**Formation WSUS - Serveur de MAJ  
 - sys 27 - TP**

Michel Cabaré / www.cabare.net / michel@cabare.net

WSUS Serveur de Mises à Jours   
- sys 27 – Travaux pratiques V4-02 - Oct 2021

|  |  |  |
| --- | --- | --- |
| Une image contenant objet  Description générée automatiquement  https://WWW.CABARE.NET © |  |  |

|  |  |
| --- | --- |
|  |  |

**table des matiÈres**

TP Désactivation MAJ 3

Objectif – Désactivation MAJ complète: 3

TP UpGrade et Ciblage 5

Objectif – choix d'upgrade Windows 10: 5

Téléchargement Upgrade Windows 10 sur WSUS: 5

Création de groupements d'ordinateurs et approbation manuelle WSUS: 6

Ciblage coté AD avec UO correspondante 7

Machine par défaut = WSUS désactivé 8

Machine sans UO spécifique = WSUS MAJ dans sa branche 9

Machine Dans UO UPGRADE = WSUS MAJ upgrade 11

Lancement de l'Upgrade: 11

Lancement de l'Upgrade: 12

TP MAJ Auto simple 15

Objectif – Maj de sécurité installée automatiquement : 15

1 GPO Configuration du Service Mises à Jour automatiques 15

1 GPo specifier l'emplacement du service intranet 15

1 GPo frequence des MAj 15

1 GPo pas de redémarrage auto avec utilisateur connecté 15

1 GPo pas de redémarrage auto pendant les heures d’activité 15

1 GPo toujours redémarrer à l’heure planifiée 15

TP Optimisation livraison 16

Via interface graphique – Optimisation de la livraison -WUDO 16

Gestion bande passante: 17

Téléchargement à partir d’autres PC Peer to peer : 18

GPO gestion bande passante: 19

En arrière plan 19

En avant plan 20

GPO Groupement Peer to Peer: 21

Génération de GUID 21

Ajout du GUID sur les poste du groupe 21

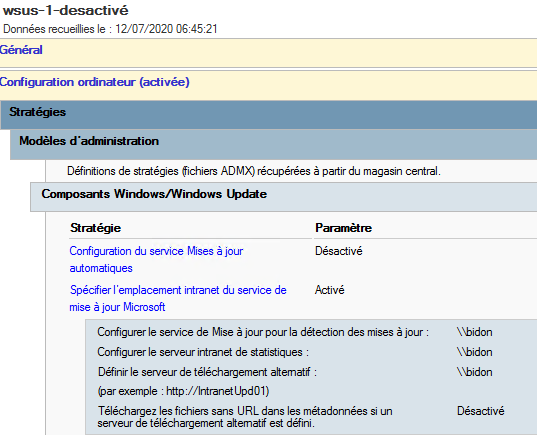
Mode de téléchargement groupe 2(http + peer to peer) 22

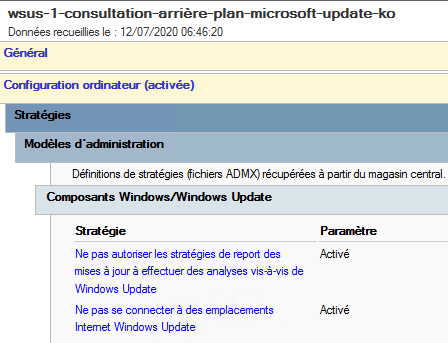
ANNEXE - Récapitulatif réglages GPO Windowsupdate 24

# TP Désactivation MAJ

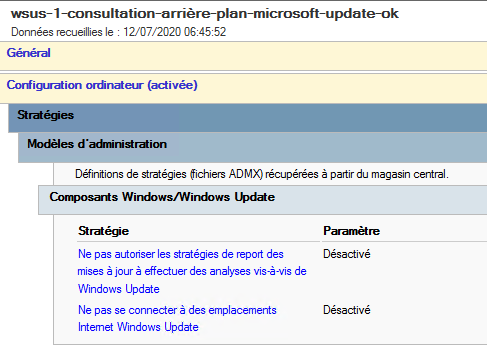
## Objectif – Désactivation MAJ complète:

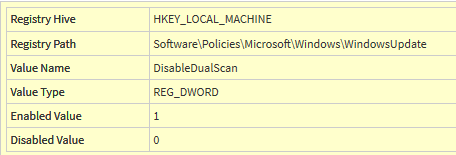
On fait 4 GPO qui donneront de fausses indications :

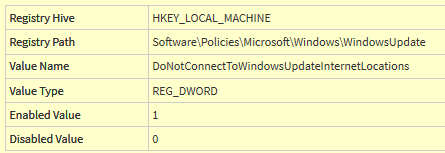




Ce qui fait que pour réautoriser WSUS et les Maj il faudra notamment :







# TP UpGrade et Ciblage

## Objectif – choix d'upgrade Windows 10:

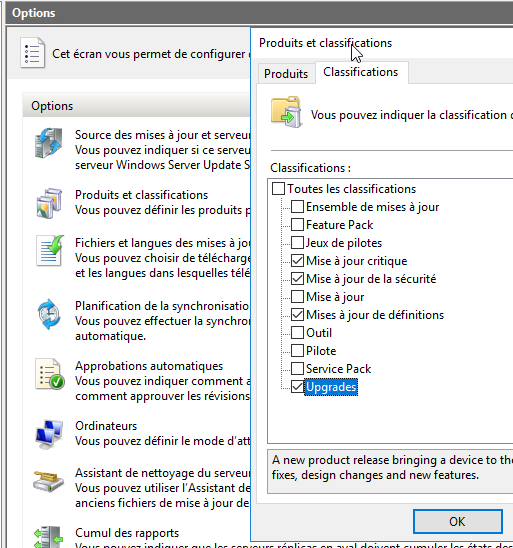
On peut imaginer avoir envie dans une structure de pouvoir gérér une mise à niveau de Windows 10 entres les versions 1511 – 1607 – 1703 …

Pour faire cela il est necessaire d'avoir :

* Installé les **MAJ upgrade** sur **WSUS**
* Créer des dossier **groupement d'ordinateur** specifiques ou chaque **Upgrade** spécifique sera **Approuvée manuellement**
* Effectuer un **ciblage** coté **AD** avec des **UO** correspondantes

