d'opérations de domaine

- Les rôles suivants sont les rôles de maître unique présents dans un domaine :
  - **Maître RID**. Chaque fois qu'un objet est créé dans AD DS, le contrôleur de domaine sur lequel l'objet est créé attribue à l'objet un numéro d'identification unique SID. Pour garantir que deux contrôleurs de domaine ne peuvent pas attribuer le même SID à deux objets différents, le maître RID alloue des blocs de RID (Relative ID) à chaque contrôleur de domaine dans le domaine.
  - **Maître d'infrastructure**. Ce rôle est responsable de la conservation des références d'objets inter-domaines, par exemple lorsqu'un groupe dans un domaine contient un membre issu d'un autre domaine. Dans cette situation,le maître d'infrastructure est responsable du maintien de l'intégrité de cette référence
    - Par exemple, lorsque vous regardez l'onglet de sécurité d'un objet, le système recherche les SID qui sont répertoriés et les traduit en noms. Dans une forêt à plusieurs domaines, le maître d'infrastructure recherche les SID dans les autres domaines.

Que sont les maîtres d'opérations ?

Maîtres d'opérations de domaine (suite)

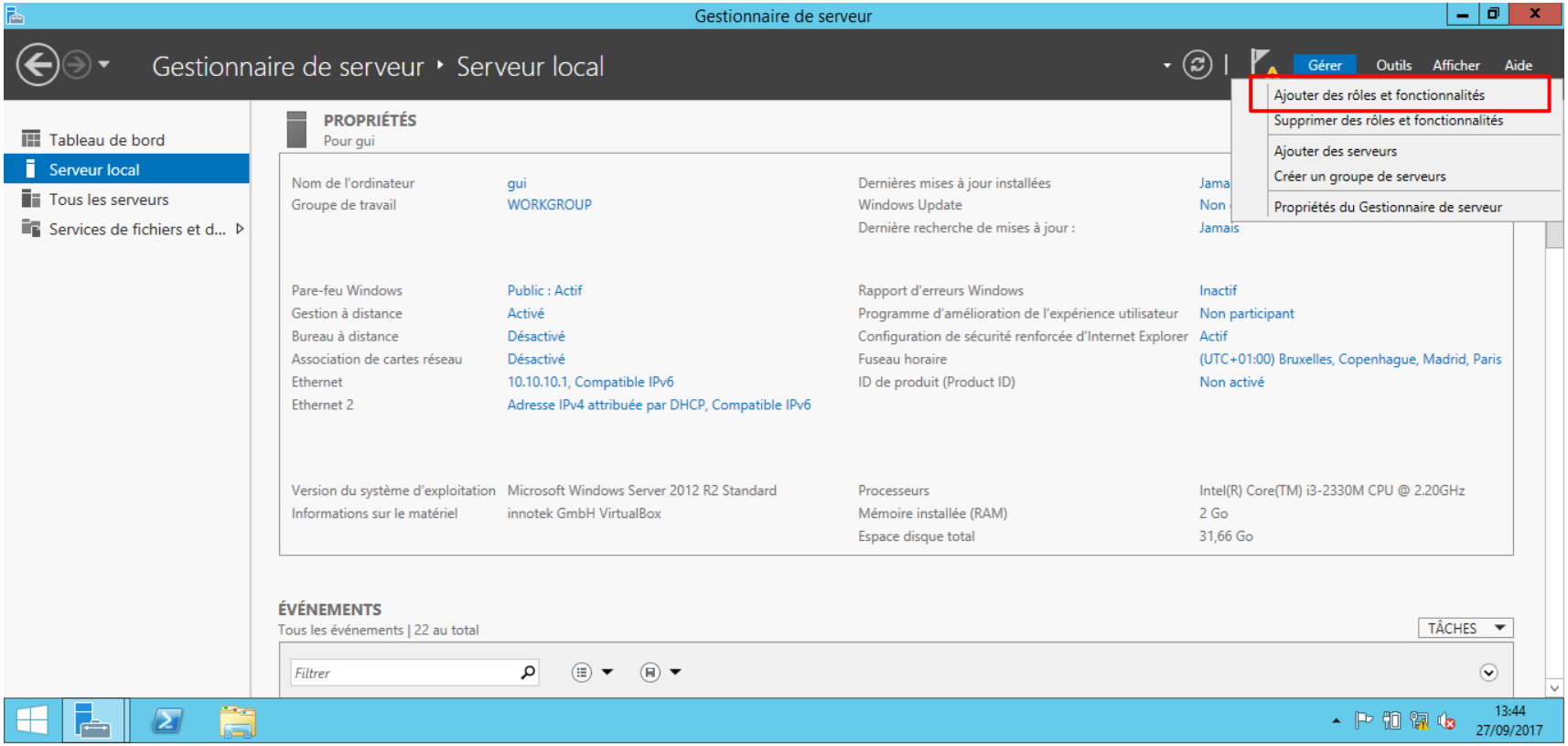
- **Maître d'émulateur de contrôleur de domaine principal (émulateur PDC)** représente la source de temps pour le domaine.
- L'émulateur PDC est également le contrôleur de domaine qui reçoit les changements de mot de passe urgents. Si le mot de passe d'un utilisateur est modifié, ces informations sont envoyées immédiatement au contrôleur de domaine détenant le rôle d'émulateur PDC. Ceci signifie que si l'utilisateur essaie ultérieurement de se connecter et qu'il est authentifié par un contrôleur de domaine dans un emplacement différent qui n'a pas encore reçu une mise à jour concernant le nouveau mot de passe, le contrôleur de domaine dans l'emplacement où l'utilisateur essaie de se connecter contacte le contrôleur de domaine détenant le rôle d'émulateur PDC et vérifie les modifications récentes.
- L'émulateur PDC est également utilisé lors de la modification d'objets GPO. Lorsqu'un objet GPO autre qu'un objet GPO local est ouvert pour être modifié, la copie qui est modifiée est celle qui est stockée sur l'émulateur PDC.

Partie 3 : Installation d'un contrôleur de domaine

- Installation d'un contrôleur de domaine à partir du Gestionnaire de serveur
- Installation d'un contrôleur de domaine sur une installation minimale de Windows Server 2012
- Mise à niveau d'un contrôleur de domaine

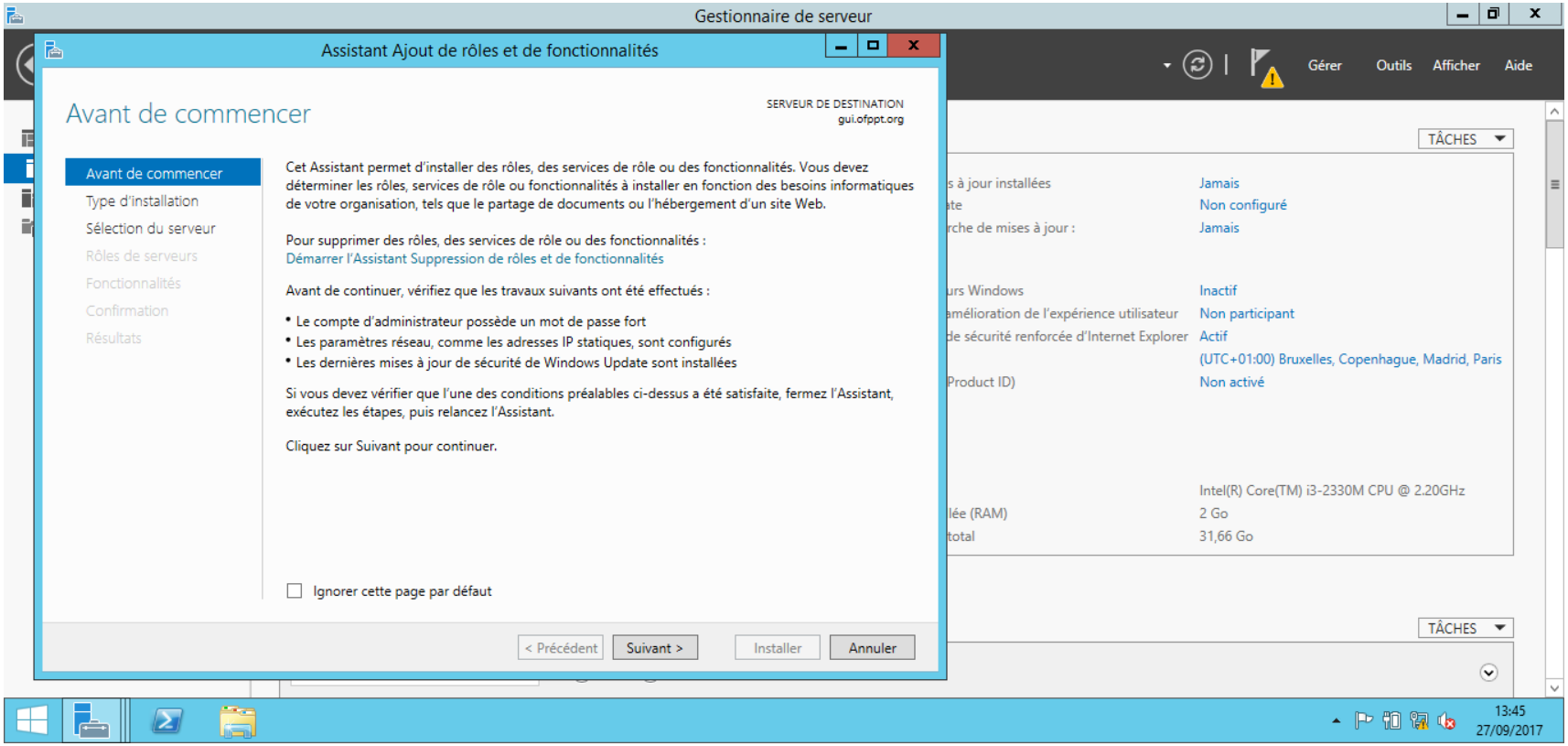
Installation d'un contrôleur de domaine à partir du Gestionnaire de serveur

