



**CloudReady.ch**  
Observatoire  
Suisse Romand  
du Cloud Computing



update back to:  
[Info@CloudReady.ch](mailto:Info@CloudReady.ch)



**ISEIG**  
Institut Suisse d'Enseignement  
de l'Informatique  
de Gestion

# Exploiter, surveiller et assurer la maintenance des services

Module 188 (Swiss ICT, CFC informaticien: exploitation et infrastructure, 2021)

[PK@ISEIG.ch](mailto:PK@ISEIG.ch) CC-BY-NC-SA

2022-10 > ... > v2024-11

<http://pascal.kotte.net> «Coach en apprentissages numériques»

<http://ict-m188.QuickLearn.ch>

<https://github.com/CloudReady-ch/ISEIG-LAB/blob/master/ICT-188/0.intro.md>

Pour une informatique suisse éthique et durable

<http://join.cloudready.ch> (cofondateur de <http://MyDataVaud.ch>,  
<http://OpenRomandie.ch> et <http://FSnet.ch>, entre autre...)

Pour un réseau d'informaticiens professionnels, rejoindre <http://adiseig.ch>

Licence.

[Creative Commons — Attribution - Pas d'Utilisation Commerciale - Partage dans les  
Mêmes Conditions 4.0 International — CC BY-NC-SA 4.0](#)  
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.fr>

Le contenu est essentiellement en Français, mais comprendra des termes usuels en anglais, ce que j'appelle du Frenglish, et je mets entre «» les termes anglophones.

Des parties du support de formation sont associées avec des contenus externes (liens), dont une partie sera sur Wikipedia, parfois la version anglaise car la version française inexistante ou insuffisante. Mais la plupart iront sur les supports de l'auteur principal de cette formation: <http://Blog.kotte.net> Soit sur CloudReady.ch ou Quicklearn, parfois <http://blog.ict-a.ch> – Commentaires, avis et contributions welcome.

## Salut et bienvenue à l'[ISEIG](#)

### **Cadre de bienveillance**

- JE pas TU (pas de jugement, nous sommes tous des croyants détenir le savoir), par contre «Tu» est OK.
- [Kotté toltèque](#)
- Ce qui s'échange ici, ne sort pas d'ici... (confidentialité et anonymisation des histoires vécues)
- Pas d'insultes... (et le moins de gros mots possibles)
- Respect, de soi, des autres et sans oublier le prof. (cela veut dire ne pas perturber la classe)

**Horaires:** 8h30 – 11h40 / 12h40 – 16h, 2 pauses autour de 10h, 14h45: Pas de sorties libres durant le cours (≠ EPSIC?)

#### Tour classe

- ? nom, prénom, surnom, pseudo de guerre, jeux vidéo, Discord, Github, passions, horreurs/peurs, rêves employeur, nb personnes dans team, utilisateurs/postes, sites/datacentres, nb applications/catalogue de services

**Warning:** Il est supposé que lorsque vous tapotez vos claviers en cours de formation, c'est pour :

- Prendre des notes sur les points importants du cours, questions à poser ou valider.
- aller voir et compléter les infos présentées, essayer l'application exposée, et vérifier si on connaît effectivement le sujet...

**Si on ne pose pas de question, c'est que c'est OK...**

Or si l'attention en cours est réduite, et la moitié du temps utilisé à autres choses, et que du coup, les questions de compréhension ne sont pas posées à l'enseignant. Alors, bien que cette formation ne nécessite aucun travail «hors de la classe» si attentif, il risque d'être difficile et il sera tardif, au moment du test, de se dire «j'aurai peut-être dû faire plus attention». Test avec support et internet, mais plus «dur»...

### Les accords toltèques

<https://medium.com/lean-design/le-5-%C3%A8me-accord-tolt%C3%A8que-a8fd2838f322>

Et Blackcoach

[https://youtu.be/saPZsc\\_ECoM](https://youtu.be/saPZsc_ECoM) – 11mn

## Exploiter, surveiller et assurer la maintenance des services

### Objectifs opérationnels

#### Sommaire (plan)

- A: 0+6 = intro + services périph.
- B: 1+5 = Doc + gestion des droits
- C: 2+4 = logs et monitoring
- D: 3 = updating

- 1 Analyser à l'aide de la documentation d'exploitation les systèmes en place et leur environnement.
- 2 Surveiller et exploiter les services en utilisant les outils à disposition.
- 3 Installer et tester les mises à jour ainsi que les correctifs (patches) des services concernés manuellement et à l'aide de systèmes de déploiement de logiciels et mettre à jour la documentation d'exploitation.
- 4 Intégrer les systèmes dans les outils de monitoring existants et vérifier les valeurs mesurées.
- 5 Administrer et documenter les autorisations selon le concept d'autorisations en vigueur.
- 6 Définir les adaptations requises par les systèmes périphériques nécessaires à l'exploitation des services.

### Domaine de compétence

#### Objet

### System Management

Serveur avec des services de fichiers, d'impression et de répertoire, DHCP, DNS, LAN avec stations de travail (Clients) prêt à fonctionner.

Les modules ont été regroupés et réorganisés dans un enchaînement différent afin de faciliter un fil rouge d'apprentissage.

Voici le lien vers le site officiel:

<https://www.modulbaukasten.ch/module/188/1/fr-FR?title=Exploiter,-surveiller-et-assurer-la-maintenance-des-services>

Et voici les sujets abordés:

1.1 Connaître le contenu, la structure et l'application d'une documentation d'exploitation. 1.2 Connaître l'importance d'une documentation d'exploitation exhaustive et mise à jour afin d'assurer la maintenance. 1.3 Connaître les caractéristiques des services les plus répandus (p. ex. services de fichiers, d'impression et de répertoire, DHCP, DNS) et leur contribution à la fonctionnalité d'un réseau.

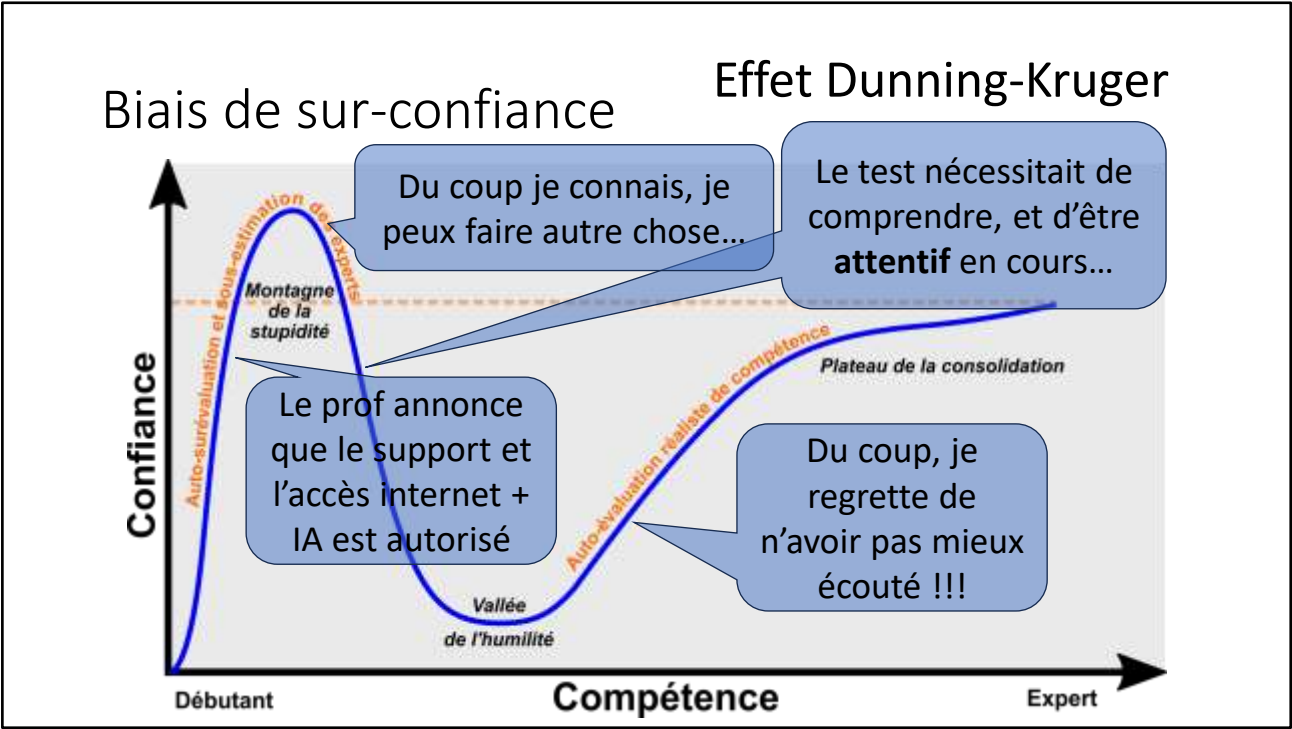
2.1 Connaître les outils intégrés dans le système d'exploitation et dédiés à sa surveillance ainsi que leur domaine d'application. 2.2 Connaître les principales valeurs de mesure de la performance et pouvoir les interpréter.

3.1 Connaître la procédure d'installation des mises à jour et des correctifs. 3.2 Connaître des sources fiables pour des mises à jour et des correctifs ainsi que les mesures de sécurité correspondantes (p. ex. valeurs de hachage et clés). 3.3 Connaître les conséquences et les dangers possibles inhérents aux mises à jour et aux correctifs par rapport à une entreprise. 3.4 Connaître des scénarios de test des mises à jour et des correctifs.

4.1 Connaître des techniques possibles (p. ex. SNMP, WMI) pour la saisie centralisée des données de performance et leurs mécanismes de sécurité. 4.2 Connaître les étapes de configuration à effectuer sur un système de serveur pour activer les mesures de performance (p. ex. SNMP, WMI). 4.3 Connaître les étapes pour intégrer les serveurs dans un outil de monitoring existant. 4.4 Connaître des possibilités pour définir des valeurs seuils judicieuses et installer une alarme.

5.1 Connaître le contenu, la structure et l'application d'un concept d'autorisations. 5.2 Connaître les possibilités des services pour définir des autorisations d'accès à des ressources. 5.3 Connaître la procédure pour adapter des autorisations selon le concept existant d'une entreprise. 5.4 Connaître des méthodes pour documenter les adaptations d'autorisations.

6.1 Connaître les exigences posées aux systèmes périphériques des services correspondants (p. ex. entrées DNS pour atteindre le service ou adaptations requises des règles de pare-feu). 6.2 Connaître des possibilités pour décrire les exigences posées aux systèmes périphériques correspondants de sorte à assurer leur mise en œuvre par des tiers. 6.3 Connaître des possibilités pour tester les adaptations apportées aux systèmes périphériques.



L'objectif de l'apprentissage pour devenir «Pro» rapidement, sera de vous confronter le plus vite possible, à la vallée de l'humilité.

Le test final sera en mode «jeux de rôle» avec mises en situation, et avec accès aux support et à Internet, sans interconnexions sur les réseaux sociaux toutefois, bureau nu et sans ses propres équipements (sac, smartphone, fermés et prêt à partir). Ses notes et supports, posée en amont du test, uniquement sur la machine fournie par l'école.

Être confronté à une simulation de situation réelle, permet de mesurer son propre niveau de maturité sur les sujets abordés.

Références:  
[https://fr.wikipedia.org/wiki/Effet\\_Dunning-Kruger](https://fr.wikipedia.org/wiki/Effet_Dunning-Kruger)  
<https://youtu.be/DtwK0h1Oo1w>

Plus d'infos sur nos biais cognitif, cf <http://zetetique.quicklearn.ch>

Introduction aux services dans l'informatique, et pour le contexte d'un opérateur d'exploitation dans une infrastructure informatique. Année 2 CFC informaticien.

## A: 0(+6). Introduction

Définir les adaptations requises par les systèmes périphériques nécessaires à l'exploitation des services.

Introduction, c'est quoi un service, et typologies...  
+ les services infras:

6. Définir les adaptations requises par les systèmes périphériques nécessaires à l'exploitation des services.

6.1 Connaître les exigences posées aux systèmes périphériques des services correspondants (p. ex. entrées DNS pour atteindre le service ou adaptations requises des règles de pare-feu).

6.2 Connaître des possibilités pour décrire les exigences posées aux systèmes périphériques correspondants de sorte à assurer leur mise en œuvre par des tiers.

6.3 Connaître des possibilités pour tester les adaptations apportées aux systèmes périphériques.

## C'est quoi un service (informatique/numérique)

Rédigez une définition d'un service numérique dans le contexte d'infrastructure IT

Envoyer par email [pk@edu.iseig.ch](mailto:pk@edu.iseig.ch)

**Exo 1:** pourra servir pour 1/10 pts au test.

### •Questions de Réflexion :

- C'est quoi un service (informatique/numérique)
- Comment fonctionnent-ils en général et donner un exemple?
- Quelles sont les principales caractéristiques d'un service ?
- Pourquoi les services sont-ils essentiels pour le bon fonctionnement des systèmes ?

(en option par groupe de 2 ou 3)

Un navigateur web, est la partie cliente d'un service numérique hébergé sur un serveur web, qui génère les codes html 5 nécessaires pour «simuler» (dans le cas de Web app) une application locale, en réutilisant les ressources locales au maximum, afin de minimiser l'impact sur le serveur.

Un exercice collectif sera réalisé plus tard (Slide 21)

## C'est quoi un service (informatique/numérique)

### •Exercice 1

- par groupe de 2 (3 max)
- ~20 min

•**Objectif** : Comprendre la définition et les caractéristiques des services informatiques.

•**Tâche** : Chaque groupe doit rechercher et définir ce qu'est un service, en se concentrant sur ses caractéristiques principales (fonctionnement en continu, automatisation, importance pour le système).

### •Questions de Réflexion :

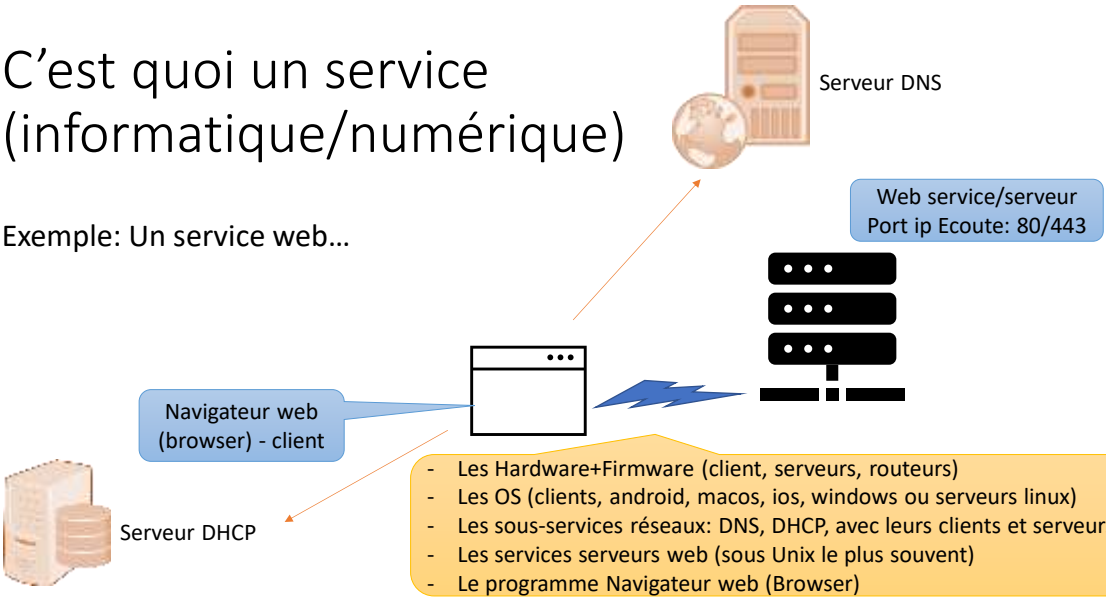
- Comment fonctionnent-ils ?
- Quelles sont les principales caractéristiques d'un service ?
- Pourquoi les services sont-ils essentiels pour le bon fonctionnement des systèmes ?

### •Partage des Résultats

- jour (semaine) suivant...

# C'est quoi un service (informatique/numérique)

Exemple: Un service web...



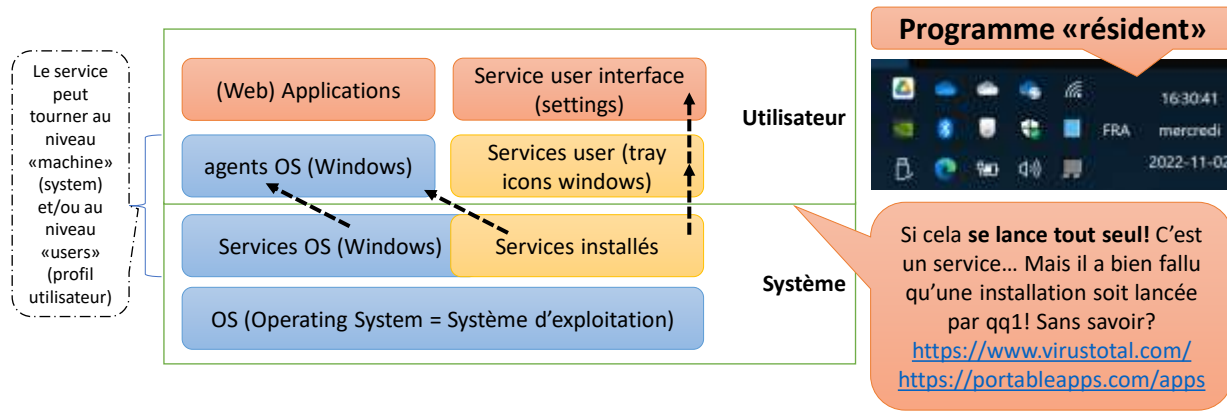
C'est un programme, qui n'est pas directement une application pour utilisateurs.  
Il peut tourner sur le poste de l'utilisateur, ou sur un autre appareil relié en réseau.

<https://medium.com/responsibility-digital/microsoft-imite-firefox-b823e07cf95>  
<https://medium.com/conseillers-num%C3%A9riques-suisses-romands/reconfigurer-edge-pour-arr%C3%AAter-de-te-spammer-l%C3%A9cran-f7bab261af9>

cf. <http://network.quicklearn.ch>  
IANA standards DHCP: <https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml>  
DNS: <https://www.iana.org/domains>

## C'est quoi un service (informatique/numérique)

C'est un programme, qui n'est pas directement une application pour utilisateurs.  
Il peut tourner sur le poste de l'utilisateur, ou sur un autre appareil relié en réseau.



Beaucoup d'applications vont installer des « services » qui vont assurer des fonctions plus ou moins utiles, souvent leurs propres notifications pour assurer des mises à jour, mais aussi des injonctions « marketing » indésirables, quand ce ne sont pas des véritables « troyens »:

<https://www.journaldugeek.com/2022/03/16/kaspersky-telegram-pourquoi-les-antivirus-et-logiciels-russes-sont-devenus-un-danger/>

Et du coup même des utilitaires « innocents » peuvent installer des programmes résidents, dans le système ou dans le profil user, et cela va devenir un « service » résident de plus. Et je ne vous parle pas de toutes les saletés préinstallées par le constructeur même du PC neuf... Qu'il FAUT NETTOYER, voir réinstaller Windows vierge. Mais même alors, il y encore des trucs de Microsoft inutilisés dans programmes que l'on pourrait désinstaller (mais si on veut se « protéger » des abus de Microsoft, alors il sera mieux d'installer Ubuntu à la place).

Désactivation au démarrage et nettoyage du PC:

- Piriform Ccleaner (mais gaffe avant de l'installer => VirusTotal.com)

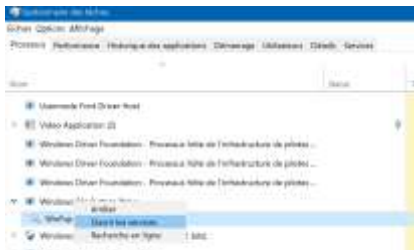
<https://medium.com/quicklearn/ccleaner-de-piriform-b54351a49fa>

- IOBit !! => PUP (<https://www.malwarebytes.com/blog/detections/pup-optional-cacaoweb>) Pas recommandé – surtout l'uninstaller iobit, check it avec virustotal.

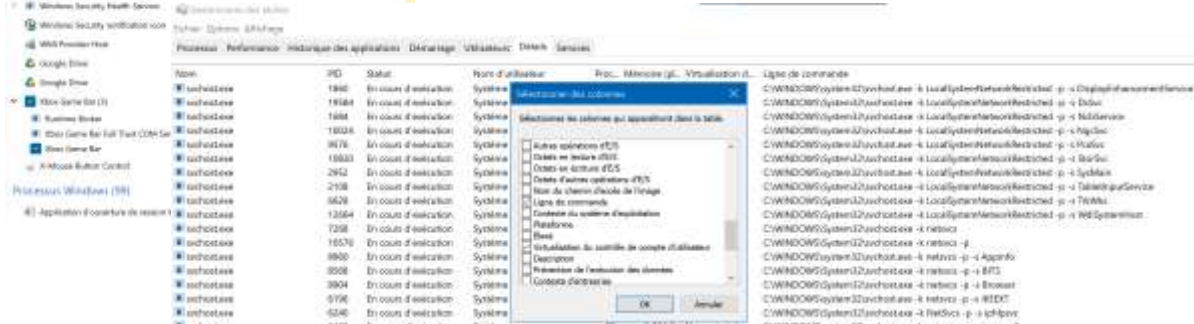
- [Shodan Search Engine](https://www.shodan.io/) <https://www.shodan.io/>



# Task manager (gestionnaire de tâches)



Pour mieux retrouver les services/processus associés à quoi, ou qui  
Afficher la colonne «ligne de commande»



Ctrl-alt.-del > Task manager, ou clic droit sur la barre des tâches: Il permet «Gestionnaire des tâches»

Explorations ensembles sur les options disponibles, et son utilisation.

Merci David Lazarevic: Depuis Powershell:

```
get-service -ServiceName "event*"
```

```
get-process -ProcessName "*exemple*"
```

# Services réseaux et Cloud, et sécurité...

- Discussions et échanges
  - Illustration Email client, SMTP, IMAP/POP3
  - DHCP et configurations automatiques
  - DNS et configurations automatiques vs manuel
  - IPv4 vs IPv6 et IPv4 privée + NAT

<http://Network.quicklearn.ch>

Contrôle des connaissances de base les réseaux et révisions

[Cybercriminalité, ce que votre banque oublie de vous dire... | by Pascal Kotté | Conseillers Numériques Suisses Romands | Medium](#)

[Antivirus sur Mac, Linux, Android, iPhone, ou pas? Pas plus que pour Windows! | by Pascal Kotté | Conseillers Numériques Suisses Romands | Medium](#)

[Suisse: 6'000 emails compromis, changez vos mots de passe ou activer 2FA | by Pascal Kotté | Conseillers Numériques Suisses Romands | Medium](#)

[Histoires de VPN. Pourquoi c'est bien, pourquoi ce n'est... | by Pascal Kotté | Conseillers Numériques Suisses Romands | Medium](#)

[C'est quoi, les "Creative Commons" et "Open" c'est pour ouvrir quoi ? | by Pascal Kotté | CloudReady CH | Medium](#)

Quelques articles à disposition, pour assurer un support à ces échanges.

<http://network.QuickLearn.ch>

<https://kb.mailfence.com/kb/auto-configuration-custom-domain>

<https://medium.com/conseillers-num%C3%A9riques-suisse-romands/cybercriminalit%C3%A9-ce-que-votre-banque-oublie-de-vous-dire-9f6fcfbdb242>

<https://medium.com/conseillers-num%C3%A9riques-suisse-romands/antivirus-sur-mac-linux-android-iphone-ou-pas-pas-plus-que-pour-windows-9d022ff1ddbd>

<https://medium.com/conseillers-num%C3%A9riques-suisse-romands/suisse-6-000-emails-compromis-changez-vos-mots-de-passe-ou-activer-2fa-105bdb6e6bae>

<https://medium.com/conseillers-num%C3%A9riques-suisse-romands/histoires-de-vpn-3eef950edd6>

<https://medium.com/cloudready-ch/cest-quoi-les-creative-commons-et-open-c-est-pour-ouvrir-quoi-90e050c650b3>

## Exemple de services «périphériques»

- SMTP/POP3/IMAP – Acheminement des emails
- DNS
  - Remplacer un nom de domaine (préfixe URL) par son IP
  - Mais pas que...
  - TXT record pour appropriation de services web (M365, G Suite, Mailchimp...)
  - Services Records
    - \_ldap records (Active Directory, Radius, Autoconfig email...)
    - SPF/DKIM => sécurisation emails



Cette photo par Auteur inconnu est soumise à la licence CC BY-SA

Se prendre un nom de domaine  
Mondomaine.ch (10F/an)  
p.ex. Gandi.net ou infomaniak.ch

[Créer et gérer son propre nom de domaine \(email@domn.ch et site web\) | by Pascal Kotté | QuickLearn | Medium](#)

[Emailing, publipostage. Niveau avancé: SPF et DKIM et autres... | by Pascal Kotté | QuickLearn | Medium](#)

## Les services «utilisateurs» et «infras»

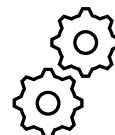


Le catalogue de services exposé aux usagers va intégrer les prestations assurées par leur département «IT» et leurs sous-traitants, ou fournisseurs: Ce sont les services finaux

- Fourniture et maintenance d'un équipement informatique (avec son OS, et sécurisé)
- Fourniture et maintenance d'un réseau avec accès Internet (sécurisé)
- Mise à disposition d'imprimantes, emails, espaces de stockage backupés (& sécurisé)
- Fourniture des informations aux usagers pour utiliser l'IT (formation & sécurité)
- Déploiement et maintenance d'un logiciel sur les bons postes
- ... (iot, webcam, badge, distributeurs...)

Et il y a ceux que les utilisateurs ne voient pas, ou peu: «infras» (*périphériques*)

- Mise à jour des logiciels sur les postes
- Fourniture d'une adresse IP (DHCP)
- Gestion des noms pour IP (DNS)
- identification et annuaire des utilisateurs (AD/DC)
- ...



Il y a dualité dans la nomenclature:

- Les services utilisateurs, sont les applications finales, visibles et utilisées par eux.
- Alors que les services numériques informatiques invisibles par les usagers, mais géré par l'IT, seront souvent des services utilisés par plusieurs applications métiers, ou des applications génériques pour les utilisateurs, et donc, bien plus critiques encore.

