

WSUS | WINDOWS SERVER
UPDATE SERVICES

GESTION DES MISES À JOURS EN ENTREPRISE

1ERE ÉDITION



IT-CONNECT
FLORIAN BURNEL



© Florian Burnel, 2022

ISBN numérique : 979-10-405-1379-7

Librinova”

Internet : www.librinova.com

Le Code de la propriété intellectuelle interdit les copies ou reproductions destinées à une utilisation collective. Toute représentation ou reproduction intégrale ou partielle faite par quelque procédé que ce soit, sans le consentement de l’auteur ou de ses ayants cause, est illicite et constitue une contrefaçon sanctionnée par les articles L335-2 et suivants du Code de la propriété intellectuelle.



Table des matières

À propos de cet eBook	3
À propos de l'auteur : Florian Burnel	3
Module 1 – Installation et configuration de WSUS	4
1. Présentation de l'environnement	4
2. Qu'est-ce qu'un serveur WSUS ?	5
I. Quel est l'intérêt de WSUS ?	5
II. Les fonctionnalités de WSUS	6
III. Historique des versions de WSUS	9
IV. L'importance des mises à jour	9
3. Installation de WSUS sur Windows Server 2022	11
I. Installation du rôle WSUS	11
II. Configuration de base de WSUS	17
III. Facultatif - SQL Server Express avec WSUS	25
4. Prise en main de la console WSUS	28
I. Menu « Mises à jour »	29
II. Menu « Ordinateurs »	32
III. Menu « Serveurs en aval »	32
IV. Menu « Synchronisations »	33
V. Menu « Rapports »	34
VI. Menu « Options »	36
Module 2 - Intégration des ordinateurs dans WSUS	38
1. Lier les machines du domaine au serveur WSUS	38
I. Modifier la méthode d'affectation des ordinateurs	38
II. Créer des groupes d'ordinateurs dans WSUS	39
III. Lier les PC et les serveurs à WSUS par GPO	41
2. Lier les machines en workgroup au serveur WSUS	53
I. Utilisation de WSUS ClientManager For Workgroups	53
3. Approuver ou refuser une mise à jour dans WSUS	56
I. Quand approuver une mise à jour ?	56
II. Approuver une mise à jour	56
Module 3 – Aller plus loin avec WSUS	58
1. Importer une mise à jour du Microsoft Catalog dans WSUS	58
I. Accès au catalogue Microsoft Update avec Edge	58
II. Télécharger et importer une mise à jour	59

2.	WSUS HTTPS avec un certificat SSL, pour plus de sécurité	61
I.	Créer le certificat SSL autosigné	61
II.	Obtenir le certificat avec l'autorité de certification (ADCS)	63
III.	Attribuer le certificat SSL au site WSUS de IIS	75
IV.	Configurer le site WSUS pour exiger le SSL.....	77
V.	Vérifier la connexion SSL de WSUS.....	78
VI.	Connexion des clients en HTTPS	79
3.	Nettoyer son serveur WSUS.....	80
I.	Nettoyage avec la console WSUS	80
II.	Nettoyage avec des scripts PowerShell.....	82
4.	WSUS dans une architecture multisite	84
I.	Les scénarios de déploiement de WSUS	84
II.	Serveur WSUS en amont et serveur WSUS répliqua	85
5.	Gérer un serveur WSUS avec PowerShell	88
I.	Le module PowerShell « UpdateServices » pour WSUS.....	88
II.	Se connecter à l'API WSUS	91
III.	Les utilitaires WSUSutil, wuauctl, et USOclient	92
6.	Gérer le service Windows Update avec « PSWindowsUpdate »	94
I.	Installation du module PSWindowsUpdate.....	94
II.	Exemples d'utilisation de PSWindowsUpdate.....	95
7.	WSUS : les autres alternatives de chez Microsoft.....	97
I.	Microsoft Endpoint Configuration Manager	97
II.	Microsoft Intune	98
III.	Azure Automation Update Management	98
IV.	Windows Autopatch	98
	Conclusion	100

À propos de cet eBook

Ce cours au format livre numérique a pour objectif de vous apprendre à installer, configurer et administrer un serveur WSUS pour assurer la gestion des mises à jour sur les appareils sous Windows desktop et Windows Server. Le rôle WSUS est disponible sur Windows Server 2022 et les versions précédentes de Windows Server.