Installer les services AD DS



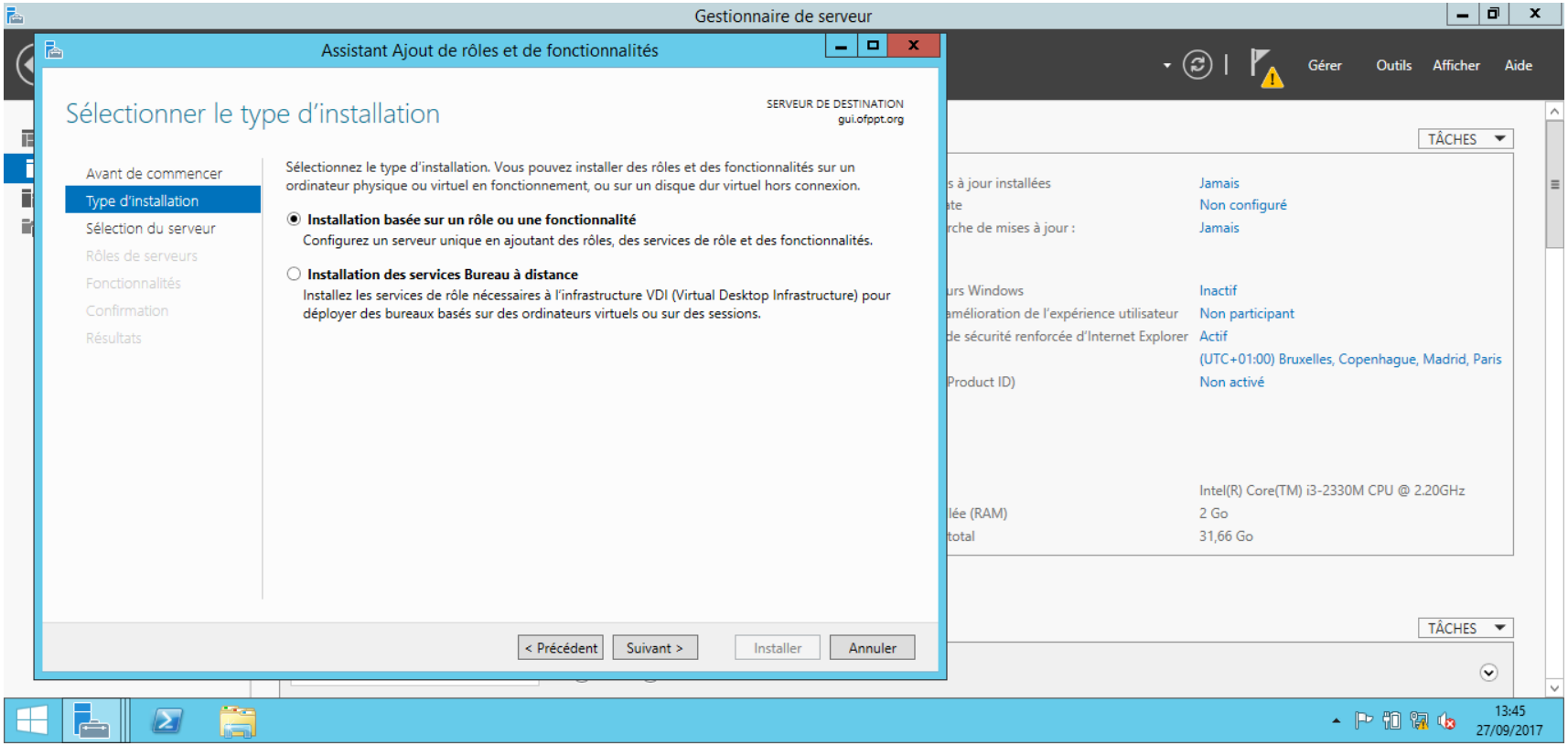
Installation d'un contrôleur de domaine à partir du Gestionnaire de serveur

Installer les services AD DS



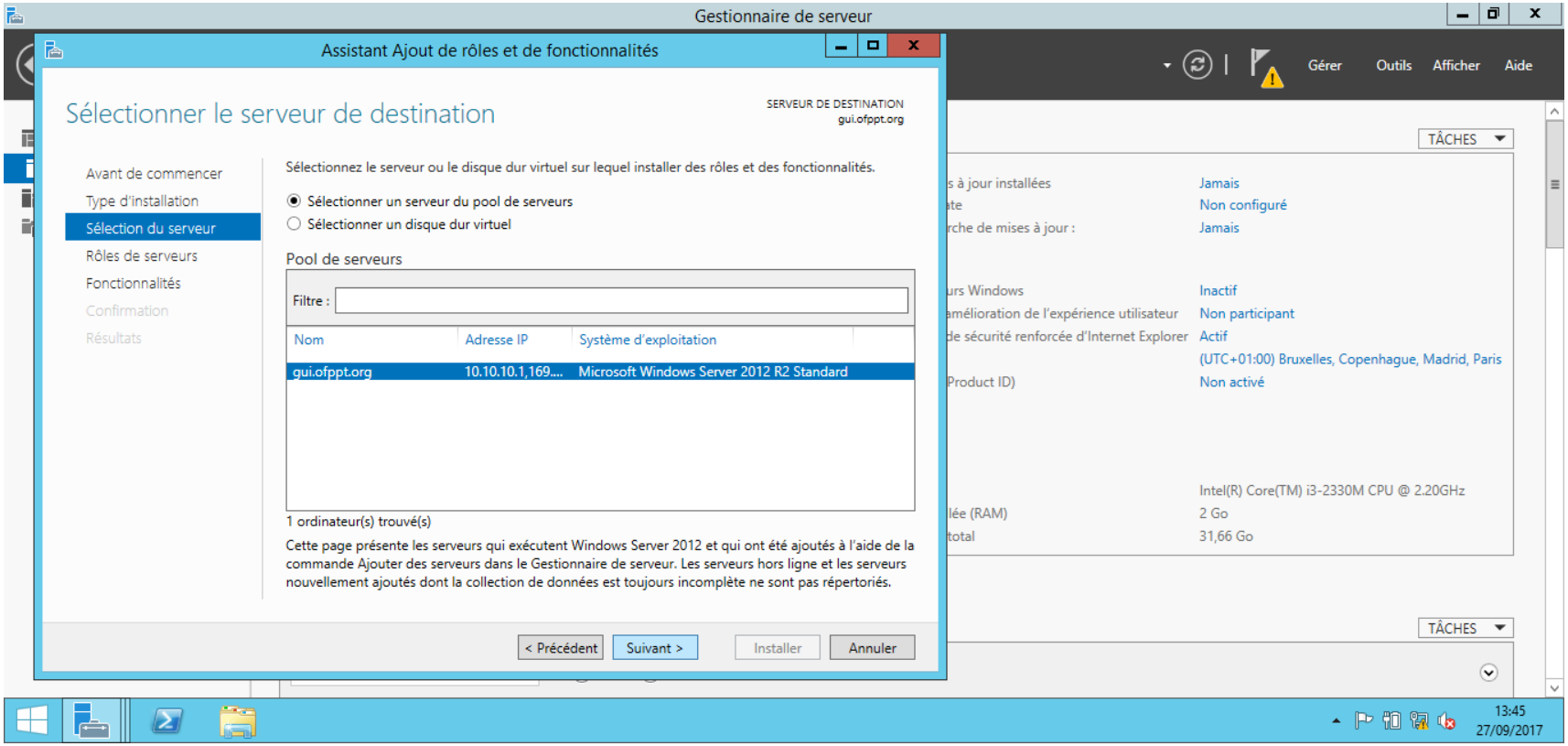
Installation d'un contrôleur de domaine à partir du Gestionnaire de serveur