## Téléchargement Upgrade Windows 10 sur WSUS:

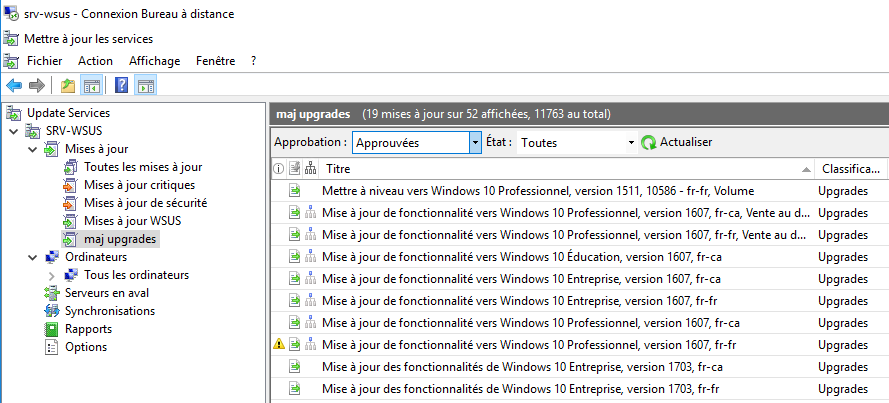
Il faut dans les **Options WSUS**, demander dans les **Produits et classifications** cocher la classification **Upgrade**



Cela devrait après synchronisation et eventuellement "ménage" (pour refuser les MAJ des versions **N** ou **collaboration**, ou les **MAJ Mises à jours**…

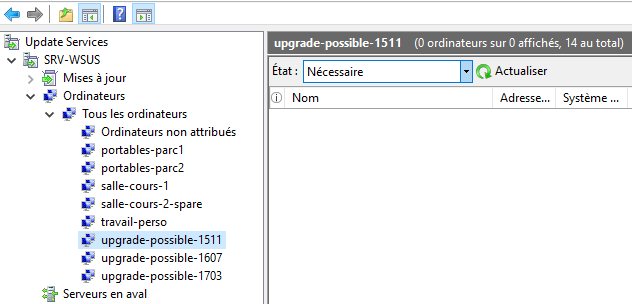
amener les MAJ suivantes :

1511- 1607 – 1703…

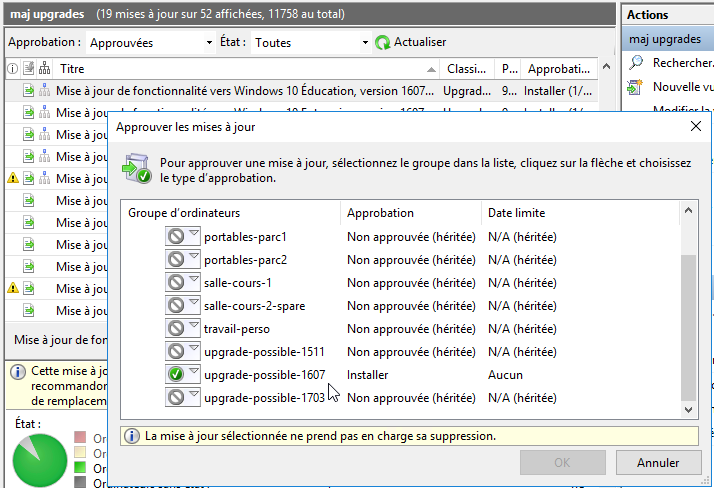


## Création de groupements d'ordinateurs et approbation manuelle WSUS:

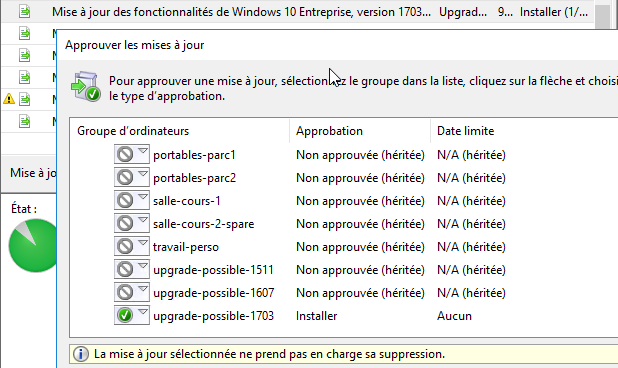
On se crée des groupement d'ordinateur par type d'upgrade souhaité



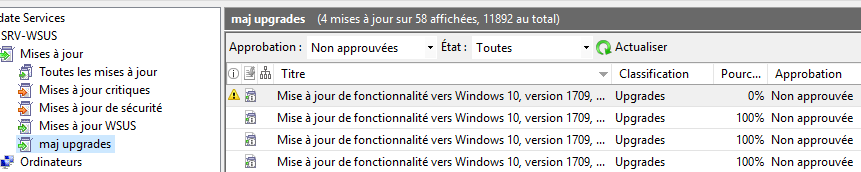
Et chaque MAJ upgrade spécifique est approuvée manuellement sur le groupement d'ordinateur correspondant, ici une **upgrades 1607**…



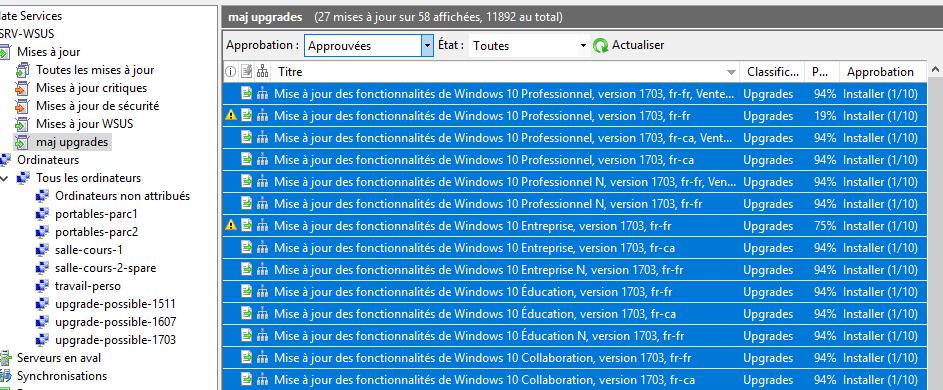
ici une **upgrades 1703**…



On peut très bien décider de ne pas approuver une upgrade particulière, par exemple ici on n’a pas encore approuvé les upgrade vers 1709…

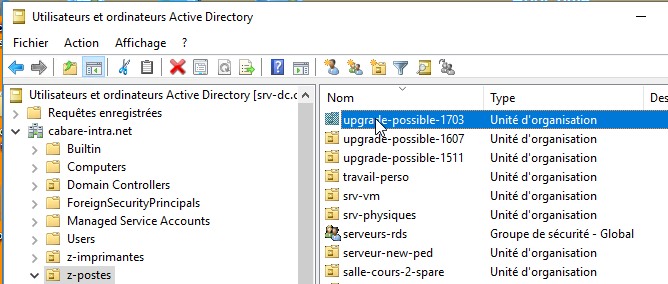


Ici on a approuvé toutes les 1703….

