

# WSUS

## **I. Installation de WSUS**

- 1/ Avant de commencer
- 2/ Type d'installation
- 3/ Sélection du serveur
- 4/ Rôle de serveurs
- 5/ Fonctionnalités
- 6/ WSUS
- 7/ Service de rôle
- 8/ Contenu
- 9/ Rôle Web Server (IIS)
- 10/ Service de rôle IIS
- 11/ Résultats

## **II. Assistant de configuration WSUS**

- 1/ Avant de commencer
- 2/ Programme d'amélioration de Microsoft Update
- 3/ Choisir le serveur en amont
- 4/ Définir le serveur proxy
- 5/ Erreur de synchronisation
- 6/ Choisir les langues
- 7/ Choisir les produits
- 8/ Choisir les classifications
- 9/ Configurer la planification de la synchronisation
- 10/ Terminé
- 11/ Étapes suivantes

## **III. Télécharger des mises à jour**

- 1/ Création des groupes d'ordinateurs et serveurs
- 2/ Configuration des règles d'approbation automatique
- 3/ Gestion du stockage WSUS
- 4/ Surveillance de l'espace disque
- 5/ Refuser les mises à jour inutiles
- 6/ Attention à certaines mises à jour
- 7/ Suppression des mises à jour anciennes
- 8/ Nettoyage des mises à jour refusées

## **IV. Exploitation et gestion du service WSUS**

- 1/ Limites de l'outil de recherche
- 2/ Approbation manuelle des mises à jour
- 3/ Étapes prévues mais non réalisées (fin de mission)

## I/ Installation de WSUS

Introduction : L'objectif de cette mission est d'installer WSUS (Windows Server Update Services), une solution logicielle développée par Microsoft permettant de centraliser la gestion et le déploiement des mises à jour logicielles dans un environnement informatique.

Présentation de WSUS : WSUS est un outil conçu pour agir comme un intermédiaire entre les *serveurs de mises à jour de Microsoft* et les *ordinateurs d'un réseau*. Il joue un rôle essentiel dans la gestion des mises à jour grâce aux fonctionnalités suivantes :

1. Téléchargement unique des mises à jour :  
Les mises à jour sont téléchargées une seule fois par le serveur WSUS, ce qui *évite que chaque ordinateur du réseau ne se connecte individuellement à Internet pour récupérer les dernières mises à jour*.
2. Gestion centralisée du déploiement :  
WSUS permet une gestion fine du processus de déploiement des mises à jour, notamment :
  - La création de *groupes d'ordinateurs* pour un déploiement spécifique.
  - *L'approbation ou le refus* des mises à jour selon les besoins.
  - La *planification* des installations pour optimiser les ressources réseau.
3. Renforcement de la sécurité :  
En s'assurant que tous les systèmes disposent des *correctifs de sécurité les plus récents*, WSUS contribue à réduire les risques de vulnérabilités.
4. Optimisation de l'utilisation du réseau :  
En *limitant les connexions simultanées à Internet*, WSUS réduit la charge sur le réseau et améliore ses performances globales.

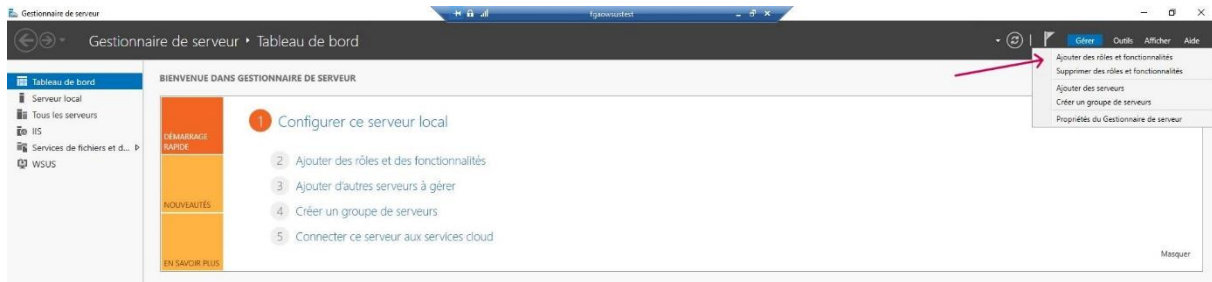
En résumé, WSUS est un outil indispensable pour les entreprises souhaitant maintenir leur parc informatique à jour de manière centralisée, sécurisée et efficace.

Prérequis pour l'installation de WSUS : Avant d'entamer l'installation de WSUS, il est nécessaire de disposer d'un *serveur dédié spécifiquement à cette solution*. Ce serveur sera configuré pour stocker les mises à jour et gérer leur déploiement.

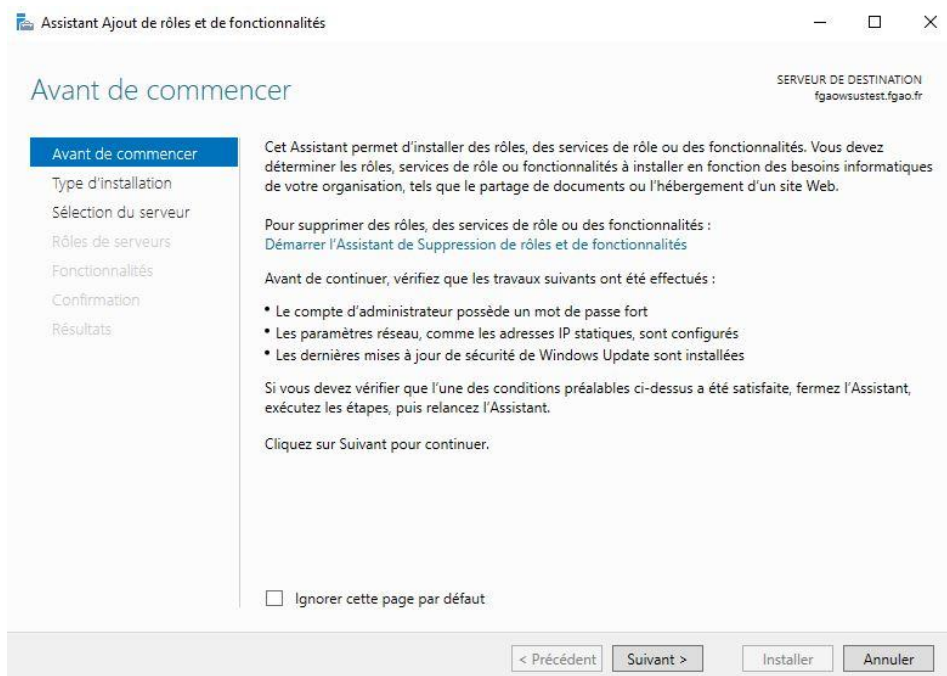
Étapes initiales de l'installation :

1. Accès au *Gestionnaire de serveur* : Depuis le serveur dédié, ouvrir le Gestionnaire de serveur. Cliquer sur Gérer, puis sélectionner Ajouter des rôles et fonctionnalités.
2. Lancer l'*Assistant Ajout de rôles et de fonctionnalités* : Une fenêtre intitulée Assistant Ajout de rôles et de fonctionnalités s'affiche. Cette interface guide l'utilisateur à travers les différentes étapes nécessaires pour installer WSUS correctement.

Les étapes détaillées de l'installation et de la configuration du WSUS seront précisées dans la suite du rapport.



## 1/ Avant de commencer



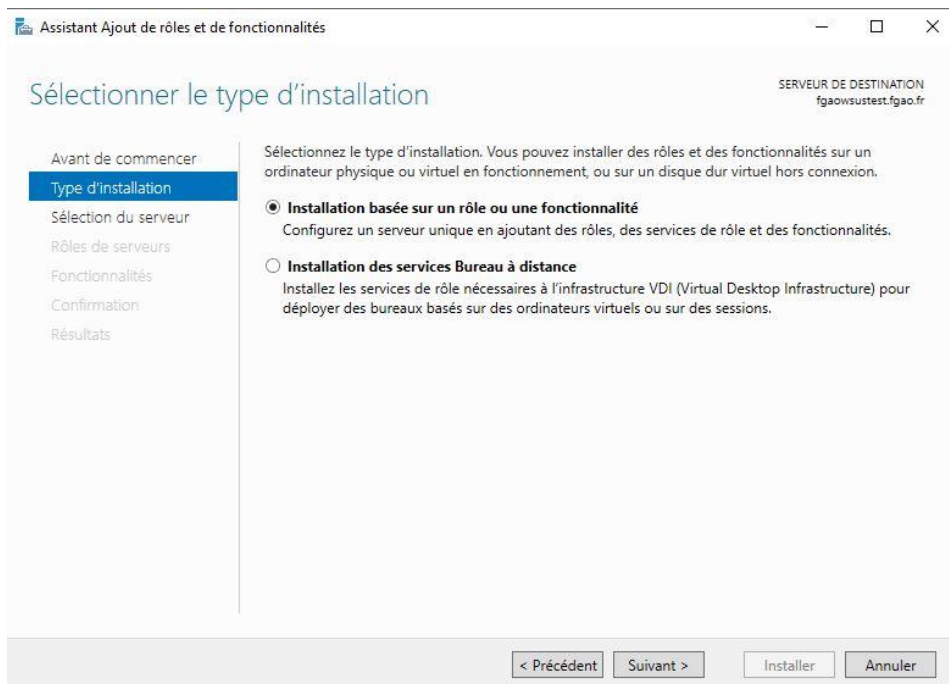
L'assistant Ajout de rôles et de fonctionnalités explique que des fonctionnalités supplémentaires peuvent être installées sur le serveur afin d'étendre ses capacités. Avant de poursuivre, il est essentiel de vérifier que certaines conditions préalables sont respectées :

- Le compte d'administrateur possède un *mot de passe fort* : Oui, il possède au moins 12 caractères incluant au moins une majuscule, minuscule, chiffre et caractère spéciaux.
- Les paramètres réseau, comme les adresses IP statiques, sont configurés : en inscrivant la commande `ipconfig /all` dans le cmd du serveur, on peut s'apercevoir que le *DHCP est désactivé* (Une adresse IP fixe est nécessaire pour que les postes clients puissent toujours contacter le serveur WSUS. Si l'adresse change, les clients ne pourront plus se connecter au serveur et les mises à jour ne fonctionneront plus).
- Les dernières mises à jour de sécurité de Windows Update sont installées : en allant dans l'historique des mises à jour, nous pouvons observer que les dernières mises à jour ont été

installées. On vérifie que le serveur est à jour via Windows Update afin de *garantir sa sécurité, sa stabilité et la compatibilité avec WSUS* avant son installation.

Ces vérifications sont indispensables pour éviter tout problème lors de l'installation ou du fonctionnement des services WSUS.

## 2/ Type d'installation



L'option « Installation basée sur un rôle ou une fonctionnalité » a été sélectionnée. Ce choix est motivé par la nécessité d'ajouter des services spécifiques au serveur. Parmi les services pouvant être intégrés, on peut inclure :

- Un serveur web : Pour héberger des sites internet.
- Un serveur de fichiers : Pour stocker et partager des données entre utilisateurs.
- Un serveur DNS : Pour gérer les noms de domaine au sein du réseau.

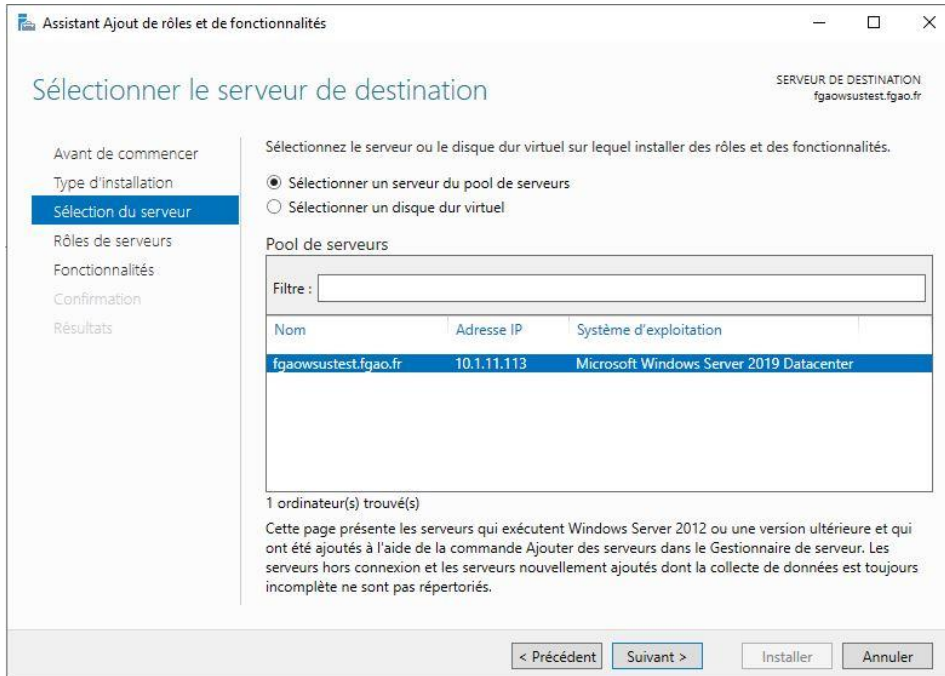
L'option Infrastructure VDI (Virtual Desktop Infrastructure) n'a pas été retenue, car *il n'est pas prévu de virtualiser les postes de travail* des utilisateurs dans ce contexte. L'objectif est plutôt de personnaliser le serveur afin qu'il réponde précisément aux besoins identifiés, par exemple en installant des logiciels spécifiques ou en ajustant certains paramètres selon les exigences du réseau.

## 3/ Sélection du serveur

Le serveur fgaowsustest.fgao.fr a été sélectionné comme cible *pour l'installation des rôles et fonctionnalités WSUS*. Ce serveur a été choisi pour les raisons suivantes : Il est dédié spécifiquement à WSUS. Il s'agit d'un serveur virtuel préalablement configuré, disposant des ressources nécessaires

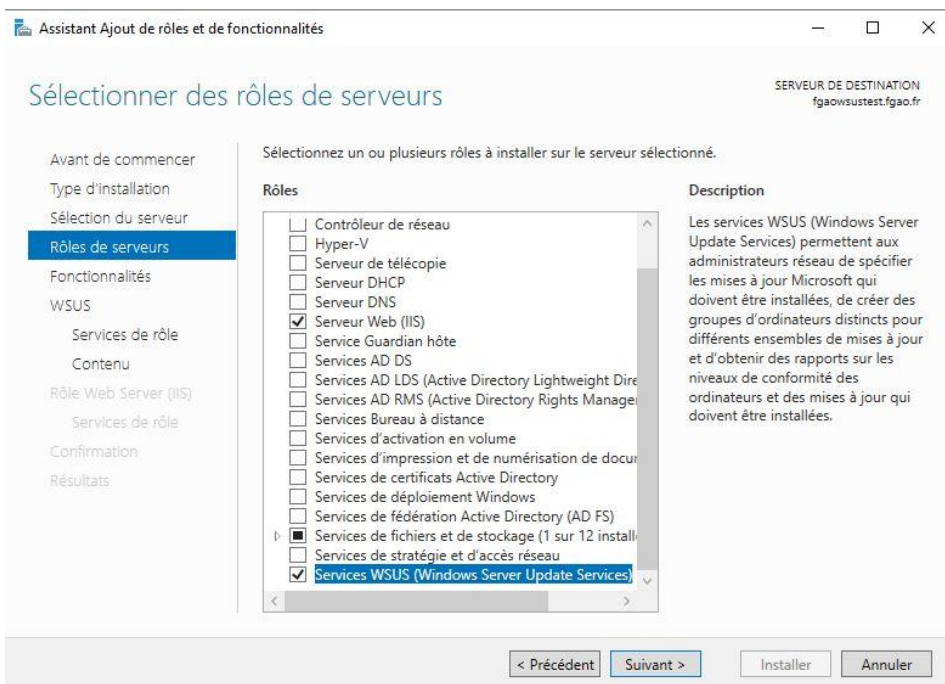
pour exécuter ce service et sa configuration initiale garantit une compatibilité optimale pour l'installation et l'utilisation de WSUS.