Installer les services AD DS



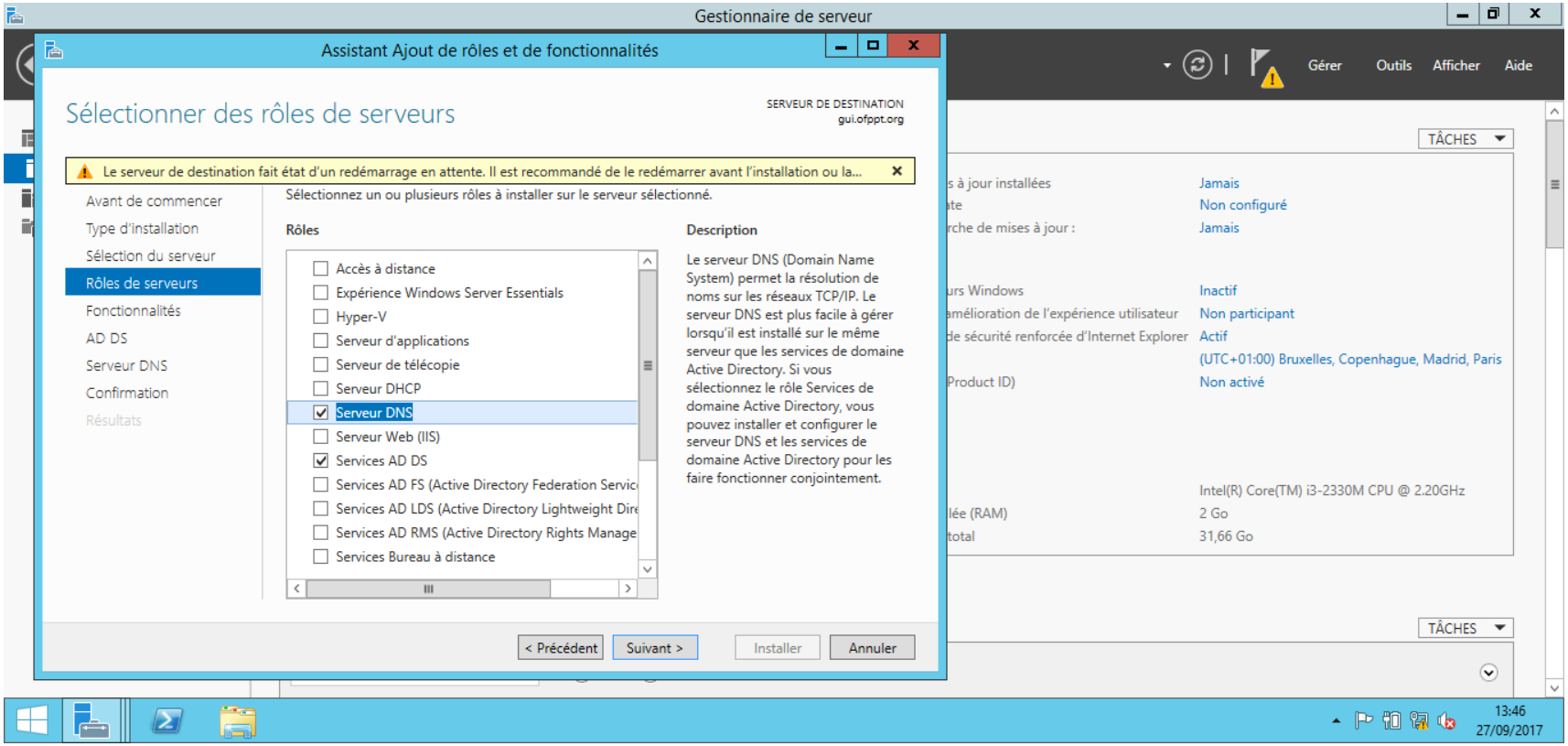
Installation d'un contrôleur de domaine à partir du Gestionnaire de serveur

Installer les services AD DS



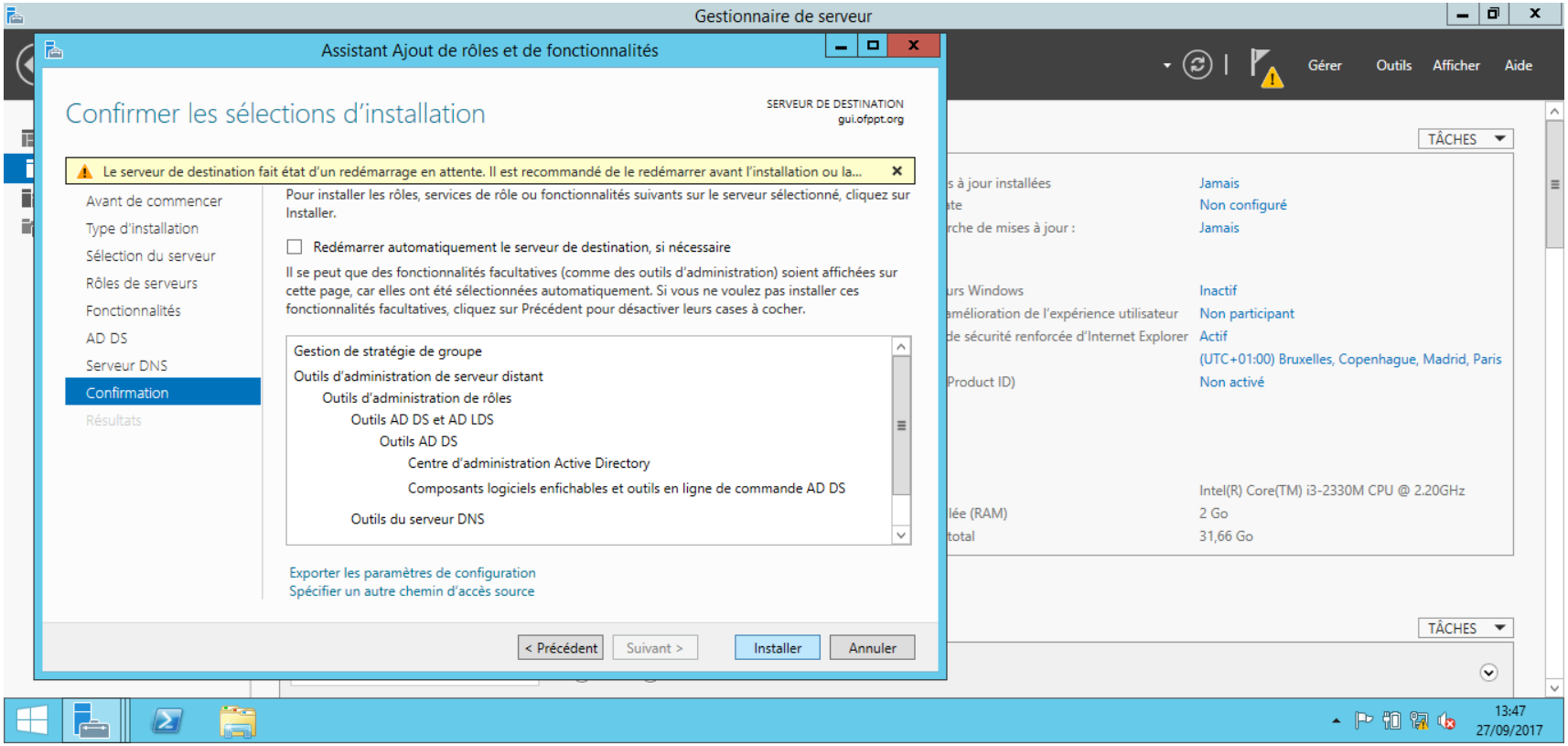
Installation d'un contrôleur de domaine à partir du Gestionnaire de serveur