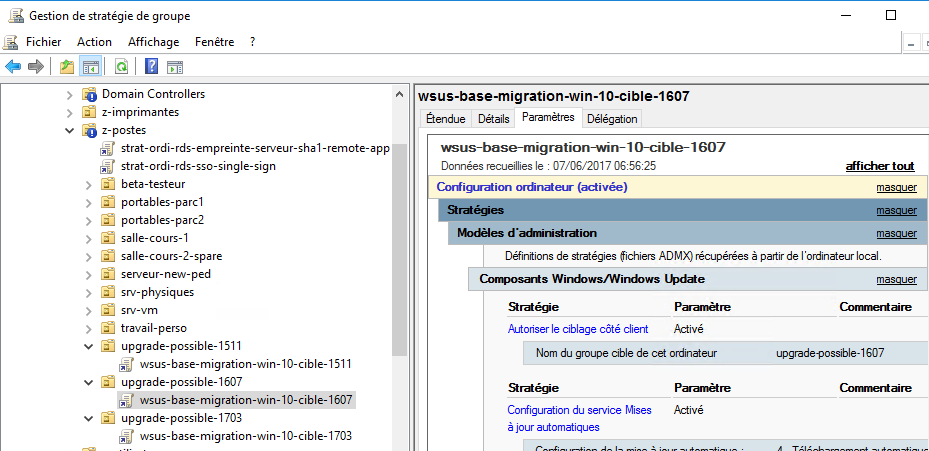


## Ciblage coté AD avec UO correspondante

Il faut bien sur coté **AD** se créer des **UO** correspondantes



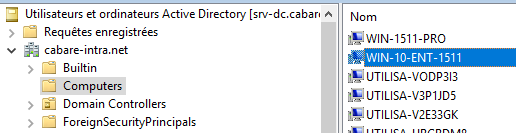
Sur lesquelles on posera des GPO avec "ciblage"



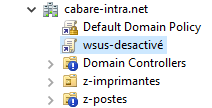
Le principe pourrait être le suivant…

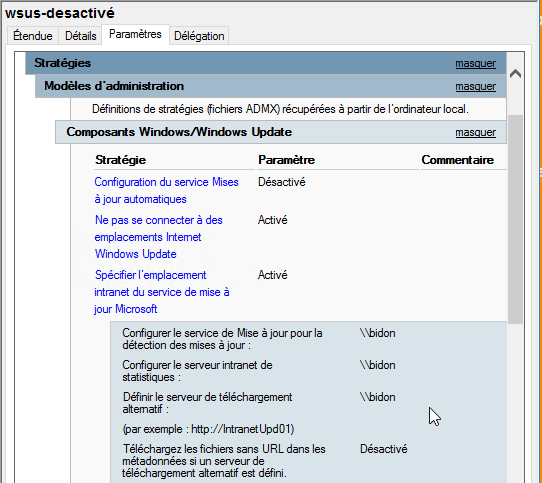
### Machine par défaut = WSUS désactivé

Pour toute machine rejointe au domaine « a la volée » et qui se retrouve dans **l’UO computers** par défaut



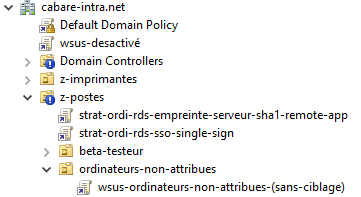
On lui applique une GPO désactivant les Mise a jour WSUS nommée par exemple ***wsus-desactivé***, posée sur tout le domaine

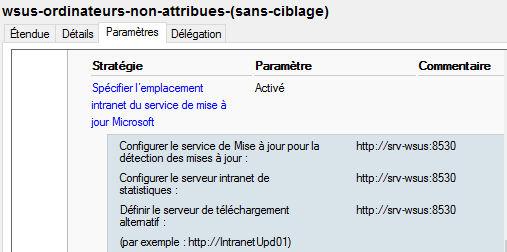




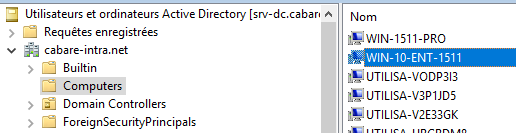
### Machine sans UO spécifique = WSUS MAJ dans sa branche

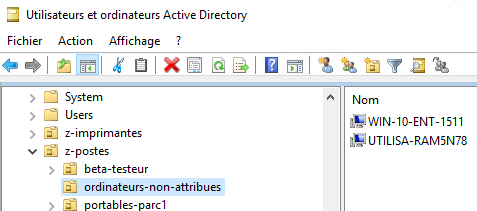
Pour toute machine posée dans une UO non spécifique, par exemple ***ordinateurs-non-attribués***, on appliqueras toutes les MAJ de la branche



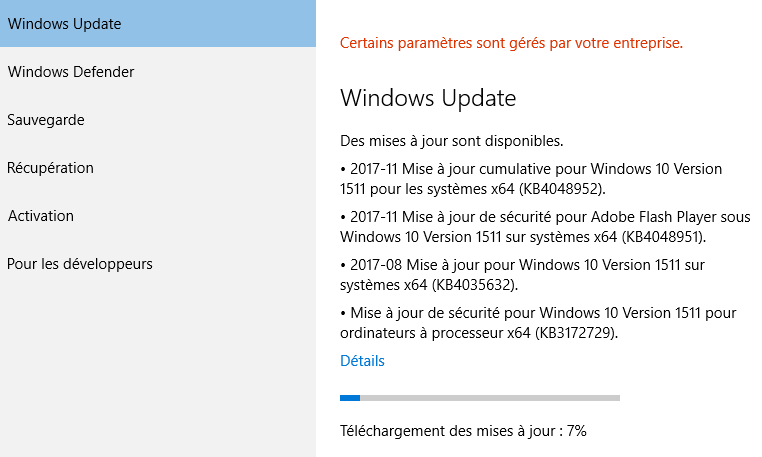


Ainsi si on déplace notre machine par exemple dans l’AD dans l’UO ***ordinateurs-non-attribues***



