Mise à jour de systêmes et logiciels

Mise à jour de SE

Le système d'exploitation Windows vous permet de choisir quand et comment obtenir les dernières mises à jour, pour assurer la sécurité et le bon fonctionnement de votre appareil.

Pour *Windows 10* :
Sélectionnez : **[Rechercher les mises à jour Windows]**. Vous pouvez également sélectionner le bouton **Démarrer**, puis **Paramètres** > **mise à jour** > **Windows Mise à jour**.

Pour être prévenu de la disponibilité d'une nouvelle MAJ : dans "**Windows Update**", cliquez sur "**options avancées**" et vérifiez que les notifications de mise à jour sont activées, sinon activez-les.

Pour *Windows 11* :
Sélectionnez **[Rechercher les mises à jour Windows]**. Vous pouvez également sélectionner **Démarrer** > **Paramètres** > **Windows jour**.

Pour *Mac* :
Dans le menu Pomme situé dans l'angle de l'écran, choisissez **Préférences Système**.

Dans la fenêtre Préférences Système, cliquez sur **Mise à jour de logiciels**.

2. Cliquez sur **Mettre à jour** ou **mettre à niveau maintenant**:

- L'option **Mettre à jour** installe les dernières mises à jour pour la version actuelle, par exemple une mise à jour de macOS Big Sur 11.5 à macOS Big Sur 11.6.

- L'option **Mettre à niveau maintenant** installe une nouvelle version majeure portant un nouveau nom, telle que macOS Monterey. La fonctionnalité Mise à jour de logiciels ne montre que les mises à niveau compatibles avec votre Mac.

Pour linux :

En ligne de commande :

* sudo apt update
* sudo apt upgrade
* sudo apt autoremove (pour éliminer les données obsolètes)

Linux utilise des ***référentiels*** pour proposer à ses utilisateurs de récupérer des applications de manière sécurisée.

Les quatres référentiels principaux sont :

1. **Principal** : Logiciel libre et OS pris en charge par Canonical (Société pour promotion de l'OS)
2. **Universe** : Logiciel libre et OS géré par la communauté
3. **Restreint** : Pilotes propriétaire pour les périphériques
4. **Multivers** : Logiciel limité par des droits d'auteurs ou des problèmes juridiques

Les référentiels (ou chaines) peuvent être désactivés selon nos choix dans l'ubuntu software center.

Ajout d'archives de paquets personnels (PPA) :
Les PPA sont des référentiels créés par les développeurs pour partager leurs logiciels.
Pour ajouter un PPA, vous aurez besoin de son "emplacement" au format :
ppa:[username]/[ppaname]

ATTENTION : Les PPA personnels ne subissent pas les mêmes validations de sécurité et représentent donc un risque.
ajouter un PPA en ligne de commande (a titre informatif) :
sudo add-apt-repository ppa:user/ppa-name

(https://doc.ubuntu-fr.org/gestionnaire_de_mises_a_jour)

Les logiciels :

1) sources fiables :

Comme le système d'exploitation, les logiciels que vous utilisez doivent être à jour mais doivent être téléchargés au bon endroit pour éviter des versions frauduleuses ou non fonctionnelles.

Seuls *deux options* nous permettent de nous assurer une sécurité optimale :

Obtenir le logiciel directement sur le site internet de l'éditeur.

Utiliser les magasins d'applications mis en place par les géants du numérique :

1) Microsoft store pour Windows
2) App Store pour Mac
3) Play Store sur Android
4) Ubuntu Software Center pour Ubuntu

Ubuntu Software Center pour Ubuntu, en interface graphique.

2) Types de mises à jours :

Les mises à jour ***critiques*** :

Les mises a jour critiques apportent des solutions à des vulnérabilités existantes. S'il existe une telle mise a jour, les postes ne

l'ayant pas effectuée sont vulnérables. Les pirates n'ont qu'à accéder aux notes de version pour connaître les failles et ensuite les exploiter.

Les mises à jour de ***version*** :

Mise à jour d'ordre pratique, améliorations et nouvelles fonctionnalités.

3) Bonnes pratiques :

1) Les faire **régulièrement**

2) Le faire depuis une **source officielle**

3) **Lister** l'ensemble des machines et des logiciels

4) Mettre à jour **automatiquement**? (Selon le contexte)

5) **Définir des règles** de réalisation de mise a jour

incluant la source, la plage horaire, les machines et logiciel concernés

6) **Sauvegarder les configurations** avant d'installer la nouvelle mise à jour

4) Mise à jour automatique

Pour windows :

Pour que les mises à jour de l'application sélectionnée se diffusent automatiquement sur les appareils clients tout de suite après le téléchargement des mises à jour sur les référentiels du Serveur d'administration, procédez comme suit :

1. Connectez-vous au Serveur d'administration qui administre les appareils clients.
2. Créez une tâche de diffusion des mises à jour de cette application pour les appareils clients sélectionnées par un des moyens suivants :

- S'il faut diffuser les mises à jour sur les appareils clients qui font partie du groupe d'administration sélectionné, créer une tâche pour le groupe sélectionné
(https://support.kaspersky.com/KSC/11/fr-FR/3773.htm).
- S'il faut diffuser les mises à jour sur les appareils clients qui font partie ou non des différents groupes d'administration, créez une [tâche pour un ensemble d'appareils]
(https://support.kaspersky.com/KSC/11/fr-FR/3779.htm).