Installer les services AD DS



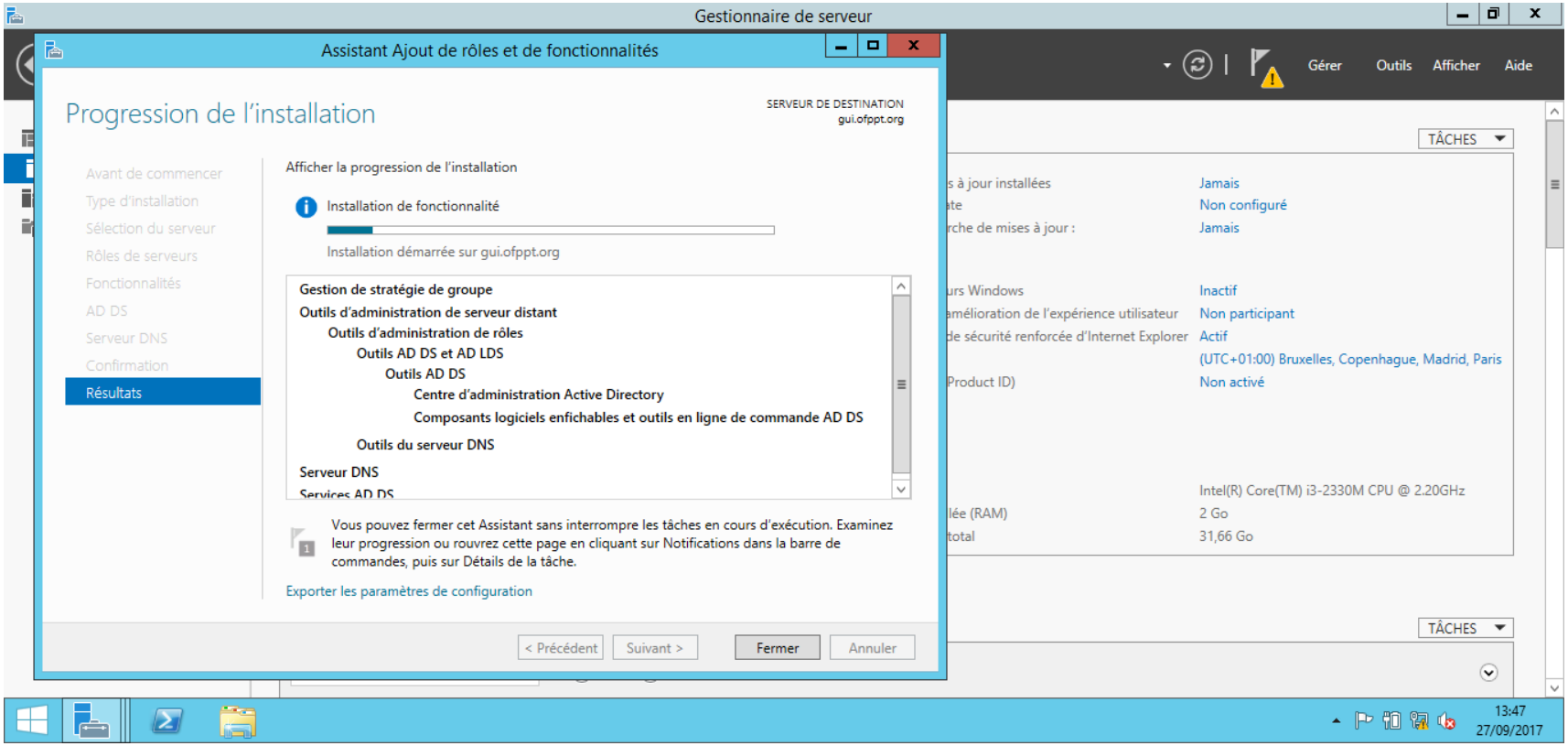
Installation d'un contrôleur de domaine à partir du Gestionnaire de serveur

Installer les services AD DS



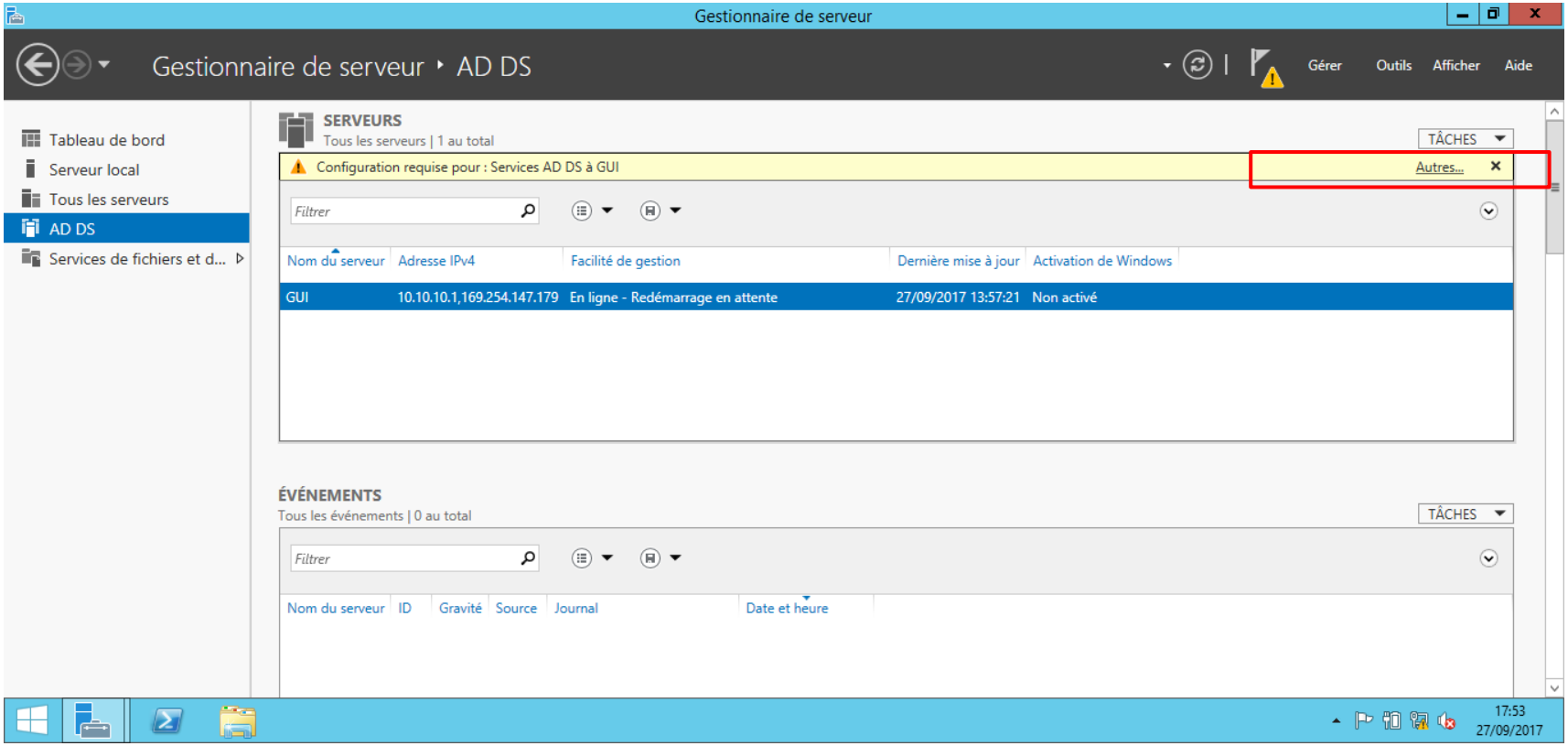
Installation d'un contrôleur de domaine à partir du Gestionnaire de serveur