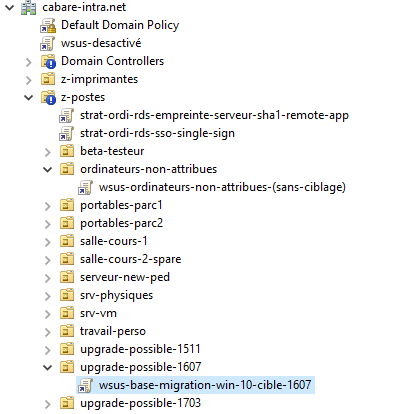


Elle recevra toutes les MAJ de sa branche, mais QUE les maj de sa branche



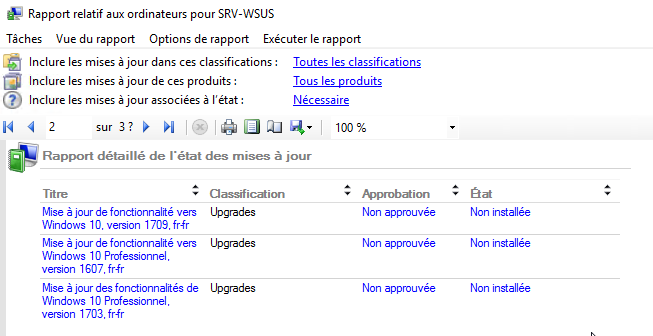
### Machine Dans UO UPGRADE = WSUS MAJ upgrade

Pour toute machine posée dans une UO spécifique d’upgrade, par exemple ***upgrade-possible-1607***, on appliqueras les MAJ de changement de branche



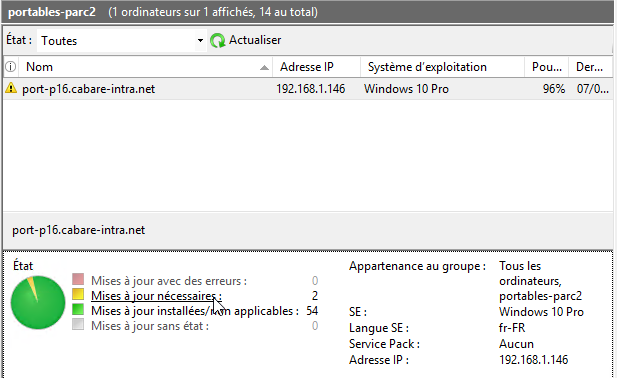
## Lancement de l'Upgrade:

Donc par exemple un ordinateur avec Windows 10 -1511, posé dans l’UO ***ordinateurs-non-attribués*** apparaîtra dans WSUS avec les MAJ upgrades nécessaires, et se mettra à jour régulièrement dans sa branche

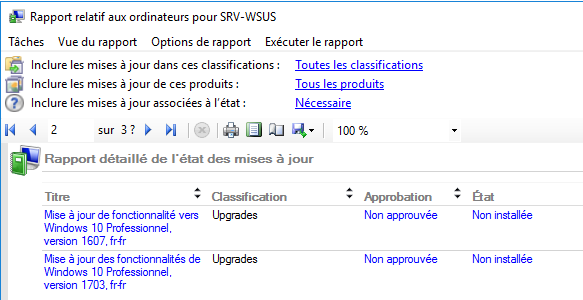


## Lancement de l'Upgrade:

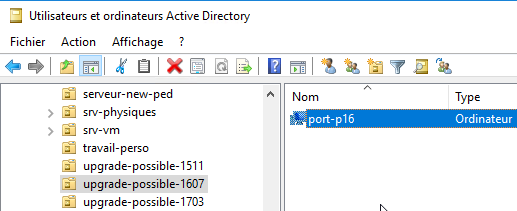
Ainsi par exemple un ordinateur avec Windows 10 -1511 apparaîtra dans WSUS avec 2 ou 3 MAJ nécessaires



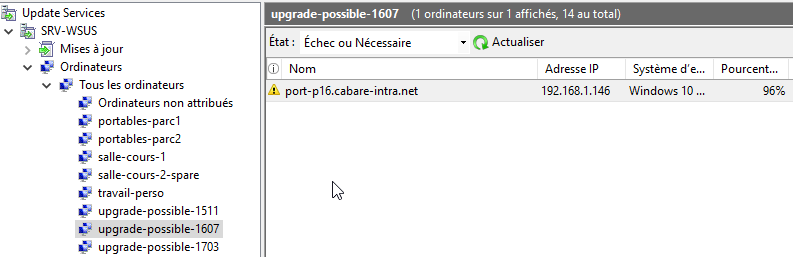
Qui ne sont pas approuvées car l'ordinateur n'est pas dans la bonne UO



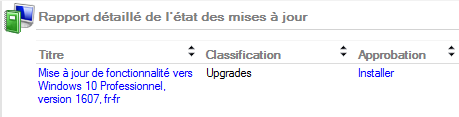
Il suffira par exemple de poser l'ordinateur dans l'UO 1607 de l'**AD**…



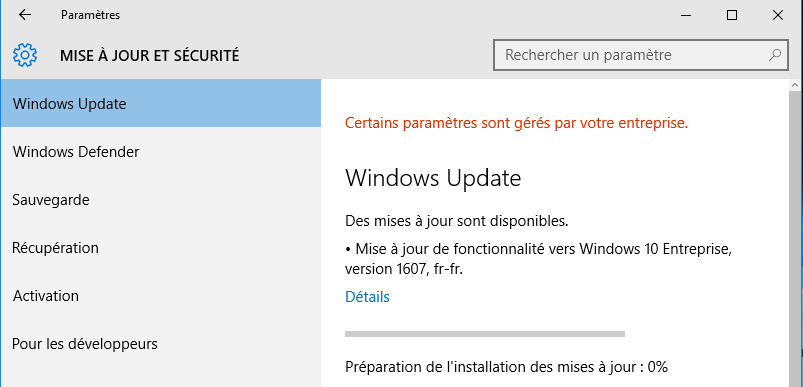
Pour que après propagation l'on obtienne un deplacement de la machine dans le groupement d'ordinateur prévu aussi dans WSUS