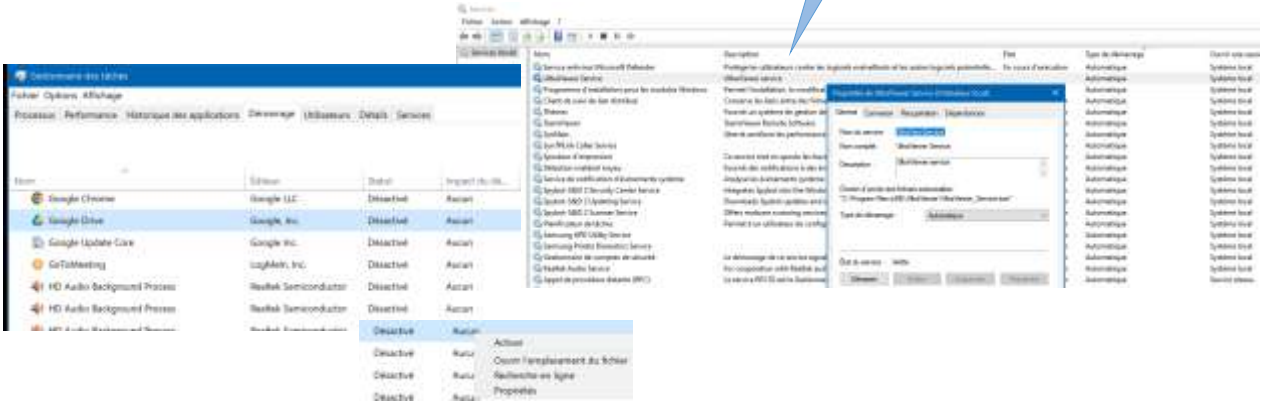
Le contenu des objectifs de cette formation, fait plus un focus sur les services infras. Mais maintenir en fonctionnement les services utilisateurs proposé dans le « catalogue des services » assurés par l'IT est la réelle finalité de l'infrastructure ICT.

15

# Activer/désactiver un service

- Gestionnaire des services, config au démarrage
  - Gestionnaire des tâches
  - Activation/Désactivation au login

Ceci utilise une MMC  
Jouez avec, c'est important!



C'est avec le gestionnaire des Services, que les services inutilisés sont désactivés, ou automatiquement lancés au démarrage, voir relancer en cas d'arrêt.

Il est aussi possible d'utiliser le task manager – Onglet démarrage: Activer désactiver (au démarrage)  
Un service désactivé est aussi (souvent) une App installée: On peut la lancer manuellement.

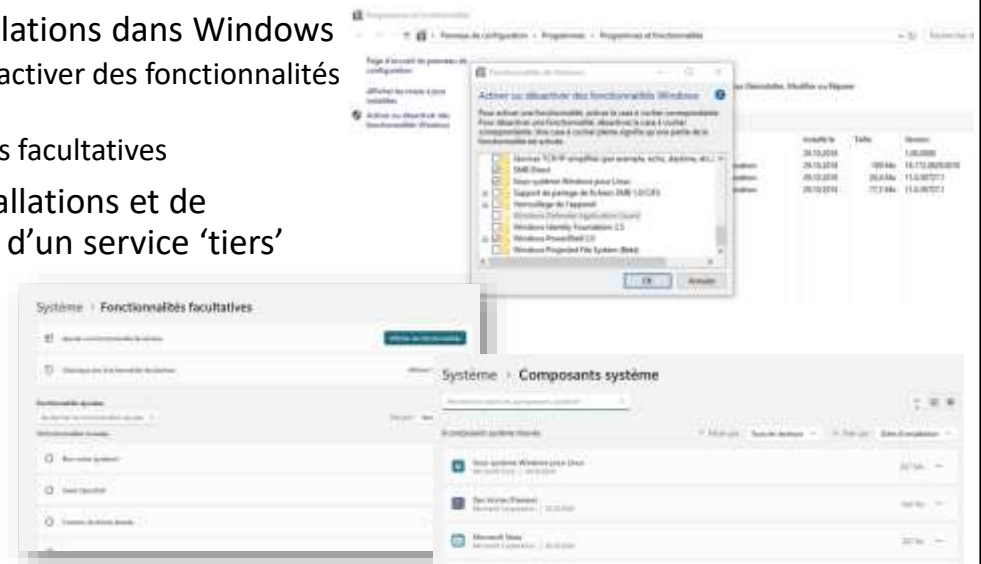
Mais tous les services ne tournent pas nécessairement dans l'onglet « Services » de Windows. Certains se présentent sous la forme d'applications «portables» lancée au démarrage automatiquement, sans même être visible dans la liste des applications installées.

Le site  
<https://portableapps.com/>

Propose de déployer des applications sans installations.  
Mais un programme « non déclaré » s'il se lance tout seul, devient « un service »:  
Par exemple, un troyen...

## Activer/désactiver, installer un service (Windows)

- Options d'installations dans Windows
  - Activer ou désactiver des fonctionnalités Windows
  - Fonctionnalités facultatives
- Packages d'installations et de désinstallations d'un service 'tiers' (Non Windows)



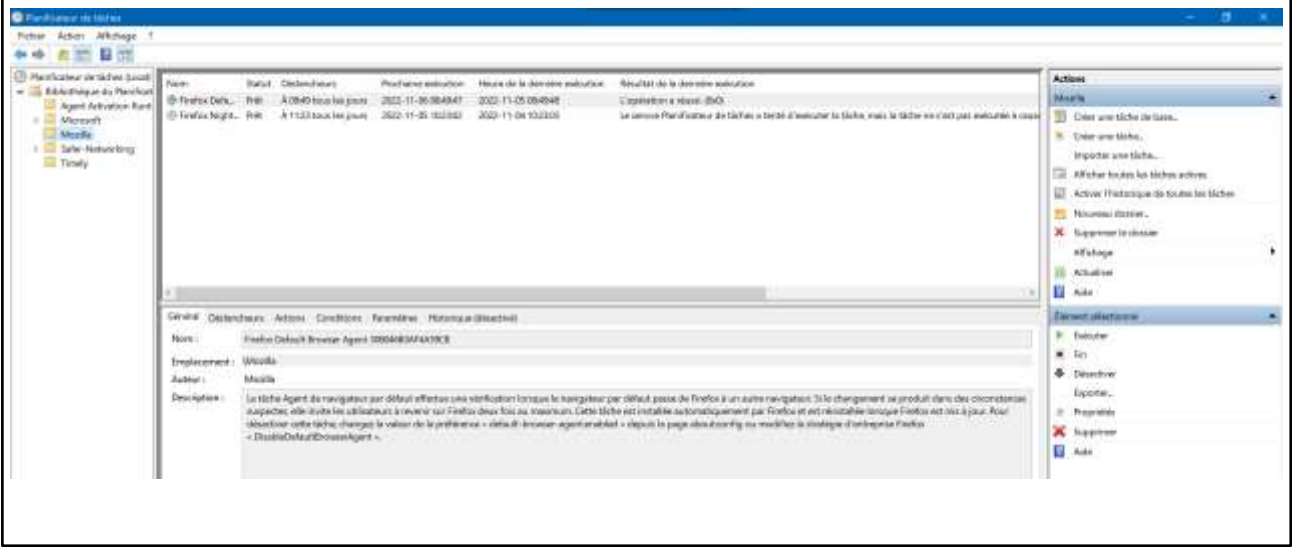
Exemple: sous-système Linux pour Windows

[Passer de Win10 à Linux. C'est pas si compliqué ! | by Pascal Kotté | LesEnfantsDu.Net | Medium](https://medium.com/lesenfantsdu-net/passer-de-win10-%C3%A0-linux-5799c79d33f7)

<https://medium.com/lesenfantsdu-net/passer-de-win10-%C3%A0-linux-5799c79d33f7>

Tâches planifiées, cron sous Unix

Run Once  
Active Setup



Les services ne sont pas nécessairement actifs en permanence, et des « Scheduler », vont

<https://www.malekal.com/les-taches-planifiees-de-windows>

Crontab: <https://geekflare.com/fr/crontab-linux-with-real-time-examples-and-tools/>  
<https://fr.wikipedia.org/wiki/Cron>

Mais on a aussi des espaces nombreux pour des exécutions « runonce » dans la machine ou sur le profil utilisateur:

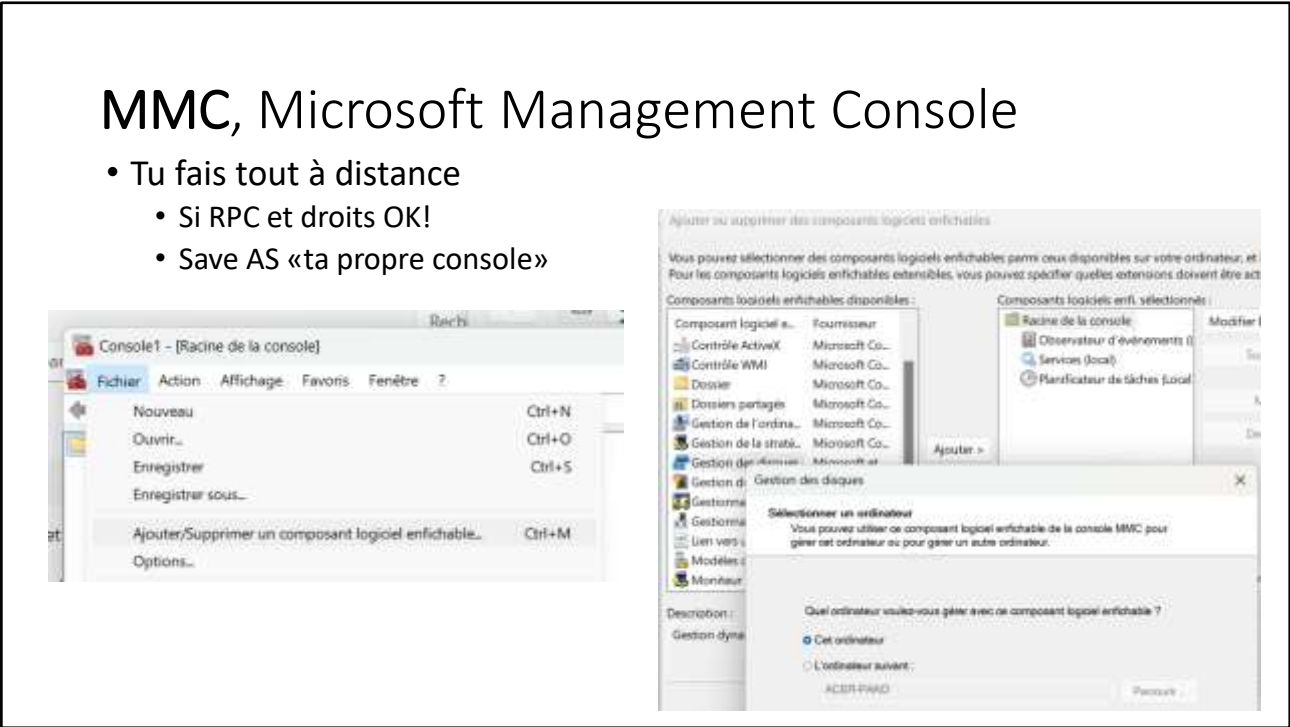
<https://learn.microsoft.com/en-us/windows/win32/setupapi/run-and-runonce-registry-keys>

Active setup <https://www.tech2tech.fr/packaging-quelques-mots-sur-active-setup>



# MMC, Microsoft Management Console

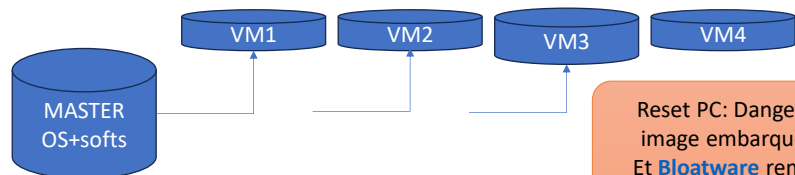
- Tu fais tout à distance
  - Si RPC et droits OK!
  - Save AS «ta propre console»



Comment rapidement déployer des nouvelles machines, avec toutes les bonnes applications et services préinstallés?

## Déploiement par «Clonage»

- Déploiement d'une image (option via [PXE](#)) depuis une machine de référence (master).
  - WAIK > ADK: similaire aux machines OEM  
[Téléchargez et installez Windows ADK | Microsoft Learn](#)
  - Outils tiers: ! Doit assurer le reset [GUID](#)
- Pour les serveurs
  - L'hyperviseur va intégrer le clonage de serveurs, mieux, le clonage lié (différentiel)



Windows se déploie lui-même via une image, puis un setup (gain de temps) et garde copie en local, mise à jour

Reset PC: Danger, si PC infesté, image embarquée douteuse... Et [Bloatware](#) remis si intégrés...

Windows 7

<https://www.microsoft.com/fr-fr/download/details.aspx?id=5753>

Windows 11

<https://learn.microsoft.com/fr-fr/windows-hardware/get-started/adk-install>

<https://fr.wikipedia.org/wiki/Bloatware> - Logiciels indésirables, le plus souvent...

[https://fr.wikipedia.org/wiki/Universally\\_unique\\_identifier](https://fr.wikipedia.org/wiki/Universally_unique_identifier)

[https://fr.wikipedia.org/wiki/Preboot\\_Execution\\_Environment](https://fr.wikipedia.org/wiki/Preboot_Execution_Environment) (PXE)

# Les services dans le Cloud

- Amazon
- Google
- Azure

## 3 Clouds

- IaaS
- PaaS
- SaaS

### Modèle classique

Données

Applications

Bases de données

Système d'exploitation

Virtualisation

Matériel serveur

Stockage

Réseaux

### Modèle IaaS

Données

Applications

Bases de données

Système d'exploitation

Virtualisation

Matériel serveur

Stockage

Réseaux

### Modèle PaaS

Données

Applications

Bases de données

Système d'exploitation

Virtualisation

Matériel serveur

Stockage

Réseaux

### Modèle SaaS

Données

Applications

Bases de données

Système d'exploitation

Virtualisation

Matériel serveur

Stockage

Réseaux

GAFAM

BATX

- Hidora
- Exoscale
- Infomaniak
- Etc...

Version modifiée d'un modèle IaaS de <http://blog.blaisethirard.com/>

PascalHRezolution.ch ICC BY-SA 2016

L'entreprise a le contrôle

Le fournisseur a le contrôle

<https://medium.com/cloudready-ch/cest-quoi-iaas-paas-et-saas-le-cloud-c169451d73bc>

Explication complémentaires disponible en ligne sur cet article:  
Les services numériques déportés dans le nuage, deviennent très nombreux:  
<https://medium.com/cloudready-ch/cest-quoi-iaas-paas-et-saas-le-cloud-c169451d73bc>

Option; **Ethique numérique, durable et responsable?**  
C'est quoi? Et comment on peut faire?  
<https://medium.com/cloudready-ch/ethique-num%C3%A9rique-durable-et-responsable-89083a6a5789>

Documentation: Les Termes et conditions des services Cloud et sous-services Cloud, par exemple, affichage d'une carte Google map, sur un site web. Il va utiliser un sous-service Google non documenté, et pourtant, si plus de 100 visiteurs (? Jour/semaine/mois... à vérifier) il va y avoir le site en erreur, car il faut « payer » ce sous-service. (périphériques). A l'heure des micro-services, l'inventaire des éléments requis pour le bon fonctionnement des services de l'IT, ne sont jamais, à jour.

## SSII ou SS2I, vs ESN, ou encore MSP

- SSII – Sociétés de services et ingénierie en informatique
- => ESN (Entreprise de Services Numériques)  
[Entreprise de services du numérique — Wikipédia \(wikipedia.org\)](https://fr.wikipedia.org/wiki/Entreprise_de_services_du_num%C3%A9rique)
- MSP – Managed Service Provider, qui va utiliser un RMM (Remote Monit. & Mgmt.)

**Le département informatique:** est la partie internalisée de ces activités, qui intègre les produits des constructeurs, éditeurs et ESN externes.

**C'est quoi, la mission de l'IT?**  
**Votre servez à quoi?**

«Fournir facilement la bonne information aux bonnes personnes (uniquement) et au bon moment !»

<http://pascal.kotte.net>

Et pas de créer de la complication inutile!

La dimension « Cloud » est entrée dans les habitudes au point de transformer les SSII historique, en deux types de sociétés de services:

- Ceux qui fournissent un service Cloud (ESN).
- Et ceux qui fournissent des services informatiques, ou de l'infogérance (MSP).

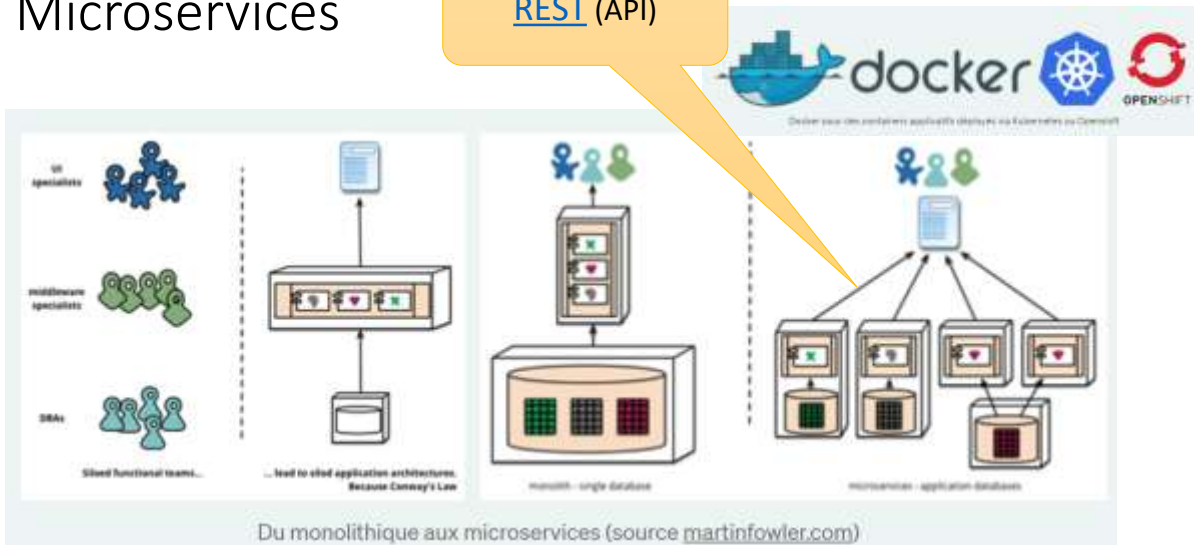
<https://www.capital.fr/votre-carriere/esn-entreprise-de-services-numeriques-definition-et-fonctionnement-1405805>

<https://www.digitalmarketinglab.fr/quest-ce-que-la-prestation-de-services-numeriques/>

[https://fr.wikipedia.org/wiki/Entreprise\\_de\\_services\\_du\\_num%C3%A9rique](https://fr.wikipedia.org/wiki/Entreprise_de_services_du_num%C3%A9rique)

# Microservices

REST (API)



<https://medium.com/cloudready-ch/microservices-cest-quoi-f73d9ac48d94>

Les architectures micro-services, alimentent les services Cloud 24/7, et sont facilités grâce aux solutions de type container (Docker).

Explications en ligne: (Auteur: Pascal Kotté)

<https://medium.com/cloudready-ch/microservices-cest-quoi-f73d9ac48d94>

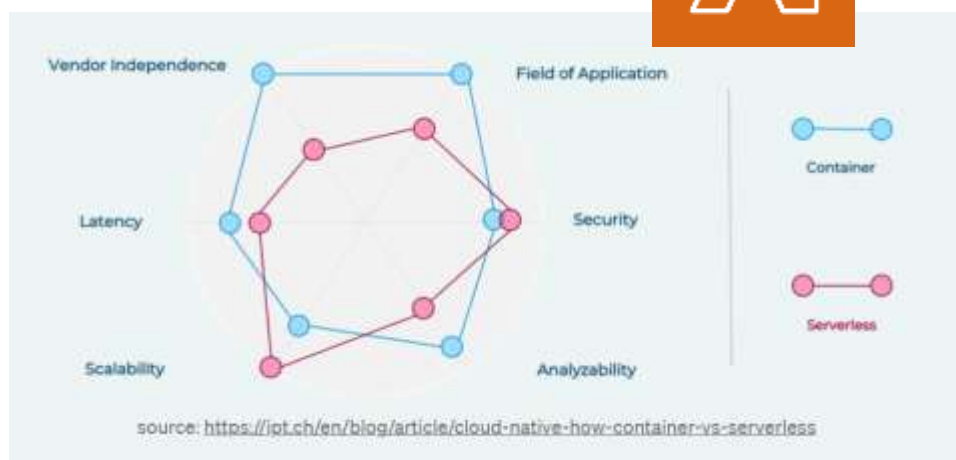
<https://medium.com/cloudready-ch/ipaas-cest-quoi-3f4b8ec84924>

[https://fr.wikipedia.org/wiki/Representational\\_state\\_transfer](https://fr.wikipedia.org/wiki/Representational_state_transfer)

## DEVOPS to NoOPS

Google Cloud

Serverless computing



Les micro-services peuvent aussi utiliser des plateformes de type « Serverless », c'est-à-dire, sans serveurs, mais uniquement avec des routines qui exploitent des briques de micro-services « prêts à servir ». Et donc, il est possible de coder directement un programme, sans devoir provisionner ni dimensionner des services serveurs. La facturation est faite en fonction des volumes de charges de ces programmes (le nombre d'utilisateurs actifs). Amazon Lambda a été le précurseur, suivi par Google engine, puis Microsoft Fabric.

Les fiches ci-dessous sont en anglais, car les descriptions des articles en français n'étaient pas assez explicitement détaillés.

[https://en.wikipedia.org/wiki/Serverless\\_computing](https://en.wikipedia.org/wiki/Serverless_computing)

[https://en.wikipedia.org/wiki/AWS\\_Lambda](https://en.wikipedia.org/wiki/AWS_Lambda)

[https://en.wikipedia.org/wiki/Microsoft\\_Azure](https://en.wikipedia.org/wiki/Microsoft_Azure)

<https://cloud.google.com/serverless?hl=fr>

Problème, le code produit n'est pas transportable hors sa plateforme. Cela devient captif.

C'est aussi avec du Cloud que <https://www.missingmaps.org> est possible  
[Missing Maps](https://www.missingmaps.org)

Avec OpenStreetMap - <https://www.openstreetmap.org/#map=18/46.53552/6.66660>

Dans la même veine, la tendance NoCODE, mais avec des pièges...

<https://youtu.be/qHPBB5lHSol?si=lgyme9Pd2dOduzQT>

## En résumé, un service numérique

### Peut s'analyser sur 3 niveaux de perspectives, dans le domaine de l'IT:

1. Au niveau **système**, sous Windows, ce sont les services démarrés avec la machine, au-dessus de l'OS, livré par l'OS ou ajouté par des installations tierces: Accessibles dans le gestionnaire des services.
2. Au niveau **infrastructure**: Ce sont les programmes résidents ou automatiques, pour partie sur les postes clients, ou sur des équipements réseaux, ou sur des serveurs locaux ou dans le Cloud (et parfois tout cela à la fois).
3. Au niveau **entreprise**: Ce sont les outils, matériels et logiciels mis à disposition des utilisateurs de l'organisation, par le département informatique (L'IT): Qui composent le catalogue des services pour les utilisateurs. Cela est aussi vrai pour les ESN qui produisent un service Cloud (ex Gmail) pour leurs clients.



## A: (6). Services sous-jacents/infra

Définir les adaptations requises par les systèmes périphériques nécessaires à l'exploitation des services.

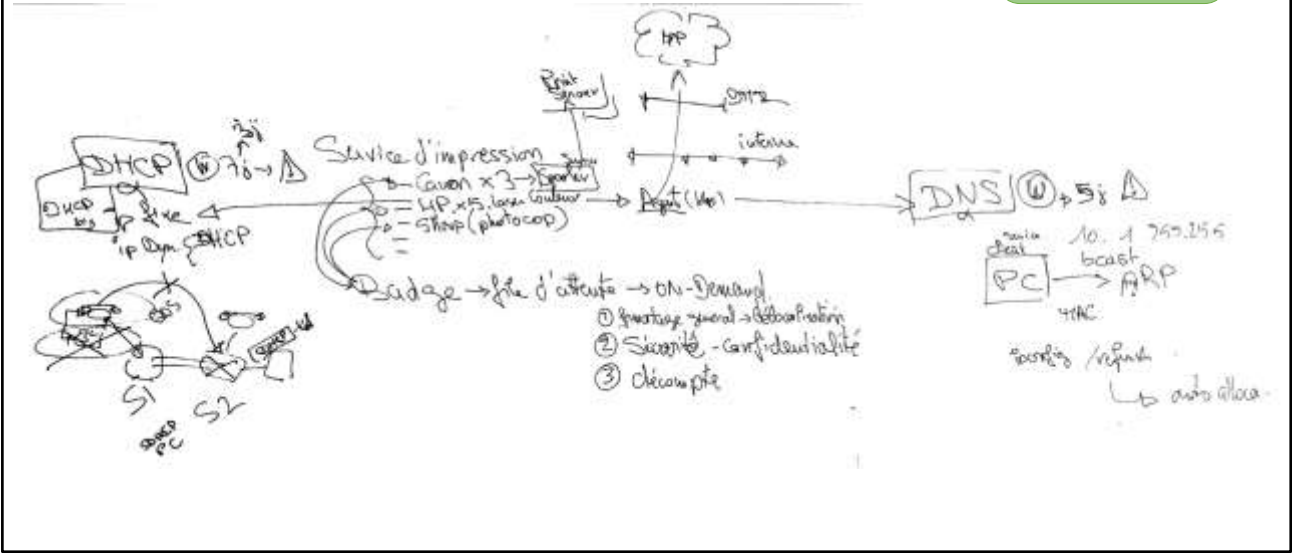
Connaître les exigences posées aux systèmes périphériques des services correspondants (p. ex. entrées DNS pour atteindre le service ou adaptations requises des règles de parefeu).

Connaître des possibilités pour décrire les exigences posées aux systèmes périphériques correspondants de sorte à assurer leur mise en œuvre par des tiers.

Connaître des possibilités pour tester les adaptations apportées aux systèmes périphériques.

# Exemple des services d'impressions

Avec la fonction «follow me»



Présentation et illustration du fonctionnement devenu extrêmement sophistiqué des services d'impressions dans une entreprises avec l'option « Follow me »  
Souvent les badges nécessitent un serveur Radius:  
[https://fr.wikipedia.org/wiki/Remote\\_Authentication\\_Dial-In\\_User\\_Service](https://fr.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Service)  
Ou autre IAM serveur: (Identity and Access Management)

Exercice collectif en classe.

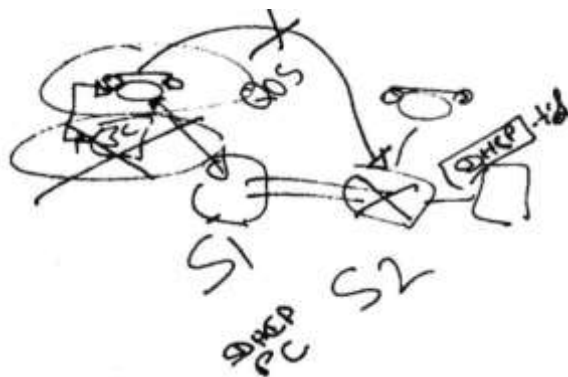
## Sans une doc Adhoc et du monitoring

- Pas de vision claire de ce qu'il se passe en cas de problèmes

- Histoire vécue et réelle

La mise hors-service de plus 100 postes, sur une erreur de procédure de reprise...

Sans un diagnostic du problème.



La documentation et le monitoring nécessaire et indispensable.

- En cas de panne générale grave, ou de crash et nécessité de recouvrement.

Lister les bonnes pratiques collectivement (si assez de temps dispo).