Installer les services AD DS



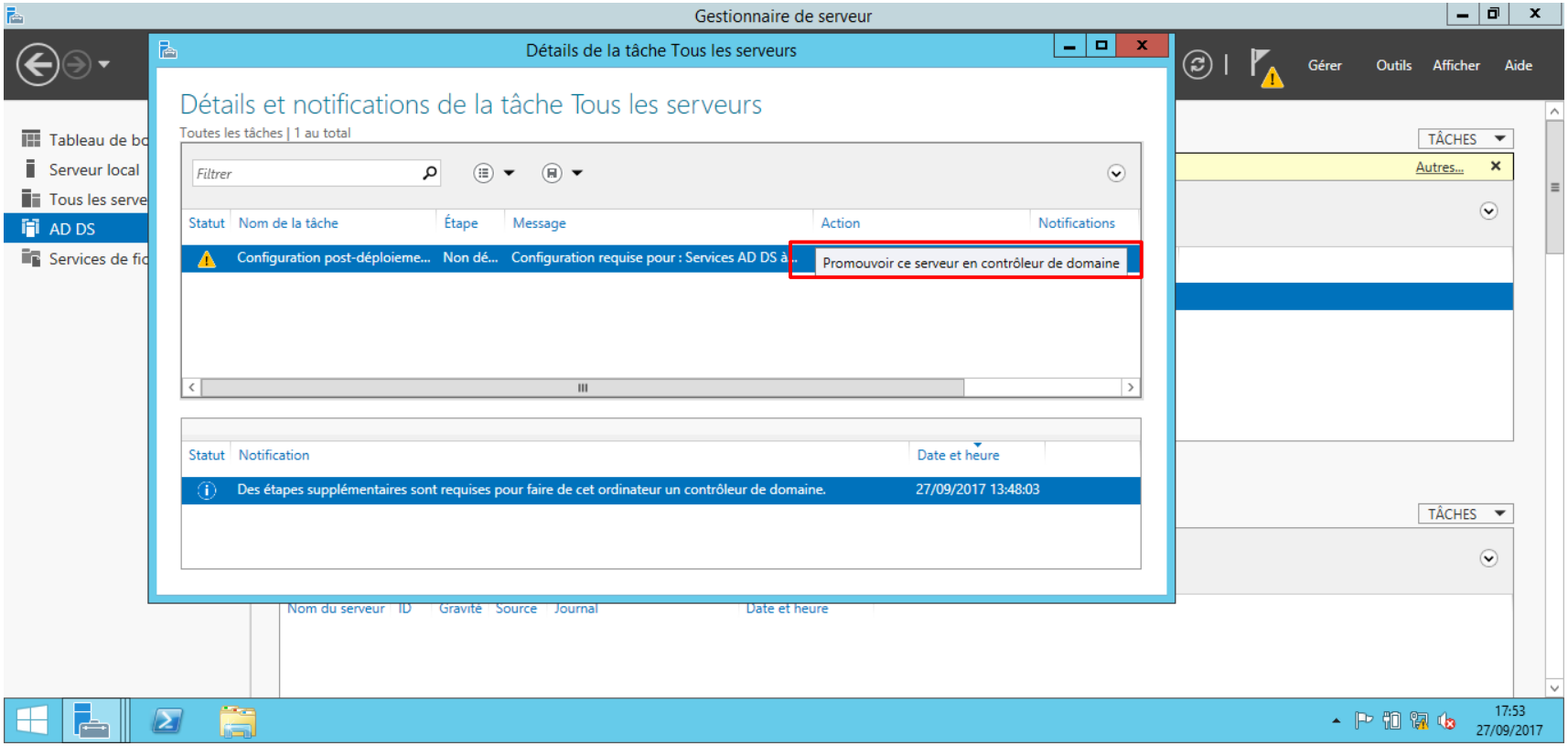
Installation d'un contrôleur de domaine à partir du Gestionnaire de serveur

Promouvoir le serveur en tant que DC



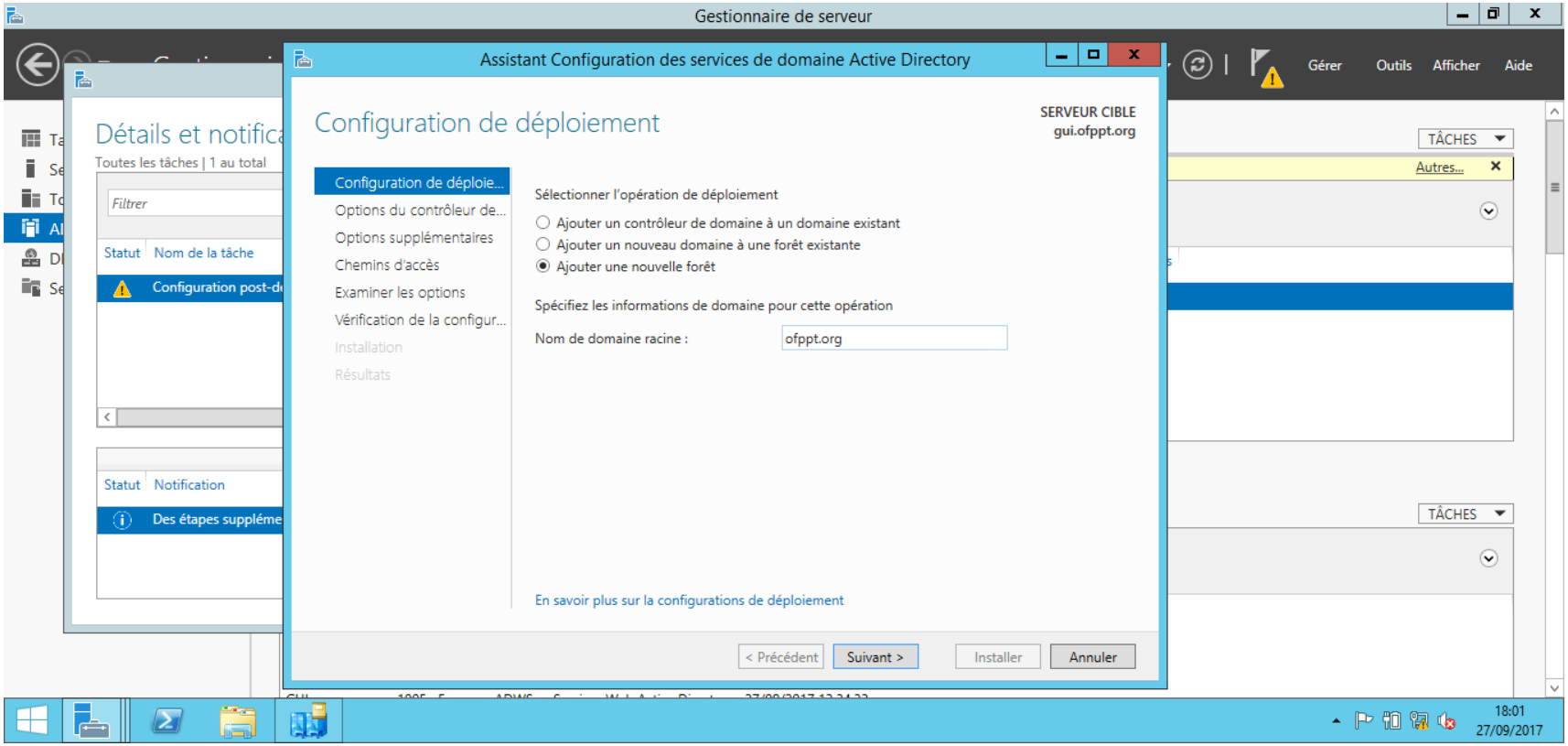
Installation d'un contrôleur de domaine à partir du Gestionnaire de serveur