Le choix de ce serveur cible permet de s'assurer que l'installation des rôles WSUS se fera dans un environnement adapté et prêt à l'emploi, réduisant ainsi les risques d'erreurs ou de conflits liés aux ressources.



#### 4/ Rôle de serveurs

Les rôles de serveurs à installer sont sélectionnés. Les rôles suivants sont requis pour WSUS : Serveur Web IIS, services de fichiers et de stockage et le services WSUS (rôle principal).



Pourquoi IIS et les services de fichiers sont-ils souvent cochés par défaut lors de l'installation de WSUS ?

- Serveur Web IIS (Internet Information Services) : IIS est utilisé pour *créer une interface web permettant de gérer WSUS*. Il assure également la *distribution des mises à jour* aux clients via le protocole HTTP.
- Services de fichiers et de stockage : Ces services permettent de *stocker localement* les fichiers de mise à jour téléchargés depuis Microsoft, optimisant ainsi les performances et *limitant l'utilisation de la bande passante* Internet.

## 5/ Fonctionnalités

Ici, il est proposé de sélectionner les fonctionnalités supplémentaires nécessaires pour le bon fonctionnement de WSUS. Les fonctionnalités choisies sont les suivantes :

1. **Base de données interne Windows (WID)**  
Stockage des données WSUS : WID est utilisée comme *base de données* par défaut pour WSUS. Elle stocke des informations essentielles telles que les mises à jour, les ordinateurs clients et les groupes. Cette solution convient parfaitement pour des installations de petite ou moyenne envergure.
2. **Composants .NET Framework 4.7**  
Environnement d'exécution : WSUS repose sur .NET Framework *pour exécuter plusieurs de ses composants*. ASP.NET et les services WCF sont notamment indispensables *pour l'interface web et les communications* avec les clients.
3. **Outils d'administration de serveur distant**  
Gestion à distance : Ces outils permettent d'administrer le serveur WSUS à distance, une fonctionnalité *pratique lorsque le serveur n'est pas accessible localement*.
4. **Prise en charge WoW64**  
Compatibilité 32 bits : Cette fonctionnalité *garantit la compatibilité des applications 32 bits sur un système d'exploitation 64 bits*, ce qui peut être requis pour certains composants WSUS.
5. **Service d'activation des processus Windows**  
Gestion des services : Ce service *assure le bon fonctionnement et la gestion des services* Windows, notamment ceux utilisés par WSUS et IIS.
6. **Services SNMP**  
Surveillance réseau : SNMP (Simple Network Management Protocol) peut être utilisé pour *surveiller l'état du serveur WSUS et collecter des données* sur son utilisation.
7. **System Data Archiver**  
Archivage des données : Cette fonctionnalité est utile pour *archiver les anciennes données* WSUS, *libérant ainsi de l'espace disque* et améliorant les performances du serveur.

## 8. Windows Defender Antivirus

Sécurité : Windows Defender *protège le serveur* contre les menaces et garantit un environnement sécurisé pour WSUS.

## 9. Windows PowerShell

Automatisation : PowerShell est un outil puissant permettant *d'automatiser les tâches administratives* et de gérer WSUS par le biais de scripts.

## 10. XPS Viewer

Affichage de documents : Bien que moins directement lié à WSUS, cet outil peut être utilisé pour *afficher des rapports* ou des documents générés par le service.

## 6/ WSUS

L'assistant permet de choisir les fonctionnalités spécifiques à intégrer au service WSUS. Ces fonctionnalités peuvent être comparées aux options d'un véhicule : il est possible d'avoir une configuration de base ou une version enrichie avec des outils avancés.

1. Connexion au service Microsoft pour les mises à jour : WSUS doit se connecter régulièrement aux serveurs de Microsoft pour télécharger les mises à jour pour ensuite les distribuer à ses clients, ici les ordinateurs du réseau.
2. Sécurité de la communication : La communication entre le serveur WSUS et les ordinateurs clients doit être sécurisée à l'aide du protocole *SSL afin de chiffrer les données et protéger les informations sensibles*.

The screenshot shows the 'Assistant Ajout de rôles et de fonctionnalités' (Add Roles and Features Wizard) for Windows Server Update Services (WSUS). The window title is 'Assistant Ajout de rôles et de fonctionnalités' and the destination server is 'SERVEUR DE DESTINATION fgaowsustest.fgao.fr'. The main heading is 'Services WSUS (Windows Server Update Services)'. On the left, a navigation pane lists the steps: 'Avant de commencer', 'Type d'installation', 'Sélection du serveur', 'Rôles de serveurs', 'Fonctionnalités', 'WSUS', 'Services de rôle', 'Contenu', 'Rôle Web Server (IIS)', 'Services de rôle', 'Confirmation', and 'Résultats'. The 'WSUS' step is currently selected. The main content area displays the following information:

Windows Server Update Services (WSUS) permet aux administrateurs de gérer le téléchargement et l'installation des mises à jour à partir du site Web Microsoft Update sur le réseau local.

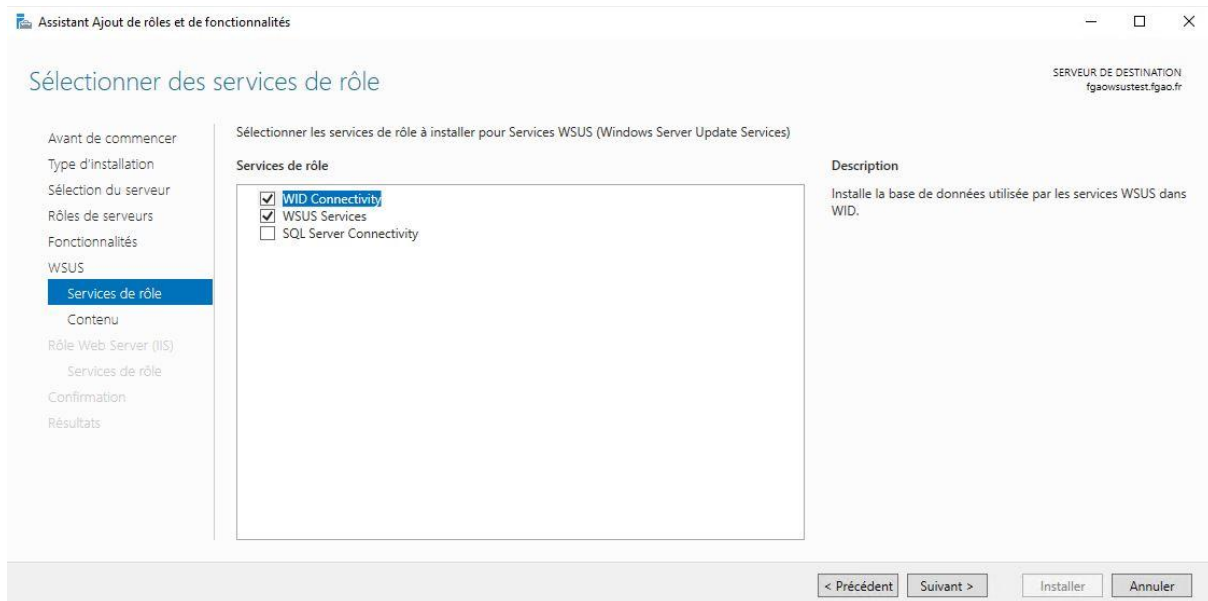
À noter :

- Au moins un serveur WSUS sur un réseau doit être capable de télécharger des mises à jour à partir de Microsoft Update. Les autres serveurs WSUS peuvent obtenir des mises à jour à partir de ce serveur ou de Microsoft Update.
- Les communications WSUS serveur à serveur et serveur à client doivent être configurées de façon à utiliser le protocole SSL (Secure Sockets Layer).

At the bottom of the wizard, there are four buttons: '< Précédent', 'Suivant >', 'Installer', and 'Annuler'.

## 7/ Service de rôle

L'onglet service de rôle nous présente plusieurs options liées au rôle WSUS. Voici les détails des choix disponibles :



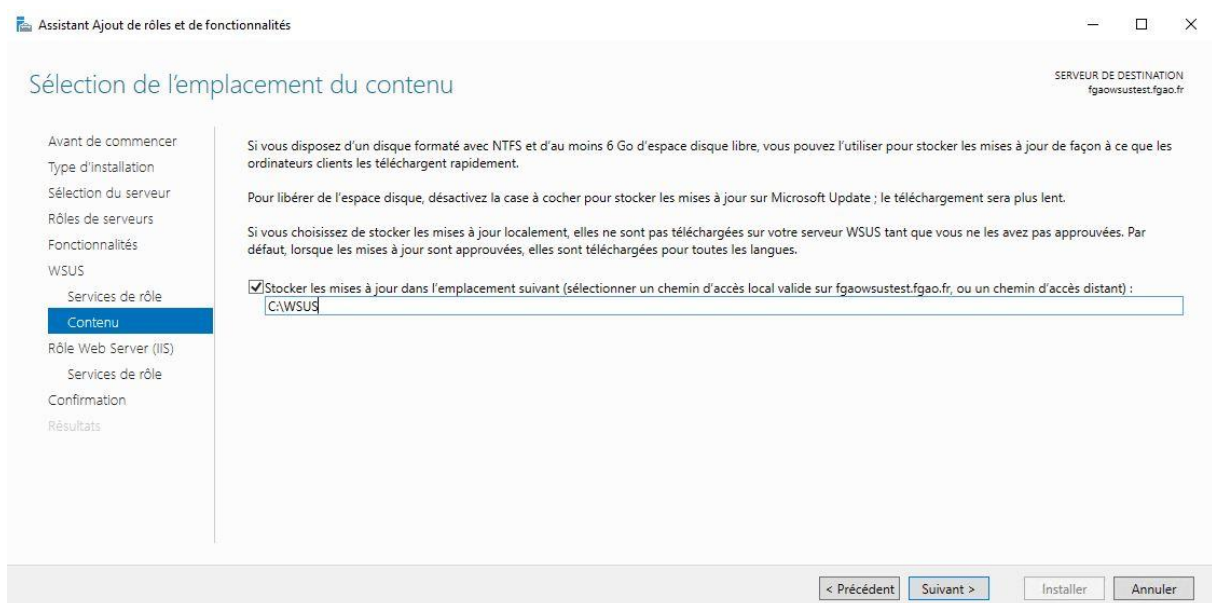
- WID Connectivity** (Windows Internal Database) : Cette option permet d'utiliser la base de données interne Windows (WID) pour *stocker les informations de WSUS*, telles que les mises à jour disponibles, les groupes d'ordinateurs clients, et les rapports d'état. L'avantages c'est qu'elle est facile et rapide à configurer et idéal pour les petites installations où la simplicité est une priorité. Cela dit, elle est *moins performante et moins flexible qu'une base de données SQL Server*. Peu adaptée pour des environnements complexes ou de grande taille.
- WSUS Services** : Ce service représente le cœur de WSUS. Il comprend les composants essentiels pour gérer l'ensemble du cycle de vie des mises à jour, notamment : le *téléchargement des mises à jour, l'approbation des correctifs et la distribution vers les ordinateurs clients*. Ce service est indispensable pour que WSUS puisse fonctionner. Il doit être systématiquement sélectionné lors de l'installation.
- SQL Server Connectivity** : Cette option permet de connecter WSUS à une base de données SQL Server externe. SQL Server offre des performances plus élevées, une extensibilité accrue et des fonctionnalités avancées pour la gestion des bases de données. L'avantage c'est qu'il est recommandé pour les grandes installations ou les réseaux complexes et permet une meilleure gestion des données et des rapports. Mais cela *nécessite une configuration plus complexe et peut entraîner des coûts supplémentaires liés à la licence SQL Server*.

Clarifications et choix : Dans cette configuration, **WID Connectivity** et **WSUS Services** ont été sélectionnés. Cela permet de *configurer un serveur WSUS capable de gérer efficacement les mises à jour en utilisant la base de données interne Windows*.

(Pour des besoins spécifiques ou une croissance future, il est toujours possible de migrer ultérieurement vers une base de données SQL Server pour bénéficier de meilleures performances et d'options avancées.)

## 8/ Contenu

L'installation de WSUS consiste à définir l'emplacement où seront stockées les mises à jour téléchargées depuis Microsoft Update. Ces mises à jour seront ensuite distribuées aux ordinateurs clients du réseau.



### Options disponibles pour le stockage

1. **Stocker les mises à jour dans un emplacement défini** : Cette option permet de spécifier un chemin sur le serveur (local ou distant) où les fichiers de mise à jour seront stockés. Les ordinateurs clients téléchargent les mises à jour directement depuis le serveur WSUS, ce qui *améliore les performances si le réseau est lent ou soumis à des contraintes de bande passante*. Mais cela nécessite un *espace disque supplémentaire* sur le serveur pour héberger les fichiers de mise à jour.
2. **Ne pas stocker les mises à jour localement** : Avec cette option, les fichiers de mise à jour ne sont pas stockés sur le serveur. Les ordinateurs clients les récupèrent directement depuis Microsoft Update. Ce choix *libère de l'espace disque* sur le serveur mais les *téléchargements peuvent être plus lents, surtout si le réseau est lent ou si le nombre d'ordinateurs clients est important*.

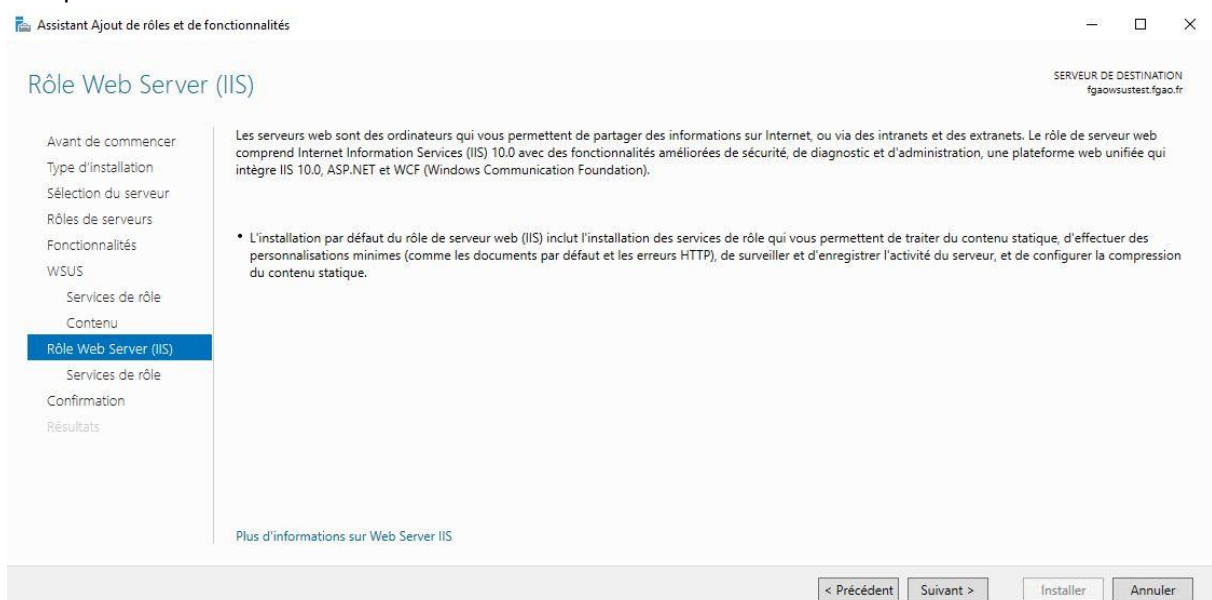
Critères pour le choix de l'option : le choix de l'option de stockage dépend des besoins et des ressources disponibles.

- Espace disque disponible : Si le serveur dispose d'un espace disque suffisant, il est préférable de stocker les mises à jour localement pour améliorer les performances.
- Bande passante réseau : Dans un réseau à faible bande passante, le stockage local réduit le temps de téléchargement pour les clients.
- Nombre d'ordinateurs clients : Plus le nombre d'ordinateurs est élevé, plus le stockage local devient avantageux pour répartir la charge réseau.

Décision prise : Ici, l'option de stockage local a été choisie. Les mises à jour seront stockées dans le répertoire C:\WSUS sur le serveur. Cela garantit des téléchargements rapides et un meilleur contrôle sur la distribution des mises à jour.