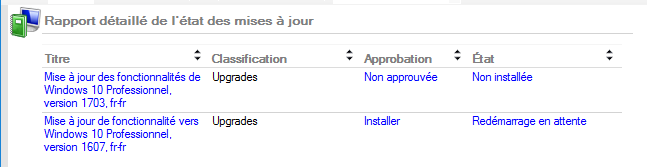
Avec maintenant une **Approbation** detype **Installer**



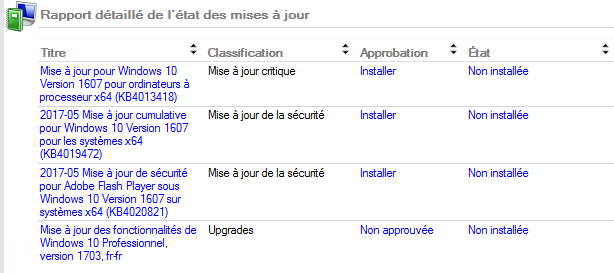
Et notre machine va récupérer sa Mise a jour / Migration de branche



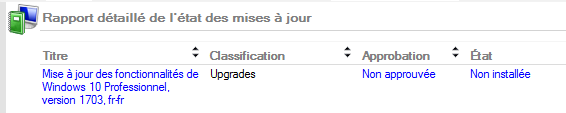
Il suffira d'attendre un redémarrage, pour que désormais on ait une seule **MAJ Upgrade** applicable, celle correspondant à la version upgrade 1703…



Bien sur récupèrera ensuite les **Maj de Sécurité** dédiées à la version 1607



Et au final il ne restera que la **MAJ Upgrade 1703**



# TP MAJ Auto simple

## Objectif – Maj de sécurité installée automatiquement :

On souhaite installer les MAJ de sécurité critiques des que possible, sans intervention de la part de l’utilisateur, ce qui pourrait demander 5 GPO

### 1 GPO Configuration du Service Mises à Jour automatiques

* configuration du service mes mises a jour automatique 4 - planif et installation
* installer durant les heures de maitenance desactiver
* jour de l'installation planifiée tous les jours 5h
* Chaque semaine

### 1 GPo specifier l'emplacement du service intranet

* Activation avec les paramètres WSUS de renseigné

### 1 GPo frequence des MAj

* verifier la présence des mises a jours 1 h

associées à

### 1 GPo pas de redémarrage auto avec utilisateur connecté

* À désactiver

### 1 GPo pas de redémarrage auto pendant les heures d’activité

* À désactiver

### 1 GPo toujours redémarrer à l’heure planifiée

* À paramétrer avec un intervalle detemps (20 mn?)

# TP Optimisation livraison

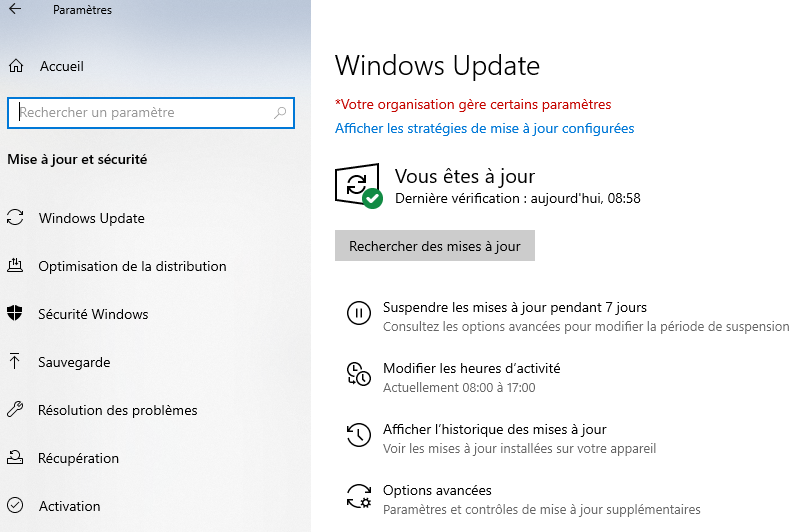
## Via interface graphique – Optimisation de la livraison -WUDO

On parle de **Windows Update Delivery Optimization**

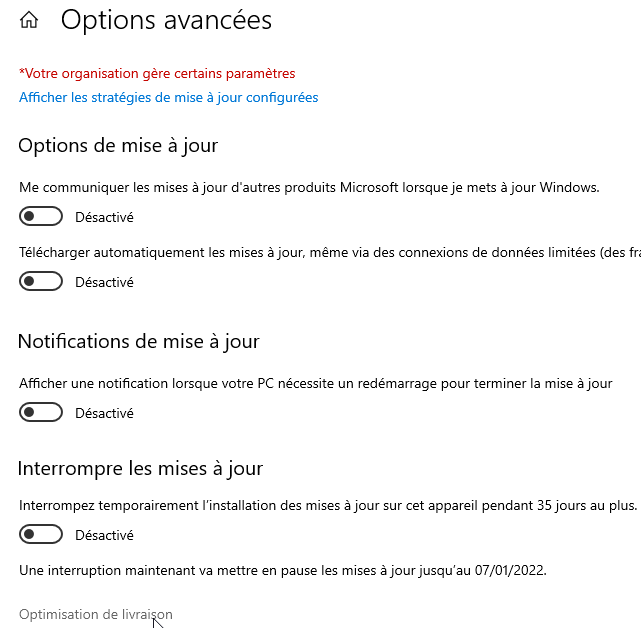
Les réglages se trouvent regroupées dans