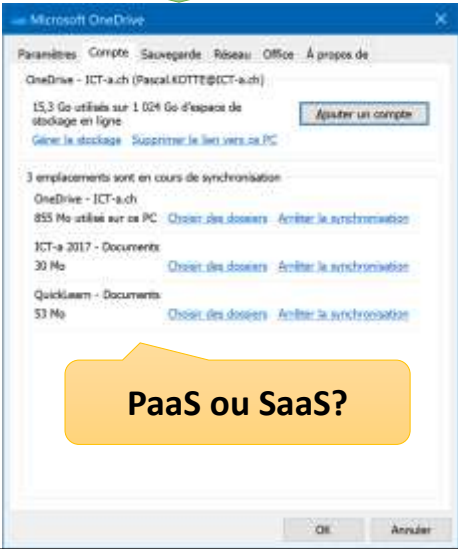
- Sera repris par la suite dans le § suivant.

## Exemple de service: OneDrive

- Pour assurer un backup en temps réel
- Accessible depuis partout/internet
- Un partage de documents
- Disposer d'un stockage «non local» (capacité+)



Avec Cryptolocker  
detection (\$)



PaaS ou SaaS?

Explorer son équivalent OneDrive.

Exercice en classe:

- Retrouver le nom des exécutables, pour la partie perso, et la partie pro.
- Localiser les
- Y a-t-il un service installé?
- Est-ce tout de même un service?
- ...

PaaS ou SaaS?

C'est une question intéressante ! En fait, même lorsque tu configures et personnalises Office 365 avec des équipes, des sites SharePoint et des synchronisations OneDrive, cela reste principalement dans le domaine du **SaaS (Software as a Service)**. Voici pourquoi :

- Office 365** : C'est une suite SaaS qui inclut des applications comme Teams, SharePoint et OneDrive. Ces services sont fournis via Internet et gérés par Microsoft.
- Teams et SharePoint** : Bien que tu puisses personnaliser et configurer des sites SharePoint et des équipes dans Teams, tu utilises toujours des outils et des services fournis par Microsoft via le cloud.
- OneDrive** : Il s'agit d'un service de stockage en ligne, également fourni en tant que

SaaS.

Cependant, il est vrai que certaines fonctionnalités de personnalisation et de développement dans SharePoint peuvent ressembler à des services PaaS, car elles permettent de créer des applications et des workflows personnalisés. [Mais globalement, l'ensemble de l'écosystème Office 365 est considéré comme du SaaS.](#)

## Exemple de services

- AD + **Microsoft ID Entra**
- DNS ou Azure DNS
- DHCP (pourquoi pas dans Azure?)

<http://dns.quicklearn.ch>

Car c'est un service nécessairement local, qui ne peut être déporté sur un serveur 'SaaS' lequel ne serait pas accessible via IP, tant que le service DHCP n'aura pas attribué une adresse IP à ce poste.

**DHCP DISCOVER**

**DHCP SERVER**

**UDP:** source port=68; destination port=67  
**IP:** source=0.0.0.0; destination=255.255.255.255,  
**Ethernet:** source=sender's MAC; destination=FF:FF:FF:FF:FF:FF

### Azure private DNS Zone

**Comment check si DHCP est OK?**

1. ipconfig /release
2. ipconfig /renew
3. Ipconfig /all => check date/h

AD et ADD  
<https://learn.microsoft.com/fr-fr/training/modules/configure-azure-active-directory/>

DNS  
<https://learn.microsoft.com/fr-fr/learn/modules/implement-windows-server-dns/>  
<https://learn.microsoft.com/fr-fr/training/modules/host-domain-azure-dns/>

DHCP  
[Dynamic Host Configuration Protocol — Wikipedia](https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol)  
[https://en.wikipedia.org/wiki/Dynamic\\_Host\\_Configuration\\_Protocol](https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol)  
<https://learn.microsoft.com/fr-fr/learn/modules/deploy-manage-dynamic-host-configuration-protocol/>  
<https://learn.microsoft.com/fr-fr/learn/modules/implement-ip-address-management/>

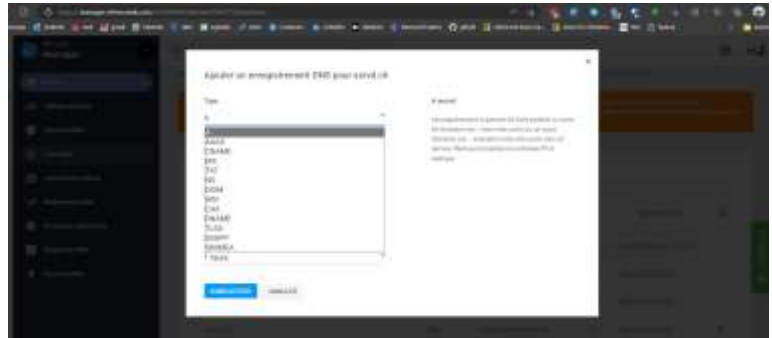
Redondance pour DHCP, possible:  
<https://rdr-it.com/windows-serveur-configuration-du-basculement-dhcp/>

## Présentation gestion DNS chez Infomaniak ou Gandi

- Comment gérer et ajouter un Record DNS sur un espace public.

Plus de détails sur le service DNS ici

<http://dns.quicklearn.ch>



La gestion d'un DNS est hors-sujet, mais fait partie des services infrastructures ou «périphériques» fondamentaux.

Il est nécessaire toutefois de savoir utiliser un service DNS via un opérateur Registrar ou revendeur de domaine.

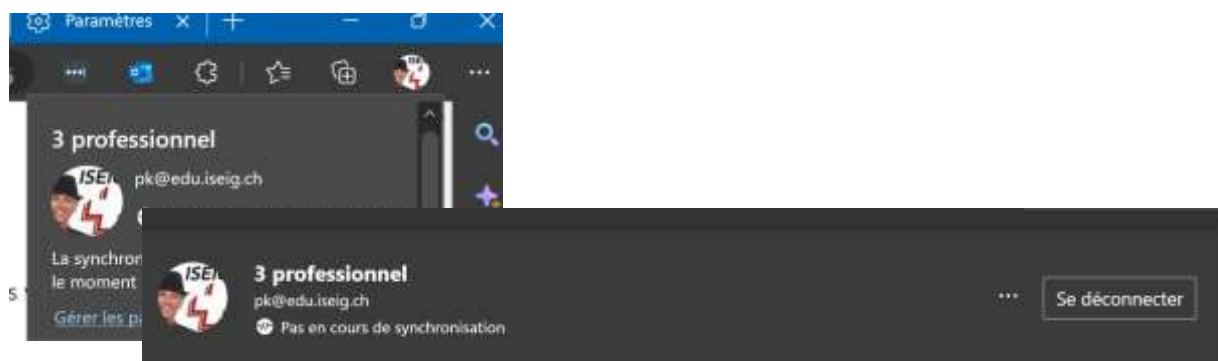
Recommandation à tout apprenti informaticien: Se prendre un domaine DNS pour son propre usage,

Exercice collectif possible pour ceux qui veulent:

- Louer un domaine .ch (Cout 10F/année), faire une redirection sur une publication Medium, ex. <http://blog.quicklearn.ch>
- Activer la mailbox gratuite «catchall», éventuel redirection sur sa propre mailbox.

## Les services clients «Edge» + «Windows»

- Pour faciliter «la vie» des utilisateurs Microsoft propose de «mémoriser» les accès dans Windows, depuis Edge...
- Et cela va pourrir la vie des responsables de la sécurité...



Il est important de sensibiliser les utilisateurs

Et en tant que opérateur systèmes, de maitriser la gestion des profils et comptes mémorisés.

Petite exploration sur le nettoyage des Cookies, des Notifications, et usage du profil...

Et même le mode faussement surnommé «anonyme» des navigateurs web.

Voir aussi:

<http://teams.quicklearn.ch>

<https://medium.com/quicklearn/se-connecter-%C3%A0-365-microsoft-office-f1ac2e5d87fa>



Rester connecté à toutes vos applications

☐ Autoriser mon organisation à gérer mes appareils

Non, se connecter à cette application uniquement

OK

Accès Professionnel ou Scolaire

Accéder à des ressources comme la messagerie, les applications et le réseau. En vous connectant, vous acceptez que votre entreprise ou votre établissement puisse contrôler certains éléments de votre appareil, par exemple les paramètres que vous êtes autorisé à modifier. Pour plus d'informations à ce sujet, posez la question.

Se connecter

 Compte professionnel ou société


 Министерство образования и науки Российской Федерации

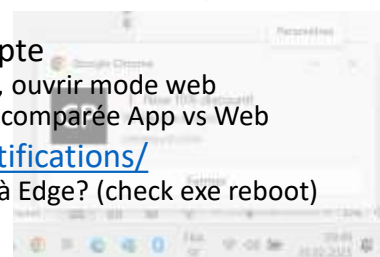
 Compte professionnel ou scolaire  
pe@redacted.fr

Compte professionnel ou scolaire

34

## Exercice: Notifications Web + Web App + Extensions (Plugins)

- Utilisez Edge pour ouvrir la page [tel.search.ch](https://tel.search.ch)
  - Installer cet annuaire comme une application dans votre machine
  - Créer un identifiant associé à un email ou LinkedIn ou Google...
  - Quelles informations cela va-t-il transmettre à Search.ch ?
  - Qui est derrière le site et collecte ces informations?
  - Option: Y créer votre entrée personnelle, et activer l'option \* sans pub
- Utilisez Edge pour ouvrir un document word (Office.com)
  - Comparer l'empreinte mémoire RAM avec le même document ouvert en local (Word ou LibreOffice Writer)
- Installer l'extension Bitwarden et utiliser/créer un compte
  - Y importer vos mots de passe enregistrés de vos navigateurs, ouvrir mode web
  - Installer l'application Bitwarden/Windows ? Empreinte RAM comparée App vs Web
- Tester notification: <https://cleverpush.com/en/test-notifications/>
  - Est-ce que cela disparaît après fermeture/reboot? Est-ce limité à Edge? (check exe reboot)
  - Comment supprimer cela?



<https://www.airship.com/fr/ressources/definition/notifications-web/>

[https://fr.wikipedia.org/wiki/Server\\_push](https://fr.wikipedia.org/wiki/Server_push)

## B: 1(+5). Documentation

Analyser à l'aide de la documentation d'exploitation les systèmes en place et leur environnement.

### 1. Analyser à l'aide de la documentation d'exploitation les systèmes en place et leur environnement.

1.1 Connaître le contenu, la structure et l'application d'une documentation d'exploitation.

1.2 Connaître l'importance d'une documentation d'exploitation exhaustive et mise à jour afin d'assurer la maintenance.

1.3 Connaître les caractéristiques des services les plus répandus (p. ex. services de fichiers, d'impression et de répertoire, DHCP, DNS) et leur contribution à la fonctionnalité d'un réseau.

5. Administrer et documenter les autorisations selon le concept d'autorisations en vigueur.

## En cas de crash, la doc est où?

- Et les mots de passe de récupération, restauration, réparation ?

[RoboForm Password Manager: Say Goodbye to Writing Down Passwords](#)

Surtout si aucune des machines n'arrivent plus à ouvrir une session sur le réseau, ou plus simplement, le serveur de fichiers est «Crash» et il faut le réparer en suivant le process, avec le mot de passe de restauration des bandes, documenté dans un fichier Keypass (ou Bitwarden), sur le «serveur de fichier»...

[Les coffres à mots de passe. Comment sécuriser et partager, sans... | by Pascal Kotté | UDON LiN | Medium](#)



Cette photo par Auteur inconnu est soumise à la licence [CC BY-SA-NC](#)

Documenter les services, c'est aussi prévoir le pire, et l'anticiper.

<https://medium.com/udon-lin/les-coffres-%C3%A0-mots-de-passe-80e919c844f8>

### Important:

Tous les articles mis en ligne par l'auteur de ce support, sont ouvert à améliorations, et une bonne partie via des « Blogs » sur Medium, afin de faciliter les commentaires et corrections, et de compléter avec toutes contributions, autres profs, élèves, experts...

NB. Pour les fautes d'orthographes, merci de penser à mettre un commentaire privée, comme la plateforme le permet.

## Les types de documentations (par destinataires)



- Pour les usagers: Intranet, helpdesk, service desk
- Pour les contrôleurs externes: Auditeurs
- Pour les gestionnaires techniques des installations informatiques
  - Pour les opérateurs informatiques internes – Checklist de maintenance
  - Pour les développeurs/installateurs internes – checklist de déploiements
- Pour les intervenants externes des installations informatiques
- Pour les gestionnaires organisationnels des services numériques
  - A usage interne à l'entreprise (IT manager, Qualité, Sécurité)
  - A usages avec prestataires (sous-traitants, avant l'audit...)

Il n'y a pas « une » doc, mais des « docs »

<https://www.atlassian.com/fr/work-management/knowledge-sharing/documentation/standards>

<https://www.atlassian.com/fr/itsm/knowledge-management/what-is-a-knowledge-base>

<https://www.ninjaone.com/fr/gestion-de-la-documentation-informatique/>

Autres exemples

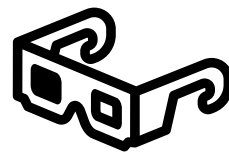
Directement utiliser des modules de « Learning platform »

- Zoho Learn, manual + learn module: <https://youtu.be/2ILAm6ujtfs> (première partie seulement)

- Google site

- Excel sheet

## Les contenus (usages)



- **Manuels: Comment on fait pour faire cela ?**
  - Utilisateurs d'applications métiers ou standard
    - Mise en œuvre dans le contexte de l'organisation (URL de l'intranet qui héberge les docs)
  - Interne à l'IT: procédures internes (création utilisateur)
    - Checklist
- **Éléments de configurations**
  - Comment et où sont installés les composants d'un service
    - Procédure de rollback et de réinstallation «from scratch»
    - Liste des paramètres spécifiques
- **Éléments d'exploitation ( section 5 de la formation)**
  - L'annuaire des utilisateurs, et de leurs droits d'accès
  - L'inventaire et la localisation des équipements et des logiciels (avec leurs clefs licences)
- **Éléments de sécurité**
  - Données sensibles, et ayants-droits: Méthodes et outils de sécurisations (Mots de passe services)

Votre IT manager vous demande de documenter le service DNS:  
- Vous y mettez quoi dedans?

Être lucide sur les éléments qui DOIVENT être documentés.

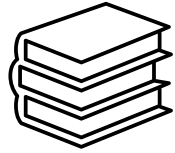
Les éléments de configurations principaux (primaires) = les attributs requis par les autres services.

- IP du serveur DNS

Les éléments de configurations pour restaurations ou contrôles:

- La liste des Records DNS, quand mis en place, par qui, pour qui, pour quoi, pour quelle durée...

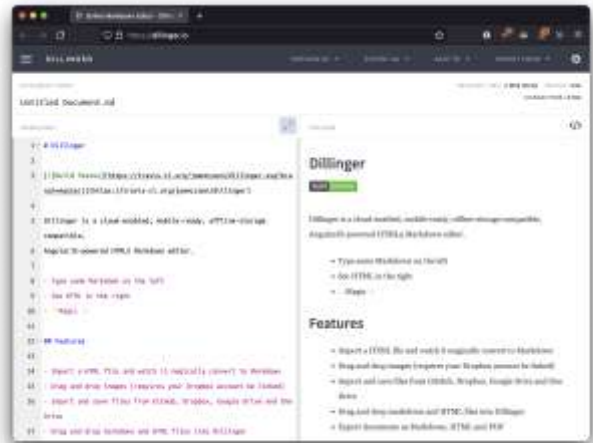
## Les outils pour documenter



- Traitement de textes
- Tableurs
- Schémas (Visio)
- Intranets (FAQ) en mode web
- Knowledge base (KB) ou bases de connaissances
  - Souvent associées aux plateformes de service desk et combiné avec inventaires
- [Github](#) ([markdown](#)), ou un [Google site](#)...

Et pour maintenir à jour des données massives et complexes?

=> **Inventaires !!**



On documente pour les autres, mais aussi pour soi-même.

Dans les contenus des inventaires, c'est la notion de CMDB. (sera repris plus loin)

### RECOMMANDATION:

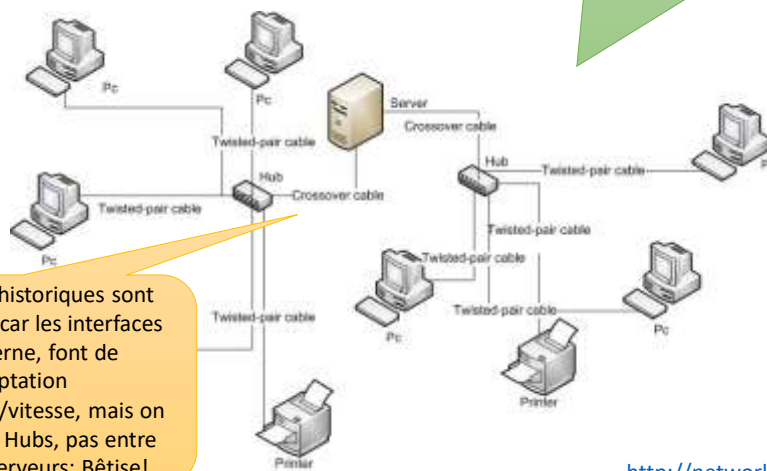
Se familiariser brièvement avec VISIO, version « online » fournie avec le compte @edu.iseig.ch

Utilisation de draw.io (EPSIC)



## Schémas de réseaux

[Computernetwork - Réseau informatique — Wikipédia \(wikipedia.org\)](https://fr.wikipedia.org/wiki/Computernetwork)



Les câbles croisés historiques sont devenus obsolètes car les interfaces Ethernet moderne, font de l'autoadaptation émission/réception/vitesse, mais on les utilisait entre 2 Hubs, pas entre des Hubs et des serveurs: Bêtise!

Quelles couches de l'OSI sont-elles présentées ici?  
Combien de réseaux y a-t-il ici?  
Et c'est quoi le Bug sur ce schéma?

<http://network.quicklearn.ch>

Source: Wikipedia

Réponse: Si le serveur héberge un routage IP entre ses 2 interfaces Ethernet, cela pourrait alors être un seul réseau au niveau 3, et 2 réseaux au niveau 2.

Sauf que ce schéma ne représente aucune information de la couche 3, c'est une représentation des couches 1 et 2 uniquement.

REVISION SUR LES RESEAUX:

Aller relire l'article <http://network.quicklearn.ch> (Pascal Kotté) pour comprendre le fonctionnement des réseaux, afin d'être capable de faire le «reverse engineering» et lire ou produire une documentation correcte.

EXERCICE EN CLASSE:

Comment représenteriez-vous les couches 3, et 7 ?

Utiliser draw.io ou Visio sur le compte @edu.iseig.ch



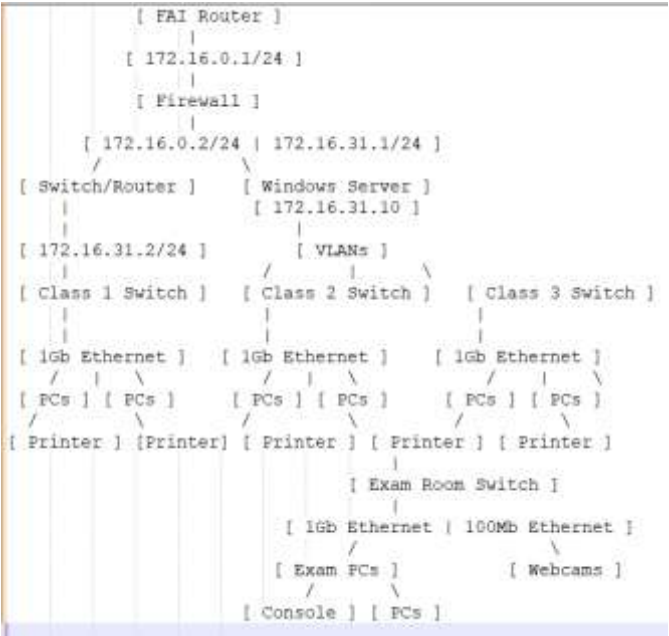
## Exercice – Dessiner et documenter le réseau ci-dessous

- 3 classes (école) de 12 pcs avec Ethernet 1Gb, avec 1 imprimante 100Mb chaque classe, dans 3 vlans séparés, connectées par un Switch 1/10Gb local dans chaque classe, raccordés à un 10 Gb switch/routeur central.
- 1 salle d'examen, avec 8 webcams sur un VLAN isolé (ip fixées 192.168.2.10 à 17 (routeur .1), 16 PCs Gb d'examens sur un VLAN identique à la console d'examens, tous sur le même switch 10Gb: IP=192.168.1.0/24, dhcp 10 à 99 pour les PC (routeur .1).
- 1 bureau avec 2 postes et 1 console d'examens, sur un 4<sup>ème</sup> Vlan. IP = 192.168.4.0/24, Switch routeur port 4, ip=192.168.4.1, dhcp:ip de 192.168.4.10 à 99, et photocopieur/scanner sur l'ip fixe 192.168.4.100.
- Tous les réseaux connectés à l'internet via un Firewall matériel, avec un routeur fourni par le FAI, dont l'IP publique est dynamique, mais l'IP interne est 172.16.0.1/24 sur l'IP du Firewall 172.16.0.2.
- Le switch routeur est connecté sur le Firewall avec l'IP 172.16.31.2/24 et le firewall avec 172.16.31.1
- L'école n'utilise que les services Microsoft 365 sans serveurs, excepté un vieux serveur Windows qui sert de DHCP, avec l'IP 172.16.31.10

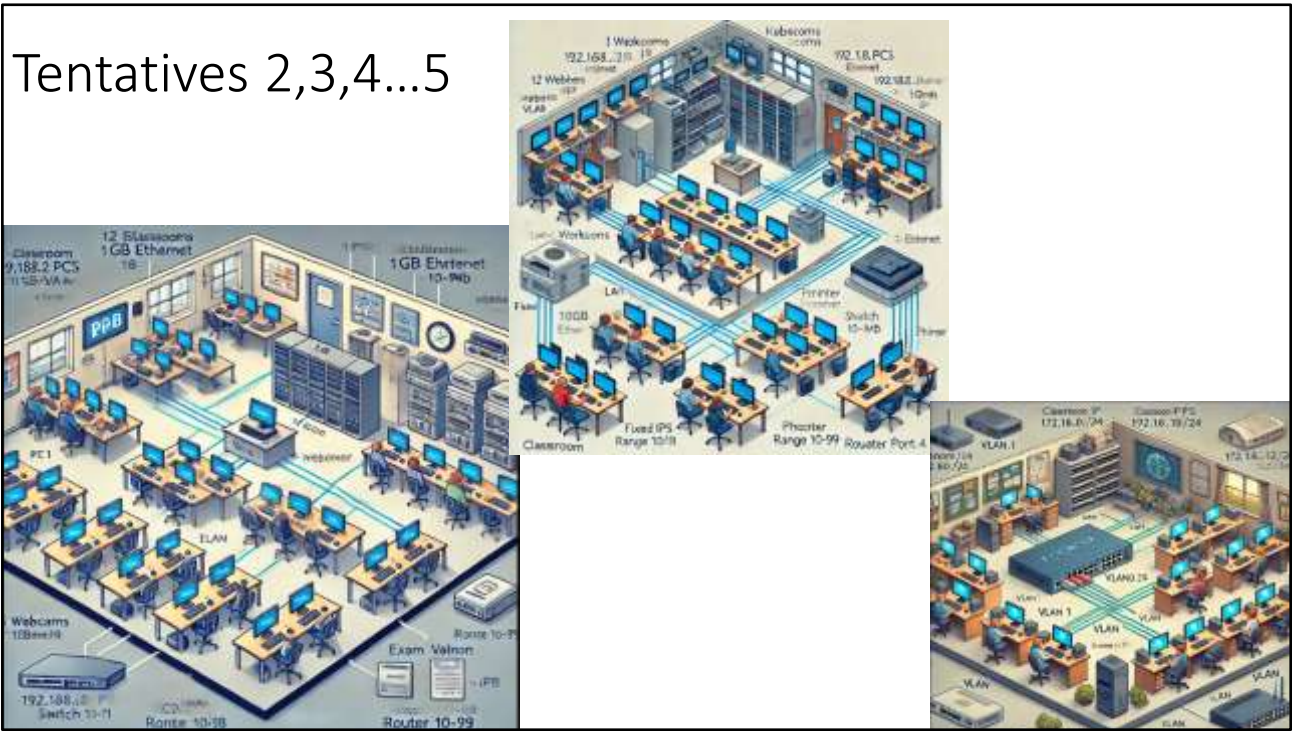
C'est volontairement mal fait! Afin de vous faire **ressortir la liste des questions pertinentes à poser**, pour compléter le schéma!

Utiliser draw.io ou Visio sur le compte @edu.seig.ch

Soluce  
ChatGPT=3/6



Tentatives 2,3,4...5



<pre>Internet     (IP publique dynamique)   [FAI: Routeur]   IP interne : 172.16.0.1/24    ----- (Connexion WAN)   [Firewall Matériel]   IP interne WAN : 172.16.0.2/24   IP interne LAN : 172.16.31.1/24    ----- (Connexion LAN)   [Switch/Routeur Central]   IP : 172.16.31.2/24   DHCP Server : 172.16.31.10    --- VLAN 10 (Classe 1)    --- [Switch Local]      --- PC 1 à 12 (IP DHCP : 192.168.10.x)      --- Imprimante (IP fixe : 192.168.10.100)    --- VLAN 20 (Classe 2)    --- [Switch Local]      --- PC 1 à 12 (IP DHCP : 192.168.20.x)      --- Imprimante (IP fixe : 192.168.20.100)    --- VLAN 30 (Classe 3)    --- [Switch Local]      --- PC 1 à 12 (IP DHCP : 192.168.30.x)      --- Imprimante (IP fixe : 192.168.30.100)    --- VLAN 40 (Salle d'examen)    --- [Switch 10 Gb]      --- PC 1 à 16 (IP DHCP : 192.168.1.10-99)      --- Webcam 1 à 8 (IP fixe : 192.168.2.10-17)    --- VLAN 50 (Bureau)    --- [Switch Local]      --- Poste 1 et 2 (IP DHCP : 192.168.4.10-99)      --- Console d'examen (IP DHCP : 192.168.4.x)      --- Photocopieur/Scanner (IP fixe : 192.168.4.100)</pre>	<p>Pour créer un schéma fidèle avec toutes les machines correctement connectées sur les VLAN et LAN correspondants, voici une représentation structurée sous forme de diagramme textuel en couches. Chaque machine, switch, et routeur sera positionné dans le bon segment réseau.</p> <p>Schéma textuel détaillé :</p> <p><b>Légende</b></p> <ol style="list-style-type: none"><li>Routeur FAI - Firewall<ul style="list-style-type: none"><li>Gère la connexion à Internet.</li><li>Lien entre l'extérieur et le réseau interne.</li></ul></li><li>Firewall - Switch central<ul style="list-style-type: none"><li>Protège et isole les VLAN du réseau interne.</li></ul></li><li>Switch central - VLANs<ul style="list-style-type: none"><li>Sépare chaque salle (classes, bureau, salle d'examen) en VLAN distincte pour isoler le trafic.</li></ul></li><li>Switch locaux - Équipements<ul style="list-style-type: none"><li>Distribue les connexions Ethernet aux PC, imprimantes, webcams, et autres équipements locaux.</li></ul></li></ol> <p>Ce schéma met en avant la topologie réseau, en respectant vos contraintes techniques. Je peux également vous fournir une version graphique si cela vous est utile.</p>
--	--

## Les plateformes (semi) automatisées



Logiciels d'inventaires plus ou moins évolués

- Avec ou sans agents de mises à jour automatisés
- Avec ou sans rapprochement avec les droits et la structure business de l'organisation (Organigramme)

La notion de [CMDB](#) (ITIL v2) ou [CMS](#) (ITIL v3) *Configuration Management DataBase ou System*. Doit fournir les informations à jour (automatiques) **AVEC** les instructions sur les droits d'accès validés (avec traçabilité). Cf. part.5 +loin



[https://fr.wikipedia.org/wiki/Information\\_Technology\\_Infrastructure\\_Library](https://fr.wikipedia.org/wiki/Information_Technology_Infrastructure_Library)

On a évoqué: GLPI, iTOP <https://www.combodo.com/itop> , ServiceNow, Zabbix, OTRS, SCCM... CF aussi en annexe.