Promouvoir le serveur en tant que DC



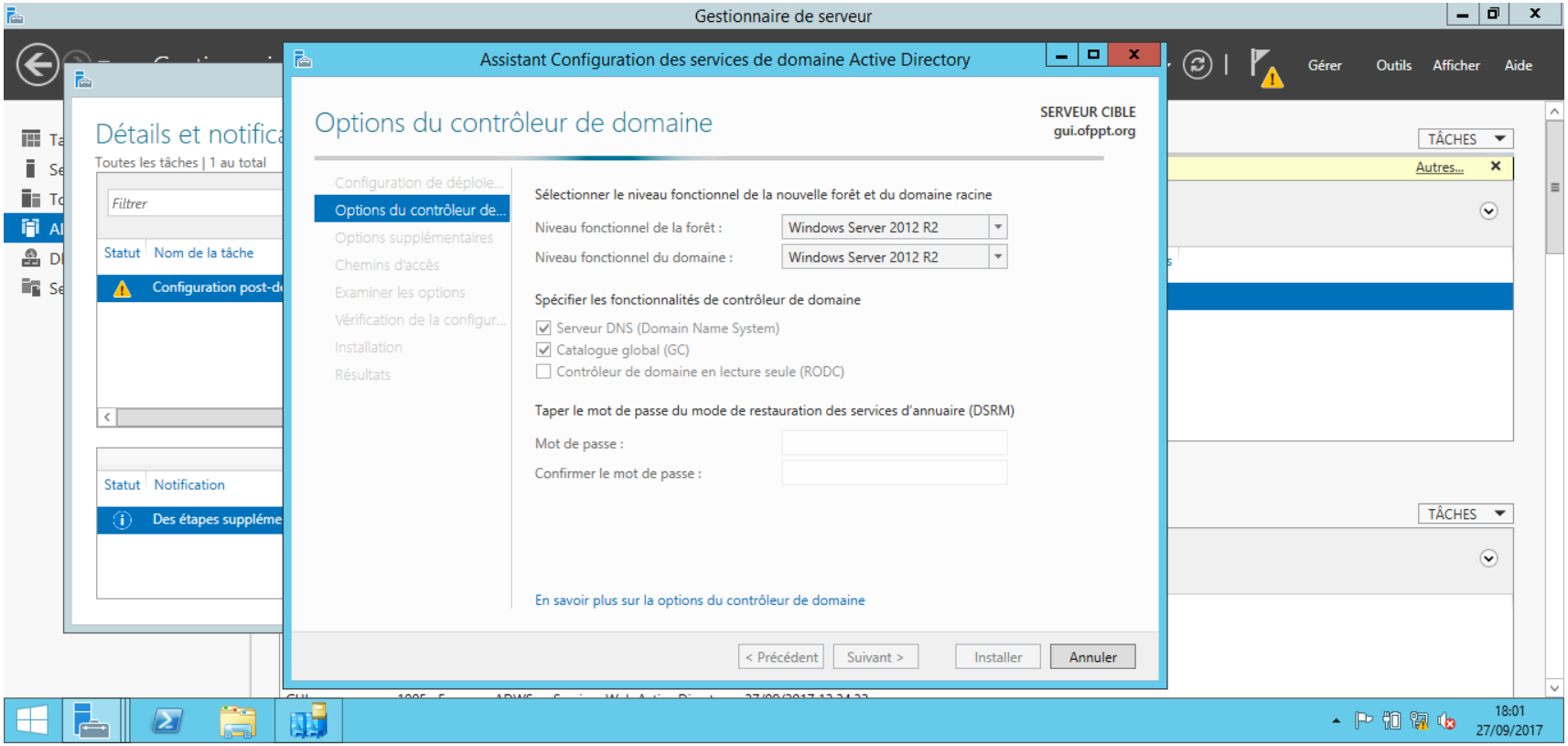
Installation d'un contrôleur de domaine à partir du Gestionnaire de serveur

Promouvoir le serveur en tant que DC



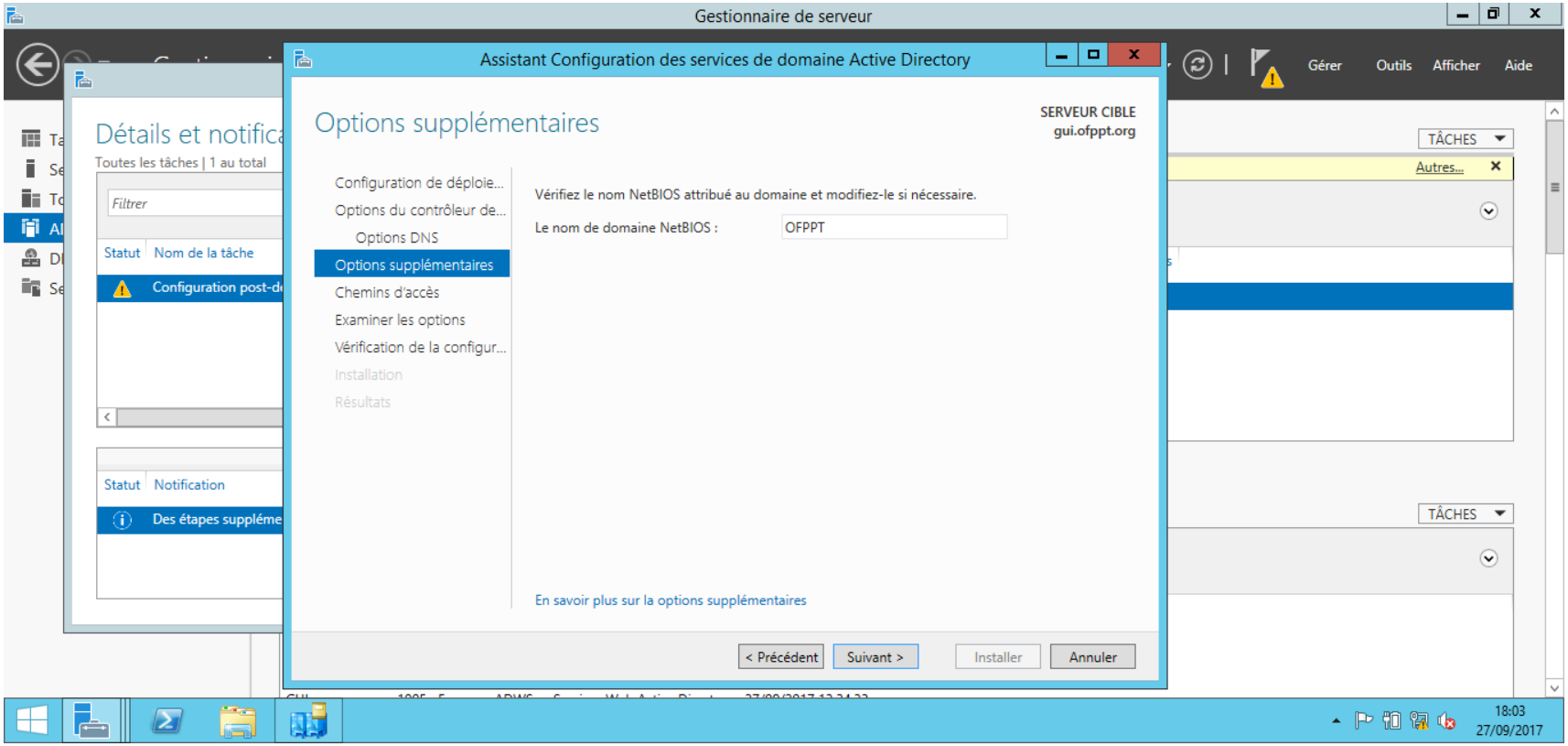
Installation d'un contrôleur de domaine à partir du Gestionnaire de serveur

Promouvoir le serveur en tant que DC



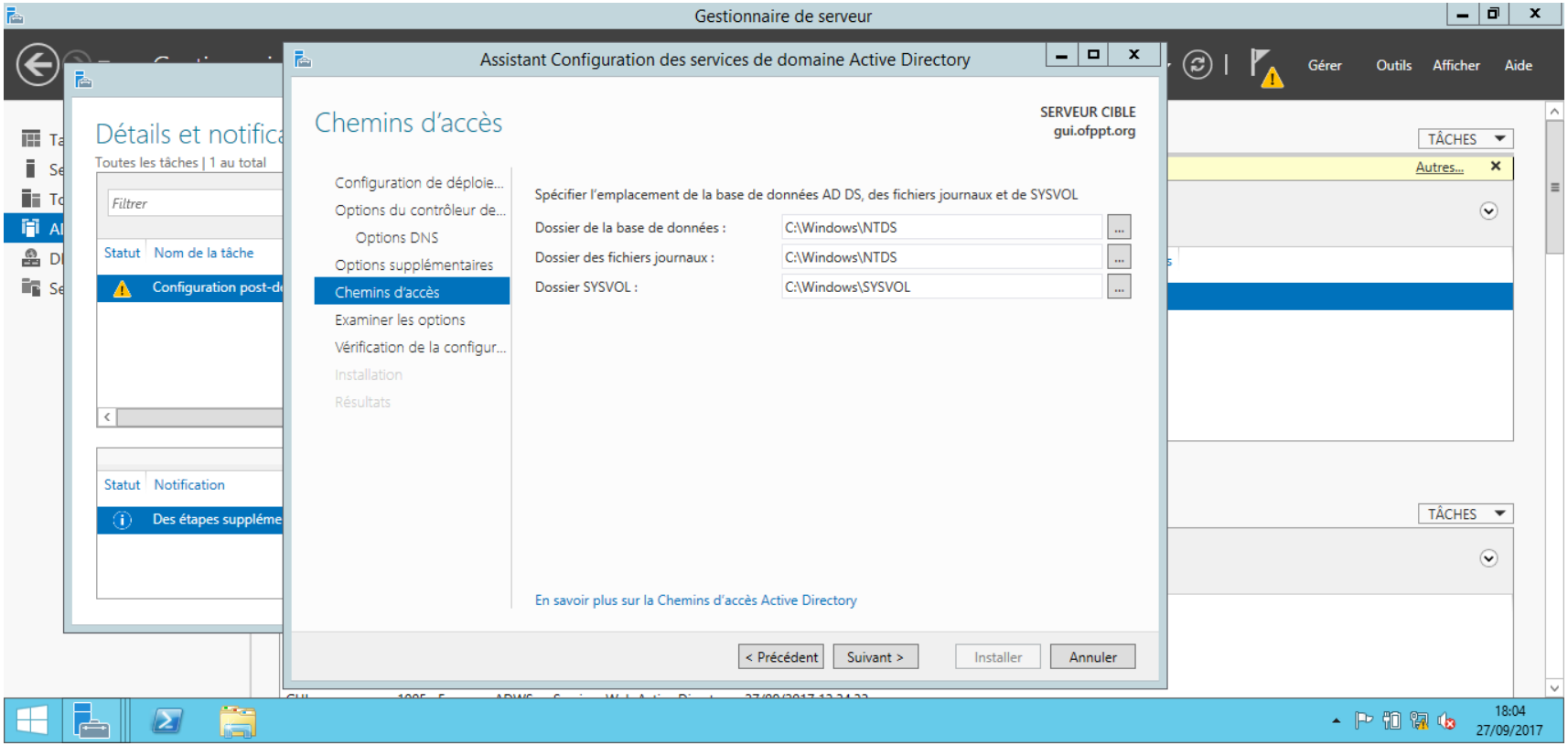
Installation d'un contrôleur de domaine à partir du Gestionnaire de serveur