**Windows update / Options avancées / Optimisation de la distribution (Livraison)/**

**Windows update / Options avancées**



**Optimisation de la distribution (Livraison)**



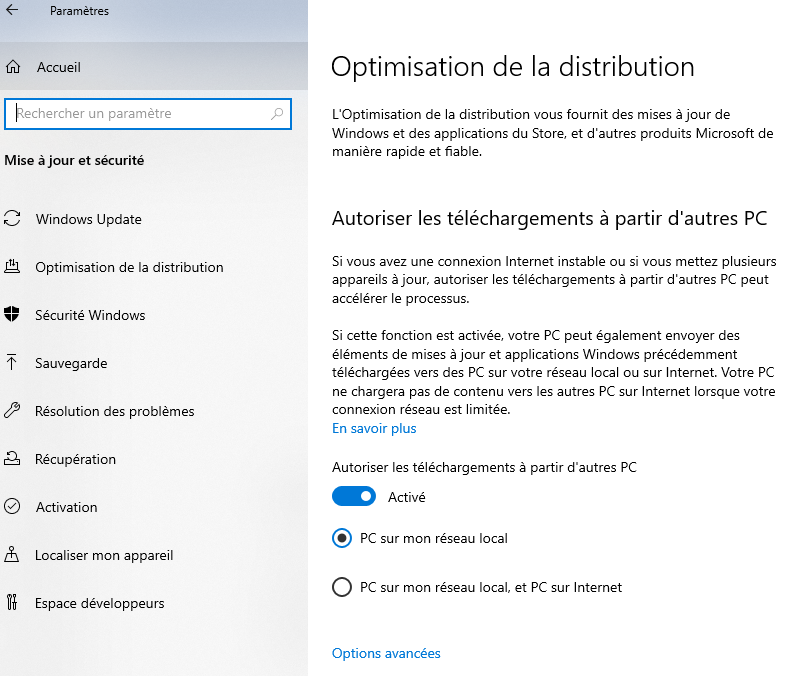
## Gestion bande passante:

Les limites de bande passante peuvent s'appliquer différemment selon que les téléchargements se fassent en arrière-plan, ou en premier plan

Si on limite uniquement aux mises à jour automatiques gérées par l'optimisation de la distribution, qui sont des téléchargements en arrière-plan.

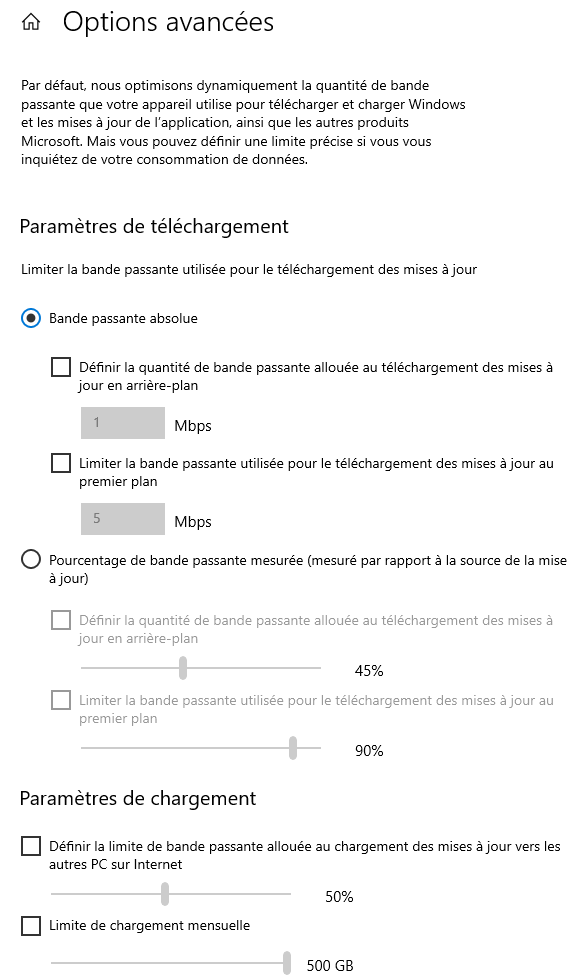
**Alors si on initie manuellement** un téléchargement (en mettant à jour Windows ou en téléchargeant une application du Store, **les limites de bande passante ne sont pas appliquées**.

**Windows update / Options avancées**

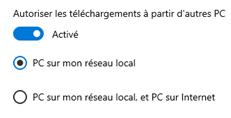


Il est possible de limiter (en Mbps) la bande passante utilisée pour télécharger les mises à jour en arrière-plan et au premier plan.

En parallèle celle utilisée pour télécharger des mises à jour vers d’autres PC sur Internet peut aussi être limitée.



## Téléchargement à partir d’autres PC Peer to peer :

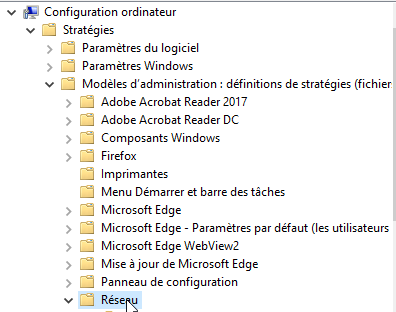
L’optimisation de la distribution envoie également des mises à jour et applications de votre PC à d’autres PC sur votre réseau local ou sur des PC sur Internet, sur la base de vos paramètres. Le partage de ces données entre des PC permet de réduire la bande passante Internet nécessaire pour maintenir plusieurs appareils à jour ou peut faciliter le téléchargement si votre connexion Internet est limitée ou non fiable

L’optimisation de la livraison crée un cache local et y stocke brièvement les fichiers qu’elle a téléchargés.

[Delivery Optimization for Windows client updates - Windows Deployment | Microsoft Docs](https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization)

## GPO gestion bande passante:

### En arrière plan

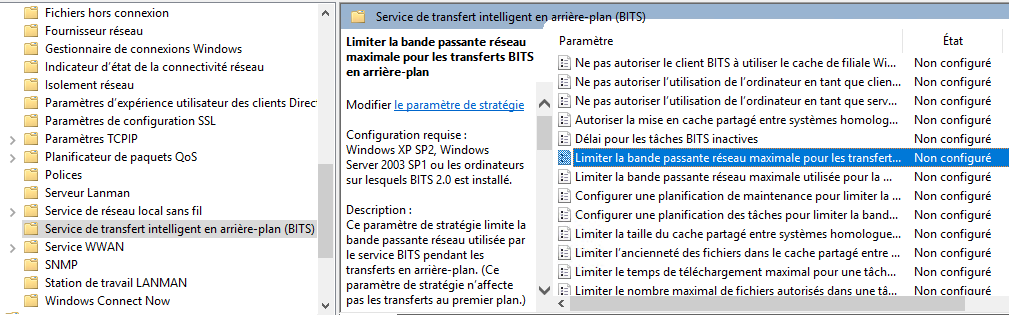
Pour la gestion de la bande passante en arrière plan, c’est une **GPO ordinateur**, dans les **modèles d’administration**, …