Ceci permet de lancer l'Assistant de création de tâche. Suivez ses instructions, exécutant les conditions suivantes :

1. Dans la fenêtre de l'Assistant > Type de tâche dans l'entrée de l'application nécessaire, sélectionnez la tâche de diffusion des mises à jour.

Le nom de la tâche de diffusion des mises à jour, qui s'affiche dans la fenêtre Type de tâche, dépend de l'application pour laquelle la tâche a été créée. Pour plus d'informations sur les noms des tâches de mise à jour pour les applications sélectionnées de Kaspersky Lab, cf. Manuels pour ces applications.

2. Dans la fenêtre de l'Assistant Programmation dans le champ Programmation, sélectionnez l'option de *lancement Lors du téléchargement des mises à jour dans le stockage*.

Ainsi, la tâche de diffusion des mises à jour créée sera lancée pour les appareils sélectionnés chaque fois lors du téléchargement des mises à jour sur les référentiels du Serveur d'administration.

Si la tâche de diffusion des mises à jour de l'application nécessaire a déjà été créée pour les appareils sélectionnés et que vous souhaitez une diffusion automatique des mises à jour sur les appareils clients, ouvrez la fenêtre des propriétés de la tâche et, dans la section Programmation, sélectionnez l'option de lancement Lors du téléchargement des mises à jour sur les référentiels dans le champ Programmation.

Pour Linux :

Le paquet unattended-upgrades peut être utilisé pour installer automatiquement les mises à jour de paquets. Il peut être configuré pour mettre à jour tous les paquets ou uniquement les mises à jour de sécurité. Installez d'abord le paquet en saisissant dans un terminal.

https://docs.microsoft.com/fr-fr/dynamics365/customer-service/set-up-rules-to-automatically-create-or-update-records

Regles de mise à jours :

Pour windows :

Pour créer une nouvelle règle pour les mises à jour de toutes les applications :

1. Sur la page Paramètres de l'Assistant de création d'une tâche, cliquez sur le bouton **Ajouter** .

L'Assistant se lance. Parcourez les étapes de l'Assistant à l'aide du bouton Suivant.

2. Sur la page **Type de règle**, sélectionnez **Règle pour toutes les mises à jour**.
3. Sur la page **Critères généraux**, utilisez les listes déroulantes pour définir les paramètres suivants :
   - Définir les mises à jour à installer
   - Corriger les vulnérabilités de niveau de gravité égal ou supérieur à
   - ....

suite sur :
https://support.kaspersky.com/KSC/11/fr-FR/172909.htm

Pour linux :

Les distributions linux demandent systématiquement que l'on approuve les mises a jour proposées et il est possible de déselectionner celle dont on ne veut pas.

Apt-get update permet de télécharger les paquets et de les visualiser. On peut ensuite utiliser les options fournies avec apt-upgrade pour en désélectionner.

https://doc.ubuntu-fr.org/gestionnaire_de_mises_a_jour

Difference-apt-update-upgrade-full-upgrade

https://www.lecoindunet.com/difference-apt-update-upgrade-full-upgrade

Problématique autour des mises à jour :
Automatique ou pas ? - Manuelle ou pas ? - Fin de support .

Doivent elles être systématiques ? NON

En effet, certaines mises a jour ==de version== peuvent comporter des risques de failles car les nouvelles fonctionalités n'ont pas encore été éprouvées.

Par contre, les mises à jour critiques sont indispensables à la sécurité du système.

Doit-on le faire dès qu'elles sont disponibles ? OUI/NON
Pour les mises à jour critiques OUI

Pour les mises à jour de version pour lesquelles les nouvelles fonctionnalités ne sont pas indispensables, il est mieux d'attendre qu'elles aient été éprouvées. Lire les notes de version pour y déceler d'éventuelles améliorations de bug ou de faille mineur par rapport à la version actuellement utilisée.

Lire le rapport de mise à jour est t'il indispensable ? OUI
SURTOUT SI ON NE METS PAS A JOUR
S'il n'est pas possible de mettre à jour immédiatement tout le réseau de l'entreprise pour des raisons pratiques, cela permet de connaître les failles et de les contourner par des méthodes alternatives.

Des règles peuvent être créées pour cibler le type de mises à jour et les logiciels et appareils qui seront concernés.

Manuelle ? OUI

Cela permet de cibler les éléments vus plus hauts.

Fin de support !

Les appareils et logiciels ont une durée de vie après laquelle la maintenance ne sera plus assurée. Il est donc indispensable d'anticiper la fin de la mise à disposition de mise à jour.

https://www.axis-solutions.fr/produits-microsoft-fin-de-support-2021/
https://www.axis-solutions.fr/comprendre-le-cycle-de-vie-de-votre-parc-informatique/