Mais on a une profusion de solutions...

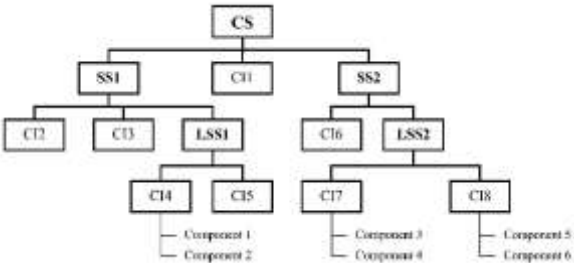
Parfois, plusieurs simples, peuvent paraître plus facile à mettre en œuvre qu'une grosse intégrée, et s'avérer requérir des redondances opérationnelles,

Parfois une grosse solution intégrée, ne sera utilisée qu'à 10 ou 20% car compliquée à mettre en œuvre.

A disposition pour en causer dans vos structures, <http://call.kotte.net>

# Gestion des configurations

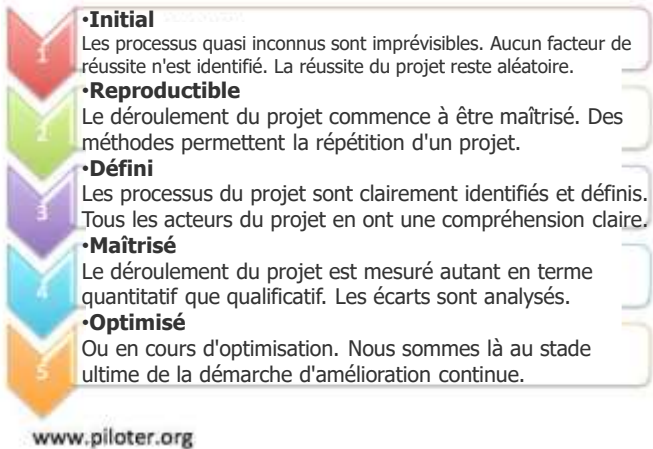
(ISO 10007) = qualité  
ITIL (ISO 20000)  
CDMB => CMS  
COBIT (ISO9000) = ISACA  
ISO 27000 (39p) = sécurité



Mais pas la gestion des droits d'accès et des autorisations...

Et non! ADUC ne peut pas être considéré comme une base documentaire

## Les 5 niveaux de maturité du modèle CMMI



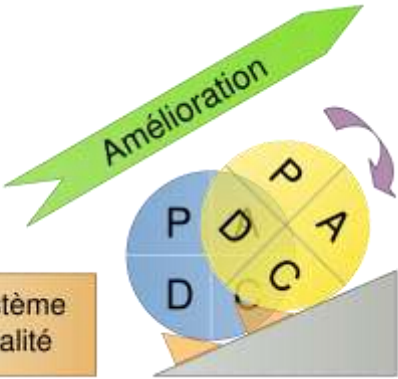
Ces éléments sont du ressort de l'IT manager, des ingénieurs, pas des opérateurs/techniciens – Mais c'est important d'avoir un aperçu des éléments qui conditionnent les organisations IT et leurs documentations.

[https://fr.wikipedia.org/wiki/Gestion\\_de\\_configuration](https://fr.wikipedia.org/wiki/Gestion_de_configuration)  
Qualité - [https://fr.wikipedia.org/wiki/ISO\\_10007](https://fr.wikipedia.org/wiki/ISO_10007)  
Organisation – ITIL - [https://fr.wikipedia.org/wiki/ISO/CEI\\_20000](https://fr.wikipedia.org/wiki/ISO/CEI_20000)  
<https://fr.wikipedia.org/wiki/COBIT>  
[https://www.piloter.org/gouvernance/CMMI\\_gouvernance\\_SI.htm](https://www.piloter.org/gouvernance/CMMI_gouvernance_SI.htm)  
<https://cmmiinstitute.com/company> = ISACA  
[https://fr.wikipedia.org/wiki/ISO/CEI\\_27000](https://fr.wikipedia.org/wiki/ISO/CEI_27000) = Sécurité

# Gestion des procédures et des incidents

L'amélioration de la qualité des services dépend aussi, de la capacité à documenter correctement les incidents, et identifier les problèmes sous-jacents afin d'en réduire les occurrences. *(Par ex. faire un manuel ou une checklist pour éviter d'oublier une étape la prochaine fois...)*

## Roue de Deming



1=5W who,what,where,when,why

2 = Test + Prod

- 1. **Plan** : préparer, planifier (ce que l'on va réaliser) ;
- 2. **Do** : développer, réaliser, mettre en œuvre (le plus souvent, on commence par une phase de test) ;
- 3. **Check** : contrôler, vérifier ;
- 4. **Act** (ou **Adjust**): agir, ajuster, réagir (si on a testé à l'étape *do*, on déploie lors de la phase *act*).

Ces éléments sont du ressort de l'IT manager, des ingénieurs, pas des opérateurs/techniciens – Mais c'est important d'avoir un aperçu des éléments qui conditionnent les organisations IT et leurs documentations.

[Roue de Deming — Wikipédia \(wikipedia.org\)](#)

[https://fr.wikipedia.org/wiki/Roue\\_de\\_Deming](https://fr.wikipedia.org/wiki/Roue_de_Deming)

<https://fr.wikipedia.org/wiki/QQQQCCP>

[https://fr.wikipedia.org/wiki/D%C3%A9coupage\\_de\\_l'information\\_par\\_priorit%C3%A9](https://fr.wikipedia.org/wiki/D%C3%A9coupage_de_l'information_par_priorit%C3%A9)

<https://medium.com/conseillers-num%C3%A9riques-suisse-romands/criticite%C3%A9-3da6955752a9>



## Incidents / problèmes sur les services



- Selon ITIL

- Incident = un ticket d'assistance (initialement incluant aussi demandes standards, maintenant on différencie les incidents, des demandes)
  - Incident = quelque chose qui fonctionnait avant, ne fonctionne plus
  - Demande = nouvelles configurations, aide pour utilisation...
- Problème = une situation qui peut générer plusieurs incidents
  - Court terme = une interruption identifiée de service = «incident principal» (master) et les autres incidents peuvent y être «raccordés». (incident parent / incidents enfants)
  - Long terme = problème, une analyse posée des incidents effectifs le plus d'impacts sur la productivité, afin de générer des améliorations pour en réduire les occurrences (formations, documentation, automatisation, corrections...)

- ISTQB: incident = Erreur, problème = défaillance.

Gestion des risques, dans un catalogue de services ICT: <https://medium.com/conseillers-num%C3%A9riques-suisse-romands/criticit%C3%A9-3da6955752a9>

Une plateforme de helpdesk comme Easyvista, Servicenow, Zendesk, FreshDesk (FreshWorks), vont normalement proposer de gérer des tickets avec la résolution d'incident parent, et auto-cloture des incidents enfants.

## B: (5). Administrer les droits d'accès

Administrer et documenter les autorisations selon le concept d'autorisations en vigueur.

5. Administrer et documenter les autorisations selon le concept d'autorisations en vigueur.

5.1 Connaître le contenu, la structure et l'application d'un concept d'autorisations.

5.2 Connaître les possibilités des services pour définir des autorisations d'accès à des ressources.

5.3 Connaître la procédure pour adapter des autorisations selon le concept existant d'une entreprise.

5.4 Connaître des méthodes pour documenter les adaptations d'autorisations.

## Comment je sais les droits attribués aux utilisateurs ?



Chaque service applicatif pour les usagers, tout comme les services d'infrastructures, doivent disposer de:

- Des profils de configurations explicites des droits d'accès à des données ou applications, surtout si elles comprennent:
  - Des données personnelles (Soumise aux lois LPD en Suisse, RGPD en Europe)
  - Des données personnelles sensibles (mêmes lois)
  - Des données techniques ou économiques sensibles
- Un enregistrement des ordres d'autorisations délivrées, par les décideurs eux-mêmes autorisés.
- Un état présentable des bénéficiaires validés en cas d'audit de contrôle, ou une nécessaire remise en service « from scratch ». Inventaire des droits.

En clair: Si je veux « auditer » pour vérifier qui est censé avoir accès à quoi ?

Le plus simple est la création de « profils rôles » dans l'entreprises, et pour chaque, établir la liste des « droits nécessaires » dans l'IT.

Puis de disposer d'une liste mise à jour par les RH, de qui est avec quels rôles...

L'IT doit appliquer les droits, voir les RH directement, afin de s'assurer d'avoir un accès limité à mes besoins et mes « pouvoirs ».

## Profils de configurations «utilisateur»



Pour une application métier, comme une «comptabilité», ce n'est pas à l'IT d'attribuer les «règles d'accès», mais au responsable métier (chef comptable, CFO) de déterminer quelles règles existent, et doivent être attribuées à qui.

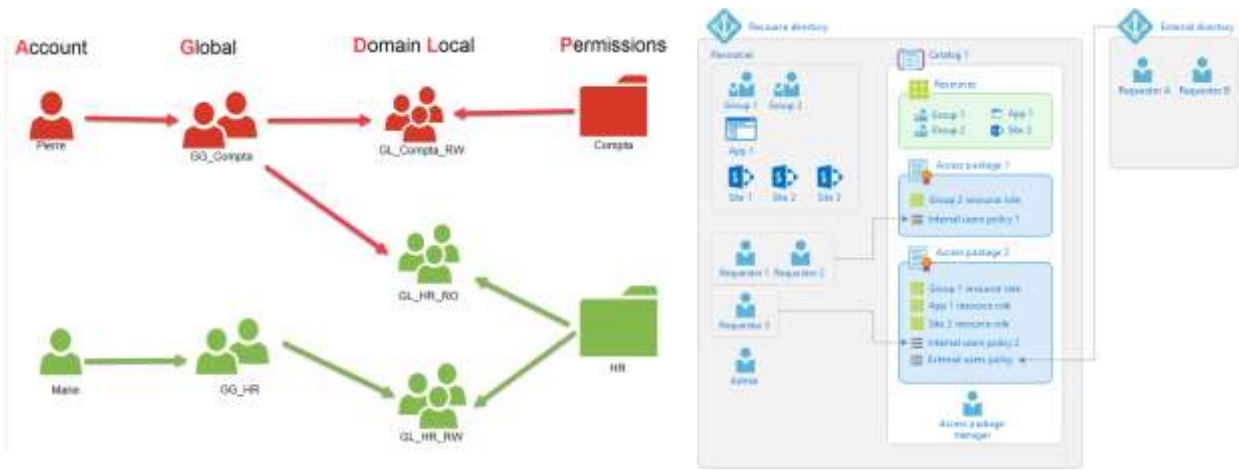
Le rôle de l'IT, sera de se donner les moyens:

- De ne pas se tromper (et conserver les traces/preuves)
- De conserver les assignations pour pouvoir remettre en œuvre le tout correctement, en cas de «crash rebuild»
- De ne pas oublier de révoquer les droits quand cela est nécessaire, et le rappel aux métiers, et aux RH, d'avertir l'IT.

C'est pour faire cela correctement, qu'existe ITIL ou COBIT...

La mise en application est généralement intégrée dans AD (Active Directory), avec des droits inclus

# AGDLP

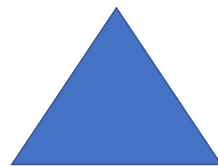


Droits NTFS, et AGDLP...  
<https://rdr-it.com/blog/agdpl-agudlp-comment-bien-gérer-les-droits-sur-un-serveur-de-fichiers-windows-serveur/>

- Ce qu'il faut retenir, c'est
1. la nécessaire création de groupes globaux, explicites, pour gérer les «profils»:
    - Qui est censé avoir droit, à faire quoi?
  2. Des groupes et settings de sécurité doivent alors être mis en œuvre pour appliquer correctement les droits aux membres de ces groupes.
  3. Un processus traçable et clair doit permettre de suivre l'ajout en la suppression des membres dans ces groupes.
    - Qui a décidé, quand, et fait-il partie de la «liste des personnes» autorisées.

Mode étendu et advanced:  
<https://learn.microsoft.com/fr-fr/azure/active-directory/governance/entitlement-management-overview>

## Liste des Autorisations



Les assignations individus / droits d'accès doivent être répertoriées afin d'en permettre la vérification effective par un tiers (audit).

Question:

- Est-ce que l'AD peut servir de base documentaire pour faire cela ?
- Pourquoi ?

La réponse est NON

Car même si les assignations dans une compta étaient ensuite faites manuellement, en regardant un nom de service, ou un groupe dans l'AD: On ne saurait pas si une personne n'a pas modifié cela dans l'AD par la suite, ni par qui (ou pas très facilement).

Que ce soit manuel ou automatique, AD va configurer des droits, selon des instructions qui doivent être externes à l'AD, accessible et lisible par un auditeur.

# Et les mots de passe?



- Puis-je demander/accepter un mot de passe d'un utilisateur, pour dépanner une poste/une application pour cet utilisateur?

Non, bien entendu

LA délégation des droits d'accès sur des données privées nécessite un contrat spécifique, et de confiance qui est délicat.



Cela veut dire que vous devez refuser les mots de passe de vos utilisateurs.  
Et leur demander de le saisir.

## Mise en pratique, droit d'un partage (fileshare)

- Comment cela se passe-t-il chez vous ?

Comment s'assurer que les personnes qui sont autorisées, le sont bien par les bonnes personnes responsables, et non sur «une information» volante et approximative. Et comment puis-je tracer l'information



### Atelier Pratique avec Azure

- Créer un « Dossier partagé » accessible uniquement par la personne autorisée. Qu'il pourra monter sur sa machine (lecteur réseau) ou ouvrir via «Azure Storage Explorer»

Cela doit passer par votre compte étudiant "gratuit" @edu.iseig.ch, avec 100\$ de crédit Azure.

[https://microsoftlearning.github.io/AZ-104-](https://microsoftlearning.github.io/AZ-104-MicrosoftAzureAdministrator/Instructions/Labs/LAB_07-Manage_Azure_Storage.html)

[MicrosoftAzureAdministrator/Instructions/Labs/LAB\\_07-Manage\\_Azure\\_Storage.html](https://microsoftlearning.github.io/AZ-104-MicrosoftAzureAdministrator/Instructions/Labs/LAB_07-Manage_Azure_Storage.html)

<https://learn.microsoft.com/fr-fr/azure/storage/files/storage-files-introduction>



## Création et gestion d'un fileshare dans Azure

- Monter et gérer un service via un Cloud – <http://azure.com/>

Via le compte étudiant @edu.iseig.ch et sélectionner 1 collègue pour y accéder (toujours sur son compte @edu.iseig.ch)

<https://azure.microsoft.com/fr-fr/free/students/>

[AZ-103-MicrosoftAzureAdministrator/03 - Implement and Manage Storage \(az-103-MicrosoftAzureAdministrator \(github.com\)\)](#)

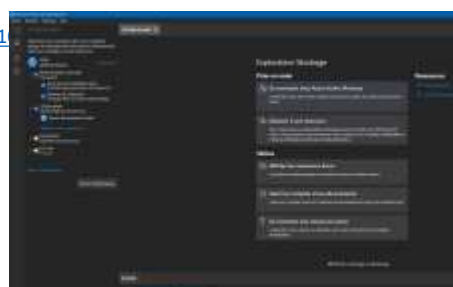
<https://azure.microsoft.com/en-us/features/storage-explorer/>

Cf. [Microsoft Virtual Training Days](https://mvtd.events.microsoft.com/) <https://mvtd.events.microsoft.com/>

<https://mvtd.events.microsoft.com/Azure>

[Présentation d'Azure Files | Microsoft Learn](#)

<https://learn.microsoft.com/fr-fr/azure/storage/files/storage-files-introduction>



[https://github.com/CloudReady-ch/ISEIG-](https://github.com/CloudReady-ch/ISEIG-LAB/blob/faddabe644708d6a0808e5755af75d39c7740a0a/AZ-103/01.AzurAdmin.md)

[LAB/blob/faddabe644708d6a0808e5755af75d39c7740a0a/AZ-103/01.AzurAdmin.md](https://github.com/CloudReady-ch/ISEIG-LAB/blob/faddabe644708d6a0808e5755af75d39c7740a0a/AZ-103/01.AzurAdmin.md)

[https://github.com/CloudReady-ch/AZ-103-](https://github.com/CloudReady-ch/AZ-103-MicrosoftAzureAdministrator/blob/master/Instructions/Labs/03%20Implement%20and%20Manage%20Storage%20(az-100-02).md)

[MicrosoftAzureAdministrator/blob/master/Instructions/Labs/03%20Implement%20and%20Manage%20Storage%20\(az-100-02\).md](https://github.com/CloudReady-ch/AZ-103-MicrosoftAzureAdministrator/blob/master/Instructions/Labs/03%20Implement%20and%20Manage%20Storage%20(az-100-02).md)

Nouvelle version

[https://microsoftlearning.github.io/AZ-104-](https://microsoftlearning.github.io/AZ-104-MicrosoftAzureAdministrator/Instructions/Labs/LAB_07-Manage_Azure_Storage.html)

[MicrosoftAzureAdministrator/Instructions/Labs/LAB\\_07-Manage\\_Azure\\_Storage.html](https://microsoftlearning.github.io/AZ-104-MicrosoftAzureAdministrator/Instructions/Labs/LAB_07-Manage_Azure_Storage.html)

### Autres docs découvertes

[https://mvtd.events.microsoft.com/?ocid=AID3032310\\_QSG\\_529831](https://mvtd.events.microsoft.com/?ocid=AID3032310_QSG_529831)

<https://learn.microsoft.com/en-us/azure/storage/files/storage-how-to-create-file-share?tabs=azure-portal> x3

<https://jeffbrown.tech/azure-files/>

<https://youtu.be/H04e9AgbcSc>

## Gestion des comptes «machines»

Dans le catalogue des services IT délivrés aux utilisateurs, se trouve la mise à disposition et la maintenance d'un poste de travail.

- 30 (à 90) jours sans être allumé et connecté, selon les organisations: Un PC Windows membre d'une AD ne permettra plus d'être utilisé pour se connecter aux ressources du domaine de l'organisation.
  - Correction: dans AD/ordinateurs reset du compte computer + avec un compte local admin sur le poste: Remis en mode «workgroup» (déconnecter du domaine) et le reconnecter.



<https://learn.microsoft.com/fr-fr/troubleshoot/windows-server/identity/troubleshoot-errors-join-computer-to-domain>

<http://support.microsoft.com/?kbid!6393>

<https://support.microsoft.com/en-us/topic/resetting-computer-accounts-in-windows-762e3208-0e05-1696-75fa-333d90717d1e>

<https://forums.commentcamarche.net/forum/affich-1650439-probleme-connexion-controlleur-de-domaine>

Comment mesurer et afficher des compteurs pour évaluer la performance d'un système.  
Comment collecter et surveiller les tendances et évolutions, y compris à travers un réseau.

## C: 2+4. Monitoring, add counters

Surveiller et exploiter les services en utilisant les outils à disposition.

Intégrer les systèmes dans les outils de monitoring existants et vérifier les valeurs mesurées.

2. Surveiller et exploiter les services en utilisant les outils à disposition.

2.1 Connaître les outils intégrés dans le système d'exploitation et dédiés à sa surveillance ainsi que leur domaine d'application.

2.2 Connaître les principales valeurs de mesure de la performance et pouvoir les interpréter.

4. Intégrer les systèmes dans les outils de monitoring existants et vérifier les valeurs mesurées.

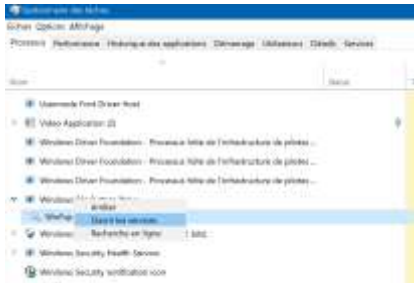
4.1 Connaître des techniques possibles (p. ex. SNMP, WMI) pour la saisie centralisée des données de performance et leurs mécanismes de sécurité.

4.2 Connaître les étapes de configuration à effectuer sur un système de serveur pour activer les mesures de performance (p. ex. SNMP, WMI).

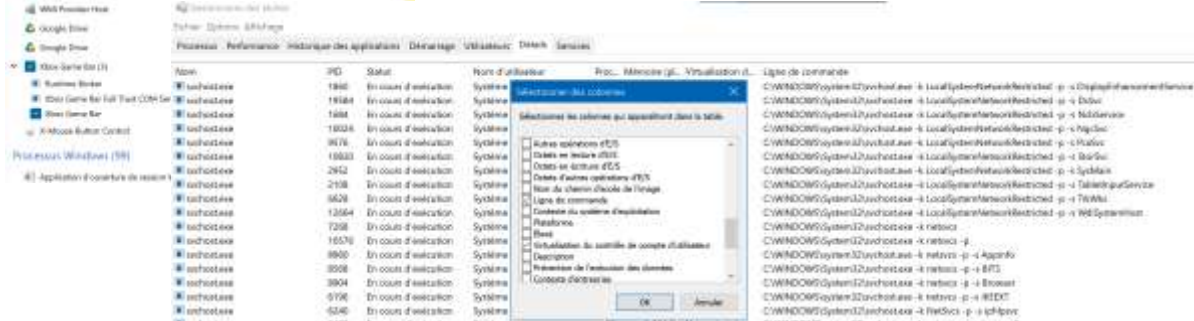
4.3 Connaître les étapes pour intégrer les serveurs dans un outil de monitoring existant.

4.4 Connaître des possibilités pour définir des valeurs seuils judicieuses et installer une alarme.

# Task manager (gestionnaire de tâches) - AGAIN

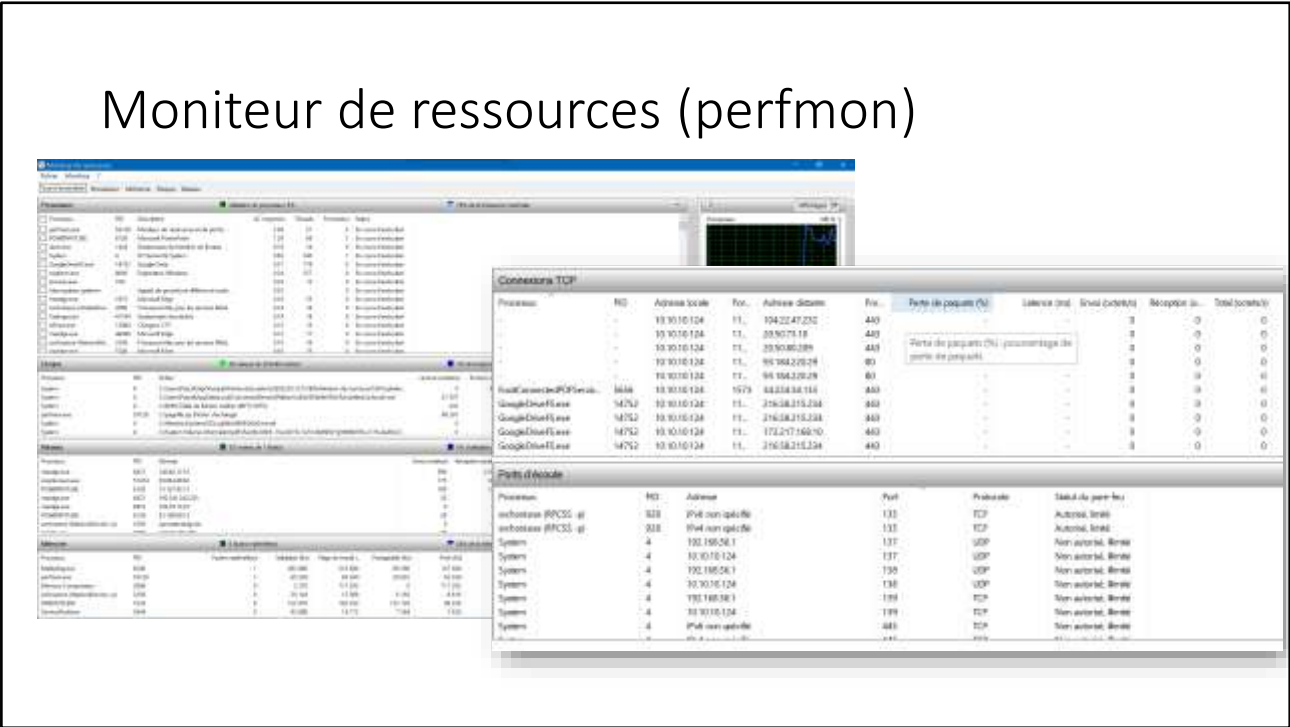


Pour mieux retrouver les services/processus associés à quoi, ou qui  
Afficher la colonne «ligne de commande»

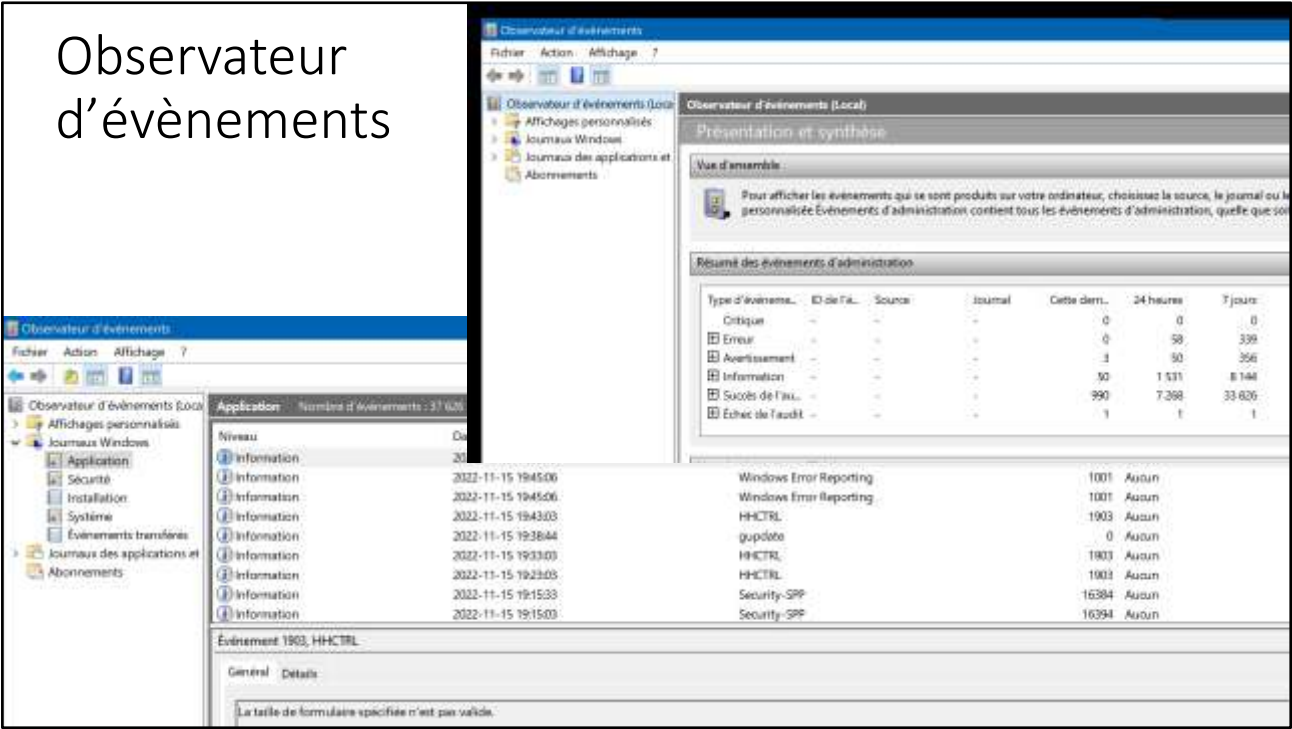


Ctrl-alt.-del > Task manager, ou clic droit sur la barre des tâches: Il permet «Gestionnaire des tâches»

## Moniteur de ressources (perfmon)



Cet outil est fondamental pour explorer et détecter ce qu'il se passe « maintenant » sur la machine (Windows).