## 9/ Rôle Web Server (IIS)

Cette étape vise à ajouter le rôle de serveur web IIS (Internet Information Services), qui est indispensable au bon fonctionnement de WSUS.



Pourquoi IIS est-il nécessaire pour WSUS ?

1. Interface d'administration web : IIS fournit une *interface web conviviale permettant de gérer WSUS*. Cette interface facilite la gestion des mises à jour, des ordinateurs clients et des rapports depuis un navigateur web.
2. Communication avec les clients : Les *ordinateurs clients utilisent IIS pour se connecter au serveur WSUS* et télécharger les mises à jour.
3. Hébergement de services web : IIS peut héberger des services web nécessaires à *WSUS pour communiquer avec d'autres applications ou systèmes*.

## 10/ Service de rôle

Les **services de rôle à installer pour le Serveur Web IIS** (Internet Information Services) sont sélectionnés. Ces services sont essentiels pour *permettre à IIS de fonctionner comme un serveur web* et de supporter les fonctionnalités nécessaires à WSUS.

Services de rôle sélectionnés :

1. **Serveur Web**

Service de base indispensable pour qu'IIS puisse fonctionner en tant que serveur web.

2. Fonctionnalités **HTTP communes**

**Contenu statique** : Permet de *servir des fichiers HTML, CSS, JavaScript, images, et autres types de contenu*.

**Document par défaut** : *Spécifie la page web affichée par défaut lorsqu'une URL ne contient pas de nom de fichier spécifique.*

3. **Performance**

Compression de contenu dynamique : *Réduit la taille des fichiers* envoyés aux clients, améliorant ainsi les performances et réduisant l'utilisation de la bande passante.

4. Sécurité

**Filtrage des demandes** : Protège le serveur en *filtrant les requêtes entrantes*, permettant de *bloquer les accès non autorisés*.

**Authentification Windows** : Permet de sécuriser l'accès au serveur en utilisant les *identifiants du domaine*.

5. Développement d'applications

**.NET Extensibility 4.7** : Permet de *développer des applications web dynamiques* basées sur le framework .NET.

**ASP.NET 4.7** : Fournit les outils nécessaires *pour exécuter des applications web ASP.NET*.

**Extension ISAPI** : Permet de *charger des modules externes pour étendre les capacités d'IIS*.

6. Outils de gestion

**Console de gestion IIS** : *Interface graphique* permettant de configurer et gérer facilement IIS.

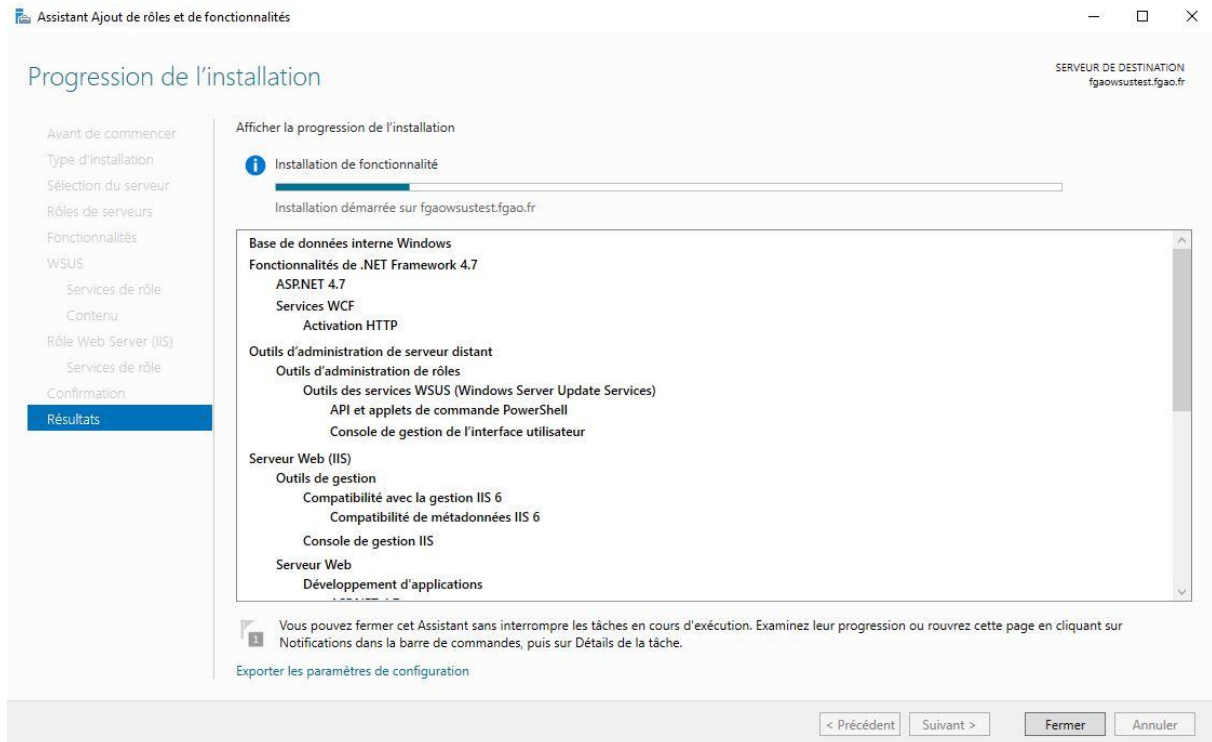
**Compatibilité avec la gestion IIS 6** : Assure la prise en charge des configurations et métadonnées existantes *pour une transition plus fluide* (On garde la compatibilité avec les anciennes configurations pour faciliter la migration vers une version plus récente).

Pourquoi ces services sont-ils sélectionnés par défaut ?

Ces services sont présélectionnés car ils répondent aux besoins essentiels d'un serveur web IIS dans le cadre de l'installation de WSUS, c'est-à-dire : Fournir une interface d'administration, gérer et sécuriser les communications avec les clients, permettre le développement et l'hébergement d'applications web et enfin, garantir des performances optimales et une compatibilité avec les anciennes versions d'IIS.

## 11/ Résultats

Nous avons ici, la progression de l'installation des services et fonctionnalités sélectionnés :



Cette dernière étape confirme que l'installation des services sélectionnés est en cours et offre une vue détaillée de la progression.

Il est crucial de ne pas fermer cette fenêtre tant que l'installation n'est pas terminée, car cela pourrait interrompre le processus.

Prochaines étapes :

Une fois l'installation terminée, les fonctionnalités accessibles seront :

Le serveur Web IIS qui permettra de créer et de gérer des sites web.

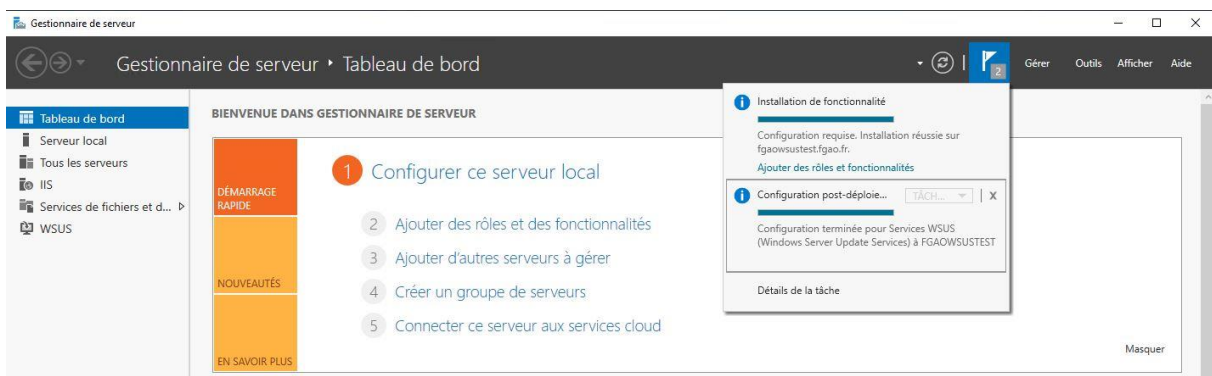
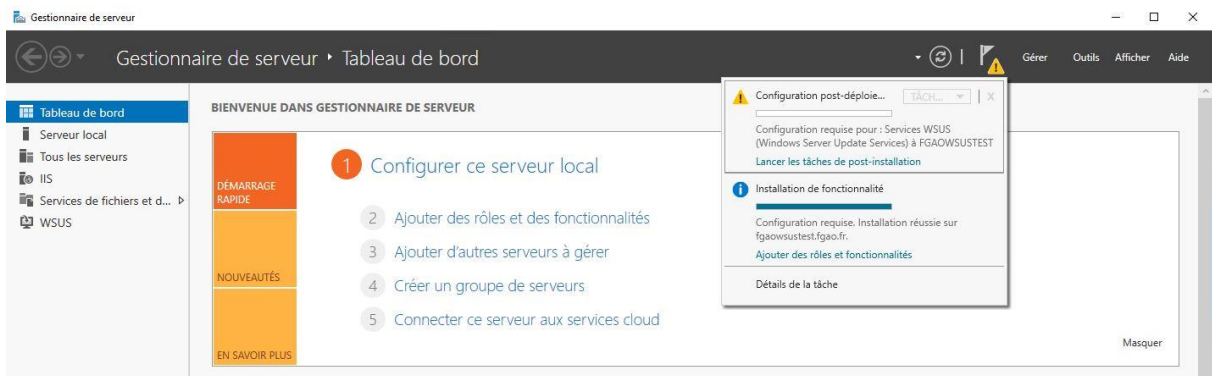
Le WSUS qui sera prêt pour la configuration et la gestion des mises à jour dans l'environnement réseau.

Cette étape marque la fin de l'installation des rôles et fonctionnalités sélectionnés, préparant ainsi le serveur pour la configuration complète de WSUS.

## II/ Assistant de configuration WSUS

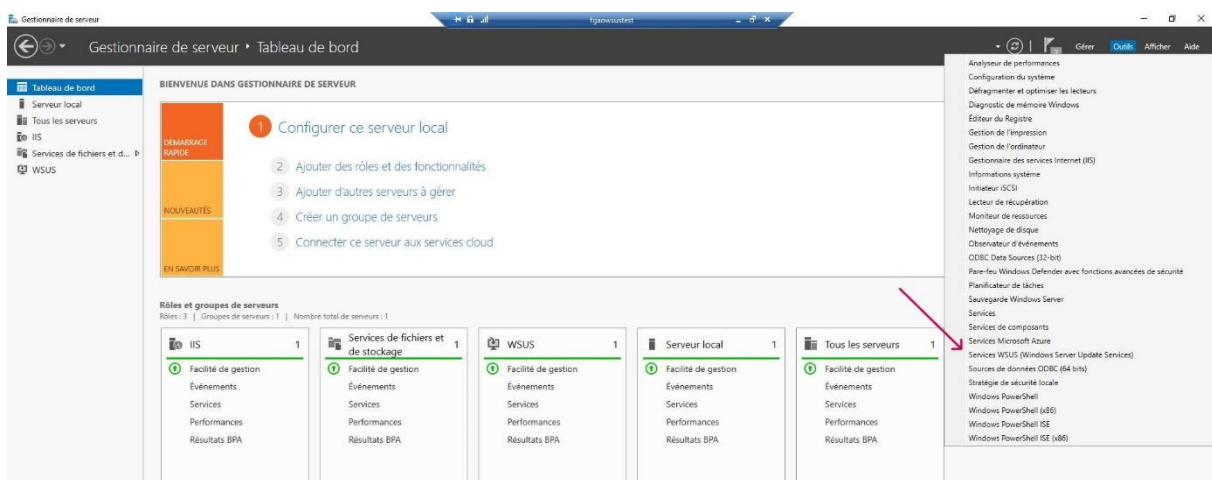
Étapes après l'installation de WSUS :

Une fois l'installation terminée, accédez aux notifications du Gestionnaire de serveur. Cliquez sur la notification intitulée « Configuration post-déploiement » et sélectionnez « Lancer les tâches de post-installation ».

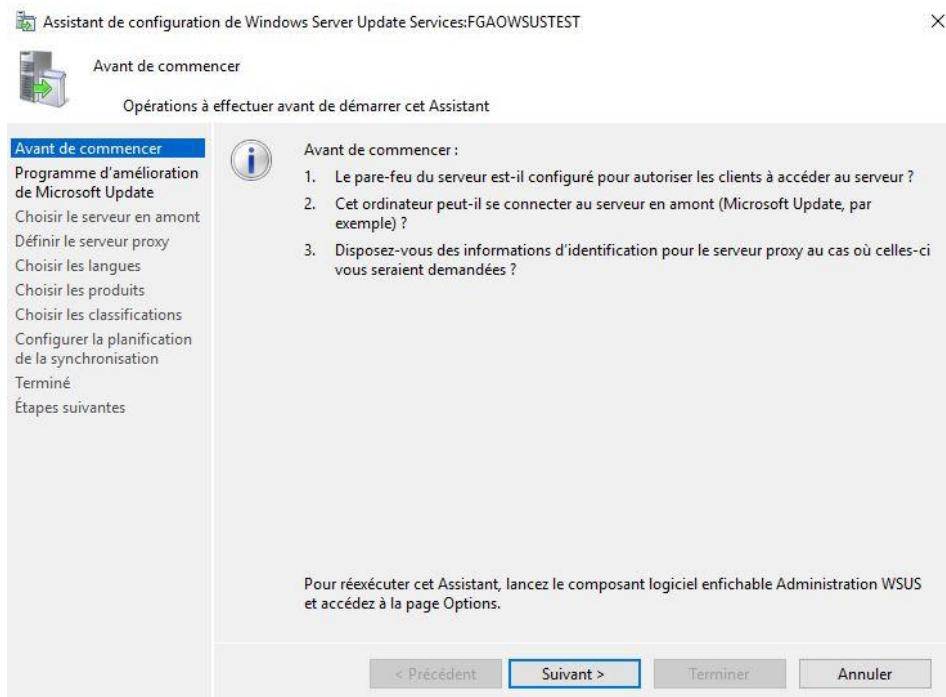


Après avoir terminé cette étape, allez dans le menu « Outils » et sélectionnez « Services WSUS (Windows Server Update Services) » pour accéder à la console de gestion WSUS.

L'assistant de configuration de Windows Server Update Services va s'ouvrir.



## 1/ Avant de commencer



1. Vérifier que le pare-feu du serveur autorise les clients à accéder au serveur WSUS : *Les clients doivent pouvoir communiquer avec le serveur WSUS sur des ports spécifiques.*

Port 8530 pour les mises à jour en HTTP (par défaut) et port 8531 si WSUS est configuré pour utiliser HTTPS.

Pour vérifier les règles dans le pare-feu Windows, il faut ouvrir le Pare-feu Windows avec fonctions avancées. Aller dans *Règles de trafic entrant* et rechercher les *règles concernant les ports 8530 (HTTP) ou 8531 (HTTPS)*. Si ces règles sont présentes, activées et en mode autoriser, alors la communication entre les clients et le serveur WSUS est possible.

2. Vérifier que l'ordinateur peut se connecter au serveur Microsoft Update : WSUS doit pouvoir synchroniser ses mises à jour avec les serveurs Microsoft. En l'occurrence ici *il nous faut une connexion internet.*

3. Vérifier si des informations d'identification pour le proxy sont nécessaires : Si votre organisation utilise un proxy pour accéder à Internet, vous devez configurer WSUS avec les informations d'identification du proxy.