…

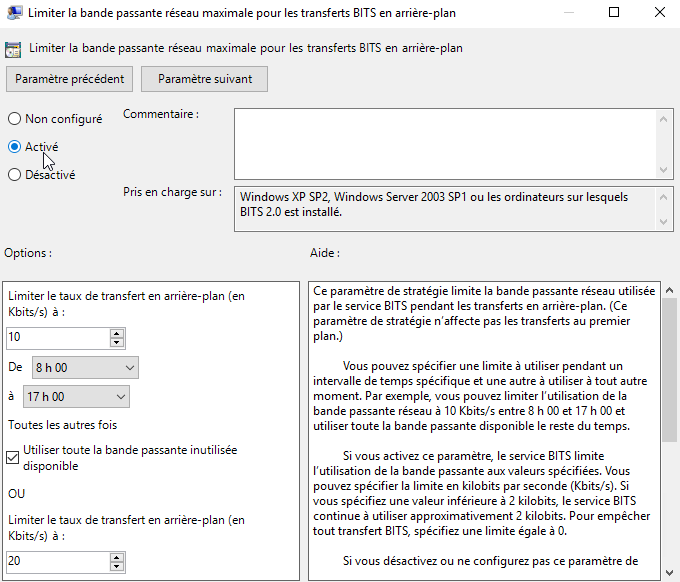
**Réseau**



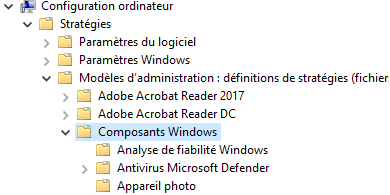
**Service de transfert intelligent en arrière pan (BITS)**



Que l’on active et paramètre



### En avant plan

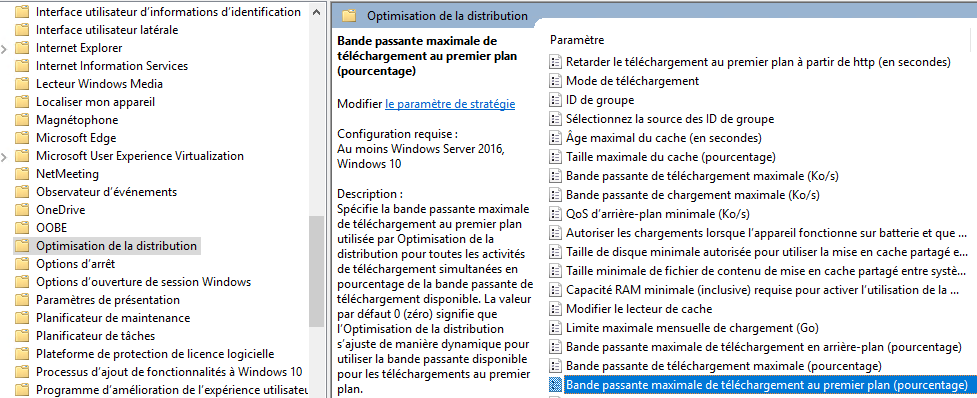
Pour la gestion de la bande passante en avant plan, c’est une **GPO ordinateur**, dans les **modèles d’administration**, **Composants Windows**

**…**

**/ Optimisation de la distribution**

…

On retrouve l’équivalent (et bien plus) du réglage que l’on avait en arrière-plan



|  |  |
| --- | --- |
|  |  |
|  |
|  |
|  |
|  |
| Peer to peer |
| Peer to peer |
|  |
|  |
|  |
| Bande passante en Ko/S |
| Bande passante en Ko/S |
|  |
|  |
|  |
|  |
|  |
|  |
| Existe déjà dans réseau |
|  |
| Bande passante en % |
|  |
| Equivalent horodatage |
| Equivalent horodatage |

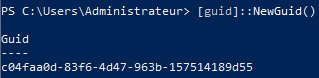
## GPO Groupement Peer to Peer:

Par défaut, tous les ordinateurs d’un domaine vont être habilités à faire du **Peer to peer** pour peu que la fonctionnalité soit activée. On peut restreindre ce mode de fonctionnement à un groupe (ou à des groupes) de machines

* On va générer un GUID pour un groupe de machine,
* GUID que l’on paramétrera sur chaque poste du groupe
* Et on va indiquer un mode de transmission mixte **http/peer to peer**

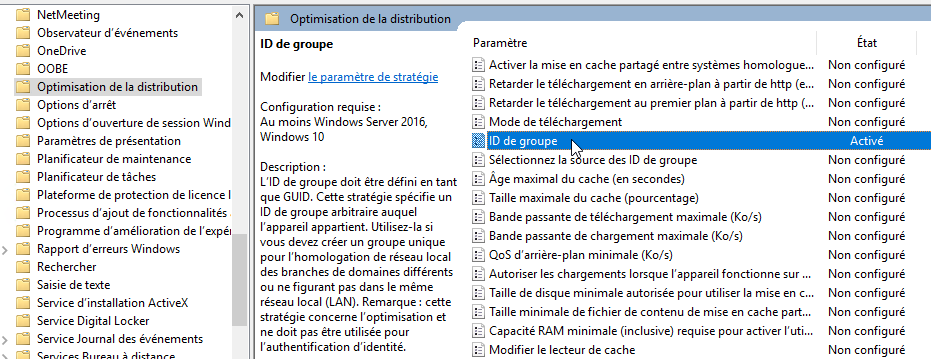
### Génération de GUID

On génère un **GUID** avec la commande **powershell** **[guid]::NewGuid()**

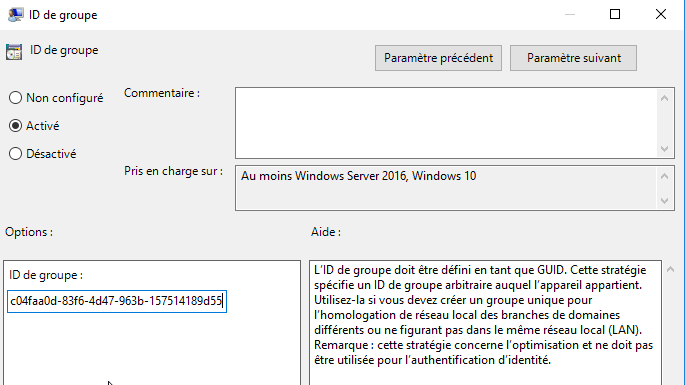


### Ajout du GUID sur les poste du groupe

Il s’agit de la **GPO** **ID de groupe** dans **Optimisation de la distribution**