C'est l'application centrale et lieu pour surveiller la bonne santé d'un ordinateur.

# Outils de mesure des performances

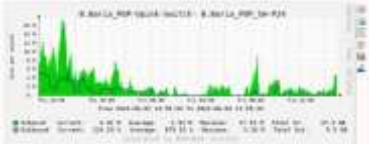
## Systèmes (windows/linux/mobile)

- Task manager
- Perfmon
- Analyseur de performances
- Tierces (Speecy,

On va voir cela juste après

## Réseaux (NMS)

- MRTG (perl multiOS)
- Cacti



SNMP/local Agents/https

## Supervision

- Ex. Nagios
- Zabbix (Linux)



[https://fr.wikipedia.org/wiki/Network\\_management\\_station](https://fr.wikipedia.org/wiki/Network_management_station)

[https://fr.wikipedia.org/wiki/Multi\\_Router\\_Traffic\\_Grapher](https://fr.wikipedia.org/wiki/Multi_Router_Traffic_Grapher)  
<https://github.com/oetiker/mrtg>

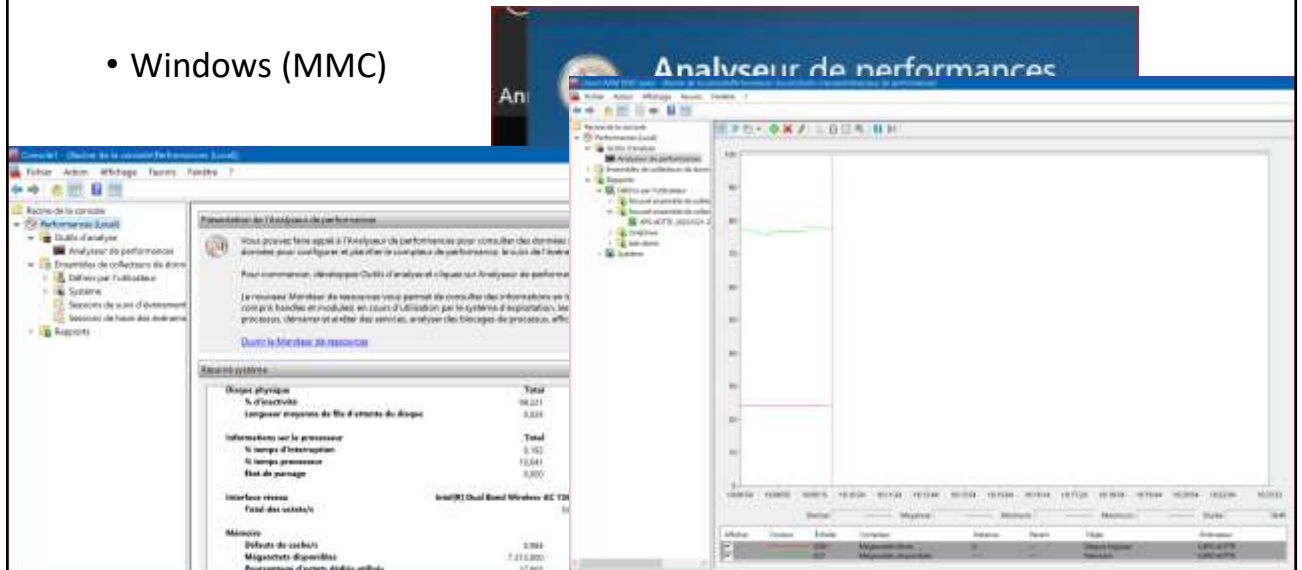
<https://fr.wikipedia.org/wiki/Cacti>  
<https://github.com/Cacti/cacti>

[https://fr.wikipedia.org/wiki/Supervision\\_\(informatique\)](https://fr.wikipedia.org/wiki/Supervision_(informatique))

<https://www.lemagit.fr/conseil/Monitoring-reseau-les-7-outils-Open-source-quil-vous-faut>  
<https://geekflare.com/fr/best-open-source-monitoring-software/>

## Mise en pratique – Analyseur performance

- Windows (MMC)



### Analyseur de performances

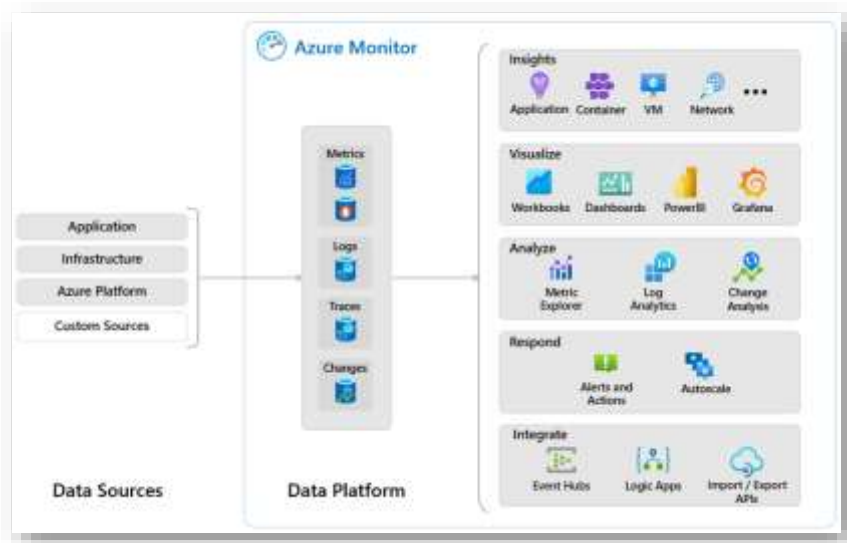
- Modifier la durée totale, exemple, mesurer sur 10h au total: Check que du coup nécessaire plus petite durée intervalle sera de 36 secondes...
- Repérer les mises à l'échelle des compteurs sélectionnés. (Clic droit sur les compteurs)
- MMC – jouer avec Multiples Analyseurs, et sauvegarder...
- Monitorer plusieurs compteurs de différentes machines sur le même graphique.



## Azure Monitor et ++ solutions/marché

- Pour Linux [M/Monit](#)
- ManageEngine RMM Central
- Spicework
- [Servicenow](#)
- [Acronis\(?\)](#)
- ...

Cf. Annexes



Stage 2...

Cf. jouer avec Azure Monitoring

<https://learn.microsoft.com/en-us/azure/azure-monitor/overview>

<https://blog.netwrix.fr/2018/11/21/les-10-meilleurs-outils-logiciels-de-surveillance-de-windows-server/>

<https://mmonit.com/wiki/MMonit/SupportedPlatforms>

<https://www.getapp.fr/directory/1767/remote-monitoring-and-management/software>

[NetFlow — Wikipédia \(wikipedia.org\)](https://fr.wikipedia.org/wiki/NetFlow)

# Standards réseaux, monitoring

- [ICMP](#) (ping)
- [SNMP](#) (mrtg,cacti,zabbix...)

## Service

- [ARP](#) (identifier MAC adrs)  
  ipv4
- [DNS](#)
- DHCP

SNMP object ID	Device Type	Manufacturer	Device Model	Resource Type
1.3.6.1.4.1.789	San Device	NetApp		Network Attached Storage
1.3.6.1.4.1.4326	Switch	NetGear		Infrastructure Device
1.3.6.1.4.1.4326.3	Switch	NetGear		Infrastructure Device
1.3.6.1.4.1.3324.1	Router	NetScreen		Infrastructure Device
1.3.6.1.4.1.3324.1.7	Router	NetScreen	Firewall	Infrastructure Device
1.3.6.1.4.1.23.1.6	Server	NetWare	Server	Computer
1.3.6.1.4.1.46	Switch	Nortel		Infrastructure Device
1.3.6.1.4.1.1872	Switch	Nortel		Infrastructure Device
1.3.6.1.4.1.2172	Switch	Nortel		Infrastructure Device
1.3.6.1.4.1.45.3	Switch	Nortel	BayStack Product	Infrastructure Device
1.3.6.1.4.1.36.2.15.3.9.1	Switch	RoamAbout	Access Point	Infrastructure Device
1.3.6.1.4.1.59.1.2.3	Workstation	Silicon Graphics		Computer
1.3.6.1.4.1.2389.3.1.3.1.2	Printer	Sharp		Network Printer
1.3.6.1.4.1.202	Switch	SMC		Infrastructure Device
1.3.6.1.4.1.42.2.1.1	Unit	Sun		Computer
1.3.6.1.4.1.42.2.12.9.3.3	Unit	Sun		Computer
1.3.6.1.4.1.42.2.28.13.3.14.1	San Device	Sun	StoreEdge	Network Attached Storage
1.3.6.1.4.1.128.2.1.4	Printer	Tektronix		Network Printer
1.3.6.1.4.1.255.8.62.1	Printer	Xerox		Network Printer
1.3.6.1.4.1.8072.3.3.10	Linux			Computer

[https://fr.wikipedia.org/wiki/Internet\\_Control\\_Message\\_Protocol\\_V6](https://fr.wikipedia.org/wiki/Internet_Control_Message_Protocol_V6)  
[https://fr.wikipedia.org/wiki/Simple\\_Network\\_Management\\_Protocol](https://fr.wikipedia.org/wiki/Simple_Network_Management_Protocol)  
[https://fr.wikipedia.org/wiki/Address\\_Resolution\\_Protocol](https://fr.wikipedia.org/wiki/Address_Resolution_Protocol)

adresse IP privée automatique (APIPA), il aura une adresse IP 169.254.\*.\*  
[https://fr.wikipedia.org/wiki/Automatic\\_Private\\_Internet\\_Protocol\\_Addressing](https://fr.wikipedia.org/wiki/Automatic_Private_Internet_Protocol_Addressing)  
Adresse IP privées: 10.\*.\*.\*, 172.16-31.\*.\*, 192.168.\*.\*  
[https://fr.wikipedia.org/wiki/R%C3%A9seau\\_priv%C3%A9](https://fr.wikipedia.org/wiki/R%C3%A9seau_priv%C3%A9)

<https://ipcost.com/fr>  
<https://www.myip.com/>  
<https://mon-ip.info/>

nslookup myip.opendns.com resolver1.opendns.com

<https://fr.wikipedia.org/wiki/IPv6>  
<http://www.ipv6-test.ch/>

What Is My IP Address

My IP Address

IP address

62.202.191.12

Hostname

12.191.202.52.dynamic.cust.swisscom.net

IP Address Location

Country

Switzerland (CH)

State/Region

Vaud

City

ISP

Swisscom Internet Services AG - Ethernet

Organization

Network

Usage Type

Corporate / Business

Timezone

CET

Local Time

Thu, 03 Oct 2024 20:12:59 +0200

Coordinates

46.16270

IPv6 Leak Test

IPv6 Address

N/A

WebRTC Leak Test

Local IP address

192.168.1.110

Public IP address

62.202.191.12

• NAT et ip privées et ip publiques (ipv4)

• <https://browserleaks.com/ip>

• <https://www.myip.com/>

• <https://ipcost.com/fr>

• <https://whatismyipaddress.com/>

IP Class

Starting IP

Ending IP

Def Subnet mask

No of hosts

Class A

10.0.0.0

10.255.255.255

255.0.0.0

1,67,77,216

Class B

172.16.0.0

172.31.255.255

255.255.0.0

10,48,576

Class C

192.168.0.0

192.168.255.255

255.255.255.0

65,536

Class D

224.0.0.0

239.255.255.255

No subnet mask. For Multicasting

Class E

240.0.0.0

255.255.255.254

No subnet mask. For R&D

169.254.\*\*\*.\*\*\*

Automatic Private IP addressing (APIPA)

Network Connection Details

Property

Value

Connection-specific DNS Suffix

Description

144 (P5) Dual Band Wireless AC 11AB

Physical Address

38-63-74-B9-4B-F1

DHCP Enabled

Yes

Automatic Private IP Address

169.254.110.10

IPv6 Address

2002::1

Voir aussi

<https://test-ipv6.com/>

[What Is My IP Address? - ifconfig.me](https://ifconfig.me/)

<https://ifconfig.me/> avec possibilité de le faire en ligne de commande

69

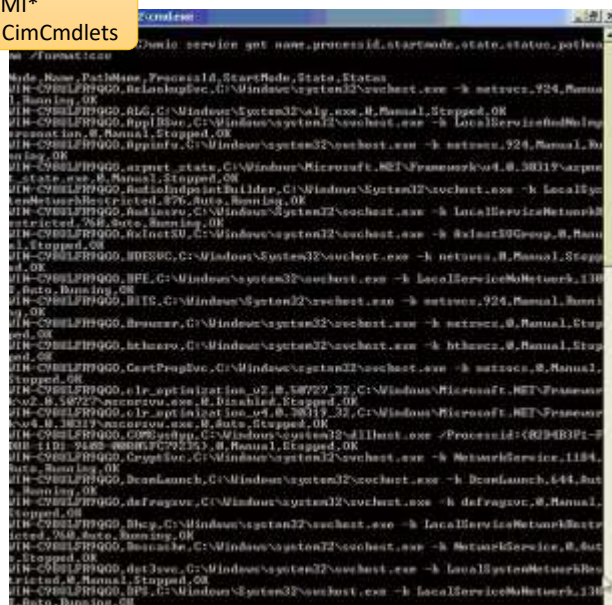
## WMIC & commandes Windows

Get-Command -Noun WMI\*

### Get-Command -Module CimCmdlets

- **WMIC** => (w10) **PowerShell CMI** Get-Command -Module
- **Sc** (sc qc <service>, sc stop <service> )
- **Net** (net statistics WORKSTATION) SMB uniquement
  - Net stop <service>
- **Nbtstat** (Netbios infos)
- **Netstat** -ab (IP infos +ports écoutes)
  - [https://fr.wikipedia.org/wiki/Liste\\_de\\_ports\\_logiciels](https://fr.wikipedia.org/wiki/Liste_de_ports_logiciels)
- **Arp** -a
  - Gère les MAC addresses Ethernet (ip v4)
  - netsh interface ipv6 show neighbors (ip v6)
- **Ping** (utilise ICMP)
  - Souvent désactivé par sécurité
- **Ipconfig** (dhcp actions)
  - Identification des DNS, DHCP, Routeur
- **Nslookup** (dns actions)
- **Tracert** (traceroute) lister les réseaux (hop)
- ...

**Astuce:** commande `> fichier.txt` pour créer un fichier texte avec le résultat.



[https://fr.wikipedia.org/wiki/Windows\\_Management\\_Instrumentation](https://fr.wikipedia.org/wiki/Windows_Management_Instrumentation)

<https://www.malekal.com/tutoriel-wmic>

<https://www.malekal.com/netstat-lister-connexions-ports-ouverts-windows>

<https://www.malekal.com/liste-des-ports-ports-reseaux-de-connexion-et-ce-que-cest>

A noter que getmac ne permet que d'avoir les MAC locales à la machine (ipconfig /all le fait aussi bien)

```
getmac /v /fo list
```

```
netsh interface ipv6 show int
```

```
netsh interface ipv6 show neighbors interface=43
```

(ou remplacer 43 par le bon

index de l'interface souhaitée)

Windows Management Instrumentation (WMI) est l'implémentation de Microsoft du Web-Based Enterprise Management (WBEM), le standard du Distributed Management Task Force (DMTF). Il prend en charge le modèle de données CIM (Common Information Model), qui décrit les objets d'un environnement de gestion. WMI s'exécute en tant que service portant le nom d'affichage « Windows Management Instrumentation » et le nom de service « winmgmt ». D'autres

services qui dépendent du service WMI s'arrêtent également, tels que l'hôte de l'Agent SMS ou le pare-feu Windows. ([Sources](#))

L'utilitaire de ligne de commande [WMIC](#) fournit une interface de ligne de commande pour Windows Management Instrumentation (WMI). Il est compatible avec les interpréteurs de commandes et les commandes utilitaires existantes.

Cet outil est déconseillé à partir de Windows 10, version 21H1 et à partir de la version de canal semi-annuel 21H1 de Windows Server. L'utilitaire est remplacé par Windows PowerShell pour WMI.

<https://nicolascoolman.eu/2022/02/12/microsoft-deprecie-loutil-windows-wmic>

```
C:\Windows\System32>wmic csproduct get name
```

```
Name
```

```
Aspire A515-58M
```

```
C:\Windows\System32>WMIC Bios get serialnumber
```

```
SerialNumber
```

```
NXKHGEZ00931301B683400
```

# Exercice: traceroute (-h40 -d)

Pourquoi, des lignes \* \* \* et aussi temps morts après le 3 valeurs ms, pour les lignes qui affichent une IP seulement

C:\Users\pascal>tracert geneve.ch

Détermination de l'itinéraire vers geneve.ch [193.134.183.201]  
avec un maximum de 30 sauts :

1 1 ms 1 ms 1 ms internetbox.hum [192.168.1.1]  
2 43 ms 34 ms 4 ms 100.85.192.1  
3 0 ms 4 ms 3 ms ae22-1150.lpc-lss090-w-pe-08.bluelwin.ch [213.3.220.253]  
4 0 ms 3 ms 3 ms eth12-1150.lsic120p-cys001.bluelwin.ch [213.3.220.254]  
5 5 ms 5 ms 4 ms 213.3.220.189  
6 5 ms 4 ms 3 ms 1001as-015-as11.bb-ip-plus.net [193.134.95.66]  
7 \* \* \* Délai d'attente de la demande dépassé.  
8 \* \* \* Délai d'attente de la demande dépassé.  
9 \* \* \* Délai d'attente de la demande dépassé.  
10 \* \* \* Délai d'attente de la demande dépassé.  
11 \* \* \* Délai d'attente de la demande dépassé.  
12 11 ms 11 ms 11 ms ae-16.r06.frmig013.de.bb.gin.ntt.net [129.250.66.67]  
13 89 ms 39 ms 63 ms ae-2.r20.frmig013.de.bb.gin.ntt.net [129.250.6.13]  
14 12 ms 11 ms 11 ms ae-0.ad2.frmig007.de.bb.gin.ntt.net [129.250.5.36]  
15 181 ms 49 ms 69 ms ae-0.f9-networks.frmig007.de.bb.gin.ntt.net [129.241.10.17]  
16 \* \* \* Délai d'attente de la demande dépassé.  
17 47 ms 80 ms 70 ms 107.162.251.256  
18 111 ms 89 ms 61 ms 107.162.248.161  
19 162 ms 161 ms 181 ms 107.162.249.4  
20 \* \* \* Délai d'attente de la demande dépassé.  
21 64 ms 52 ms 76 ms teg-0-1-0.er01.lyo02.fr.ip-max.net [46.20.254.2]  
22 17 ms 10 ms 17 ms bel-er01.lyo01.fr.ip-max.net [46.20.254.110]  
23 19 ms 12 ms 16 ms teg-1-0-1.er01.gva09.ch.ip-max.net [46.20.249.168]  
24 15 ms 17 ms 83 ms teg-0-1-0.er01.gva09.ch.ip-max.net [46.20.253.15]  
25 53 ms 90 ms 46 ms teg-2-0-0.er01.gva20.ch.ip-max.net [46.20.253.21]  
26 96 ms 58 ms 24 ms bel20-er00.gva20.ch.ip-max.net [46.20.254.59]  
27 17 ms 16 ms 18 ms 46.20.248.147  
28 180 ms 97 ms 30 ms 100.53.249.22  
29 \* \* \* Délai d'attente de la demande dépassé.  
30 17 ms 16 ms 17 ms webcross.ville-geneve.ch [193.134.176.29]

C:\Users\pascal>tracert paris.fr

Détermination de l'itinéraire vers paris.fr [194.157.110.192]  
avec un maximum de 30 sauts :

1 1 ms 1 ms 1 ms internetbox.hum [192.168.1.1]  
2 6 ms 6 ms 8 ms 100.85.192.1  
3 45 ms 110 ms 89 ms ae22-1150.lpc-lss090-w-pe-08.bluelwin.ch [213.3.220.253]  
4 49 ms 74 ms 91 ms eth12-1150.lsic120p-cys001.bluelwin.ch [213.3.220.254]  
5 28 ms 87 ms 82 ms 213.3.220.189  
6 6 ms 10 ms 9 ms 1001as-015-as11.bb-ip-plus.net [193.134.95.66]  
7 \* \* \* Délai d'attente de la demande dépassé.  
8 \* \* \* Délai d'attente de la demande dépassé.  
9 \* \* \* Délai d'attente de la demande dépassé.  
10 35 ms 64 ms 102 ms 115-lef01-c2-02-30-3-223.fr.lnx.sbo.bbox.fr [62.36.3.223]  
11 107 ms 65 ms 96 ms bel-er01-cro.net.bbox.fr [212.186.176.161]  
12 17 ms 17 ms 17 ms 8.la16.bcr01-t03.net.bbox.fr [212.194.171.93]  
13 \* \* \* Délai d'attente de la demande dépassé.  
14 \* \* \* Délai d'attente de la demande dépassé.  
15 87 ms 53 ms 71 ms 89.81.70.217  
16 17 ms 17 ms 17 ms 81.32.79.108  
17 \* \* \* Délai d'attente de la demande dépassé.  
18 \* \* \* Délai d'attente de la demande dépassé.  
19 \* \* \* Délai d'attente de la demande dépassé.  
20 \* \* \* Délai d'attente de la demande dépassé.  
21 \* \* \* Délai d'attente de la demande dépassé.  
22 \* \* \* Délai d'attente de la demande dépassé.  
23 \* \* \* Délai d'attente de la demande dépassé.  
24 \* \* \* Délai d'attente de la demande dépassé.  
25 \* \* \* Délai d'attente de la demande dépassé.  
26 \* \* \* Délai d'attente de la demande dépassé.  
27 \* \* \* Délai d'attente de la demande dépassé.  
28 \* \* \* Délai d'attente de la demande dépassé.  
29 \* \* \* Délai d'attente de la demande dépassé.  
30 \* \* \* Délai d'attente de la demande dépassé.

Voir aussi les « looking glasses » - [https://en.wikipedia.org/wiki/Looking\\_Glass\\_server](https://en.wikipedia.org/wiki/Looking_Glass_server)  
(pas en français)  
<https://netactuate.com/lg/>  
<https://dnschecker.org/online-traceroute.php>

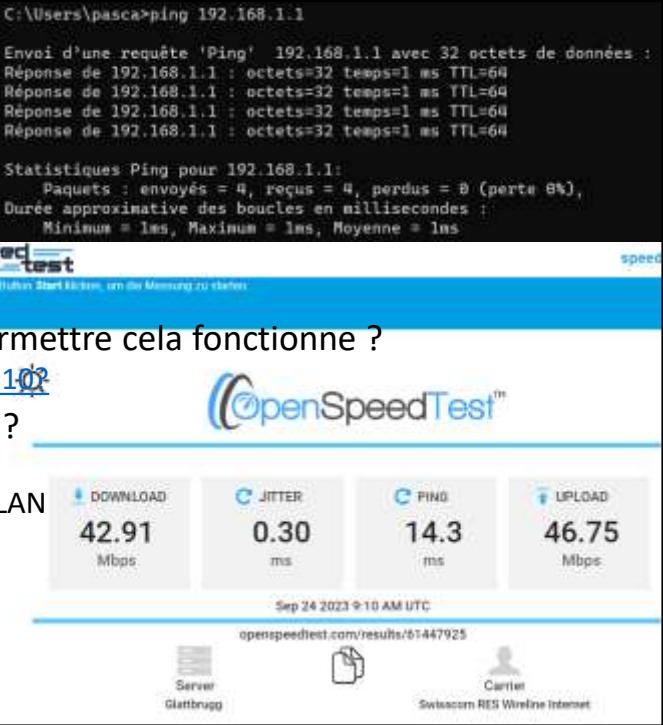
Aussi, trace route graphiques (mais il va dessiner depuis le serveur de test, aux USA...)  
<https://gsuite.tools/traceroute>  
<https://geekflare.com/fr/online-traceroute-tools/>

On peut réduire le délai de cette construction via des paramètres qui suppriment la tentative de résolution du nom (reverse DNS), et réduisent le délai d'attente de la réponse (timeout), et d'allonger le maximum par défaut de 30 «hops» (routeurs):  
tracert -d -h 150 -w 200 destination.tld

<https://trouver-ip.info/localiser-ip/>

## Exercice - ping

- Faire un Ping du voisin
  - Est-ce que cela fonctionne ?
  - Pourquoi ?
- Quelle action nécessaire pour permettre cela fonctionne ?
  - [Comment faire ping vers Windows 10?](#)
- Que cela mesure-t-il exactement ?  
Et pour un accès Internet ?
  - Présence et connectivité OK via le LAN
  - Débit (speed)
  - [Latence](#) (Latency)
  - [Gigue](#) (Jitter)



Comment autoriser Ping, entre 2 W10/11?  
<https://medium.com/conseillers-num%C3%A9riques-suisses-romands/comment-faire-ping-sous-windows-10-4123cbb32787>

Voir aussi tests performances de l'accès Internet  
Best  
<https://www.nperf.com/fr/>  
Avec Jitter:  
<https://www.speedtest.ch/> (Germain)  
<https://openspeedtest.com/about-speed-test>  
<https://test-debit-internet.fr/test-ping/>  
<https://www.speedtest.net/fr>

Alternative: slide suivante et  
<https://www.cnlab.ch/fr/speedtest>  
Version Web: <https://speedtest.cnlab.ch/fr/>  
<https://ux.cnlab.ch/benchmarking/home>



# Plus d'options avec Nperf.com



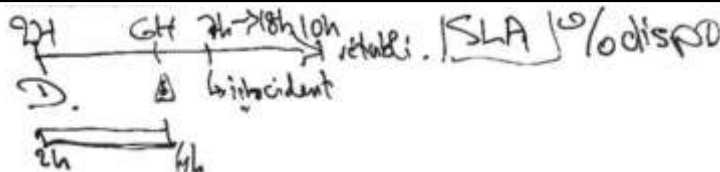
En plus de récupérer vos IPv4 et v6 publiques, on accède à des statistiques locales par opérateur: [Comparer]

Et des rapports et avis sont publiés:  
[https://media.nperf.com/files/publications/CH/2023-01-17\\_fixed-internet-connections-survey-nPerf-2022\\_EN.pdf](https://media.nperf.com/files/publications/CH/2023-01-17_fixed-internet-connections-survey-nPerf-2022_EN.pdf)  
[A propos - nPerf.com](https://www.nperf.com/fr/about-us/) <https://www.nperf.com/fr/about-us/>

- Latence (ping) :** Indique le temps nécessaire à un petit paquet de données pour effectuer un aller-retour entre votre ordinateur et notre serveur de test de débit. Plus le résultat est faible, plus votre connexion est réactive.
- Débit descendant :** Indique la quantité de données que votre connexion peut recevoir en une seconde. Plus la mesure est élevée, meilleur est le débit de votre connexion.
- Débit montant :** Indique la quantité de données que votre connexion peut envoyer en une seconde. Plus la mesure est élevée, meilleur est le débit de votre connexion.