Grâce aux différents sujets abordés dans ce cours, vous serez en mesure de déployer en production votre propre serveur de gestion des mises à jour basé sur le rôle WSUS. Au-delà du rôle WSUS en lui-même, nous verrons comment configurer le service Windows Update des ordinateurs et comment effectuer des opérations de maintenance à l'aide de PowerShell.

Ce cours s'adresse aux administrateurs système, aux étudiants en informatique, et plus généralement aux personnes qui souhaitent mettre en œuvre un serveur WSUS.

À propos de l'auteur : Florian Burnel

Véritable passionné par l'informatique et les nouvelles technologies, j'ai près de 10 ans d'expérience dans l'administration système et réseau. Généraliste, je maîtrise particulièrement les technologies Microsoft, notamment les différents rôles de Windows Server, ainsi que PowerShell. D'ailleurs, je suis actuellement Microsoft MVP dans la catégorie « *Cloud and Datacenter Management* ».

Le langage PowerShell m'accompagne au quotidien depuis des années, et je ne manque jamais l'opportunité de dégainer une console pour exécuter une commande ou créer un script pour automatiser la moindre tâche !

J'ai écrit et publié de nombreux articles au sujet des technologies Microsoft, mais aussi d'autres sujets comme Linux. Ces articles sont disponibles, comme tous les autres, sur le site IT-Connect, en libre accès.

J'en profite pour remercier Mehdi Dakhama pour sa relecture technique.

Bonne lecture !

Module 1 – Installation et configuration de WSUS

1. Présentation de l'environnement

Avant de commencer à vous parler du sujet « WSUS », je vais décrire l'environnement utilisé et vous parler des ressources matérielles (*que vous pouvez ajuster dans le cadre d'un lab*).

En utilisant deux serveurs virtuels, vous serez en mesure de mettre en place l'environnement nécessaire pour suivre ce cours sur WSUS. Plus précisément, nous avons besoin d'une machine sous Windows Server pour installer les rôles ADDS (Active Directory) et WSUS, ainsi qu'une seconde machine qui jouera le rôle de client WSUS, cela peut-être une machine sous Windows Server ou Windows *desktop*.

Dans l'idéal et dans le but de reproduire un environnement de production, il faudrait utiliser un serveur virtuel différent pour les rôles ADDS et WSUS. C'est ce que je vais faire pour ma part. La mise en place de l'Active Directory ne sera pas abordée dans ce cours.

Remarque importante : mon serveur WSUS est une version anglaise avec un pack de langue français.

- **Serveur ADDS – Contrôleur de domaine**

Caractéristiques	Valeurs
Nom du système	SRV-ADDS-01
Système d'exploitation	Windows Server 2019
Nom de domaine Active Directory	it-connect.local
Ressources matérielles	2 vCPU – 4 Go RAM – 64 Go

- **Serveur WSUS**

Caractéristiques	Valeurs
Nom du système	SRV-WSUS
Système d'exploitation	Windows Server 2022
Ressources matérielles	2 vCPU – 4 Go RAM – 128 Go

Pour le serveur WSUS, en production, j'utilise généralement la configuration matérielle suivante : 4 vCPU, 8 Go RAM et 80 Go + 200 Go pour le stockage.

- **Poste client géré par WSUS**

Caractéristiques	Valeurs
Nom du système	PC-01
Système d'exploitation	Windows 11
Ressources matérielles	2 vCPU – 4 Go RAM – 128 Go

Ce cours s'applique aussi bien à Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 qu'à Windows Server 2022.

2. Qu'est-ce qu'un serveur WSUS ?

Windows Server intègre de nombreux rôles, dont certains que vous connaissez peut-être déjà comme l'Active Directory, le DHCP, le DNS, ou encore Hyper-V pour la virtualisation. Concernant la gestion et la distribution des mises à jour de façon centralisée, il y a aussi un rôle : WSUS.