## 2/ Programme d'amélioration de Microsoft Update

Ici, l'assistant propose de participer au Programme d'amélioration de Microsoft Update. Cette étape n'est pas obligatoire et n'a pas d'impact direct sur le fonctionnement de WSUS. Voici ce que cela signifie et les implications pour votre rapport :

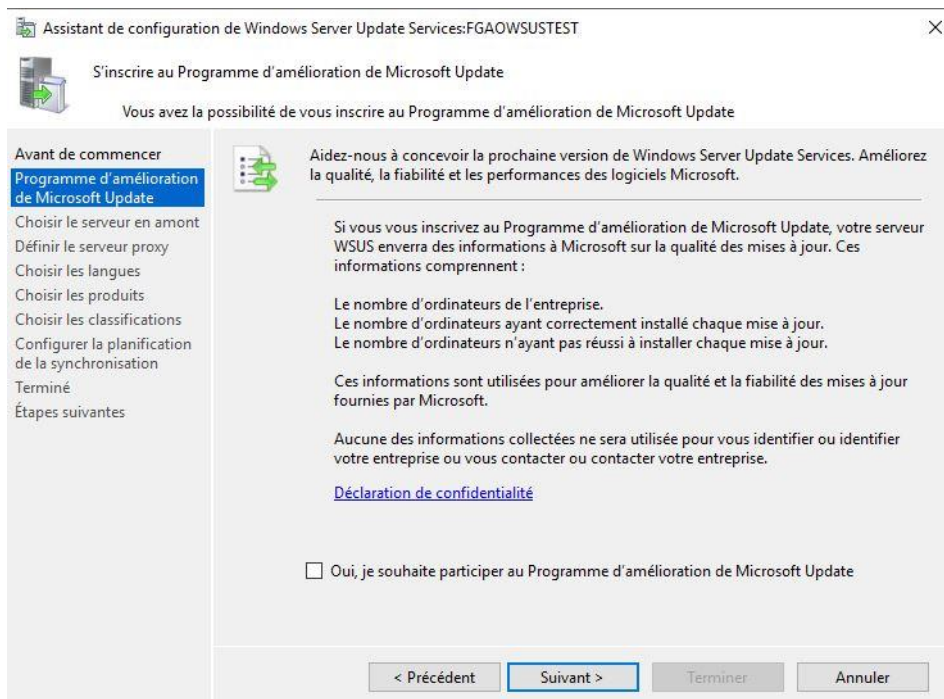
Qu'est-ce que le Programme d'amélioration de Microsoft Update ?

En participant, le serveur WSUS envoie des données anonymes à Microsoft pour améliorer la qualité et la fiabilité des mises à jour ainsi que les performances des services Windows Server Update.

Ces données incluent des statistiques comme le nombre d'ordinateurs de l'entreprise, les mises à jour téléchargées et installées et les mises à jour échouées.

Doit-on cocher cette option ?

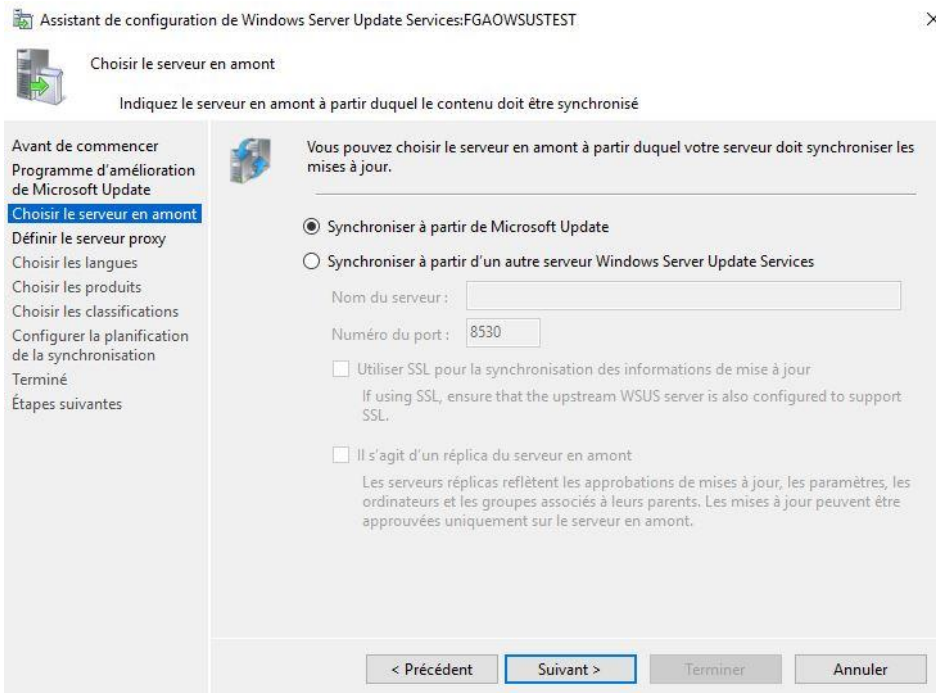
1. Oui, si : Nous voulons contribuer au développement des produits Microsoft.  
Les données partagées sont conformes à votre politique interne (souvent pour des environnements tests ou des entreprises ouvertes à partager des données anonymes).
2. Non, si : Nous travaillons dans un environnement où les données sont sensibles ou confidentielles voire nous ne souhaitons pas transmettre d'informations, même anonymes.



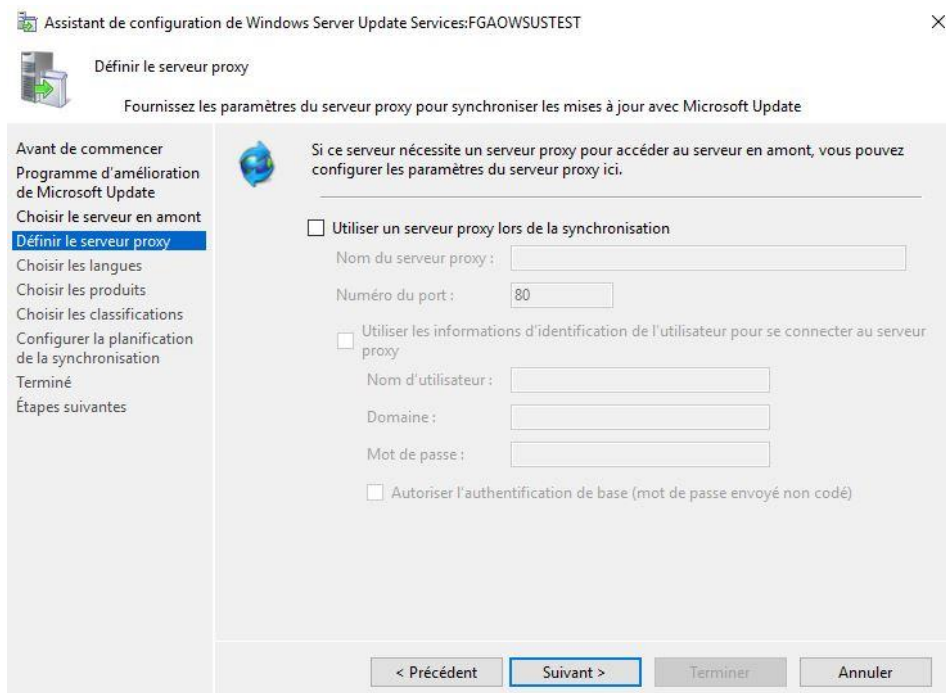
### 3/ Choisir le serveur en amont

Cette étape nous permet de choisir la source à partir de laquelle votre serveur WSUS synchronisera les mises à jour. Explication des options :

1. **Synchroniser à partir de Microsoft Update** : Nous avons choisi ici cette option qui permet au serveur WSUS de télécharger les mises à jour directement depuis les serveurs Microsoft. Cette option est utilisée si *notre serveur WSUS est autonome et n'a pas de serveur WSUS parent*. Cette option nécessite une connexion à Internet.
2. **Synchroniser à partir d'un autre serveur WSUS** : Cette option est utilisée si nous avons une hiérarchie WSUS avec un *serveur maître*, ce qui n'est pas le cas ici. Nous devons spécifier l'adresse et le port (par défaut 8530 pour HTTP ou 8531 pour HTTPS) du serveur WSUS parent. Nous pouvons également configurer notre serveur comme un réplica pour hériter des approbations et paramètres du serveur parent.



#### 4/ Définir le serveur proxy



Cette étape nous permet de configurer un serveur proxy si notre environnement nécessite un proxy pour accéder à Internet.

Rôle du serveur proxy dans WSUS : Un *serveur proxy* peut être nécessaire pour que WSUS accède à *Internet* et synchronise les mises à jour à partir de Microsoft Update. De même que suivre les politiques réseau de votre organisation (par exemple, filtrage ou sécurité).

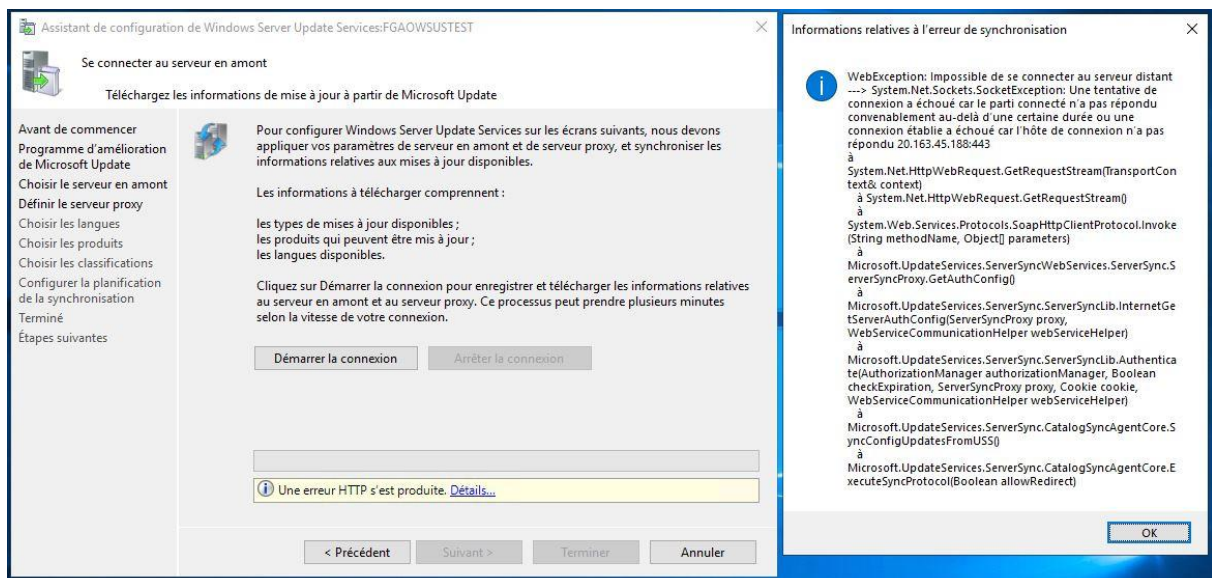
1. Ne pas utiliser de serveur proxy : Si notre serveur WSUS a un accès direct à Internet, cette option reste décochée. Cela signifie que WSUS communiquera directement avec Microsoft Update ou un serveur parent.
2. Utiliser un serveur proxy : Si cette case est cochée, nous devons fournir les informations suivantes :
  - Nom du serveur proxy : L'adresse du serveur proxy utilisé par votre réseau.
  - Numéro du port : Par défaut, le port HTTP utilisé est 80, mais cela dépend de la configuration du proxy.
  - Authentification : Si le proxy nécessite une identification, indiquez le nom d'utilisateur, le mot de passe, et éventuellement le domaine.

## 5/ Erreur de synchronisation

Lors de cette étape, le serveur WSUS tente de se connecter à Microsoft Update pour synchroniser les informations de configuration initiale. Cette connexion est essentielle pour permettre au serveur de : Télécharger les métadonnées des mises à jour disponibles, identifier les produits (Windows, Office, etc.) et classifications (mises à jour de sécurité, correctifs, etc.) pris en charge et enfin, configurer les langues disponibles pour les mises à jour.

Ces informations sont nécessaires pour que WSUS puisse personnaliser la gestion des mises à jour dans les étapes suivantes.

Erreur rencontrée :

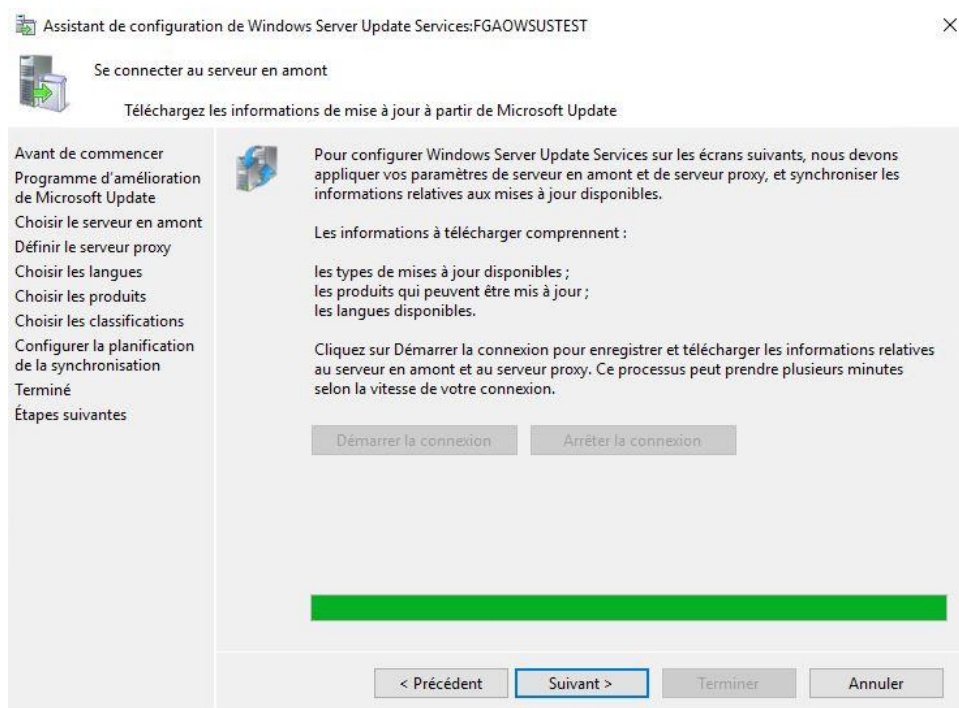


Lors de la tentative de connexion à Microsoft Update, une erreur a été générée :

- Type d'erreur : WebException

- Détail : « Une tentative de connexion a échoué car le parti connecté n'a pas répondu au-delà d'une certaine durée ou une connexion établie a échoué car l'hôte de connexion n'a pas répondu ».
- Adresse concernée : 20.163.45.188:443 (port HTTPS pour Microsoft Update).

Cause identifiée : cette erreur est due à l'absence d'accès Internet sur le serveur WSUS. Dans l'environnement actuel, les serveurs n'ont pas accès à Internet pour des raisons de sécurité. L'activation temporaire de l'accès Internet nécessite l'intervention des administrateurs réseaux.



Une fois le téléchargement terminé, la suite permet au serveur WSUS de se connecter à sa source en amont pour récupérer les métadonnées nécessaires à sa configuration. *Dans notre cas, le serveur WSUS se connecte directement à Microsoft Update, car il est configuré comme un serveur autonome (sans serveur parent).*

Les informations téléchargées comprennent :

Les types de mises à jour disponibles (mises à jour de sécurité, correctifs critiques, etc.), les produits pris en charge (comme Windows, Office, ou d'autres logiciels Microsoft) et les langues pour lesquelles les mises à jour peuvent être appliquées.

Ce téléchargement initial permet au serveur WSUS de savoir quels types de mises à jour et quels produits il pourra gérer. Ces informations serviront à personnaliser les paramètres des étapes suivantes, comme le choix des produits et classifications.

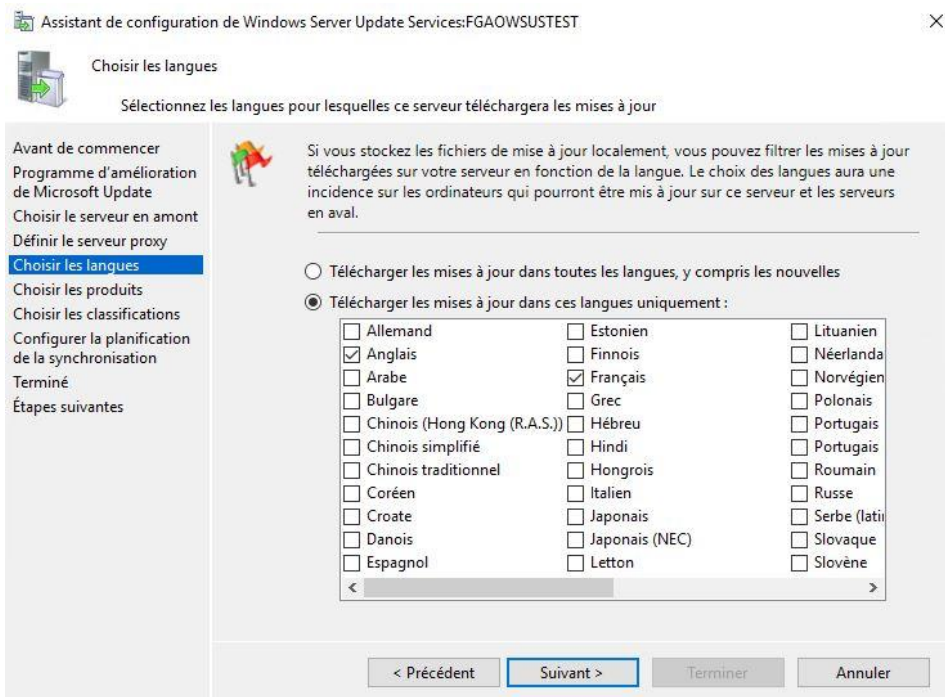
Fonctionnement : Le serveur établit une connexion avec Microsoft Update via Internet. Il télécharge uniquement les métadonnées (pas encore les mises à jour, juste des informations sur les mises à jour).