## SLA, SLM, KPI



Le service de monitoring, va tenter de mesurer «factuellement» la disponibilité effective des services, car cela peut entraîner des pénalités...

- [Service Level Agreement](#) ou Management
- [Key Performance Indicator](#) grâce au monitoring

Le [taux de disponibilité](#) = nb H (ou mn) totale effectivement disponible, sur le nb H théorique sans panne. Mais c'est toujours calculé pour en réduire l'impact au strict minimum.

*Une panne nocturne, mesurée à 2h par le monitoring, détectée par l'IT à 6h, avant ouverture officielle à 7h (début engagement de disponibilité de service), réparée à 9h, ne comptabilisera que 2h d'interruptions.*

*D'où l'intérêt de monitorer et alerter, pour réparer avant 7h!*

**Le RTO** (Recovery Time Objective) : il est important de déterminer en combien de temps un service dégradé et un retour à la normal seront effectifs.

**Le RPO** (Recovery Point Objective) : quelle est la perte de données maximale admissible ?

Sont des notions qui seront exploitées par les PRI/PRA (cf. plus loin)

[https://fr.wikipedia.org/wiki/Service-level\\_agreement](https://fr.wikipedia.org/wiki/Service-level_agreement)

[https://fr.wikipedia.org/wiki/Indicateur\\_cl%C3%A9\\_de\\_performance](https://fr.wikipedia.org/wiki/Indicateur_cl%C3%A9_de_performance)

<https://fr.wikipedia.org/wiki/Disponibilit%C3%A9>

- Task manager, démarrage – limiter au strict nécessaire



- Task manager, Performance – last reboot

Temps de fonctionnement	Cadre de niveau 1	256 Ko
0:06:43:31	Cadre de niveau 2	1,0 Mo
	Cadre de niveau 3	6,0 Mo

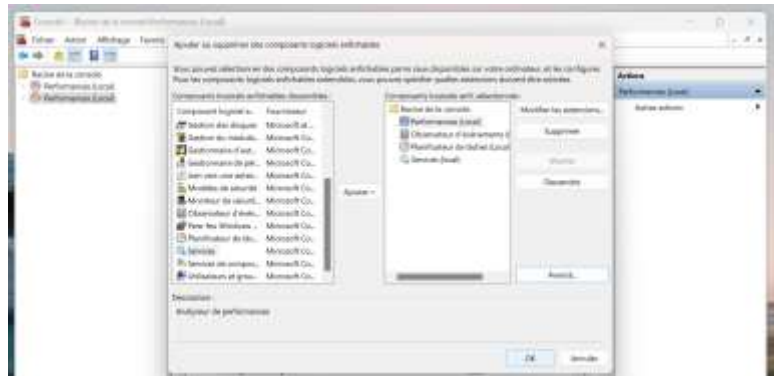
Exercice: Repérer comment lister l'historique de tous les (re)démarrages enregistrés par une machine Windows.

Eventlog, système, id à déterminer, dans le journal eventlog justement.

## Eventlog – exercices pratiques

- Fournir la liste des reboot de la dernière semaine sur son PC
- Comment faire pour ouvrir les logs d'une machine distante (sur le LAN)

Tout le monde est-il familiarisé avec MMC (Windows) ?



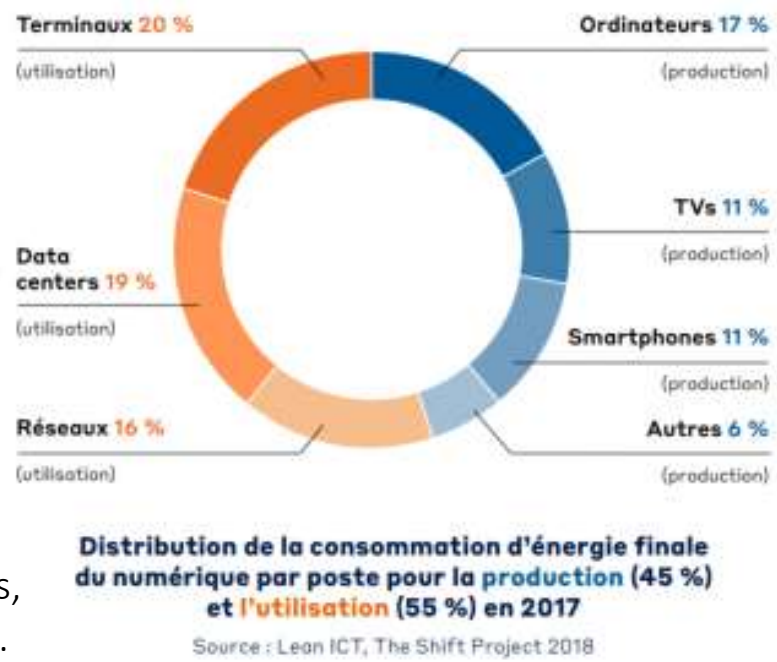
Soluce: journal système, Eventlog, 6005 pour les «boot», et 6006 pour les «shutdown» (réels, pas les faux «arrêts» Windows = hibernation).

<https://pcastuces.com/pratique/astuces/6002.htm>

## Tuning et Green IT

- Green IT
  - Eco design
  - Réduire
  - Réutiliser
  - Réparer
  - Recycler
- IT for Green

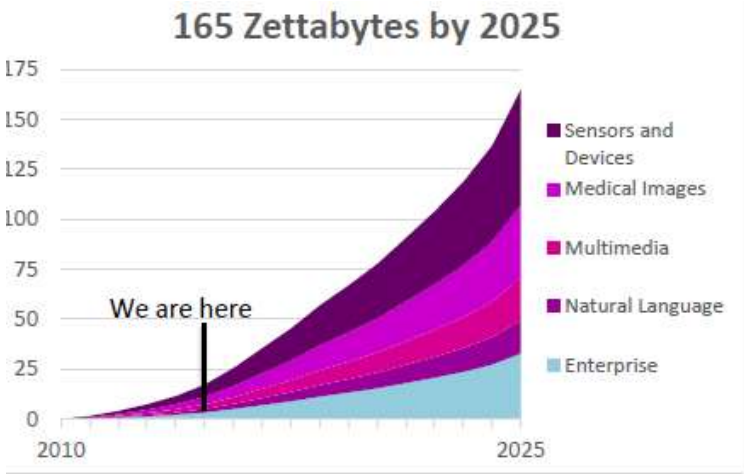
L'énergie grise  
Le gâchis  
Moins de 20% recyclés,  
le reste, en décharge...



De 1971 (5'519 Mtep) à 2018 (14'282 Mtep), x3 en 46 ans.  
Energies fossiles: 2018: 31% pétrole, 23% gaz, 27% charbon.

# Impact du Cloud – infobésités...

QUID avec l'arrivée des «IA» ?



Prefix	Size
Kilo	10 <sup>3</sup>
Mega	10 <sup>6</sup>
Giga	10 <sup>9</sup>
Tera	10 <sup>12</sup>
Peta	10 <sup>15</sup>
Eta	10 <sup>18</sup>
Zeta	10 <sup>21</sup>
Yotta	10 <sup>24</sup>

Que devrions-nous faire ?

## D: 3. Updating

Installer et tester les mises à jour ainsi que les correctifs (patches) des services concernés manuellement et à l'aide de systèmes de déploiement de logiciels et mettre à jour la documentation d'exploitation.

3. Installer et tester les mises à jour ainsi que les correctifs (patches) des services concernés manuellement et à l'aide de systèmes de déploiement de logiciels et mettre à jour la documentation d'exploitation.

3.1 Connaître la procédure d'installation des mises à jour et des correctifs.

3.2 Connaître des sources fiables pour des mises à jour et des correctifs ainsi que les mesures de sécurité correspondantes (p. ex. valeurs de hachage et clés).

3.3 Connaître les conséquences et les dangers possibles inhérents aux mises à jour et aux correctifs par rapport à une entreprise.

3.4 Connaître des scénarios de test des mises à jour et des correctifs.

## Pourquoi ?



- Pour des raisons de sécurité
- Pour corriger des bugs
- Pour ajouter des fonctions (gratuitement)

### Automatiquement:

- OS Embedded (inclus par OS)
- au lancement de l'application
- via un «résident» (bot) ou un «service»

### Manuellement:

Sauf que ce n'est plus des «updates» dans ce cas, mais des «UPGRADEs» Comme les Services Packs.

On peut utiliser les process des «patches» pour cela, si c'est gratuit, mais ce n'est plus du «patching».

- Certains « updates » spécifiques vont « nettoyer » un botnet existant, sans nécessaire installer quelque chose (enfin si, lui-même). Et la plupart des updates <https://www.catalog.update.microsoft.com/Search.aspx?q=kb890830>
- Mais la plupart servent à éviter de conserver exposé une faille de sécurité reconnue (pour en ouvrir des nouvelles à la NSA?)
- Ou à stabiliser des dysfonctionnements...

C'est donc le plus souvent à vocation « préventive ».

## Que doit-on mettre à jour ?

- Les OS
  - Windows. Légende urbaine: Linux, Mac pas besoin?
  - Android/iOS
- Les pilotes (drivers)
- Les firmwares
  - Bios, mais aussi flashprom des appareils iOE/iOT (webcam,NAS...)
- Les «Boîtiers» réseaux (Relais)
  - Routeurs, Switchs (Flash ROM ou EPROM)
- Les logiciels eux-mêmes
  - (option Microsoft seulement pour Windows)



[Microsoft Update Catalog](#)

[Mises à jour de sécurité Apple - Assistance Apple \(CH\)](#)

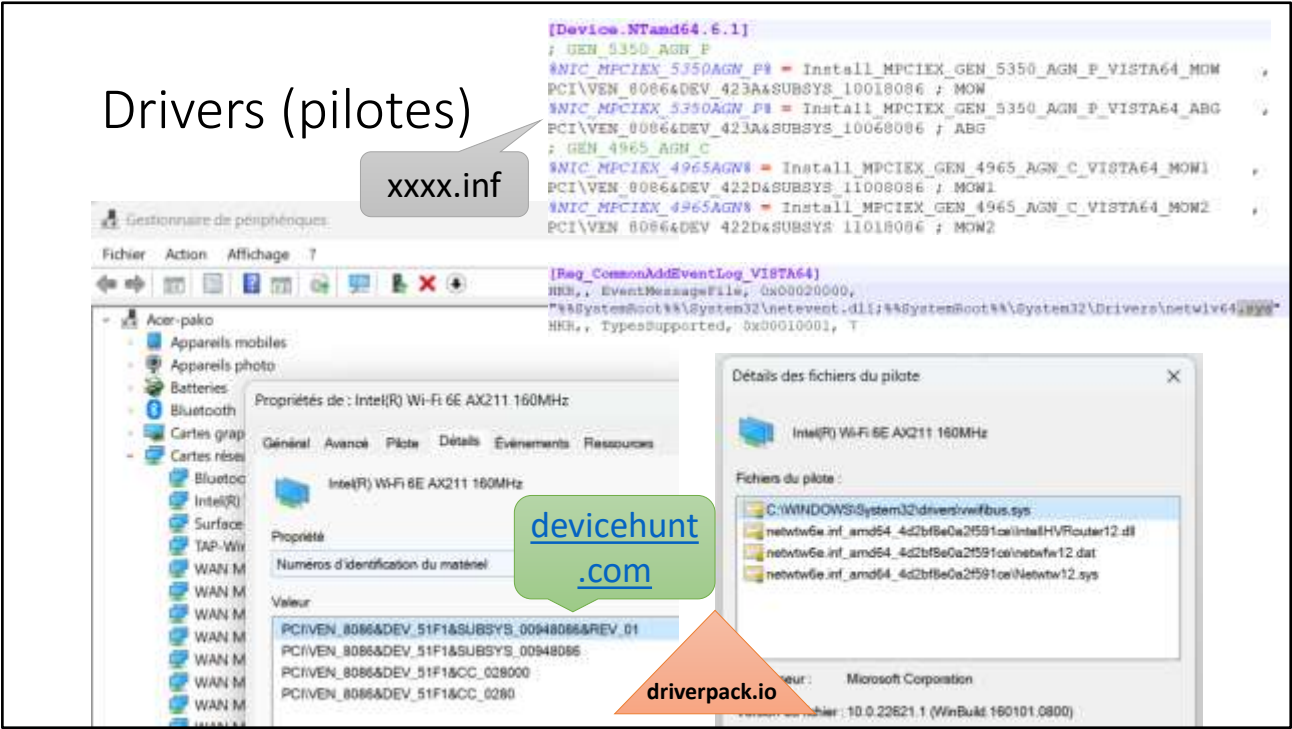
[Ubuntu Linux : mettre à jour son système en 2 minutes ! – Le Crabe Info](#)

[Microsoft Update Catalog](https://www.catalog.update.microsoft.com/Search.aspx?q=kb) <https://www.catalog.update.microsoft.com/Search.aspx?q=kb>  
[Security Update Guide – Microsoft](https://msrc.microsoft.com/update-guide) <https://msrc.microsoft.com/update-guide>

<https://support.apple.com/fr-ch/HT201222>

<https://lecrabeinfo.net/ubuntu-linux-mettre-a-jour-paquets-systeme.html>





- https://devicehunt.com/
- https://driverlookup.com/hardware-id/
- A fuir:
- https://www.malekal.com/driverpack-solution-logiciel-de-mise-a-jour-de-pilotes-a-eviter/
- Bof:
- https://www.zhangduo.com/udi.html (n'apporte rien de plus que le gestionnaire de périphériques)

## Et Linux ? Mac OS ? Et les smartphones ?



- Les systèmes Unix selon les distributions, disposent de bibliothèques signées de sources mises à disposition et téléchargeables facilement, pour l'OS comme pour les applications signées reconnues.
  - Cela n'empêche pas les cybercriminels de tenter de se faire passer pour des gentils, mais la communauté veille...
- Apple fourni des services similaires pour les Macintosh

Des plateformes MDM (Mobile Device Management) permettent:

- Inventorier le parc mobile, et vérifier versions et mises à jour
- Activer les profils pro effaçables sur des équipements perso ([BYOD](#))

[Comment installer les mises à jour sous Linux ? \(lojiciels.com\)](https://www.lojiciels.com/comment-installer-les-mises-a-jour-sous-linux/)

<https://www.lojiciels.com/comment-installer-les-mises-a-jour-sous-linux/>

<https://medium.com/lesenfantsdu-net/passer-de-win10-%C3%A0-linux-5799c79d33f7>

Linux (selon la distribution, mais similaires)

- `sudo apt update`
    - `apt list --upgradable`
  - `'sudo apt upgrade'`  
Ou bien `'sudo apt full-upgrade'`
- Faire le ménage (1 des 2)
- `sudo apt autoremove` (light)
  - `sudo apt autoclean` (deep)

## Equivalent du cleanmgr

Avec tous les logiciels, de tous les éditeurs (contrairement à Microsoft/Windows)

Avec tous les logiciels, de tous les éditeurs (contrairement à Microsoft/Windows)

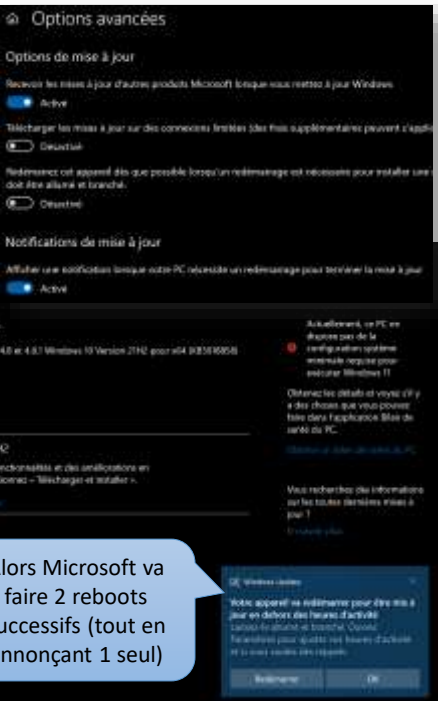
<https://lecrabeinfo.net/ubuntu-linux-mettre-a-jour-paquets-systeme.html>

Tu peux mettre à jour en une seule ligne de commande via `&& sudo apt update && sudo apt full-upgrade -y && sudo apt autoremove -y`

# Windows update

Wuauerv  
Est le service qui assure la mise à jour automatisée ou manuelle des mises à jour des composants de Windows et optionnellement de Microsoft

Mais comment sont faites les mises à jour des produits non Microsoft ?



Alors Microsoft va faire 2 reboots successifs (tout en annonçant 1 seul)

<https://www.microsoft.com/en-us/wdsi/defenderupdates>

Pour les mises à jour dans les entreprises, une solution de gestion de parcs Windows avec agent doit permettre d'assurer l'automatisation des logiciels complémentaires à Windows. Cela est critique pour des outils comme:

- Navigateurs web
- Lecteurs PDF/JPEG
- Services résidents qui ouvrent des ports réseaux sur la machine

## Comment ? Préventif ou curatif ?

Installation d'un service serveur WSUS, ou via une plateforme plus avancée, qui va intégrer les services WUA (Windows Update Agent)

- L'agent va vérifier la présence et la conformité des updates recommandés, et les installer.

1) Soit depuis l'Internet chez Microsoft (Windows update)

2) Soit par l'intermédiaire d'une plateforme tierce (cf. annexes)



Bien que les updates de Microsoft incluent aussi un MSRT mensuel, le gros du travail consiste à essayer de boucher les trous, avant agression.

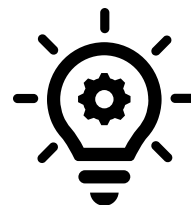
[https://learn.microsoft.com/en-us/windows/win32/wua\\_sdk/other-sources-of-windows-update-agent-information](https://learn.microsoft.com/en-us/windows/win32/wua_sdk/other-sources-of-windows-update-agent-information)

Jusqu'en 2017...

<https://learn.microsoft.com/fr-fr/security-updates/securitybulletins/securitybulletins>

<https://www.pgsoftware.fr/solution-deploiement-patches>

## Comment déployer ces mises à jour?



### Option 1

- Stage1: Tout l'IT en premier
  - Le premier DC, DNS
- Stage2: Le reste ensuite
  - Le 2<sup>nd</sup> DC, DNS, FileServer, PrintS...



[Sandboxie — Wikipedia](#)

[Bac à sable Windows - Windows Security | Microsoft Learn](#)

### Option 2 – mode « canarie »

- Stage1: x machines de tests
- Stage2: 1-2 machines de l'IT
  - DC1 et DNS1
  - 1 PC compta
  - 1 PC RH
  - 1 PC SG
  - 1 PC Business1, 1 PC B2, 1PC B3
- Stage3: 48h délai, pas d'alerte
  - Tout le reste

[CrowdStrike](#)

En option utiliser ou activer un bac à sable pour tester:

[Sandboxie — Wikipedia](#) <https://en.wikipedia.org/wiki/Sandboxie>: Merci Ethan (mais super pratique pour les updates...)

[Bac à sable Windows - Windows Security | Microsoft Learn](#)

<https://learn.microsoft.com/fr-fr/windows/security/application-security/application-isolation/windows-sandbox/windows-sandbox-overview>

Cocadmin, le bug CloudStrike...

<https://youtu.be/9qaRqO3GPTs?si=WT2ntqVq0dVJtnkf>

<https://youtu.be/E30KhHOQoOA?si=qEiTqPHbiPcnWlf4>

Et le bug Linux, trouvé car open source, installé car open source...

<https://youtu.be/Q5a92asc7hM?si=VsCnBm3qLsHUqK6s>

## Idéalement



### Déploiement

- 1 KB à la fois? Sur 1 machine représentative de chaque dans le parc.
- Aviser les «beta-testeur» de l'installation à venir, puis effectuée (avec succès, ou pas effectuée si échec)
- Laisser 1 semaine avant de déployer aux autres...

Déployer uniquement les éléments nécessaires

- Les failles de sécurité critiques ou importantes qui nous touchent
- Les bugs qui sont effectivement vécus...

Déployer en prévention les autres, mensuellement

# Par sécurité !! Motivation principale...

- Pour lutter contre les PCs Zombies ([Botnet](#))
- Extraits de Bots traités par [MSRT](#) (inclus dans Wupdate) ≈ 650



Pour références:

<https://medium.com/cloudready-ch/botnet-c-est-quoi-89710901de99>

<https://medium.com/cloudready-ch/internet-et-la-s%C3%A9curit%C3%A9-f0cd27a14408>

Microsoft:

<https://www.microsoft.com/en-us/download/details.aspx?id=9905>

<https://support.microsoft.com/fr-fr/topic/comment-faire-pour-r%C3%A9soudre-une-erreur-lorsque-vous-ex%C3%A9cutez-le-scanner-de-s%C3%A9curit%C3%A9-microsoft-6cd5faa1-f7b4-afd2-85c7-9bed02860f1c>



## Sous quelle forme se présente un update Windows?

- .cab
- .msu
- .msi(x)
- .exe
- .msp
- ...

Ouvrir avec un Winzip  
ou  
`dism /online /add-package  
/packagepath:"C:\update\cabname.cab"`

Avec MSIEXEC  
Et avec la mention du MSI  
associé ou via  
'wusa.exe mon.msu'

<https://www.catalog.update.microsoft.com/>

[Comment installer manuellement un fichier CAB dans Windows 10 ? \(lojiciels.com\)](https://www.lojiciels.com/comment-installer-manuellement-un-fichier-CAB-dans-Windows-10-? (lojiciels.com))

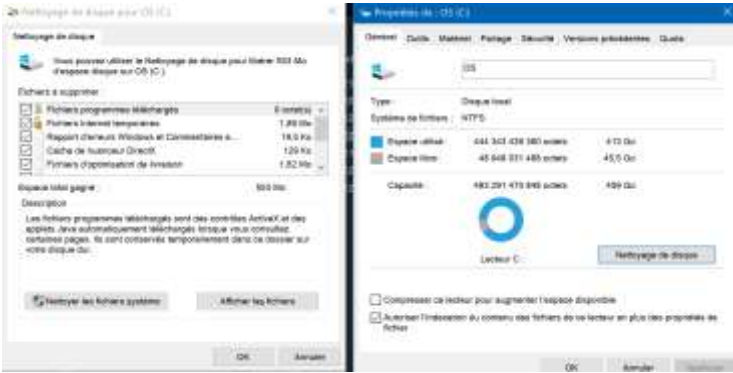
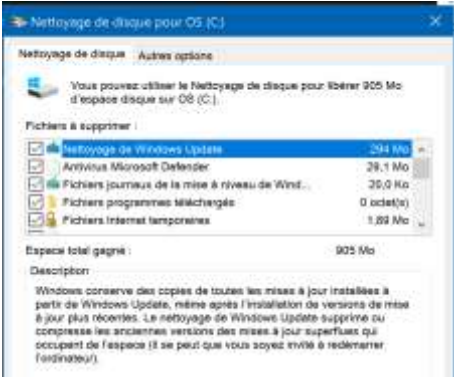
<https://www.lojiciels.com/comment-installer-manuellement-un-fichier-cab-dans-windows-10/> (Bof cet article à trouver mieux!)

<http://www.easy-pc.org/2017/01/comment-installer-les-mises-a-jour-cab-et-msu-dans-windows-10.html>

<https://social.technet.microsoft.com/Forums/windowsserver/fr-FR/46bb4be2-3c5e-4245-a61d-57c36278efc8/comment-installer-des-fichiers-msp-via-un-script-powershell->

# Windows, comment on fait le ménage après?

- Cleanmgr (Windows)



**Bonus:** Nettoyer les clefs de registres devenues invalides, c'est pas du luxe. J'utilise CCleaner de Piriform

Cela fonctionne aussi sur des OS serveurs, sauf qu'il faut ajouter la fonctionnalité [Windows Server 2008 nettoyage de disque - comment activer / installer / exécuter. \(hdd-tool.com\)](https://www.hdd-tool.com/fr/windows-server-2008/disk-cleanup-server-2008.html)

<https://www.hdd-tool.com/fr/windows-server-2008/disk-cleanup-server-2008.html>

<https://medium.com/search?q=kott%C3%A9+PC>

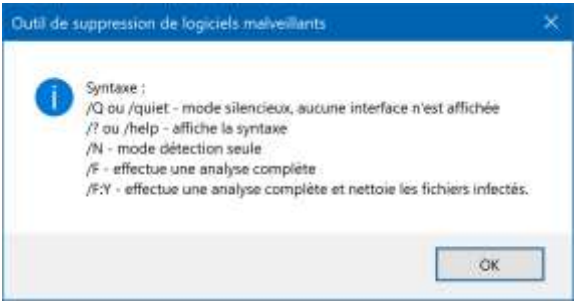
<https://medium.com/quicklearn/top-3-des-outils-pour-s%C3%A9curiser-et-nettoyer-windows-10-74ddcb3f9f24>

# Patch (EXE) de Windows

Certains «Patches» de windows ne sont pas des updates:

- [KB890830](#)

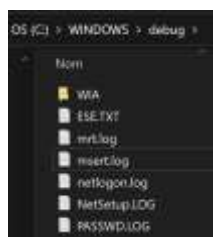
Un update qui va scanner les malwares identifiés via une application qui va faire un scan rapide: MRT.exe dans system32.  
Qui peut être utilisée manuellement pour approfondir. (Plusieurs heures)  
Log: %WINDIR%\debug folder  
Mrt.log



Exemple avec: KB890830 - MSRT  
<https://support.microsoft.com/fr-fr/topic/supprimer-des-logiciels-malveillants-sp%C3%A9cifiques-et-r%C3%A9pandus-%C3%A0-l'aide-de-l'outil-de-suppression-de-logiciels-malveillants-windows-kb890830-ba51b71f-39cd-cdec-73eb-61979b0661e0>  
  
<https://msrc.microsoft.com/> [Microsoft Security Response Center](#)

[Microsoft Safety Scanner Download](#) | [Microsoft Learn](#)

- Log = msert.log



<https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/safety-scanner-download>

# Scan vulnérabilité vs Removal!

- MBSA pour Windows (fini!) depuis 2013/2014
- Historique: Avant W10/S2016



[Microsoft Baseline Security Analyzer - Wikipedia](#)



<https://msrc.microsoft.com/>

<https://learn.microsoft.com/fr-fr/security-updates/security/20196904>  
<https://learn.microsoft.com/en-us/windows/security/threat-protection/mbsa-removal-and-guidance>

<https://learn.microsoft.com/fr-fr/windows-server/administration/windows-server-update-services/deploy/1-install-the-wsus-server-rôle>  
[Definition of a Security Vulnerability \(microsoft.com\)](#) <https://www.microsoft.com/en-us/msrc/definition-of-a-security-vulnerability?rtc=1>  
[Microsoft Security Response Center](#) <https://msrc.microsoft.com/>

# Evaluer les vulnérabilités

Asset discovery and inventory

Continuously detect risk across managed and unmanaged endpoints with built-in modules and agentless scanners, even when devices aren't connected to the corporate network. View entity-level risk assessment data to focus on your most critical assets.