WSUS signifie **Windows Server Update Service** et il s'agit du rôle intégré à Windows Server qui a une mission bien précise, mais pas évidente : **la distribution des mises à jour des produits Microsoft** sur les postes de travail et serveurs de votre entreprise.

C'est une solution gratuite, si ce n'est qu'il faut payer la licence Windows Server, qui s'adresse directement aux administrateurs d'infrastructure sous Windows Server et de parc informatique sous Windows. **WSUS s'installe exclusivement sur Windows Server.**

I. Quel est l'intérêt de WSUS ?

Vous n'êtes pas sans savoir que Windows intègre un service nommé Windows Update qui a pour objectif de rechercher les mises à jour auprès des serveurs Microsoft, puis de les installer. C'est d'ailleurs ce qu'il se passe chaque mois sur chaque machine lorsque Microsoft publie de nouvelles mises à jour par l'intermédiaire des fameux « *Patch Tuesday* ».

Puisque les machines sont « autonomes » dans la recherche et l'installation des mises à jour, vous allez me dire « *quel est l'intérêt de mettre en place un serveur WSUS ?* ».

Par défaut, une machine Windows va gérer automatiquement les mises à jour, et redémarrer un peu comme bon lui semble pour finaliser l'installation. Que ce soit sur un serveur ou un poste de travail, c'est gênant, car le redémarrage d'une machine peut-être synonyme d'un arrêt de production (selon les rôles assumés par la machine).

En entreprise, on ne peut pas se permettre de ne pas contrôler les mises à jour. Autrement dit, on ne peut pas se permettre de laisser chaque machine (voire même chaque utilisateur) gérer les mises à jour comme elle le souhaite. Vous l'aurez compris, on ne peut pas non plus accepter qu'une machine redémarre quand elle en a envie : si l'ordinateur du grand patron redémarre en pleine réunion de direction, je ne suis pas sûr qu'il apprécie.

Grâce à un serveur WSUS, nous allons répondre à cette problématique et avoir plus de contrôle sur l'installation des mises à jour. En fait, on va pouvoir choisir les mises à jour que l'on veut installer, mais aussi à quel moment on souhaite les installer.

D'un point de vue la sécurité et de la protection contre les attaques et vulnérabilités, il est indispensable d'avoir des ordinateurs et des serveurs avec un système d'exploitation à jour.

II. Les fonctionnalités de WSUS

La gestion des mises à jour est indispensable en entreprise, que ce soit avec WSUS ou une alternative, car oui il y a des alternatives. Concernant WSUS, voici les fonctionnalités principales :

- **Synchroniser** les mises à jour à partir des serveurs Microsoft
- **Approuver et refuser** les mises à jour pour toutes les machines ou certains groupes
- **Télécharger** une seule fois les mises à jour et les distribuer aux machines, cela évite que chaque machine se connecte sur Internet (auprès des serveurs de Microsoft) pour télécharger les mises à jour
- **Gérer** les mises à jour de l'ensemble des produits Microsoft (Windows 10, Windows 11, les différentes versions de Windows Server, la suite Office, Exchange Server, Microsoft Edge, etc.)
- **Suivre** l'état d'installation des mises à jour sur chaque machine gérée par WSUS
- **Contrôler** le moment où les machines installent les mises à jour