Cette opération peut prendre quelques minutes, en fonction de la vitesse de la connexion.

À la fin de cette étape, le serveur WSUS dispose des informations nécessaires pour configurer les mises à jour qu'il devra gérer, et il est prêt à passer à l'étape suivante de la configuration.

## 6/ Choisir les langues

Cette étape permet de spécifier les langues pour lesquelles le serveur WSUS doit télécharger les mises à jour. Cela permet d'*optimiser l'utilisation de l'espace disque et de réduire le volume de données téléchargées*.



Deux options principales sont disponibles :

1. Télécharger les mises à jour dans toutes les langues : Cette option télécharge toutes les mises à jour disponibles pour toutes les langues, y compris les nouvelles langues ajoutées par Microsoft. Elle est utile pour les environnements multilingues où plusieurs langues sont utilisées, mais elle *consomme plus d'espace disque et de bande passante*.
2. Télécharger les mises à jour dans des langues spécifiques uniquement : Cette option permet de sélectionner les langues pertinentes pour votre environnement. Par exemple, si l'environnement est principalement francophone et anglophone, seules les mises à jour pour français et anglais seront téléchargées. Cela permet de *réduire considérablement la taille des fichiers stockés localement et d'optimiser les ressources*.

Notre sélection : Dans notre cas, seules les langues anglais et français ont été sélectionnées. Cette configuration est idéale pour un environnement où ces deux langues sont utilisées sur les postes clients.

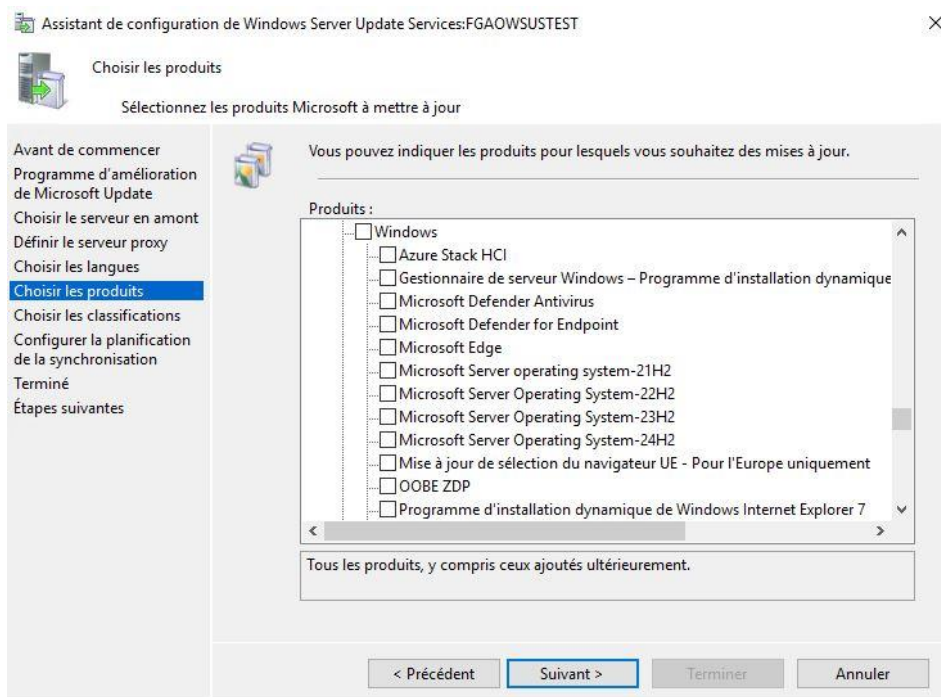
## 7/ Choisir les produits

Dans cette étape, le serveur WSUS permet de sélectionner les produits Microsoft pour lesquels il doit télécharger et gérer les mises à jour. Cela inclut les systèmes d'exploitation, les suites logicielles (comme Office), et d'autres produits Microsoft.

Rôle de cette configuration : Cette sélection *détermine les types de mises à jour qui seront téléchargées et distribuées aux postes et serveurs de l'entreprise*. En choisissant uniquement les produits nécessaires, nous optimisons l'espace disque et réduisez la charge réseau.

Voici les produits requis pour le FGV : ASP.NET Web and Data Frameworks (ASP.NET Web Frameworks), Office 2016, Microsoft SQL Server 2012, Microsoft SQL Server 2016, Microsoft Defender Antivirus, Microsoft Edge, Windows 10 LTSB, Windows Serveur 2012 R2, Windows Serveur 2012, Windows Serveur 2016, Windows Serveur 2019.

Impact de cette configuration : Si des produits manquent dans cette liste, leurs mises à jour ne seront pas disponibles via WSUS, ce qui pourrait poser des problèmes de sécurité ou de compatibilité. De même qu'une sélection trop large pourrait augmenter la consommation d'espace disque inutilement.

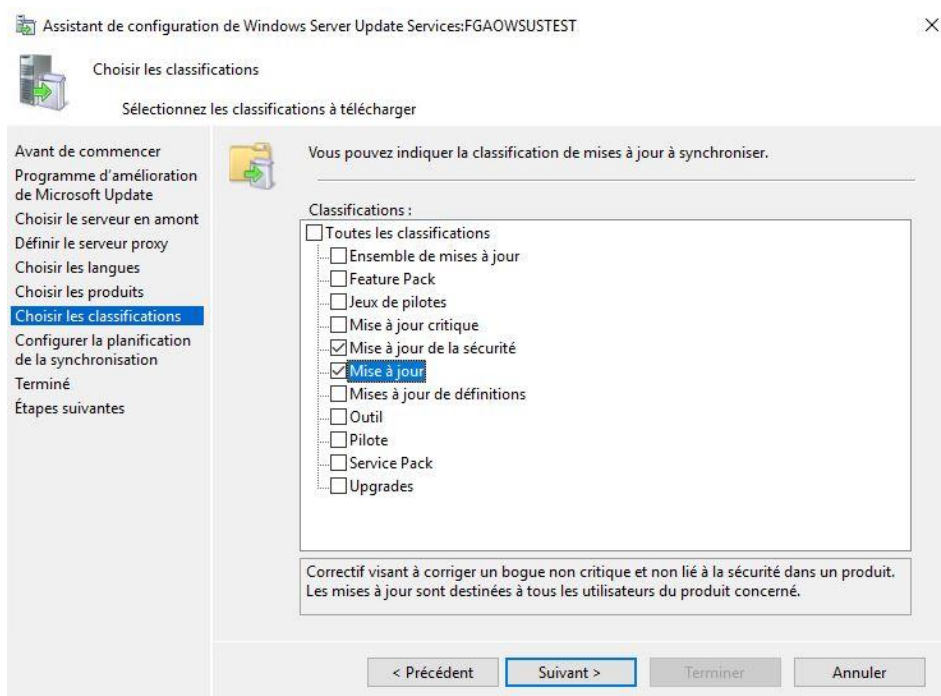


## 8/ Choisir les classifications

Cette étape consiste à sélectionner les catégories de mises à jour que le serveur WSUS devra synchroniser et distribuer. Cela permet de contrôler précisément quels types de correctifs seront proposés aux postes et serveurs du réseau.

Classifications sélectionnées et leur explication :

1. **Mises à jour critiques** : ce sont des correctifs destinés à *résoudre des problèmes majeurs* pouvant entraîner des *failles de sécurité graves* ou des *dysfonctionnements critiques* dans les produits Microsoft.  
Exemple : Un correctif pour empêcher une exploitation active d'une faille critique.
2. **Mises à jour de sécurité** : ces mises à jour *corrigent des vulnérabilités de sécurité* dans les produits Microsoft. Elles sont essentielles pour protéger le réseau *contre les attaques externes*, comme les virus, ransomwares ou autres cybermenaces.  
Exemple : Une mise à jour pour sécuriser une faille dans Windows Defender.
3. **Mises à jour** : il s'agit de correctifs généraux visant à *corriger des bugs* ou à *améliorer la stabilité des produits* sans lien direct avec la sécurité.  
Exemple : Une mise à jour pour résoudre un problème de compatibilité entre Windows et un logiciel tiers.
4. **Mises à jour de définitions** : ces mises à jour *concernent les bases de données* utilisées par les logiciels de sécurité comme Windows Defender ou Microsoft Security Essentials pour détecter les logiciels malveillants. Elles sont souvent publiées quotidiennement ou à une fréquence élevée.  
Exemple : *Une nouvelle définition ajoutant la détection d'un nouveau virus.*



En choisissant ces classifications, nous nous assurons que les vulnérabilités critiques et de sécurité sont rapidement corrigées, que les postes et serveurs bénéficient d'un fonctionnement stable grâce aux mises à jour générales. Et que les logiciels de sécurité sont constamment à jour face aux nouvelles menaces.

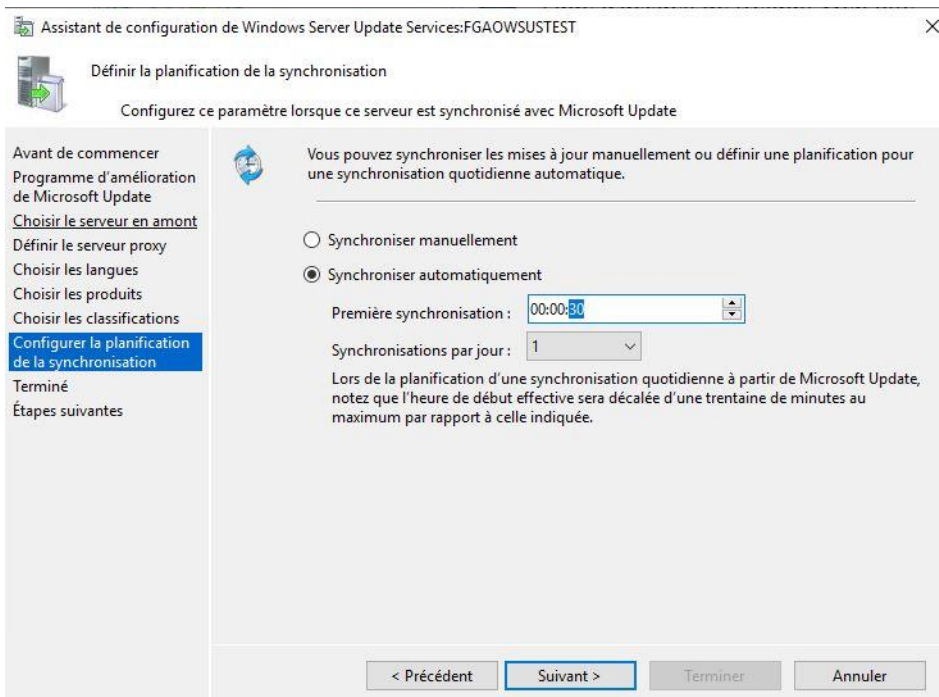
Cette configuration est équilibrée et pertinente pour un environnement professionnel, car elle se concentre sur la sécurité et la stabilité sans inclure des mises à jour moins prioritaires (comme les pilotes ou les Service Packs).

Explications courtes des autres classifications :

1. Ensemble de mises à jour : une collection combinée de plusieurs correctifs ou mises à jour regroupées pour simplifier leur installation.
2. Feature Pack : Ajout ou amélioration de fonctionnalités spécifiques à un produit Microsoft. Exemple : Activation d'une nouvelle fonctionnalité dans Windows.
3. Jeux de pilotes (Drivers) : Mises à jour pour les pilotes matériels (comme les cartes graphiques ou imprimantes).
4. Outil : Fournit des utilitaires ou outils spécifiques pour diagnostiquer ou gérer un système. Exemple : Outil de diagnostic pour un problème réseau.
5. Service Pack : Une mise à jour cumulative qui inclut toutes les mises à jour précédentes, ainsi que des correctifs supplémentaires. Souvent utilisée pour des systèmes d'exploitation ou suites logicielles.
6. Upgrades : Permet une mise à niveau majeure vers une nouvelle version d'un produit (comme passer de Windows 10 à Windows 11).

Ces classifications sont utiles dans des cas spécifiques, mais elles ne sont pas toujours nécessaires pour une configuration standard axée sur la sécurité et la stabilité.

## 9/ Configurer la planification de la synchronisation



The screenshot shows the 'Assistant de configuration de Windows Server Update Services:FGAOWSUSTEST' window. The current step is 'Définir la planification de la synchronisation'. The left sidebar contains a list of steps: 'Avant de commencer', 'Programme d'amélioration de Microsoft Update', 'Choisir le serveur en amont', 'Définir le serveur proxy', 'Choisir les langues', 'Choisir les produits', 'Choisir les classifications', 'Configurer la planification de la synchronisation' (highlighted), 'Terminé', and 'Étapes suivantes'. The main area contains the following text: 'Vous pouvez synchroniser les mises à jour manuellement ou définir une planification pour une synchronisation quotidienne automatique.' Below this are two radio buttons: 'Synchroniser manuellement' (unselected) and 'Synchroniser automatiquement' (selected). Under 'Synchroniser automatiquement', there is a 'Première synchronisation' field set to '00:00:30' and a 'Synchronisations par jour' dropdown set to '1'. A note at the bottom states: 'Lors de la planification d'une synchronisation quotidienne à partir de Microsoft Update, notez que l'heure de début effective sera décalée d'une trentaine de minutes au maximum par rapport à celle indiquée.' At the bottom of the window are four buttons: '< Précédent', 'Suivant >' (highlighted), 'Terminer', and 'Annuler'.

Par la suite nous devons définir quand et comment le serveur WSUS synchronisera les mises à jour avec Microsoft Update ou un autre serveur WSUS en amont.

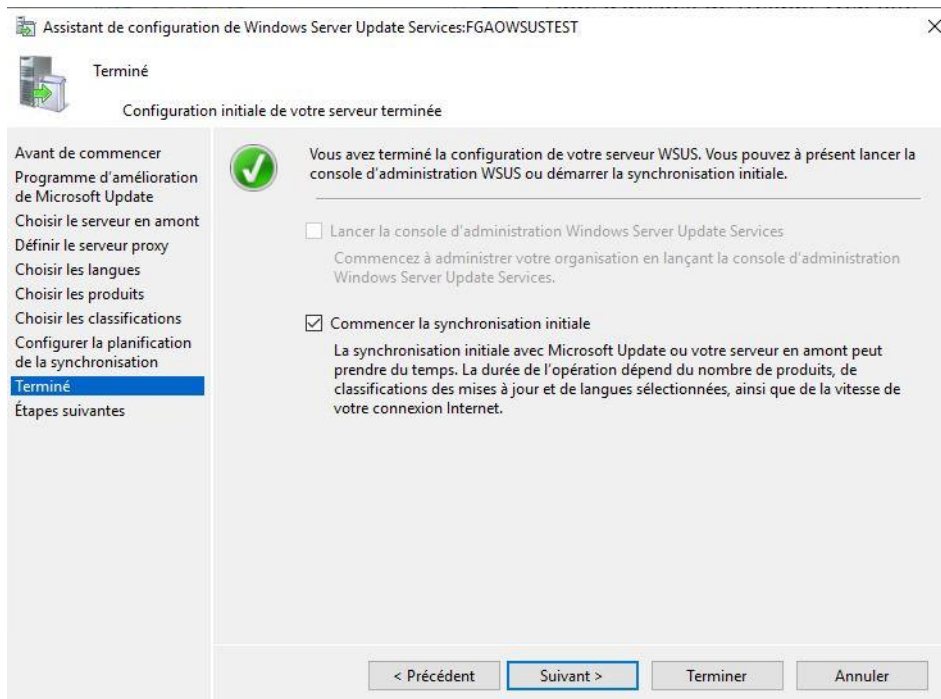
Options disponibles :

1. **Synchroniser manuellement** : La synchronisation doit être déclenchée manuellement par un administrateur, idéal pour les environnements où un contrôle strict est nécessaire.
2. **Synchroniser automatiquement** : Le serveur WSUS effectue automatiquement les synchronisations à des heures planifiées. Nous pouvons définir l'heure de la première synchronisation. Par défaut *00h30 est recommandé pour limiter l'impact sur les performances réseau durant les heures de travail.*  
Pour le nombre de synchronisations par jour, *une seule synchronisation quotidienne est souvent suffisante pour maintenir le serveur à jour.*

Au FGV, la configuration requise pour la première heure de synchronisation commence à 3h00. Cette heure est choisie pour éviter tout impact sur les performances réseau ou serveur pendant les heures ouvrées. Le nombre de synchronisation par jour est maintenu par défaut, c'est-à-dire une par jour. Cela est suffisant pour télécharger les mises à jour nécessaires sans surcharger le serveur.