## Comparez les offres en préversion

Module complémentaire pour les utilisateurs de Defender pour point de terminaison P2 et E5

### Module complémentaire Gestion des vulnérabilités Microsoft Defender

Essayez gratuitement

Les utilisateurs de Defender pour point de terminaison P2 et E5 peuvent ajouter de nouvelles offres, modules de gestion des vulnérabilités à leur abonnement existant grâce au module complémentaire Gestion des vulnérabilités Microsoft Defender.

Fonctionnalités clés :

- ✓ Centre de sécurité unifié et gestion centralisée
- ✓ Découverte des appareils gérés et non gérés
- ✓ Inventaire des appareils gérés
- ✓ Inventaire des appareils non gérés
- ✓ Évaluation des bases de référence de sécurité
- ✓ Analyses automatisées pour les appareils Windows
- ✓ Évaluation des plug-ins de navigateur
- ✓ Évaluation des certificats numériques
- ✓ Analyse des partages réseau
- ✓ Stockage des applications vulnérables

Disponible pour tous les clients

### Gestion des vulnérabilités Microsoft Defender autonome

Essayez gratuitement

Testez toutes les fonctionnalités du module complémentaire Gestion des vulnérabilités Microsoft Defender. P2 et E5.

- ✓ Évaluation des vulnérabilités
- ✓ Évaluation des configurations
- ✓ Surveillance continue
- ✓ Analyse et renseignement sur les menaces
- ✓ Définition des priorités selon les risques
- ✓ Suivi des corrections

[Gestion des vulnérabilités Microsoft Defender | Sécurité Microsoft](#)

https://www.microsoft.com/fr-ch/security/business/threat-protection/microsoft-defender-vulnerability-management

Autres solutions:

- Cf annexes, DamageEngine Patch gratuit moins de 20 ou 25 machines, multi OS (mais version payante)...

Les logiciels de patch sont censé donner des reports de vulnérabilité.

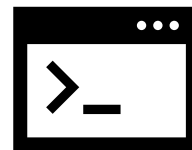
- Aussi: Nessus...
- Aussi: Darktrace

- NON pour les particuliers
- OUI pour une console de supervision en entreprises

- 2<sup>nd</sup> view scan (Spybot, malwarebyte, Clamwin...)
- +Console (solutions propriétaires \$)
- **Cela n'exclue pas l'usage de Virustotal dans les 2 cas!**



## Et pour les applications ?



- Microsoft/Windows ne proposait pas de solutions...
- Il est nécessaire de passer par les éditeurs de ces solutions
- Ou bien par des outils «partenaires», exemple: Ccleaner...
- Quelles sont les applications critiques ?

- Les navigateurs web... (lecteurs html)
- Les anti-virus (et de second passage...)
- Les lecteurs PDF...
- Les lecteurs JPEG...
- Les pilotes (mais ceux-là sont normalement intégrés Windows update)
- ...

Alleluia, Microsoft a sorti Winget et <https://winstall.app/>... A non, c'est <https://winget.pro/> une boîte autrichienne en fait ???

Non, c'est bien un nouveau feature de Microsoft: [Windows Package Manager - Wikipedia](#)

### Quelques articles pour références:

<https://www.malekal.com/installer-plusieurs-antivirus-windows-10/>

De l'auteur de ce support: PaKo

<https://medium.com/conseillers-num%C3%A9riques-suisse-romands/pourquoi-mon-pc-pourtant-sain-se-trouve-infect%C3%A9-par-un-spy-un-troyen-4507c3b4d446>

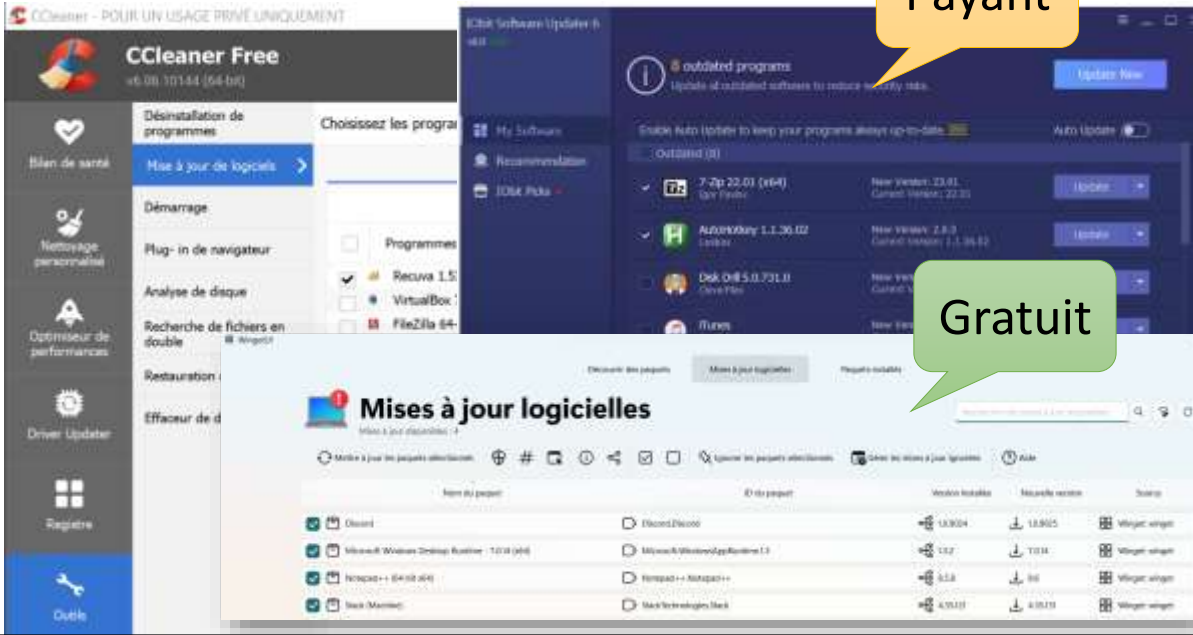
<https://medium.com/quicklearn/ccleaner-de-piriform-b54351a49fa>



Mise à jour des logiciels ?? (Windows)

Payant

Gratuit



[10 Best Free Software Updater Programs \(December 2022\) \(lifewire.com\)](https://www.lifewire.com/free-software-updater-programs-2625200)  
<https://www.lifewire.com/free-software-updater-programs-2625200>

Mais la solution Winget reste la meilleure option – Surtout avec l’outil graphique de Marti Climent, UniGetUI (ex WinGetUI)  
<https://github.com/marticliment/UnigetUI>

winstall

Winget

- Browse the winget repository - winstall
- Your own winget repository | winget.Pro

Gadget inutile  
Par contre WINGET  
MUST USE!

PaKo  
@pkotte  
Essentiel des outils sur Windows  
Last updated 2 seconds ago

NE PAS UTILISER UN TEL SCRIPT (Mauvais!)

winget install --id=Opera.OperaGX -e -h  
--scope "machine"  
(sauf que faut lancer «admin» sinon user profile)  
Winget uninstall --id=Opera.OperaGX

Une banque de dépôts externes:  
- Qui contrôle l'intégrité ?  
- Quid de «figer» les versions ?

--ignore-security-hash  
--version x.y.z

Cleaner

View App

Other apps by

Bitwarden

View App

La source "msstore" nécessite que vous consultiez les contrats suivants avant de l'utiliser.  
Terms of Transaction: https://aka.ms/microsoft-store-terms-of-transaction  
La source nécessite que la région géographique à 2 lettres de l'ordinateur actuel soit envoyée au service principal pour être  
téléchargée correctement (par exemple, «FR-FR»).

Acceptez-vous toutes les conditions des contrats suivants ?  
[Y] Oui. [N] Non: Y  
Un package existant a déjà été installé. Tentative de mise à niveau du package installé...  
Téléchargement en cours https://download.ccleaner.com/ccleaner.exe  
Le code de hachage de l'installation a été vérifié avec succès  
Démarage du package d'installation... Merci de patienter.

Merci à Naël. J'avais vu mais pas détecté la plateforme Winstall.app – Attention toutefois, ce n'est pas Microsoft l'éditeur du site, et le script fourni est assez «moisi», et non éditable. C'est un «freemium» fourni pour faire la pub de winget.pro, une entreprise commerciale.

<https://medium.com/p/1781a5d1a203>

<https://medium.com/cloudready-ch/winget-comment-installer-et-mettre-%C3%A0-jour-une-application-sous-windows-1781a5d1a203>

**Améliorations:**

Remplacer les && par un retour à la ligne et vérifier les erreurs d'exécution. (Conserver && pour les installations en chaînes dépendantes)

**Risques:**

Utiliser un tel script peut installer des packages applicatifs de versions différentes, car selon la date de son lancement (relancer le même script tous les jours? Et comment je stabilise, ou teste avant?)

- force est une option qui permet de «bypass» le check du hash de contrôle de sécurité
- scope «machine» est une option qui permet d'installer dans program files, mais installera dans user profile si pas lancé «as admin».
- h mode invisible sans interactions (donc pas de confirmation)
- disable-interactivity (pour mieux désactiver interactions? 2 niveaux de silencieux?)

102

Les packages sources sont posés dans le sous-dossier «winget» de %temp%:

user\AppData\Local\Temp\winget

Avec les fichiers de log:

--verbose

Exemple:

winget install --id=Opera.OperaGX -e -h --scope "machine"

winget uninstall --id=Opera.OperaGX

## Winget - Pratique

Lancer CMD en mode admin:

> winget show winget

> winget install --id SomePythonThings.WingetUIStore

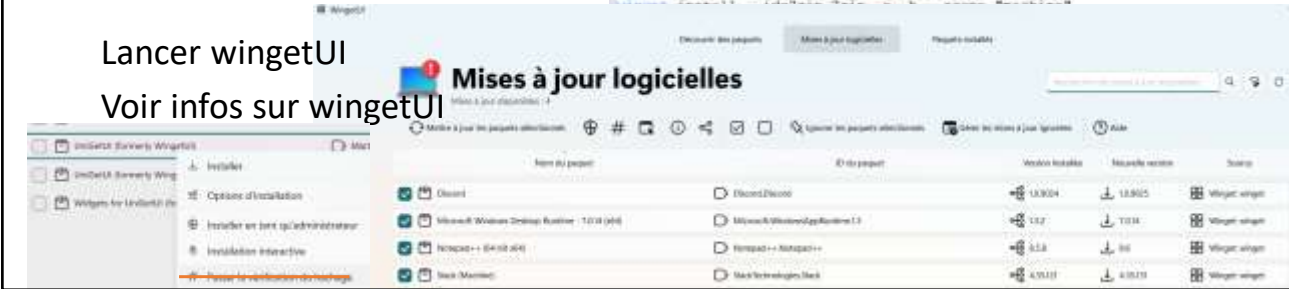
Lancer wingetUI  
Voir infos sur wingetUI

```
rem securité et système
winget install --id=SomePythonThings.WingetUIStore -e -h --scope "machine"
rem WingetUI - en est d'accord, c'est un nom de package assez moisi
winget install --id=Piriform.CCleaner -e -h --scope "machine"
winget install --id=Bitwarden.Bitwarden -e -h --scope "machine"
winget install --id=VirusTotal.VirusTotalUploader -e -h --scope "machine"
rem winget install --id=IOBit.MalwareFighter -e -h --scope "machine"
rem bug Le code de hachage de l'installation ne correspond pas : ceci ne peut
rem winget install --id=SafeNetworks.SpybotAntiBeacon -e -h --scope "machine"

rem Browser (navigateurs web)
winget install --id=Google.Chrome -e -h --scope "machine"
winget install --id=Mozilla.Firefox -e -h --scope "machine"
winget install --id=Brave.Brave -e -h --scope "machine"
winget install --id=Opera.OperaGX -e -h --scope "machine"

rem outils comm
winget install --id=Telegram.TelegramDesktop -e -h --scope "machine"
winget install --id=OpenWhisperSystems.Signal -e -h --scope "machine"
winget install --id=SlackTechnologies.Slack -e -h --scope "machine"
rem winget install --id=Telegram.TelegramDesktop -e -h --scope "machine" - bug?

rem outils, traducteur, pdf reader...
```



WingetUI  
Open source et libre de Marti CLIMENT  
<https://github.com/marticliment/WingetUI>

Astuces et infos complémentaires:  
<https://medium.com/cloudready-ch/winget-comment-installer-et-mettre-%C3%A0-jour-une-application-sous-windows-1781a5d1a203>

# Rollback ?

Identifier lequel des KB a posé un problème, le retirer

- Les lister: > `wmic qfe`
- Désinstaller: > `wusa /uninstall /kb:1234567 /quiet`

## Ou System State Restore

Restaurer la dernière config stable connue:

- Si «Points de restauration» non désactivé
- Un *system state* est lancé par *wausrv* avant

F8 n'est plus disponible (par défaut) sous Windows 10/11, mais après 3 «crash» (arrêt brutal), Windows démarre en mode réparation.

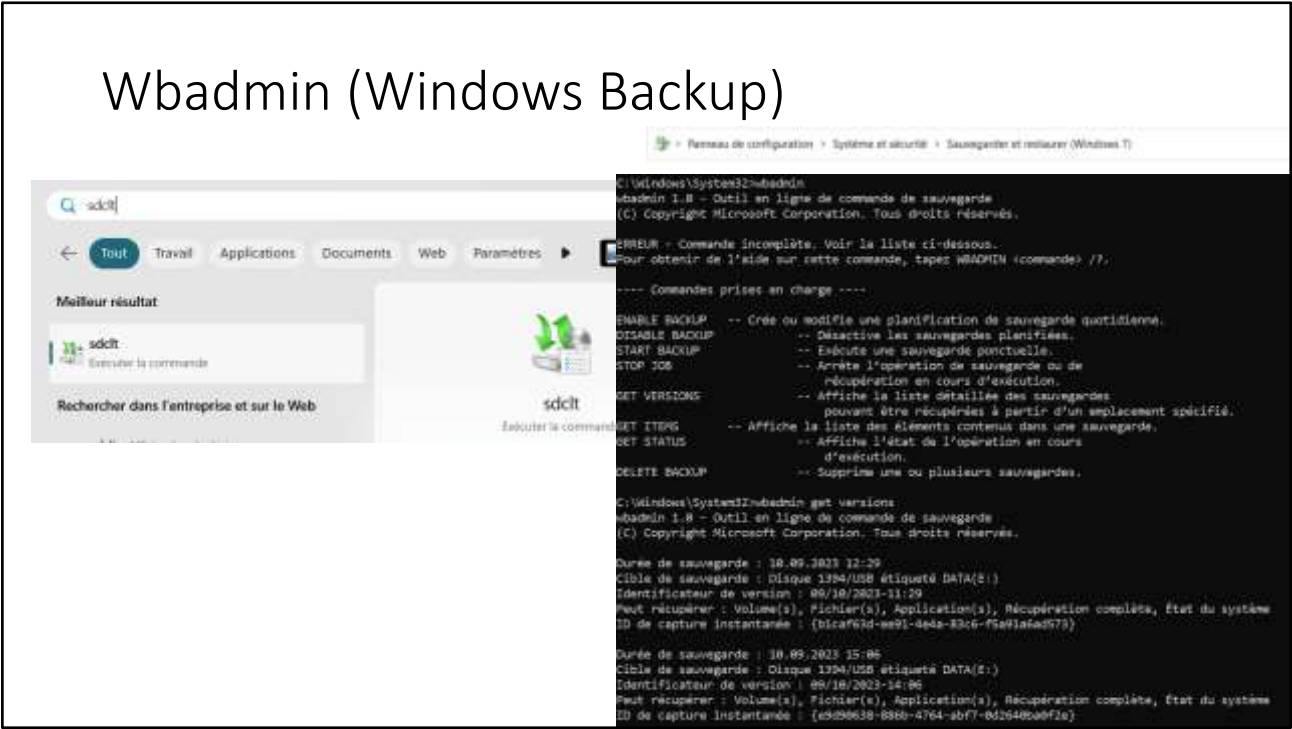


[Tutoriel sur l'activation de la touche F8 au démarrage de Windows 10 - Communauté Microsoft](#)

<https://answers.microsoft.com/fr-fr/windows/forum/all/tutoriel-sur-lactivation-de-la-touche-f8-au/7bc6d853-6dbf-421d-b185-651f2a342b24>

Pour créer une sauvegarde (un RestorePoint) en ligne de commande:  
`wmic.exe /Namespace:\\root\\default Path SystemRestore Call CreateRestorePoint "My Restore Point Name", 100, 7`

# Wbadmin (Windows Backup)



[Windows 11 : créer une sauvegarde de l'image système \(justgeek.fr\)](https://www.justgeek.fr/windows-11-creeer-sauvegarde-image-systeme-89856/)  
<https://www.justgeek.fr/windows-11-creeer-sauvegarde-image-systeme-89856/>

# DATA Roll-back ?

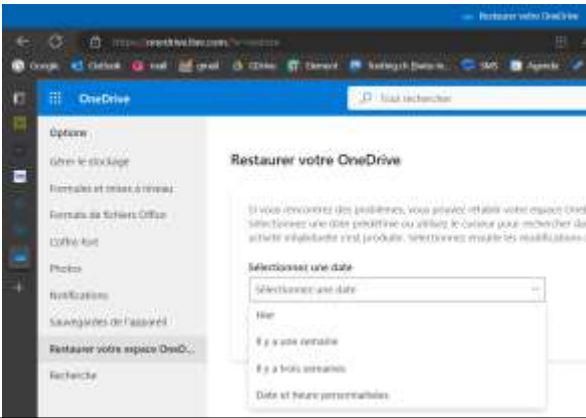


Cryptolocker – utiliser OneDrive

**ATTENTION:**

Les données critiques sont-elles correctement sauvegardées ?

- Vaudtax2024
- Fichier PST archives locales (outlook)
- Autres...

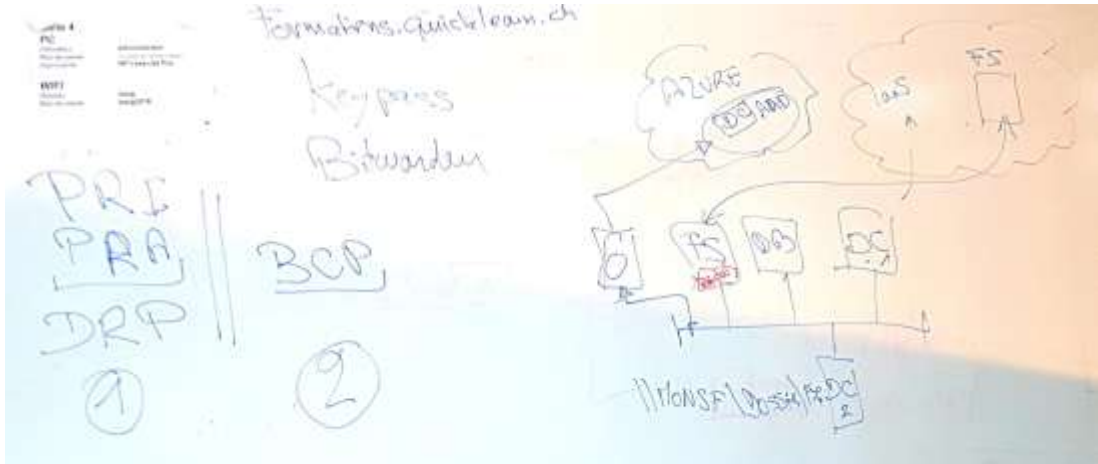


Désormais, OneDrive détecte le chiffage de fichiers et devrait demander confirmation avant écrasement dans le Cloud.

Sinon, il faudra faire un Rollback, par fichier (versions historiques) ou en bloc (et perdre les derniers, et donc les récupérer avant 1 par 1...)

# Recovery ? Plans de reprises, ou [SFT](#)?

DRP ou PRA = Disaster Recovery Plan ou Plan de Reprise d'Activité (ou PRI informatique)



Hors-sujet, mais connexe à la nécessaire capacité de maintenir les services opérationnels.

PRI ou PRA = Disaster Recovery Plan ou Plan de Reprise d'Activité  
SFT = System Fault Tolerance => Capacité de ne pas tomber en panne.

Exemple – le service Onedrive, qui permet au poste de continuer sur une copie locale sur le poste, hors connexion, et de récupérer un accès à une version enregistrée par le passé, en cas d'erreur et de suppression de données involontaires (voir un cryptage par un Malware).

<https://blog.bde-group.be/securite/la-continuite-des-activites-element-crucial-a-prendre-en-compte-dans-la-gestion-de-votre-securite/>



# Jamais sans un check, best VirusTotal

- [www.virustotal.com](http://www.virustotal.com)
- Check signatures (ex MD5 bad => SHA256 ok)



[Top 3 des outils pour sécuriser et nettoyer Windows 10](#) | by [Pascal Kotté](#) | [QuickLearn](#) | [Medium](#)

<https://medium.com/quicklearn/top-3-des-outils-pour-s%C3%A9curiser-et-nettoyer-windows-10-74ddcb3f9f24>

## Préparation du PC pour examen

- La machine ISEIG, s'assurer de la présence de toutes les mises à jour
- S'assurer de conserver les services Microsoft standard opérationnels pour ne pas «pénaliser» au test.
- Ouvrir et mémoriser dans le PC une session Edge avec votre compte @edu.iseig.ch afin de disposer d'un login facilité (mauvaise pratique, mais facilitera le test, conserver le mot de passe si besoin)
  - Ne pas initialiser la synchro onedrive
- Mettre vos notes, copie du support, toutes documentations, sur le PC ou dans votre OneDrive. (pas clef/disque externe autorisé durant l'examen)

### ENGAGEMENT de L'ISEIG

- Après le test, la machine est reformatée. **Pas de risque sécuritaire** pour votre compte @edu.iseig.ch ni votre session chatbot éventuelle.

### Attention:

L'étudiant est responsable de sa machine, et qu'elle reste opérationnelle pour le test à l'examen, si des bricolages peuvent affecter le comportement de la machine durant le test, alors il sera recommandé de la réinitialiser dès le matin, avant le test de 13h.

## Test – Un document word à remplir, 3h (+1h)



- L'ordinateur affecté est ouvert sur sa session @edu.iseig.ch (mémorisée sur ce PC)
  - Les supports et documentations de son choix doivent y être copiés en amont,
  - se munir de son mot de passe @edu.iseig.ch
  - Les sessions «connectées» sur autre chose que le compte @edu.iseig.ch doivent être fermées.
  - Office en ligne sera utilisé pour éditer le document examen dans son onedrive @edu.iseig.ch
- Préparer ses affaires comme pour partir
  - Pas droit à son ordinateur perso, ni son smartphone, docs papiers/crayons ok.
  - Récupérer son attestation (en amont) et remettre la feuille évaluation (corriger après test si besoin)
- Il n'est pas autorisé
  - De tenter de récupérer une copie du questionnaire à remplir, ni de le diffuser (c'est contrôlé).
  - De «chater» avec un tiers via Internet, ni en présentiel. 1 seul à la fois aux toilettes.
  - De conserver une clef USB ou disque externe sur le PC d'examen.
- A la fin du test, lever la main, laisser la session ouverte,
  - LAISSER VOS SESSIONS chatbot actives et ouvertes
  - L'examineur fera un export du doc rempli au format PDF, et copie docx de secours: sur le bureau par sécurité, puis clef usb (effacement après contrôle copies sur PC examinateur).

Directives officielles: Le LB couvre toutes les compétences du module. Les apprenants créent leur propre environnement système d'une petite PME avec de multiples services. Avec les commandes qui sont traitées au cours du module, cet environnement est étendu. Le LBV se compose de deux parties. Dans la partie pratique de la mise en œuvre, les services d'un réseau de PME doivent être enregistrés, gérés et mis à jour. Dans une partie écrite, en plus des questions axées sur la pratique, l'accent mis sur les questions conceptuelles devrait également être possible.

Cet examen de 3h max, +30 à 60mn pour palier TDH et dyslexies... (malus de points, sauf certificat médical)

Cet examen est conçu en mode «Jeux de rôle» et scénarios «in situ», afin de permettre à un informaticien expérimenté de passer et réussir ce test, sans avoir eu besoin de suivre le cours. Les notions abordées durant le cours doivent toutefois être connues et acquises par cette personne. L'accès en «Open source» à ce support permet de s'en assurer en amont.

# X. Annexes

Bonus

Supports libres additionnels, et contributions Welcome, envoyez vos propositions à [pk@iseig.ch](mailto:pk@iseig.ch)

## Cas pratique



- Un *user* se plaint d'un virus qui consomme CPU et mémoire sur son PC, DWM.exe
  - [Tu trouves cette info https://www.malekal.com/dwm-exe-resoudre-plantages-utilisation-anormale-cpu-windows-10-11/](https://www.malekal.com/dwm-exe-resoudre-plantages-utilisation-anormale-cpu-windows-10-11/)
- Où/comment contrôler que cet EXE est bien celui de Microsoft?
  - Car un vrai virus, va s'appeler pareil...
  - Comment est-il nommé, ou est-il localisé,
- Installer MBAM (Malwarebyte), mais sans le laisser ajouter un service (résident) sur le poste client
  - Lancer un SCAN sur la machine
  - Comment s'assurer que aucun service additionnel résident n'a été ajouté ?

On peut aussi utiliser Spybot, et faire le même exercice.

# Tools cools (end user)



## Tuning

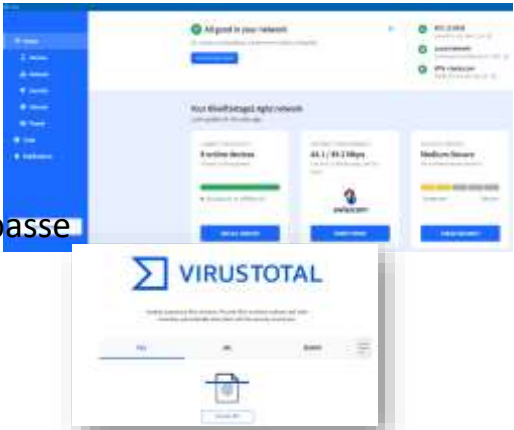
- [Piriform — Wikipédia \(wikipedia.org\)](#) : Ccleaner => [Quoique](#)
- ...