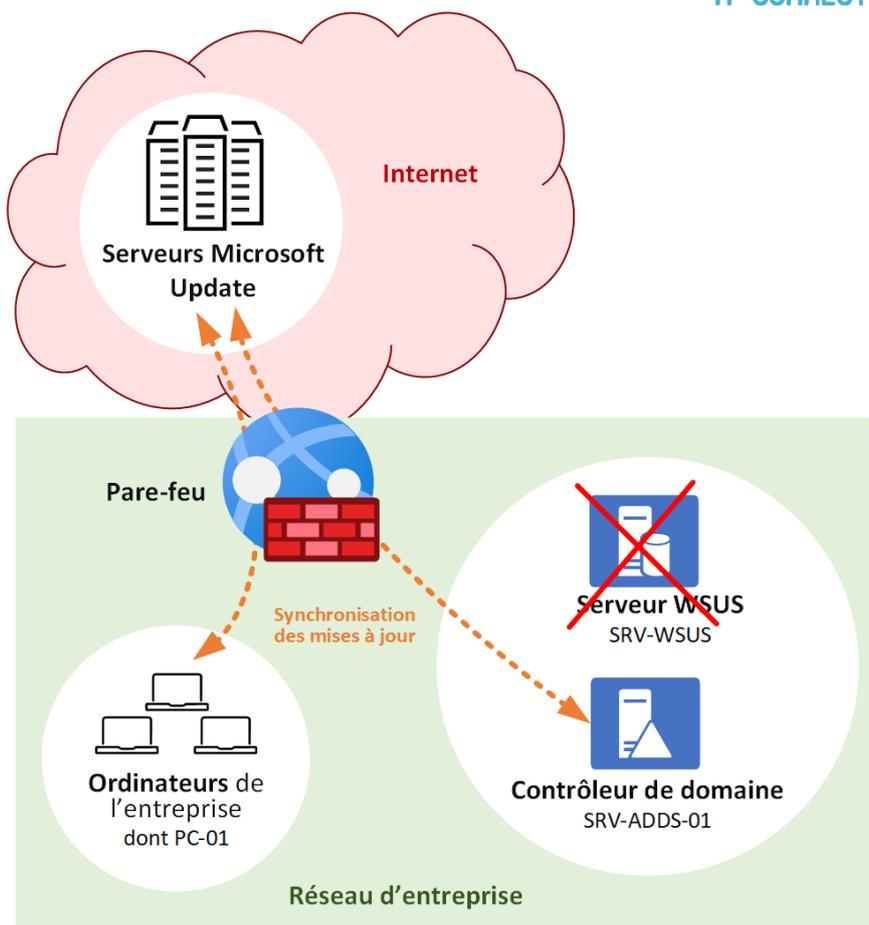
Il faut savoir que WSUS peut distribuer des mises à jour à des machines intégrées au domaine Active Directory, mais également en mode « Groupe de travail » comme nous le verrons.

J'insiste sur l'importance de gérer les mises à jour en entreprise, surtout qu'il y a des vulnérabilités corrigées tous les mois, aussi bien sur Windows que d'autres produits Microsoft. Cela ne veut pas dire qu'il faut installer les mises à jour dès qu'elles sortent, car il peut y avoir des effets de bord : on l'a constaté à plusieurs reprises ces derniers mois. Certains vont attendre quelques jours ou semaines avant d'installer les mises à jour, tandis que d'autres vont réaliser l'installation immédiatement : les avis sont partagés sur la question.