## 10/ Terminé

Cette étape finalise la configuration initiale de WSUS et propose les actions suivantes :



Options disponibles :

1. **Lancer la console d'administration WSUS** : Cette option ouvre l'interface principale de gestion WSUS après la configuration initiale et permet d'accéder à toutes les fonctionnalités administratives : gestion des mises à jour, des groupes d'ordinateurs, des rapports, etc. Cette option n'est pas cochée par défaut, car *elle peut être exécutée ultérieurement.*

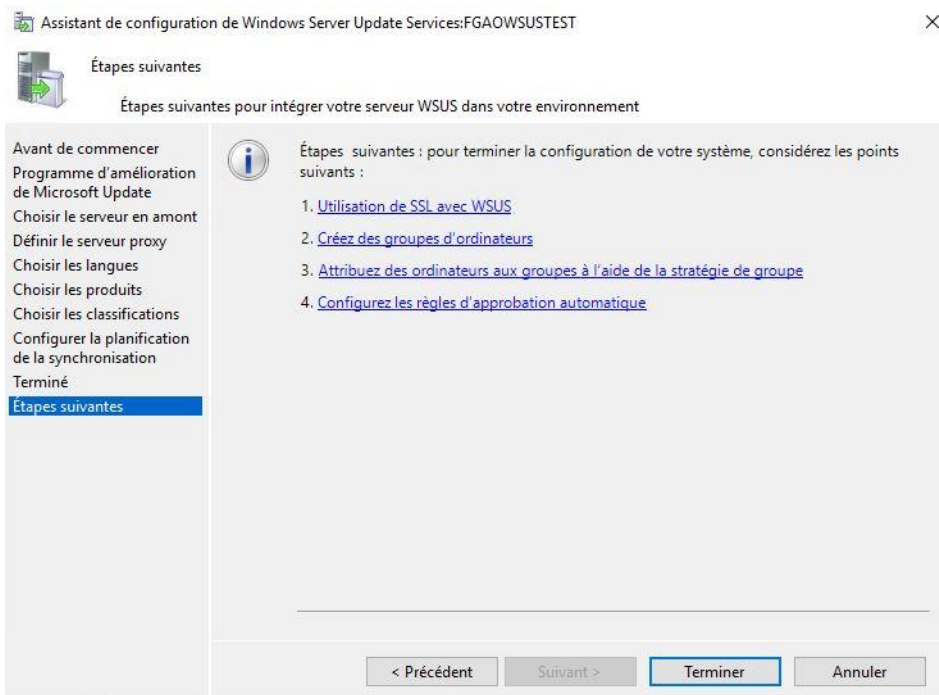
2. **Commencer la synchronisation initiale** : Cette option est cochée par défaut et *lance immédiatement la première synchronisation du serveur WSUS avec Microsoft Update* (ou un serveur parent si configuré (ici il y en n'a pas)). Cette synchronisation télécharge les informations sur les produits et classifications sélectionnés et les mises à jour disponibles pour les langues choisies. La durée de cette synchronisation dépend de la vitesse de la connexion Internet et le nombre de produits et classifications choisis.

Notre sélection concerne la synchronisation initiale, ce qui signifie que le serveur WSUS entamera automatiquement le processus de synchronisation après cette étape.

Une fois la synchronisation initiale terminée, WSUS sera prêt à gérer et distribuer les mises à jour aux postes et serveurs du réseau. Cette étape marque la fin de la configuration initiale, mais la gestion continue (ajout de groupes, approbation des mises à jour) doit être effectuée dans la console WSUS.

## 11/ Étapes suivantes

Cette dernière étape fournit des *recommandations* pour intégrer et optimiser l'utilisation de votre serveur WSUS dans votre environnement. Elle liste des actions supplémentaires pour assurer une configuration complète et fonctionnelle.



Étapes proposées :

1. Utilisation de **SSL avec WSUS** : Configurer WSUS pour utiliser SSL (*HTTPS*) afin de *sécuriser les communications entre le serveur WSUS et les clients*. Cela est particulièrement important dans les environnements où la sécurité est prioritaire.
2. Créez des **groupes d'ordinateurs** : Permet de *classer les ordinateurs (postes clients ou serveurs) dans des groupes logiques*, comme : Serveurs, Postes utilisateurs, Postes de test. Cela facilite la gestion et l'approbation des mises à jour.

3. Attribuez des ordinateurs aux groupes à l'aide de la **stratégie de groupe** : Utiliser les *GPO (Group Policy Objects)* pour attribuer automatiquement les ordinateurs aux groupes créés dans WSUS. Cela permet une gestion centralisée et automatisée des postes clients dans Active Directory.
4. Configurez les **règles d'approbation** automatique : Mettre en place des règles qui approuvent automatiquement certaines catégories de mises à jour (par exemple, mises à jour critiques ou de sécurité). Cela *simplifie l'administration et réduit les délais pour appliquer les mises à jour essentielles*.

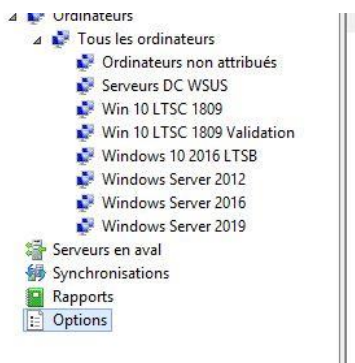
Ces étapes ne sont pas obligatoires dans l'immédiat, mais elles sont fortement recommandées pour tirer pleinement parti de WSUS. Leur mise en œuvre contribue à une gestion efficace, sécurisée, et adaptée à l'environnement d'entreprise.

### III. Télécharger des mises à jour

Pour poursuivre la configuration, il a été nécessaire d'ouvrir le service WSUS. Voici les étapes réalisées :

#### 1/ Création des groupes d'ordinateurs et serveurs

Un clic droit a été effectué sur « Tous les ordinateurs », suivi de la création des groupes suivants : Serveur DC WSUS, Win 10 LTSC 1809, Win 10 LTSC 1809 Validation, Windows 10 2016 LTSB, Windows Server 2012, Windows Server 2016, Windows Server 2019

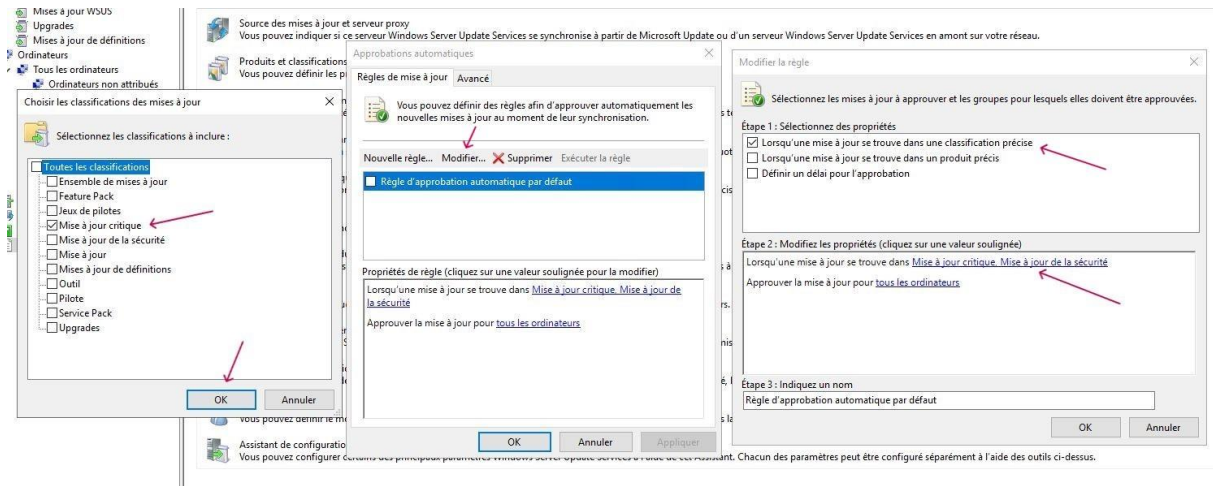


Remarque : Les *noms des groupes doivent être identiques à ceux définis dans Active Directory* pour assurer une bonne correspondance.

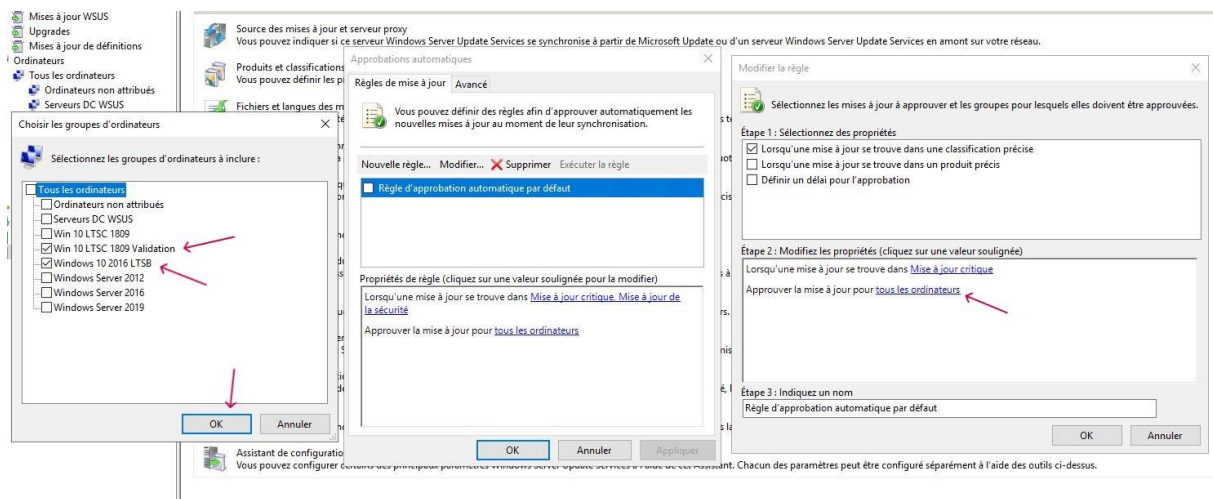
#### 2/ Configuration des règles d'approbation automatique

Ensuite, dans le menu Options, l'onglet Approbations automatiques a été sélectionné pour créer les règles de mises à jour suivantes :

**Règle 1 « Règle d'approbation automatique par défaut »** : Cliquez sur « Règle d'approbation automatique par défaut », puis sur Modifier. Cochez « Lorsqu'une mise à jour se trouve dans une classification précise ». Et dans « Lorsqu'une mise à jour se trouve dans », sélectionnez : « Mise à jour critique » (le choix « Mise à jour de la sécurité » qui était là par défaut va disparaître).

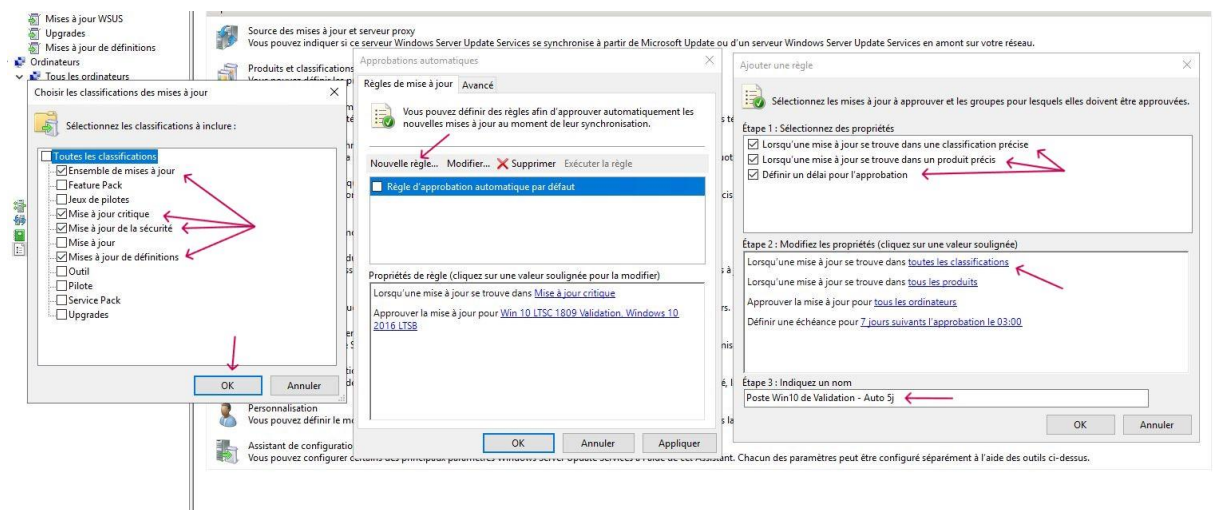


Ensuite dans Approuver la mise à jour pour, choisissez : « Win 10 LTSC 1809 Validation », « Windows 10 2016 LTSC » (le choix « tous les ordinateurs » qui était là par défaut va disparaître).



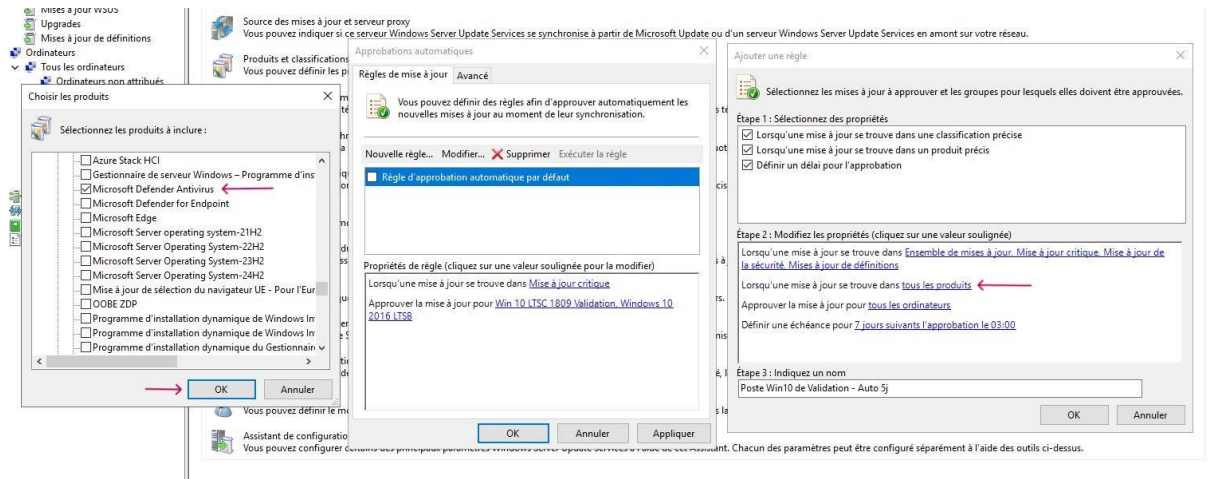
Cela permet d'approuver automatiquement les mises à jour critiques uniquement pour certains groupes de validation, afin de tester avant un déploiement global.