Promouvoir le serveur en tant que DC



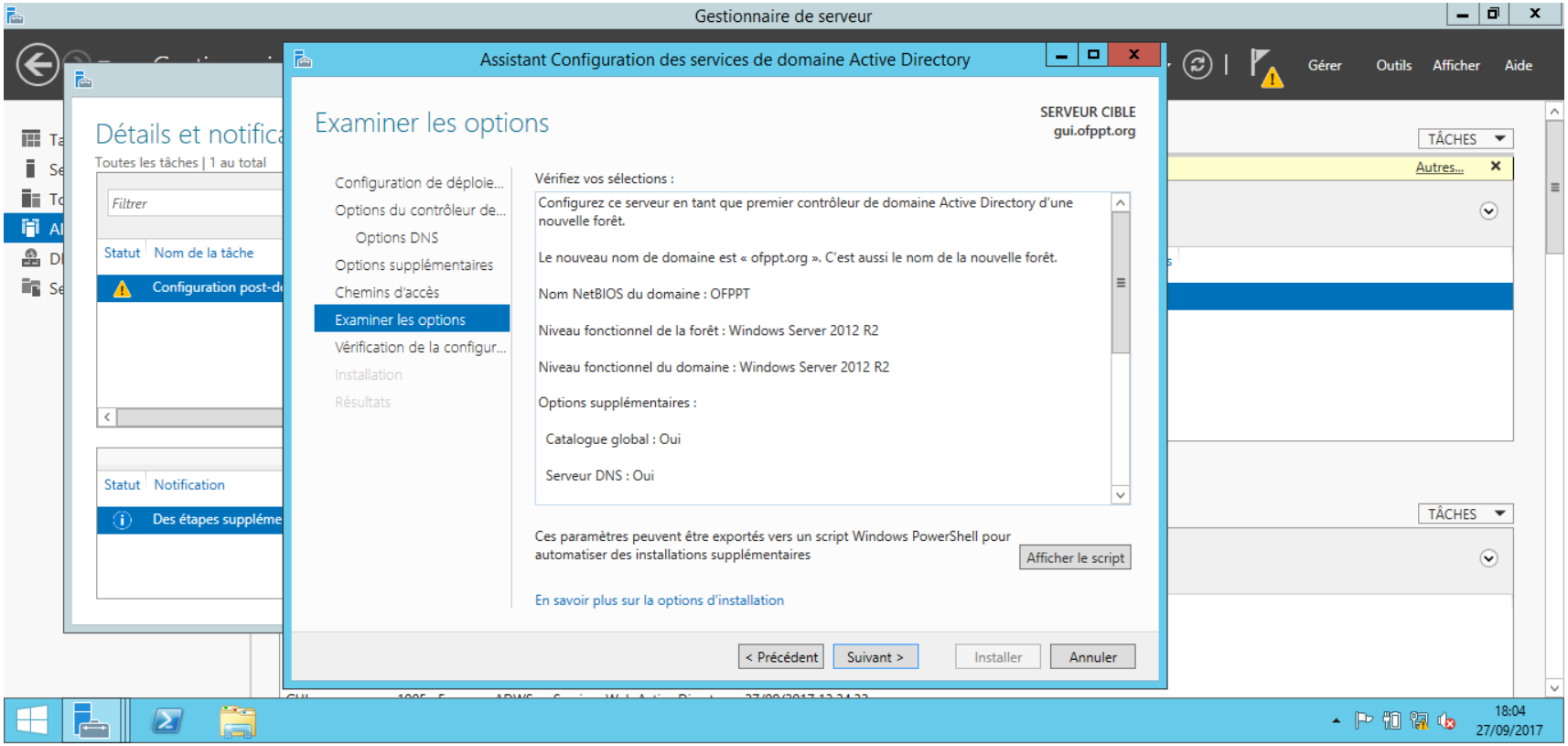
Installation d'un contrôleur de domaine à partir du Gestionnaire de serveur

Promouvoir le serveur en tant que DC



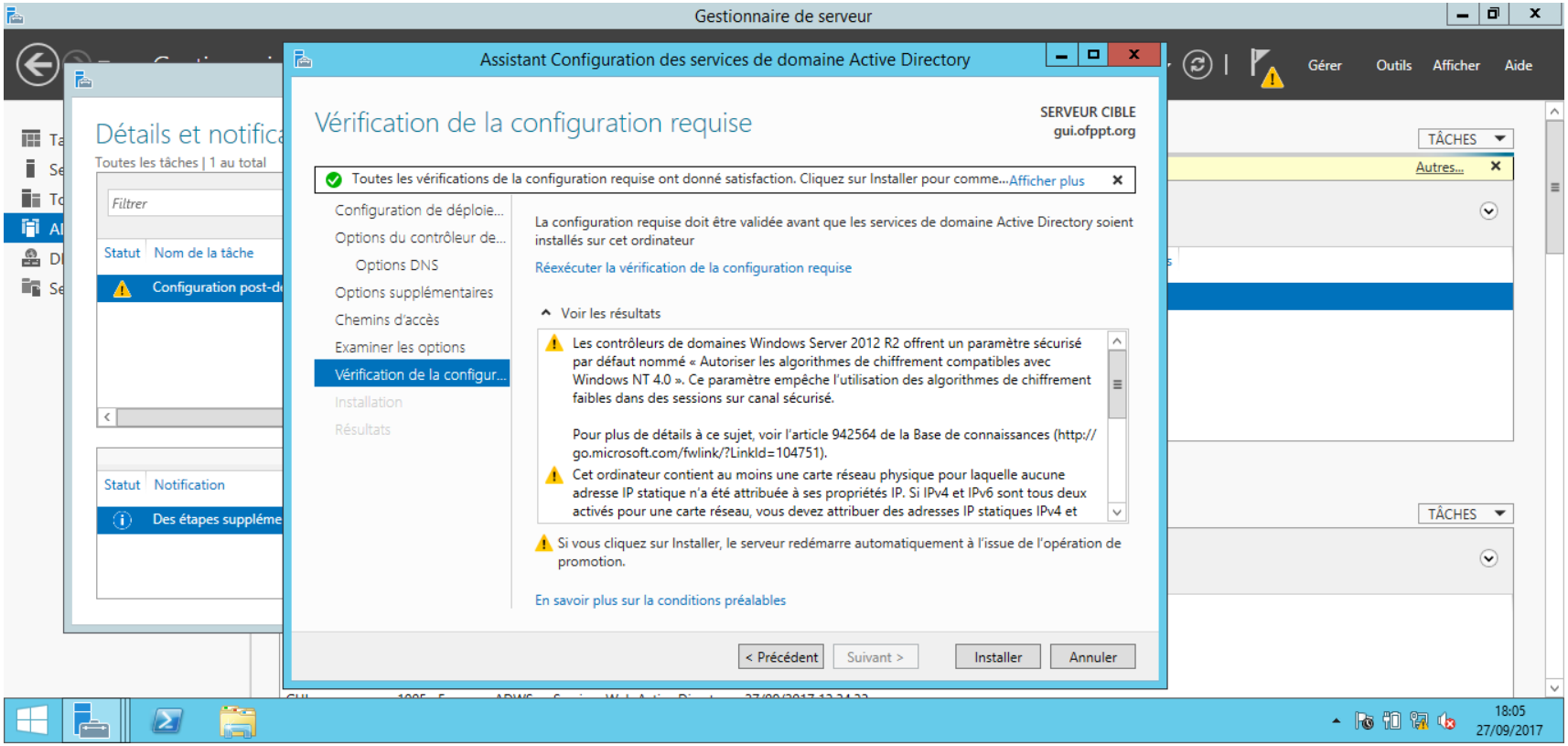
Installation d'un contrôleur de domaine à partir du Gestionnaire de serveur