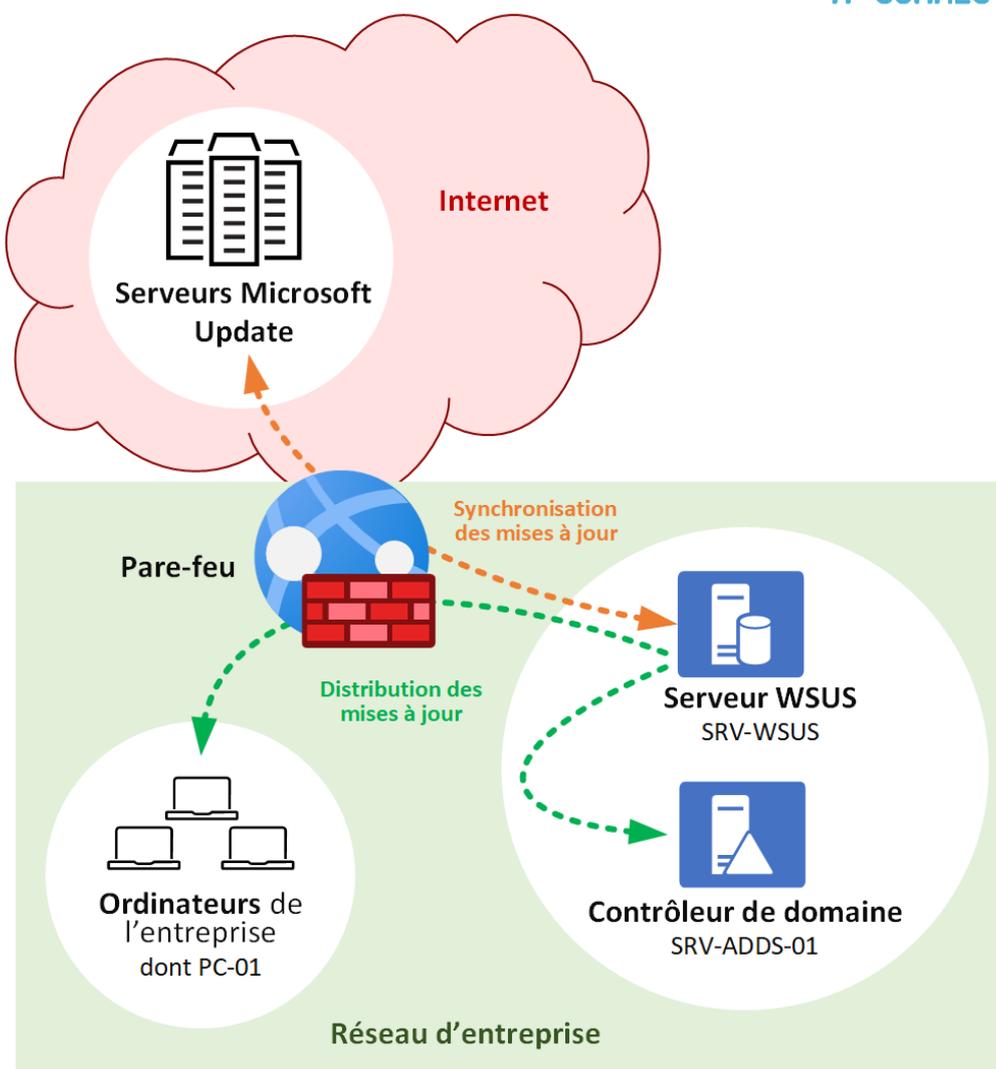
WSUS joue un rôle important dans la gestion de la bande passante Internet : il n'y a que le serveur WSUS qui récupère les mises à jour depuis les serveurs de Microsoft. Sans WSUS (ou solution équivalente), chaque machine se connecte sur Internet afin de télécharger les données. Sans un serveur WSUS, la consommation de bande passante Internet pour les flux liés aux mises à jour est beaucoup plus importante !

Il suffit de schématiser une infrastructure sans serveur WSUS et de la comparer avec une infrastructure où il y a un serveur WSUS.

Sans serveur WSUS (ou système de gestion centralisé des mises à jour équivalent), tous les flux liés aux mises à jour partent vers Internet, à destination des serveurs Microsoft.



À l'inverse, lorsque l'on met en place le serveur WSUS, ces flux sont redirigés vers le serveur WSUS de l'entreprise. Le schéma ci-dessous va vous permettre de bien comprendre la différence. Ainsi, on exploite uniquement le réseau local pour récupérer les données de mises à jour.



Pour vous convaincre définitivement de l'intérêt de WSUS, notamment dans la gestion de la bande passante, prenons cet exemple.

Nous savons que Microsoft publie les mises à jour de tous les systèmes en même temps, à savoir le deuxième mardi de chaque mois, avec le Patch Tuesday.

De ce fait, il y a des chances pour que toutes les machines se connectent sur les serveurs de Microsoft Update à peu près en même temps pour télécharger les mises à jour. D'un point de vue de votre réseau, il y aura **un pic de consommation de la bande passante Internet pendant cette période.**

Généralement, ce n'est pas anodin et selon la bande passante Internet dont vous disposez et le nombre d'ordinateurs qui effectuent le téléchargement, cela peut **perturber l'activité de votre entreprise.** Croyez-moi, j'ai déjà rencontré ce cas de figure. **WSUS répond à cette problématique car il est le seul à se connecter à Internet pour récupérer les packages de mises à jour !**