## Règle 2 « Poste Win10 de Validation - Auto 5j » :

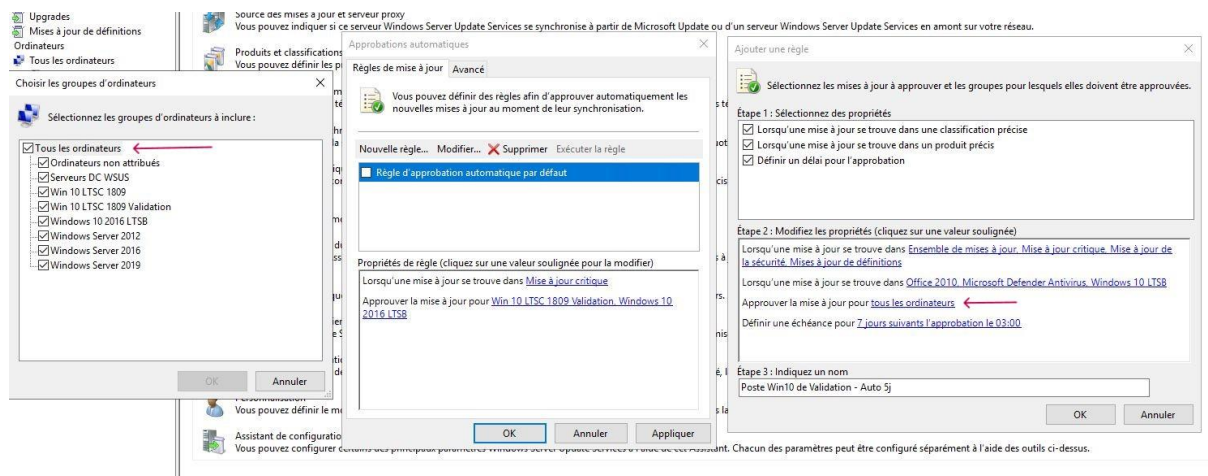


Créez une nouvelle règle et nommez-la « Poste Win10 de Validation - Auto 5j ».

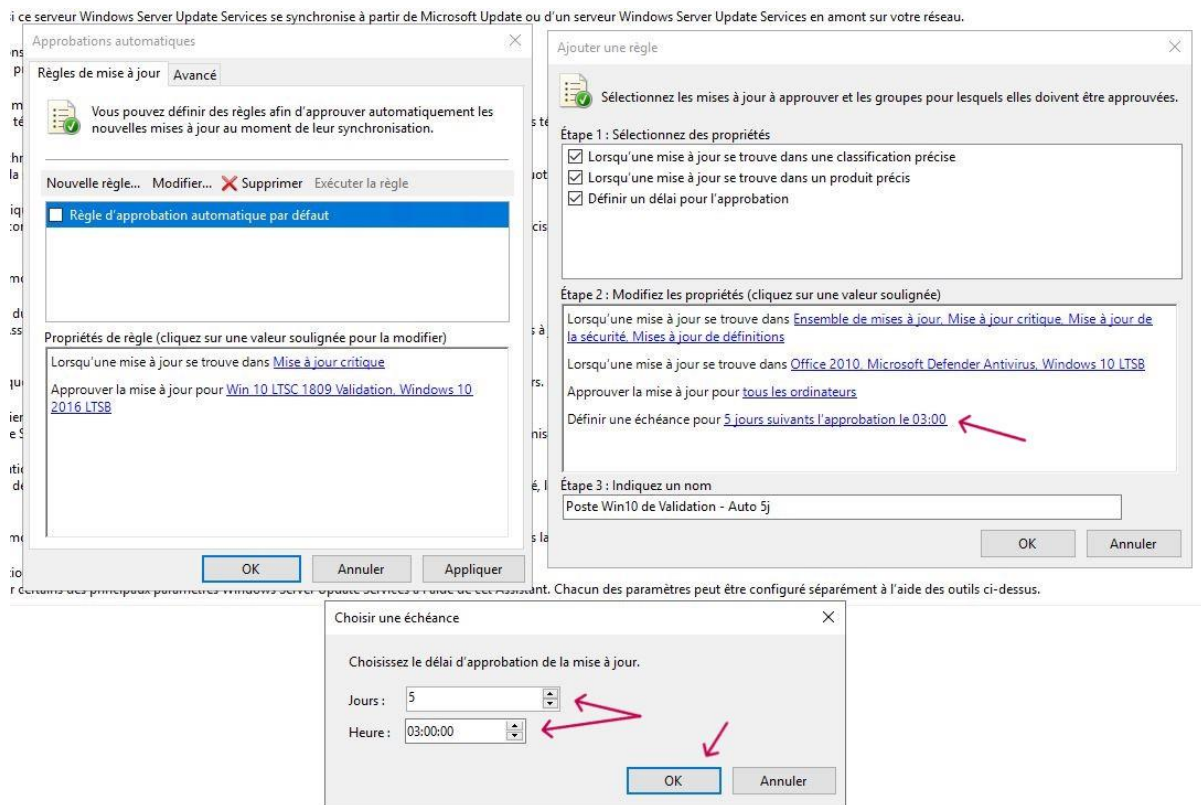
Cochez les options suivantes : « Lorsqu'une mise à jour se trouve dans une classification précise », « Lorsqu'une mise à jour se trouve dans un produit précis » et « Définir un délai pour l'approbation ». Dans « Lorsqu'une mise à jour se trouve dans », sélectionnez : « Ensemble de mises à jour », « Mise à jour critique », « Mise à jour de la sécurité », « Mise à jour » et « Mises à jour de définitions ».



Puis dans « Lorsqu'une mise à jour se trouve dans un produit », choisissez : « Microsoft Defender Antivirus », « Office 2010 » et « Windows 10 LTSB ».



Dans « Approuver la mise à jour pour », choisissez « Tous les ordinateurs ».



Définissez une échéance de 5 jours suivant l'approbation à 03:00.

*La règle 2 permet d'approuver automatiquement les mises à jour qui correspondent à certains types et produits définis, pour tous les ordinateurs, avec un délai de 5 jours.*

**Règle 3 « Poste Win10 LTSC de Validation - Auto 3J » :** Créez une nouvelle règle et nommez-la « Poste Win10 LTSC de Validation - Auto 3J ».

Cochez les options suivantes : « Lorsqu'une mise à jour se trouve dans une classification précise », « Lorsqu'une mise à jour se trouve dans un produit précis » et « Définir un délai pour l'approbation ». Dans « Lorsqu'une mise à jour se trouve dans », sélectionnez : « Ensemble de mises à jour », « Mise à jour critique », « Mise à jour de la sécurité », « Mise à jour » et « Mises à jour de définitions ».

Puis dans « Lorsqu'une mise à jour se trouve dans » choisissez : « Microsoft Defender Antivirus », « Microsoft Edge », « Office 2016 » et « Windows 10 LTSC ».

Ensuite dans « Approuver la mise à jour pour », choisissez « Win 10 LTSC 1809 Validation ». Définissez une échéance de 3 jours suivant l'approbation à 03:00.

*C'est comme la règle 2, mais sur un groupe précis et plus rapide.*

**Règle 4 « Microsoft Defender Antivirus » :** Créez une nouvelle règle et nommez-la Microsoft Defender Antivirus.

Cochez les options suivantes : « Lorsqu'une mise à jour se trouve dans une classification précise » et « Lorsqu'une mise à jour se trouve dans un produit précis ».

Dans « Lorsqu'une mise à jour se trouve dans », sélectionnez : « Microsoft Defender Antivirus ».

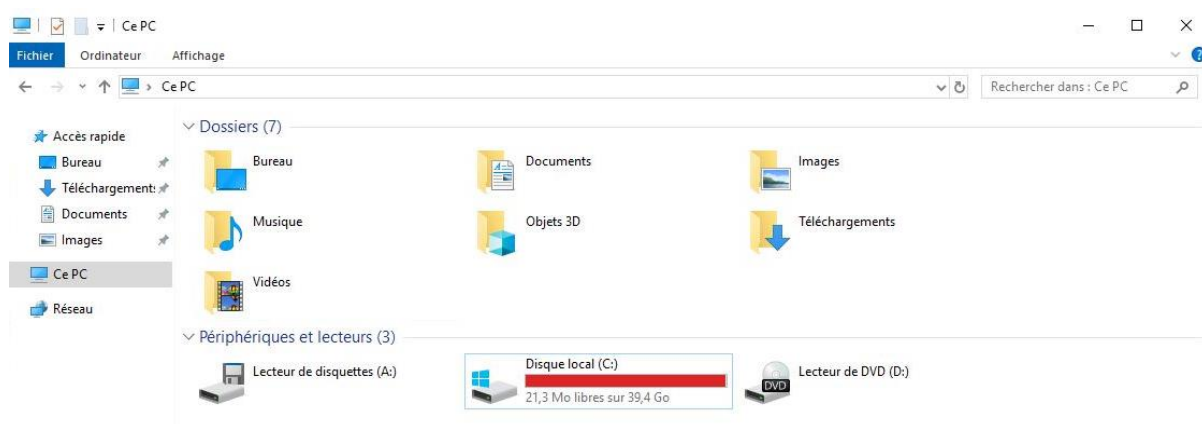
Puis dans « Approuver la mise à jour pour », choisissez : « Windows Server 2016 », « Windows Server 2019 » et « Windows Server 2012 ».

La règle 4 permet d'approuver automatiquement les mises à jour de Microsoft Defender Antivirus pour les serveurs, afin de garantir une protection continue contre les menaces.

Ces règles permettent d'automatiser l'approbation des mises à jour pour différents produits et classifications, assurant ainsi une gestion efficace et personnalisée des mises à jour dans l'environnement WSUS.

### 3/ Gestion du stockage WSUS

Après la configuration des règles et des groupes, il est essentiel de synchroniser le serveur WSUS pour qu'il puisse télécharger les mises à jour nécessaires. Cependant, cette étape doit être effectuée avec précaution pour éviter la saturation de l'espace disque :

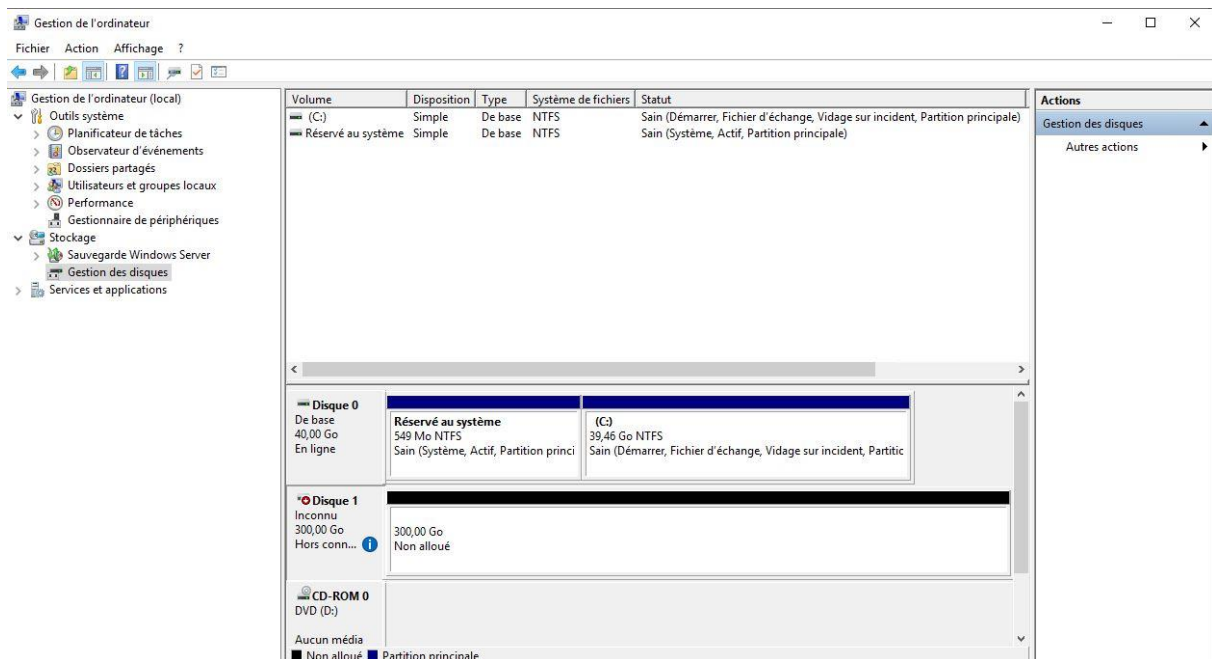


En cas de saturation de l'espace disque sur le serveur WSUS, il peut être nécessaire de tout recommencer et d'ajouter un nouveau disque pour allouer plus d'espace au service WSUS. Voici les étapes que nous avons suivies pour résoudre ce problème :

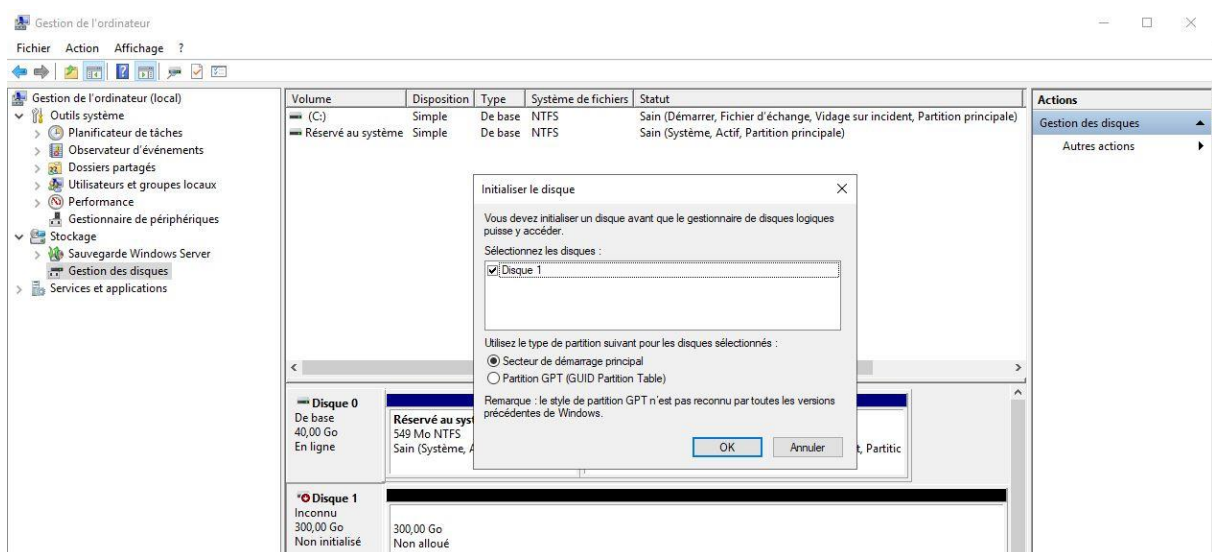
1. Ajout d'un nouveau disque par l'administrateur réseau : L'administrateur réseau a ajouté un disque supplémentaire de 300 Go dans la machine virtuelle (VM) qui héberge le serveur WSUS. Le disque est destiné à être utilisé comme stockage pour WSUS et qui va être nommé Data (E:).

Cependant, après l'ajout, le disque n'était pas visible dans l'explorateur de fichiers. Il a donc fallu l'initialiser et le configurer.