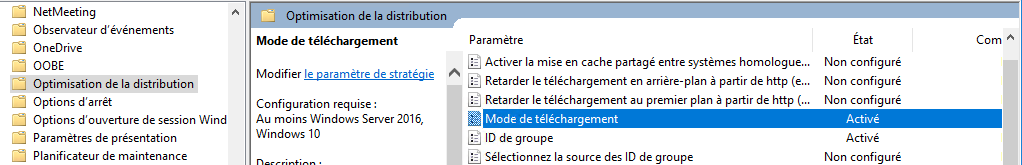
Dans laquelle on saisit notre **GUID**



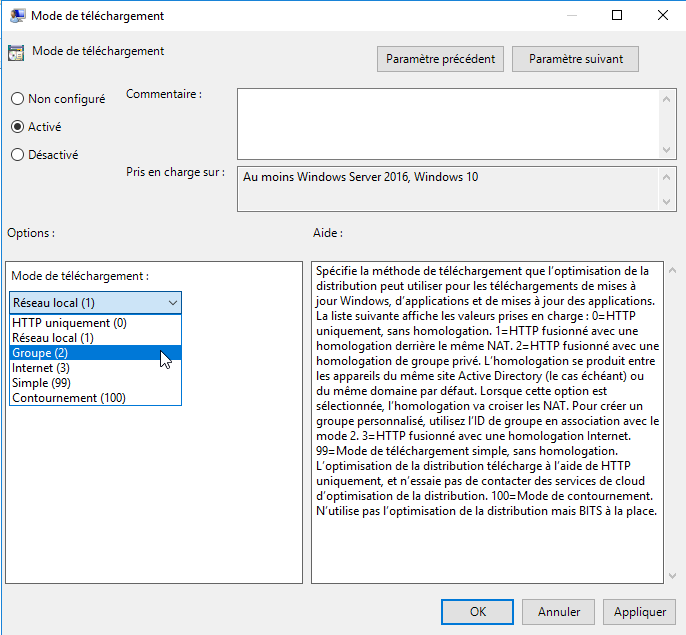
Et que l’on appliquera a toutes les machines de notre groupe **peer to Peer**

### Mode de téléchargement groupe 2(http + peer to peer)

Il s’agit de la **GPO** **Mode de téléchargement** dans **Optimisation de la distribution**



Dans laquelle on précise le mode **Groupe (2)**

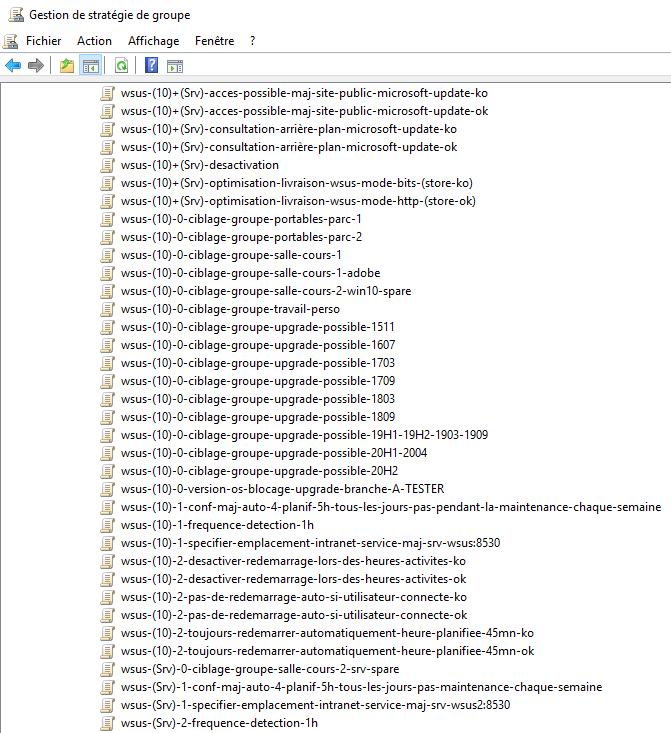


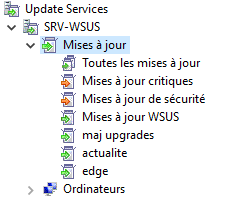
# ANNEXE - Récapitulatif réglages GPO Windowsupdate

|  |  |  |
| --- | --- | --- |
|  |  | Maj critiques (+35j) |
| Cb ou CBB (+365j) |
| depuis win 10 v1709 |

Réglages de GPO Hors Windows Update pour entreprise

|  |  |  |
| --- | --- | --- |
| depuis win 10 |  |  |
| **Obsolète** | **Obsolète après 8/2008r2** |
|  |  |
|  |  |
| OK depuis XP |  |
| depuis win 10 - v1803 |  |
|  |  |
|  |  |
| OK depuis XP |  |
| depuis win 10 - v1803 |  |
| depuis win 10 - v1803 |  |
| depuis win 10 - v1803 |  |
| **Obsolète** | **Obsolète après 7/2008r2** |
| depuis win 10 |  |
|  |  |
| OK depuis XP |  |
|  |  |
|  |  |
| depuis win 10 - v1709 |  |
| depuis win 10 |  |
|  |  |
| depuis win 10 |  |
| OK depuis XP |  |
| **Obsolète** | **Obsolète après 7/2008r2** |
| **Obsolète** | **Obsolète après 7/2008r2** |
| OK depuis XP |  |
| depuis win 10 |  |
| depuis win 10 |  |
| depuis win 10 - v1803 |  |
| depuis win 10 |  |
| depuis win 10 |  |

**Vues en place GPO**



**Ciblages groupes ordinateurs**