## Monitor + sécurité

- Fing.com (découverte réseau, mobile/pc)

## Sécurité

- BitWarden.com pour stocker les mots de passe
- Keypass (plus économique en entreprise)
- VirusTotal.com

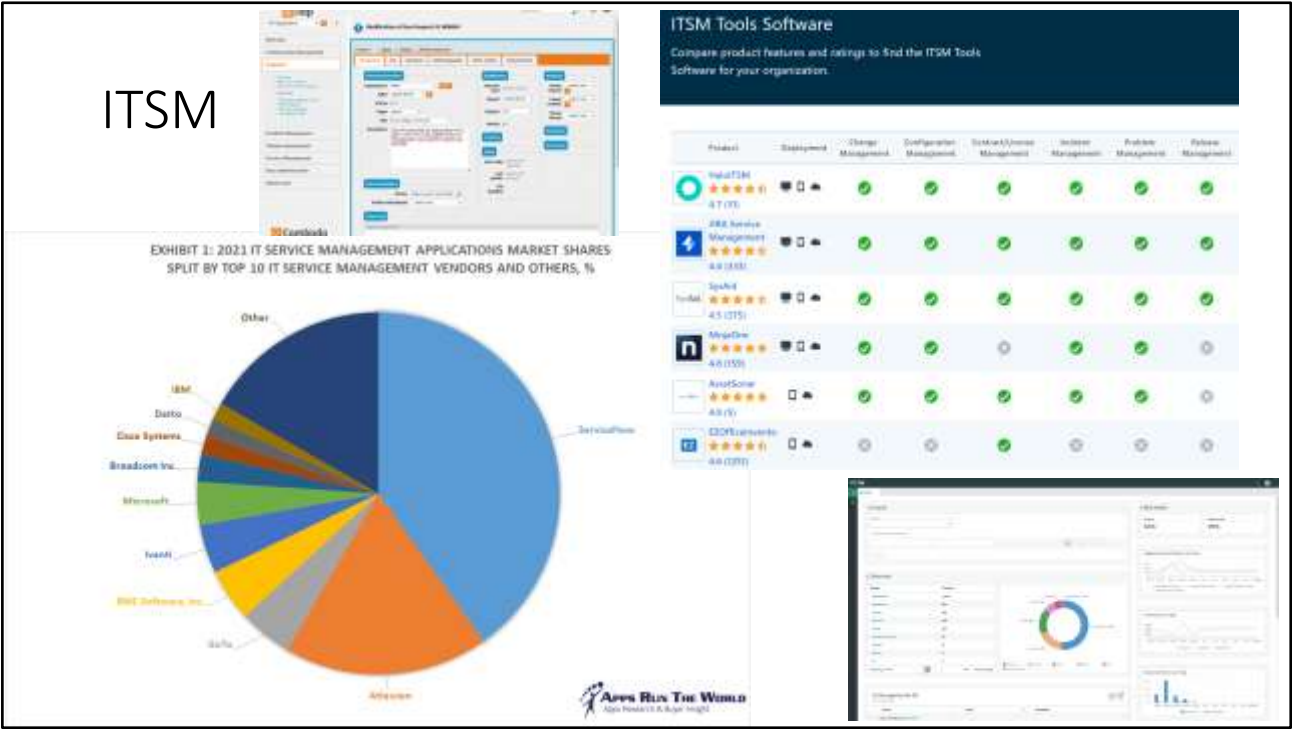


Quelques outils, plutôt destinés aux utilisateurs et non aux infrastructures IT.  
[https://www.fing.com/premium#premium\\_plans](https://www.fing.com/premium#premium_plans)

# Plateformes ITSM (Entreprises)

IT Service Management

IT Service Management



Un aperçu d'autres solutions:

- <https://www.capterra.com/sem-compare/itsm-software/>
  - <https://www.appsruntheworld.com/top-10-it-service-management-software-vendors-and-market-forecast/>
  - [https://fr.wikipedia.org/wiki/System\\_Center\\_Configuration\\_Manager](https://fr.wikipedia.org/wiki/System_Center_Configuration_Manager)
  - <https://www.microsoft.com/fr-ch/system-center>
  - <https://www.servicenow.com/now-platform.html>
- Alternatives
- <https://www.combodo.com/itop-193>



# ManageEngine

- Endpoint Central
- Patch Manager

		Free Edition	Edition Professionnelle	Edition Entreprise	Edition UEM
		Convient aux PME	Fonctionnalités de l'édition Professionnelle +		Fonctionnalités de l'édition Entreprise +
		Gère jusqu'à 25 ordinateurs et 25 appareils mobiles	Gestion des correctifs	Optimisation de la bande passante WAN	Gestion des périphériques mobiles
		Brexit des correctifs	Déploiement de logiciels	Portail Ultra-service	Gestion des périphériques Windows 10
		Déploiement de logiciels	Gestion des ressources	Logiciels Intelligents / Blocage des DEX	Déploiement d'OS
		Gestion des assets	Configurations	Mouvement des logiciels	
		Configurations	Outils système de Windows	Gestion des licences	
		Outils système de Windows	Contrôle à distance	Enregistrement des données à distance	
		Contrôle à distance	Rapports AD et de connexion des utilisateurs	Gestion des périphériques USB	
			Gestion des périphériques mobiles (Android)	Authentification à deux facteurs	
			Déploiement d'OS (Android)	Gestion des appareils mobiles (Android)	
				Déploiement d'OS (Android)	
Edition Gratuite	Professionnelle	Enterprise			
Jusqu'à 20 ordinateurs et 5 serveurs	Convient aux ordinateurs en réseau local	Convient aux ordinateurs en WAN			
Adaptée aux PME	• Correctifs pour Windows, Mac & terminaux Linux	Fonctionnalités de l'édition professionnelle +			
Entièrement fonctionnel	• Gestion des correctifs tiers	• Serveur de distribution pour l'optimisation de la bande passante			
Jusqu'à 20 ordinateurs et 5 serveurs	• Gestion des correctifs des applications serveur	• Mises à jour des définitions d'antivirus			
	• Déploiement des Service Packs	• Validation et approbation des correctifs			
	• Rapports sur la gestion des correctifs	• Authentification double facteur			
	• Administration basée sur les rôles				

Une solution avec version Freemium, pour 20 à 25 postes.

<https://www.manageengine.fr/produits/patch-management/presentation.html>  
<https://www.manageengine.fr/pdf/factsheet.pdf>

Ansible



ANSIBLE

Ansible est un outil d'automatisation et de gestion de configuration. Il simplifie le déploiement, la gestion des serveurs et l'orchestration, utilisant des playbooks YAML sans nécessiter d'agents clients sur les machines.

8. Flexibilité :

Ansible fonctionne sur une large gamme de systèmes d'exploitation, y compris Linux, Windows, macOS, et autres. Il peut être utilisé pour automatiser des tâches dans des environnements locaux, cloud ou hybrides.

Exemple de Playbook Ansible :

Voici un exemple simple de playbook Ansible pour installer Apache sur une machine Linux :

yaml

---  
- name: Installer Apache  
  hosts: all  
  become: yes  
  
  tasks:  
    - name: Installer le paquet Apache  
      apt:  
        name: apache2  
        state: present  
  
    - name: Démarrer le service Apache  
      services:  
        name: apache2  
        state: started  
        enabled: yes

**Ansible** est un outil de gestion de configuration, d'automatisation des tâches et d'orchestration des systèmes informatiques. Il est principalement utilisé pour déployer des applications, configurer des serveurs et automatiser des processus informatiques sur plusieurs systèmes ou environnements. Ansible est très populaire en raison de sa simplicité, de sa capacité à s'intégrer à différents systèmes et de sa facilité d'utilisation. Voici les principaux aspects d'Ansible :

**1. Automatisation de la gestion de configuration :**

Ansible permet de gérer la configuration des systèmes, comme l'installation de logiciels, la mise à jour des configurations et la gestion des utilisateurs, sans nécessiter d'intervention manuelle sur chaque machine. Cela est particulièrement utile dans des environnements où vous avez plusieurs serveurs ou machines à gérer.

**2. Déploiement d'applications :**

Il permet de déployer des applications de manière cohérente et automatisée sur différents serveurs. Cela peut inclure des tâches comme la configuration de bases de données, le déploiement de fichiers de configuration, ou encore l'installation de services web.

**3. Orchestration :**

Ansible permet d'automatiser des processus complexes impliquant plusieurs machines, comme la gestion de clusters de serveurs, le déploiement de services dans un ordre spécifique, ou la coordination de différentes étapes dans un pipeline de déploiement.

**4. Pas de client requis :**

119

Ansible ne nécessite pas d'agent client installé sur les machines qu'il gère. Il se connecte généralement via SSH (pour les systèmes Unix/Linux) ou WinRM (pour les systèmes Windows). Cela simplifie la gestion des machines, car vous n'avez pas besoin de déployer des agents supplémentaires.

#### 5. Langage déclaratif avec YAML :

Les tâches d'Ansible sont définies dans des fichiers appelés **playbooks**, qui sont écrits en YAML (Yet Another Markup Language). YAML est un format lisible par l'homme, ce qui rend les playbooks faciles à comprendre et à écrire, même pour les utilisateurs non techniques.

#### 6. Idempotence :

Une caractéristique importante d'Ansible est son idempotence, ce qui signifie que vous pouvez exécuter un playbook plusieurs fois sans que cela ait un effet négatif. Si l'état final désiré est déjà atteint, Ansible ne réappliquera pas les actions.

#### 7. Modules :

Ansible utilise des **modules** pour effectuer des actions spécifiques. Par exemple, un module peut être utilisé pour installer un paquet, copier un fichier, configurer un service, ou exécuter une commande sur une machine distante. Ansible possède des centaines de modules pour de nombreuses plateformes et technologies.

#### 8. Flexibilité :

Ansible fonctionne sur une large gamme de systèmes d'exploitation, y compris Linux, Windows, macOS, et autres. Il peut être utilisé pour automatiser des tâches dans des environnements locaux, cloud ou hybrides.

#### Exemple de Playbook Ansible :

Voici un exemple simple de playbook Ansible pour installer Apache sur une machine Linux :

```
---
- name: Installer Apache
  hosts: all
  become: yes
  tasks:
    - name: Installer le paquet Apache
      apt: name=apache2 state=present
    - name: Démarrer le service Apache
      service: name=apache2 state=started enabled=yes
```

Dans cet exemple :

- Le playbook installe Apache (apt: name=apache2 state=present).
- Il démarre ensuite le service Apache et le configure pour qu'il se lance au démarrage (service: name=apache2 state=started enabled=yes).

#### Avantages d'Ansible :

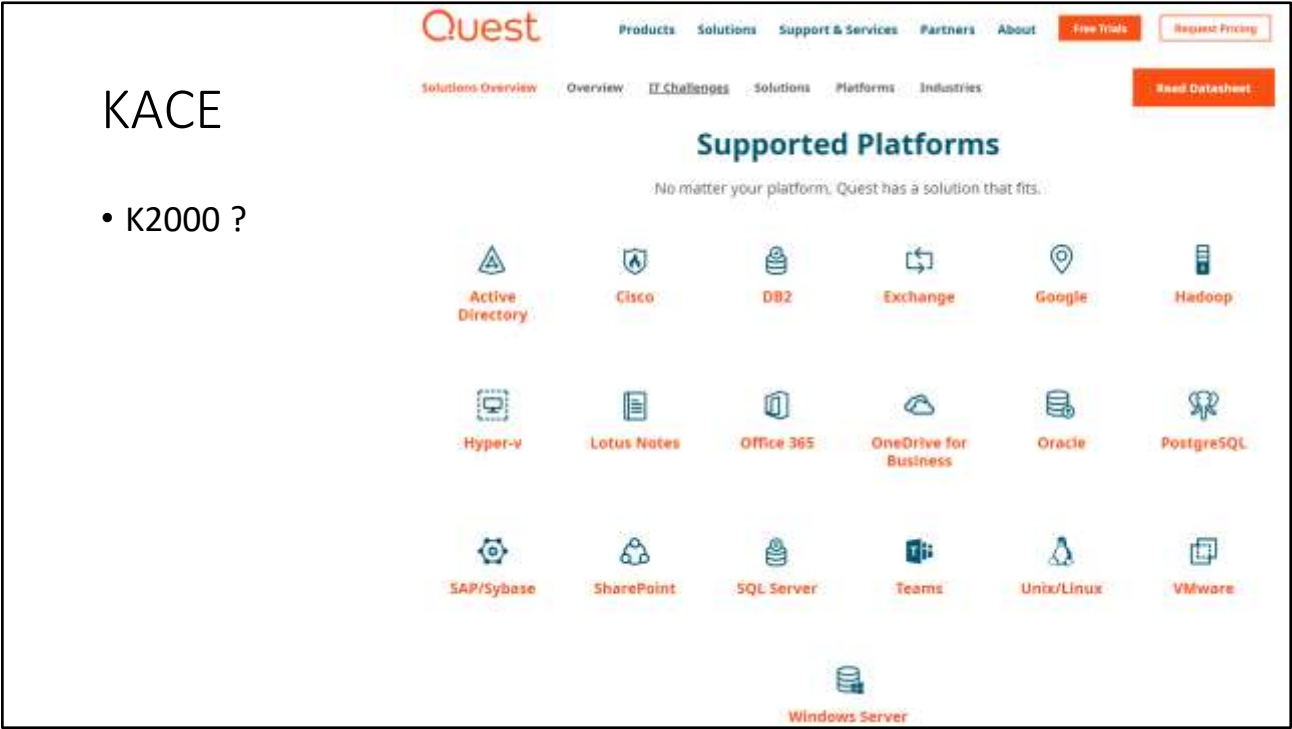
- **Simplicité** : Il est facile à installer et à configurer, et son utilisation ne nécessite pas de compétences en programmation.
- **Aucune dépendance d'agent** : Il ne nécessite pas de logiciels tiers installés sur les hôtes gérés.
- **Communauté active** : Ansible bénéficie d'une large communauté et d'une documentation complète, facilitant l'adoption et la résolution de problèmes.

#### Conclusion :

Ansible est un puissant outil d'automatisation utilisé pour simplifier la gestion des systèmes, les déploiements d'applications, et l'orchestration de tâches complexes sur plusieurs serveurs. Sa simplicité, sa flexibilité et son absence de dépendance à un agent client en font un choix populaire pour les administrateurs système, les ingénieurs DevOps et les équipes de développement.

# KACE

- K2000 ?



<https://www.quest.com/solutions/>

# Acronis

Oui bon...  
Backup  
Sécurité

Mais pas  
Tellement gestion  
des postes et  
déploiements logiciels

### Advanced Backup

Fonctionnalités Advanced Backup :

- Sauvegarde Microsoft SQL dans un cluster
- Sauvegarde Microsoft Exchange dans un cluster
- Sauvegarde des bases de données Oracle
- Sauvegarde SAP HANA
- Protection continue des données (CDP)
- Carte de la protection des données
- Score #CyberFit
- Sauvegarde directe dans un stockage dans le cloud public Microsoft Azure

### Advanced Management

Fonctionnalités Advanced Management :

- Évaluation de la vulnérabilité avec gestion des correctifs intégrés
- Application de correctifs sans échec
- Gestion des ressources grâce à l'inventaire logiciel
- Surveillance de l'intégrité des lecteurs
- Score #CyberFit
- Connexion de bureau à distance à des ressources Windows, macOS et Linux
- Transfert de fichiers
- Surveillance basée sur l'intelligence artificielle

### Advanced Email Security

Advanced Email Security permet la protection en temps réel pour vos boîtes aux lettres Microsoft 365 et Gmail :

- Antimalware
- Antispam
- Analyse d'URL dans les e-mails
- Analyse DMARC
- Anti-hameçonnage
- Protection contre l'usurpation d'identité
- Analyse des pièces jointes
- Désarmement et reconstruction du contenu
- Schéma de confiance

### Advanced Security + EDR

Fonctionnalités Advanced Security + EDR :

- Protection contre les virus et les malwares : Détection de fichier basée sur la signature locale
- Filtrage d'URL
- Sauvegarde d'investigation
- Analyse de sauvegarde centralisée à la recherche de malwares
- Restauration sûre
- Liste blanche d'entreprise
- Plans de protection intelligent (Intégration avec des alertes CPOC)
- Détection et réponse des terminaux (composant de corrélation d'événements, capable d'identifier les attaques ou menaces avancées en cours).
- Gestion du pare-feu des terminaux
- Tableau de bord de conformité du score #CyberFit et évaluation de configuration avancée

### Advanced Data Loss Prevention

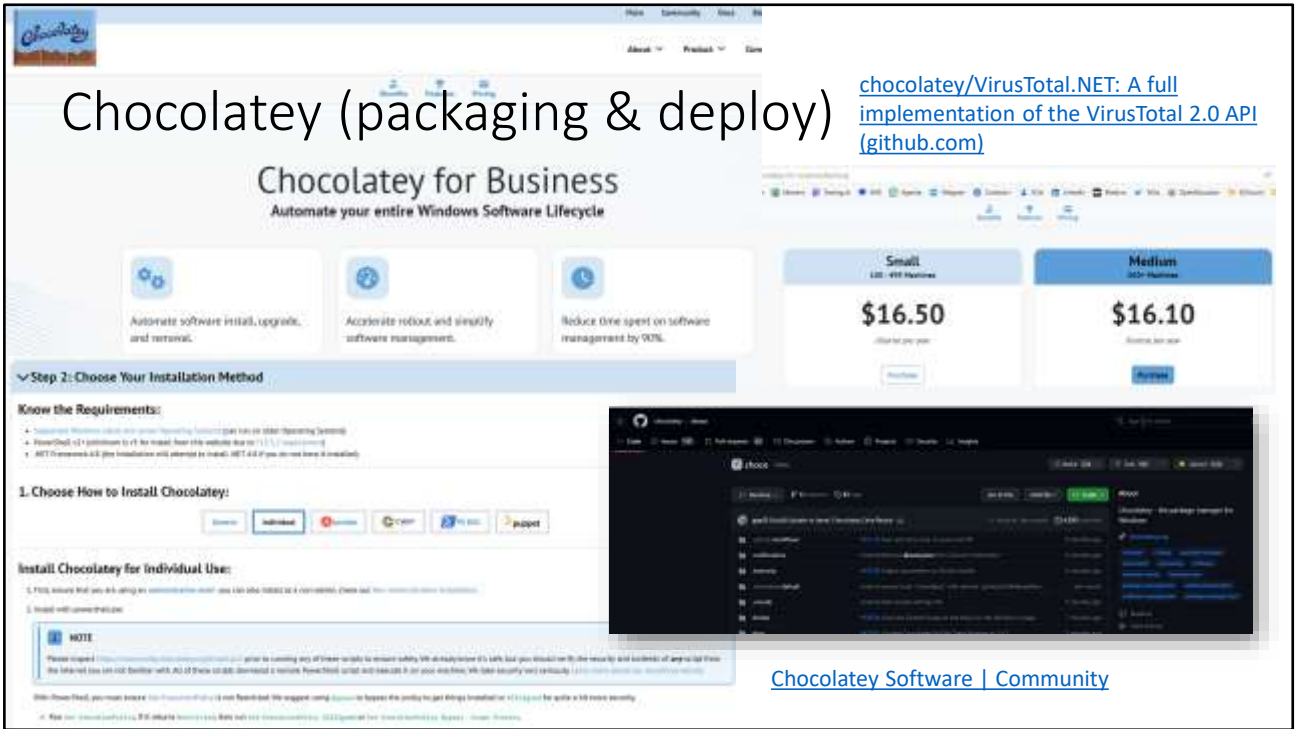
Évite les fuites d'informations sensibles en inspectant le contenu des données transférées via des canaux locaux et réseaux, en appliquant des classifications de données prédéfinies, et en affinant la règle de flux de données propre à l'organisation dans le mode de mise en application. Advanced Data Loss Prevention est applicable aux éléments suivants :

- Postes de travail
- Serveurs
- Machines virtuelles

créer des espaces de tests disponibles pendant 30 jours via [ce lien](#) ou consulter nos parcours de formations certifiantes (gratuites) en vous inscrivant sur notre [portail partenaires](#).  
<https://www.acronis.com/en-eu/products/cloud/trial-datacenters/#registration>  
<https://partners.acronis.com/login>

# Chocolatey (packaging & deploy)

[chocolatey/VirusTotal.NET: A full implementation of the VirusTotal 2.0 API \(github.com\)](https://github.com/chocolatey/VirusTotal.NET)



The screenshot displays the Chocolatey for Business website, which offers a solution to automate the Windows software lifecycle. It features three main benefits: automating software installation, upgrades, and removals; accelerating rollout and simplifying software management; and reducing time spent on software management by 90%. Pricing is shown for Small (100-499 machines) at \$16.50 and Medium (500+ machines) at \$16.10 per user per year. The 'Step 2: Choose Your Installation Method' section lists requirements and installation options (Binary, Individual, Chocolatey, PowerShell, Puppet, Ansible). A terminal window on the right shows the command 'choco install VirusTotal.NET' being executed, with output indicating the package is installed successfully.

[Chocolatey Software | Community](https://community.chocolatey.org/)

<https://github.com/chocolatey/VirusTotal.NET>  
<https://community.chocolatey.org/>

# Microsoft SCCM

- <https://www.microsoft.com/fr-ch/system-center>



- **System Center Operations Manager**  
Monitor health, capacity, and usage across applications, workloads, and infrastructure.
- **System Center Orchestrator**  
Automate your datacenter tasks; efficiently create and execute runbooks using native PowerShell scripts.
- **System Center Virtual Machine Manager**  
Deploy and manage your virtualized, software-defined datacenter with a comprehensive solution for networking, storage, compute, and security.
- **System Center Service Manager**  
Automated service delivery tool for incident resolution, change control, and asset lifecycle management.
- **System Center Data Protection Manager**  
Protect your data with backup, storage, and recovery for private cloud deployments, physical machines, clients, and server applications.

[System Center 2022 | Microsoft Evaluation Center](https://www.microsoft.com/en-us/evalcenter/evaluate-system-center-2022) <https://www.microsoft.com/en-us/evalcenter/evaluate-system-center-2022>

## Outils d'automatisation, DEVOPS



### Why Puppet

Innovate through infrastructure automation.

At Puppet, we're redefining what is possible for continuous operations. We empower IT operations teams to easily automate their infrastructure, enabling them to deliver at cloud speed and cloud-scale.

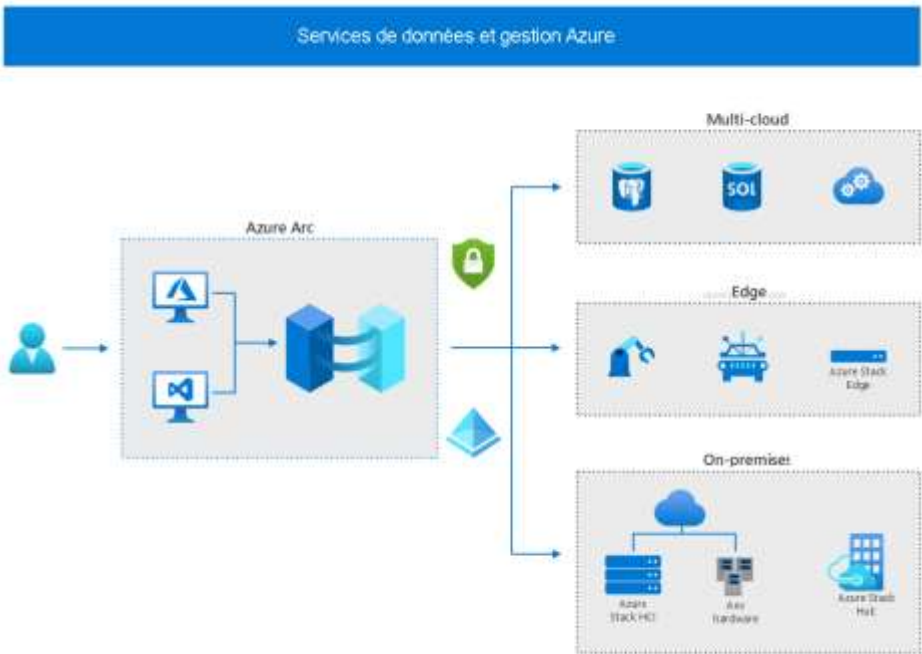
Dans l'univers Microsoft: Les Automatisations sont assurées généralement avec des Scripts en Powershell.

<https://fr.wikipedia.org/wiki/Puppet>  
<https://puppet.com/why-puppet/>



# Azure ARC

Avec Azure Arc, vous pouvez gérer vos ressources informatiques, où qu'elles soient hébergées, en utilisant les mêmes outils et pratiques de gestion Azure que ceux que vous utilisez pour gérer les ressources hébergées dans Azure.



[Décrite Azure Arc - Training | Microsoft Learn](https://learn.microsoft.com/fr-ch/training/modules/intro-to-azure-arc/2-describe-azure-arc)  
<https://learn.microsoft.com/fr-ch/training/modules/intro-to-azure-arc/2-describe-azure-arc>

# PowerToys & Sysinternals



Sysinternals

Article • 12/12/2022 • 2 minutes to read • 10 contributors

Feedback

The Sysinternals web site was created in 1996 by [Mark Russinovich](#) to host his advanced system utilities and technical information. Whether you're an IT Pro or a developer, you'll find Sysinternals utilities to help you manage, troubleshoot and diagnose your Windows systems and applications.

Learn / Windows / Development environment / PowerToys /

Feedback

## Microsoft PowerToys: Utilities to customize Windows

Article • 11/29/2022 • 5 minutes to read • 15 contributors

Feedback

Microsoft PowerToys is a set of utilities for power users to tune and streamline their Windows experience for greater productivity.

Install PowerToys

[Microsoft PowerToys](#) | [Microsoft Learn](#)

<https://learn.microsoft.com/en-us/windows/powertoys/>

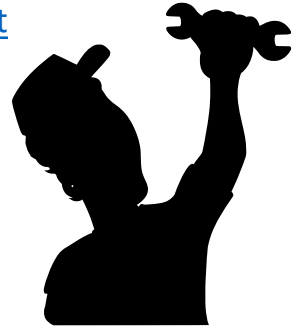
[Sysinternals Suite - Sysinternals](#) | [Microsoft Learn](#)

<https://learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite>

## SFC et DISM (vérifier le système Windows)

[Using System File Checker in Windows - Microsoft Support](https://support.microsoft.com/en-us/windows/using-system-file-checker-in-windows-365e0031-36b1-6031-f804-8fd86e0ef4ca)

- CMD (admin)
- DISM.exe /Online /Cleanup-image /Restorehealth
  - Va prendre un moment...
- sfc /scannow
  - Attendre: Verification 100% complete



Devrait restaurer une intégrité avec les bons fichiers. Si, un doute (malware), un bug...

<https://support.microsoft.com/en-us/windows/using-system-file-checker-in-windows-365e0031-36b1-6031-f804-8fd86e0ef4ca>

<https://answers.microsoft.com/en-us/windows/forum/all/sfc-scannow/bc609315-da1f-4775-812c-695b60477a93>

# WineHQ sur Linux pour EXE Windows

Merci Ethan  
pour le tuyau

Wine (à l'origine un acronyme pour « Wine Is Not an Emulator ») est une couche de compatibilité capable d'exécuter des applications Windows sur divers systèmes d'exploitation conformes à POSIX comme Linux, macOS et BSD. Plutôt que de simuler la logique interne de Windows comme une machine virtuelle ou un émulateur, Wine traduit les appels de l'API Windows en appels POSIX à la volée, éliminant les pénalités mémoire et de performance d'autre méthodes et vous permettant d'intégrer proprement les applications Windows à votre bureau.



<https://www.winehq.org/>

<https://www.winehq.org/>

Ntopng

nmap