## 2. Initialisation du nouveau disque



- Accéder à la gestion des disques : Ouvrir le menu Démarrer et tapez Gestion de l'ordinateur. Une fois dans la console, accéder à Stockage puis Gestion des disques.
- Localiser le disque ajouté : Le nouveau disque apparaît sous le nom de Disque 1 (ou un autre numéro si plusieurs disques sont présents). *Son statut est indiqué comme Inconnu et Hors connexion.*
- Mettre le disque en ligne : Faire un clic droit sur le disque et sélectionner Mettre en ligne. Le disque *passé alors de Hors connexion à Non initialisé.*
- Initialiser le disque : Faire un clic droit sur le disque maintenant indiqué comme Non initialisé. Sélectionner *Initialiser le disque (préparer le disque pour que Windows puisse l'utiliser).* Dans la fenêtre qui s'ouvre, choisir le type de partition :

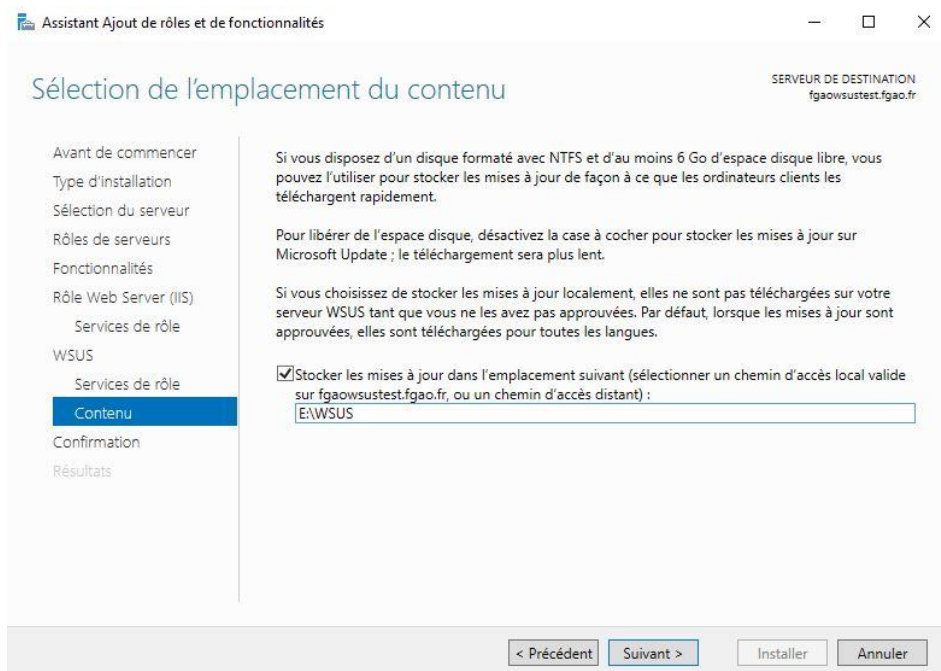


*Le choix du « Secteur de démarrage principal » a été fait pour des raisons de compatibilité et de cohérence avec l'infrastructure existante. Dans ce cas, la taille du disque ne posait pas de contrainte.*

### 3. Configuration de WSUS pour utiliser le nouveau disque

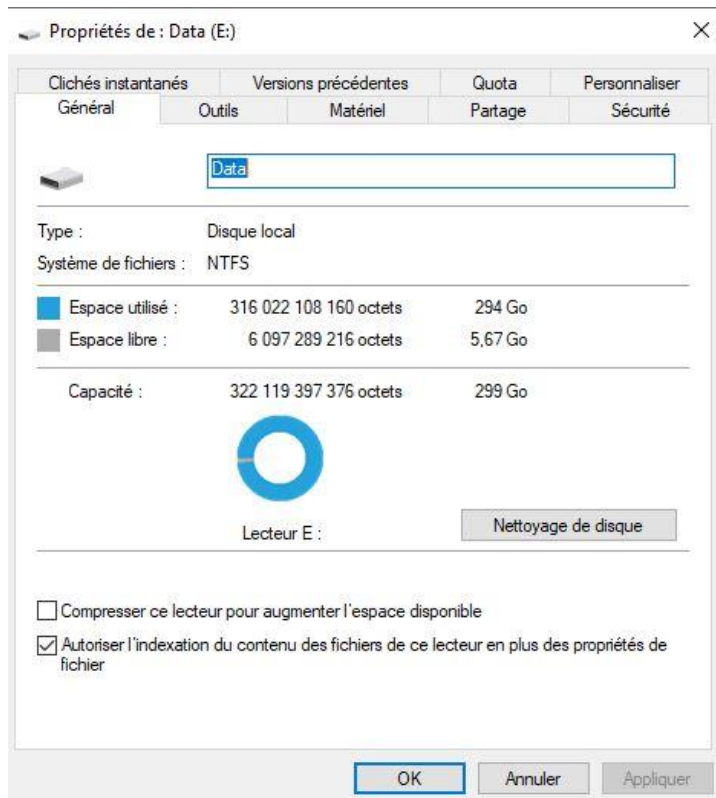
Si le disque initial est saturé, il est nécessaire de désinstaller le serveur WSUS et de recommencer la configuration. Voici les étapes à suivre :

- a) Désinstallation de WSUS : Accéder au Gestionnaire de serveur pour désinstaller le rôle WSUS. Puis supprimer les fichiers WSUS de l'ancien disque (C:).
- b) Réinstallation de WSUS : Réinstaller le rôle WSUS depuis le Gestionnaire de serveur. Lors de l'étape de configuration dans l'assistant WSUS, il faut spécifier le nouveau chemin pour le contenu WSUS : E:\WSUS.
- c) Finalisation : Une fois l'installation terminée, lancez la synchronisation initiale pour télécharger les mises à jour sur le nouveau disque.



### 4/ Surveillance de l'espace disque

Pendant la synchronisation, il est important de surveiller l'espace disponible sur le disque. Si l'espace devient insuffisant, le serveur peut rencontrer des problèmes de performance ou échouer à télécharger les mises à jour. Pour prévenir cela, il est recommandé de *supprimer régulièrement les mises à jour inutiles*.



## 5/ Refuser les mises à jour inutiles

Certaines mises à jour peuvent être refusées pour libérer de l'espace disque et réduire la charge sur le serveur WSUS. Voici les types de mises à jour à refuser :

- Mises à jour pour Microsoft Office 2016 (64 bits) : Word, PowerPoint, Outlook, OneNote, Excel
- Projets et Visio (32 bits)
- Microsoft Edge : edge-stable, edge-dev, edge-beta, edge-extended stable (x86)
- Refuser toutes les versions x86 : Elles sont inutiles si l'environnement utilise uniquement des systèmes x64 et ARM64.

## 6/ Attention à certaines mises à jour

Pour les mises à jour indiquant la version (par exemple, les mises à jour cumulatives), *conservez uniquement les deux dernières versions* et refusez les autres.

Certaines mises à jour, comme celles pour Microsoft Office 2016, ne *précisent pas la version* dans leur intitulé. Dans ce cas, il est préférable de les *conserver*, car il est impossible de savoir si une mise à jour remplace une autre.

## 7/ Suppression des mises à jour anciennes

Certaines mises à jours ne sont plus nécessaire peu importe leur catégorie car elles sont beaucoup trop anciennes. Comme toutes les *mises à jour datant d'avant 2020 qui sont à refuser*.

Notons qu'il est important de *refuser les mises à jour progressivement*, en petites séries, pour *éviter des bugs* ou des plantages du service WSUS.

## 8/ Nettoyage des mises à jour refusées

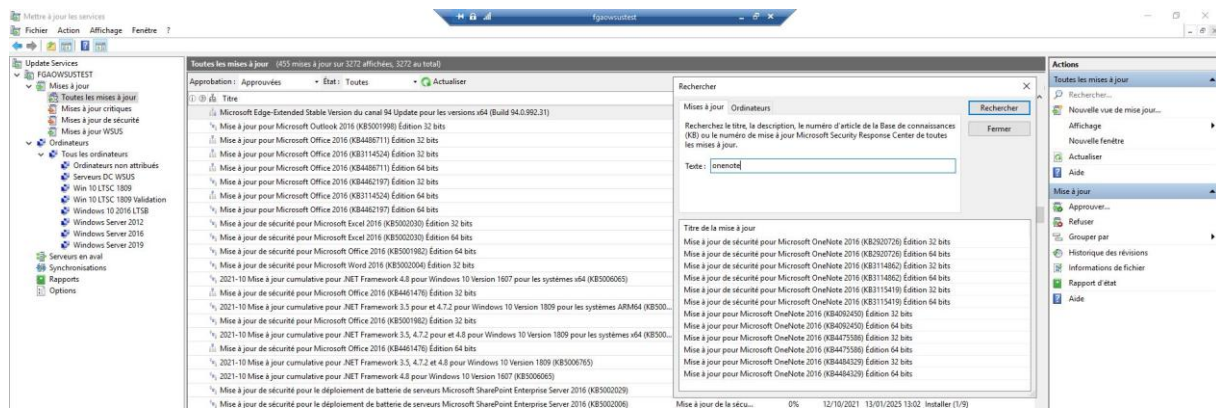
Lorsque vous refusez une mise à jour via un clic droit puis Refuser, celle-ci n'est pas supprimée immédiatement. Pour la supprimer complètement accédez à *Options puis Assistant de nettoyage du serveur WSUS*. Cochez toutes les options disponibles et cliquez sur Suivant pour exécuter le nettoyage.

Note : Le nettoyage complet peut prendre du temps en fonction du volume de mises à jour à supprimer.

# IV. Exploitation et gestion du service WSUS

## 1/ Limites de l'outil de recherche

L'outil de recherche dans WSUS peut manquer d'efficacité. Il affiche parfois des mises à jour déjà refusées, ce qui peut compliquer la gestion. Il est donc préférable de *vérifier manuellement les mises à jour à supprimer pour garantir une gestion précise*.



## 2/ Approbation manuelle des mises à jour

Après la configuration et la synchronisation des mises à jour, il est nécessaire *d'approuver les mises à jour pour qu'elles soient distribuées aux groupes d'ordinateurs et serveurs appropriés*. Bien que des règles d'approbation automatique aient été mises en place, certaines mises à jour doivent être

approuvées manuellement. La raison est que *les mises à jour concernées ne correspondent pas aux critères définis dans les règles automatiques.*

## 1. Approbation des mises à jour pour le pack Office

Pour les produits du pack Office (Word, Excel, OneNote, etc.) : Approuver pour tous les groupes sauf le groupe Serveurs DC WSUS.

The screenshot shows the WSUS console with a list of updates. An approval dialog box is open, allowing the user to select a group of computers for approval. The dialog box contains the following table:

Groupe d'ordinateurs	Approbation	Date limite
Ordinateurs non attribués	Installer	Aucun
Serveurs DC WSUS	Conserver les approbations existantes	
Win 10 LTSC 1809	Installer	Aucun
Win 10 LTSC 1809 Validation	Installer	Aucun
Windows 10 2016 LTSB	Installer	Aucun
Windows Server 2012	Installer	Aucun
Windows Server 2016	Installer	Aucun
Windows Server 2019	Installer	Aucun

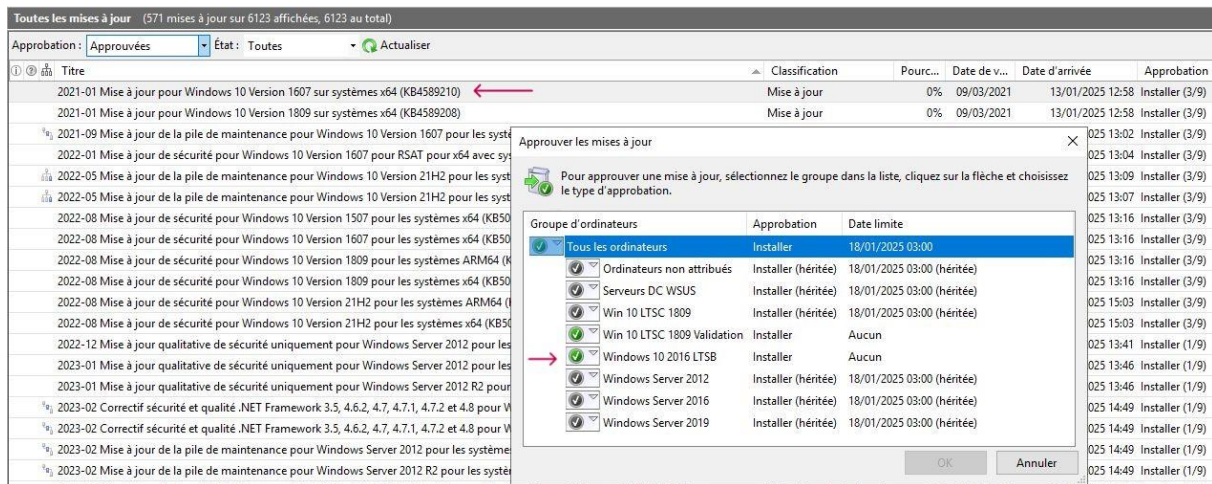
## 2. Approbation des mises à jour Windows 10

Versions 1809 et 21H2 : Approuver pour le groupe Win 10 LTSC 1809.

The screenshot shows the WSUS console with a list of updates. An approval dialog box is open, allowing the user to select a group of computers for approval. The dialog box contains the following table:

Groupe d'ordinateurs	Approbation	Date limite
Tous les ordinateurs	Installer	18/01/2025 03:00
Ordinateurs non attribués	Installer (héritée)	18/01/2025 03:00 (héritée)
Serveurs DC WSUS	Installer (héritée)	18/01/2025 03:00 (héritée)
Win 10 LTSC 1809	Installer	Aucun
Win 10 LTSC 1809 Validation	Installer	Aucun
Windows 10 2016 LTSB	Installer (héritée)	18/01/2025 03:00 (héritée)
Windows Server 2012	Installer (héritée)	18/01/2025 03:00 (héritée)
Windows Server 2016	Installer (héritée)	18/01/2025 03:00 (héritée)
Windows Server 2019	Installer (héritée)	18/01/2025 03:00 (héritée)

## Versions 1607 et 1507 : Approuver pour le groupe Win 10 2016 LTSB.



The screenshot shows the WSUS console interface. At the top, it says 'Toutes les mises à jour (571 mises à jour sur 6123 affichées, 6123 au total)'. Below that, there are filters for 'Approbation : Approuvées' and 'État : Toutes'. A table of updates is visible, with columns for 'Titre', 'Classification', 'Pourcentage', 'Date de v...', 'Date d'arrivée', and 'Approbation'. A dialog box titled 'Approuver les mises à jour' is open, showing a list of groups to approve updates for. The group 'Tous les ordinateurs' is selected. Below the group list, there is a table with columns 'Groupe d'ordinateurs', 'Approbation', and 'Date limite'. The table shows the following data:

Groupe d'ordinateurs	Approbation	Date limite
Tous les ordinateurs	Installer	18/01/2025 03:00
Ordinateurs non attribués	Installer (héritée)	18/01/2025 03:00 (héritée)
Serveurs DC WSUS	Installer (héritée)	18/01/2025 03:00 (héritée)
Win 10 LTSC 1809	Installer (héritée)	18/01/2025 03:00 (héritée)
Win 10 LTSC 1809 Validation	Installer	Aucun
Windows 10 2016 LTSB	Installer	Aucun
Windows Server 2012	Installer (héritée)	18/01/2025 03:00 (héritée)
Windows Server 2016	Installer (héritée)	18/01/2025 03:00 (héritée)
Windows Server 2019	Installer (héritée)	18/01/2025 03:00 (héritée)

Note : Par défaut, les mises à jour des versions 1809, 21H2, 1607 et 1507 de Windows 10 sont attribuées au groupe Win 10 LTSC 1809 Validation.

### 3. Approbation des mises à jour pour les serveurs

Windows Server 2012 : Approuver pour le groupe Windows Server 2012.

Windows Server 2016 : Approuver pour le groupe Windows Server 2016.

Windows Server 2019 : Approuver pour le groupe Windows Server 2019.

Ces approbations manuelles permettent de s'assurer que les mises à jour sont distribuées correctement selon les besoins des différents groupes d'ordinateurs et serveurs. Si des ajustements sont nécessaires, ils peuvent être effectués directement dans la console WSUS.

### 3/ Étapes prévues mais non réalisées (fin de mission)

Les étapes suivantes prévoyaient la *mise en production complète du service WSUS*, notamment la *configuration des stratégies de groupe (GPO)* afin de diriger les postes clients vers le serveur WSUS, ainsi que la validation du déploiement des mises à jour sur des postes de test.

Toutefois, ces manipulations impactant directement l'environnement de production, elles n'étaient pas autorisées dans le cadre du stage afin d'éviter tout risque de dysfonctionnement du système d'information. Ces actions étaient réservées aux administrateurs du système.

De plus, ces opérations devant être réalisées après la fin de la période de stage, il n'a pas été possible de les documenter par des captures d'écran. La configuration côté serveur ayant été finalisée, le service WSUS était néanmoins prêt à être mis en production par l'équipe en charge.