Promouvoir le serveur en tant que DC



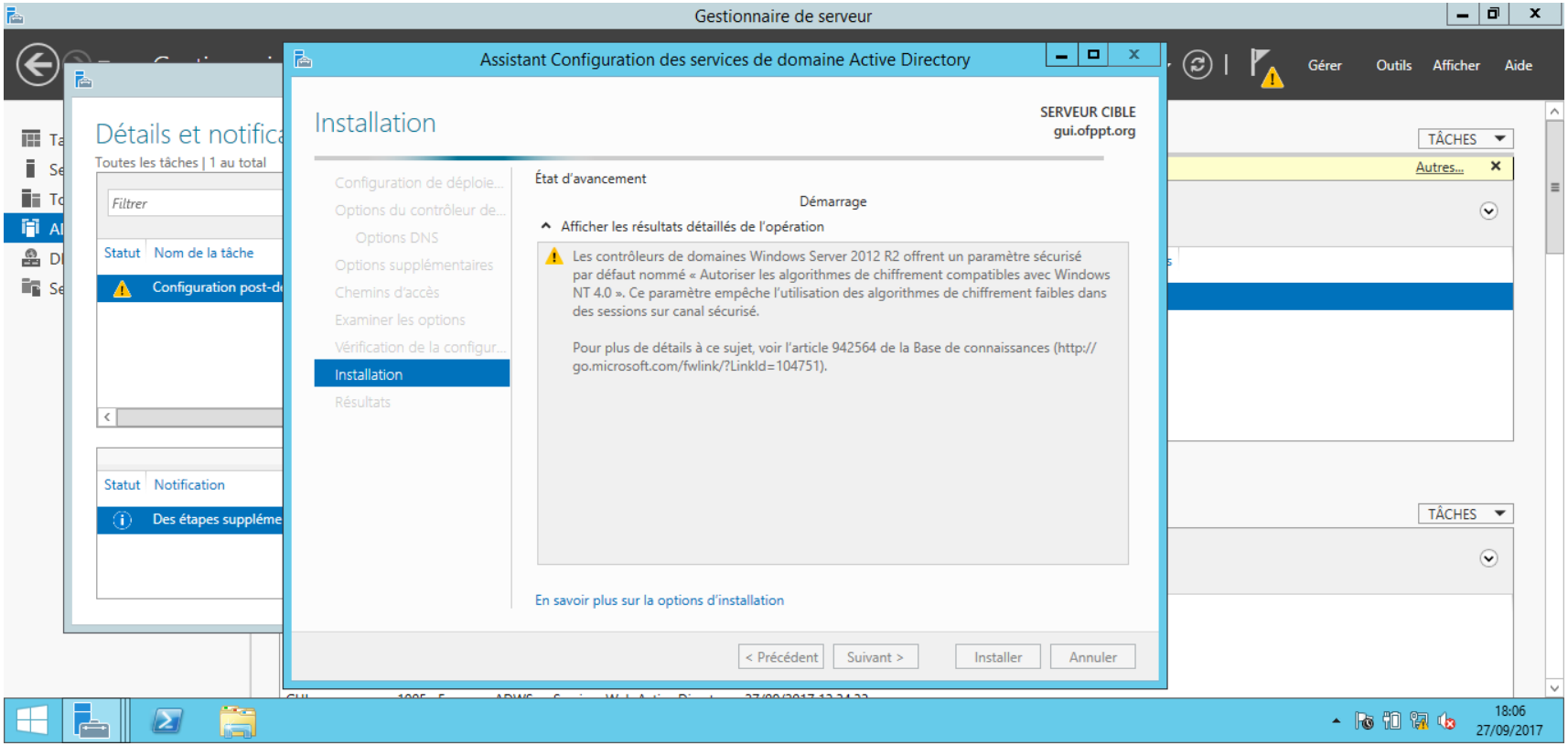
Installation d'un contrôleur de domaine à partir du Gestionnaire de serveur

Promouvoir le serveur en tant que DC



Installation d'un contrôleur de domaine à partir du Gestionnaire de serveur

Promouvoir le serveur en tant que DC



Installation d'un contrôleur de domaine sur une installation minimale de Windows Server 2012

- Pour installer les services AD DS sur le serveur, vous pouvez utiliser le Gestionnaire de serveur pour vous connecter à distance au serveur exécutant l'installation minimale. Vous pouvez également utiliser la commande Windows PowerShell **Install-Windowsfeature -name AD-Domain-Services** pour installer les services AD DS.
- Une fois que vous avez installé les services AD DS, vous pouvez terminer l'installation et la configuration d'une des manières suivantes :
  - Exécutez la commande Windows PowerShell **Install-ADDSForest** pour installer une nouvelle forêt
  - **Exécutez la commande Windows PowerShell Install-ADDSDomain** pour installer un nouveau domaine dans une forêt existante.
  - Exécutez la commande Windows PowerShell **Install-ADDSDomainController** pour installer un controleur de domaine dans un domaine existant
  - On peut vérifier l'installation du contrôleur de domaine avec la commande **Get-ADDomainController.**
  - On peut aussi utiliser la commande dcpromo en créant un fichier de réponses et en executant **dcpromo /unattend:"D:\answerfile.txt"** à une invite de commandes où "D:\answerfile.txt" est le chemin d'accès au fichier de réponses.

Installation d'un contrôleur de domaine sur une installation minimale de Windows Server 2012

Voici un exemple de texte à partir du fichier de réponses

```
[DCINSTALL]
UserName=<Compte d'administrateur dans le domaine du nouveau contrôleur
de domaine>
UserDomain=<Nom du domaine du nouveau contrôleur de domaine>
Password=<Mot de passe du compte UserName>
SiteName=<Nom du site AD DS dans lequel se trouve ce contrôleur de domaine
résidera> Ce site doit être créé à l'avance dans le composant logiciel
enfichable Dssites.msc.
ReplicaOrNewDomain=réplica
ReplicaDomainDNSName=<Nom de domaine complet du domaine dans lequel vous
souhaitez ajouter un contrôleur de domaine supplémentaire>
DatabasePath="<Chemin d'accès à un dossier sur un volume local>"
LogPath="<Chemin d'accès à un dossier sur un volume local>"
SYSVOLPath="<Chemin d'accès à un dossier sur un volume local>"
InstallDNS=yes
ConfirmGC=yes
SafeModeAdminPassword=<Mot de passe pour un compte administrateur hors
connexion>
RebootOnCompletion=oui
```

Mise à niveau d'un contrôleur de domaine

Options de mise à niveau d'AD DS à Windows Server 2012

- **Mise à niveau sur place (depuis Windows Server 2008 ou Windows Server 2008 R2)**
  - Avantage : Excepté pour les vérifications de conditions préalables, tous les fichiers et programmes restent sur place et aucun travail supplémentaire n'est requis
  - À surveiller : Peut laisser des DLL et fichiers hérités
- **Introduire un nouveau serveur Windows Server 2012 dans le domaine et le promouvoir au titre de contrôleur de domaine**
  - C'est habituellement l'option recommandée
  - Avantage : Le résultat est un nouveau serveur sans fichiers et paramètres accumulés
  - À surveiller : Peut nécessiter une charge de travail supplémentaire pour migrer les paramètres des fichiers d'utilisateurs