

**CloudReady.ch**Observatoire  
Suisse Romand  
du Cloud Computingupdate back to:  
Info@CloudReady.ch

# 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 > v2022-11-10 > v2023-05-10 > v2023-09-16

<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)  
<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

**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»...

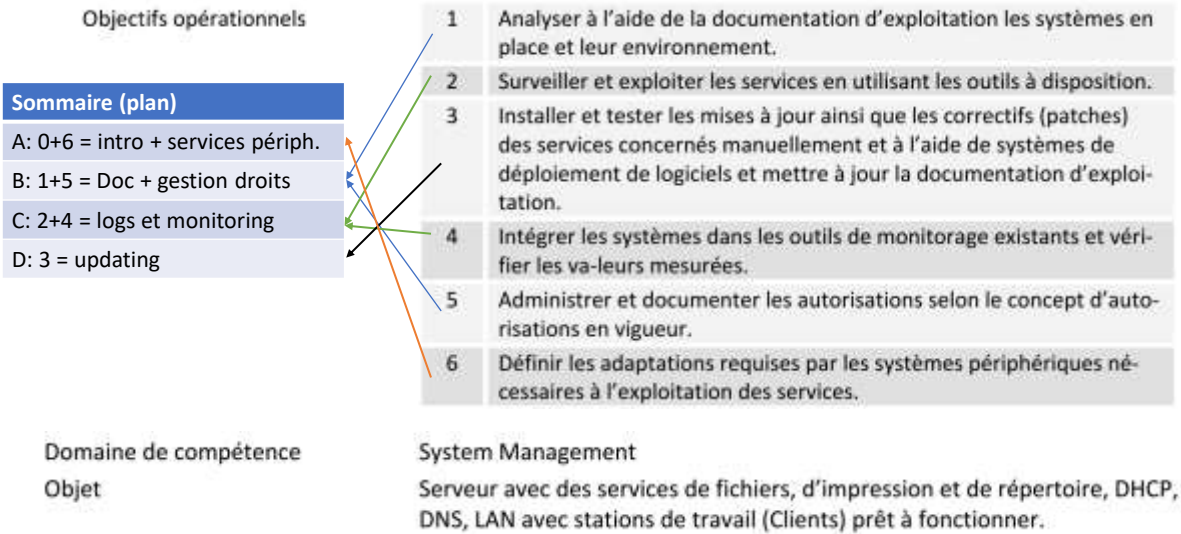
### Les accords toltèques

<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



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.

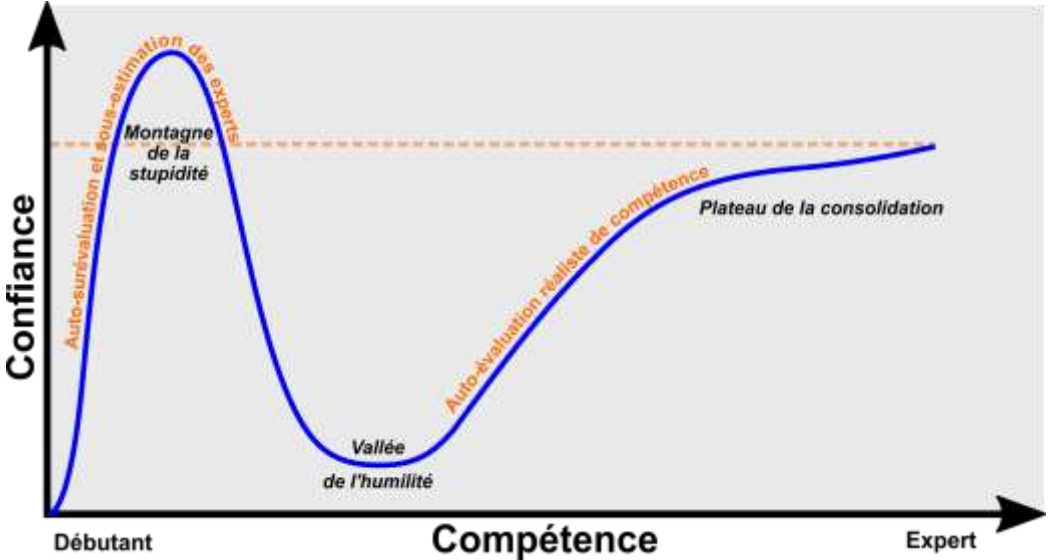
4.1 Connaître des techniques possibles (p. ex. SNMP, WMI) pour la saisie centralisée des données de performance et leurs mécanismes de sécurité. 4.2 Connaître les étapes de configuration à effectuer sur un système de serveur pour activer les mesures de performance (p. ex. SNMP, WMI). 4.3 Connaître les 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.

Biais de sur-confiance

Effet Dunning-Kruger



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)

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.

Le service peut tourner au niveau «machine» (system) et/ou au niveau «users» (profil utilisateur)

(Web) Applications

agents OS (Windows)

Services OS (Windows)

OS (Operating System = Système d'exploitation)

Service user interface (settings)

Services user (tray icons windows)

Services installés

Utilisateur

Système

Web service/serveur  
Port ip Ecoute: 80/443

Programme «résident»

Si cela **se lance tout seul!** C'est un service... Mais il a bien fallu qu'une installation soit lancée par qq1! Sans savoir?

<https://www.virustotal.com/>  
<https://portableapps.com/apps>

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 19)

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)

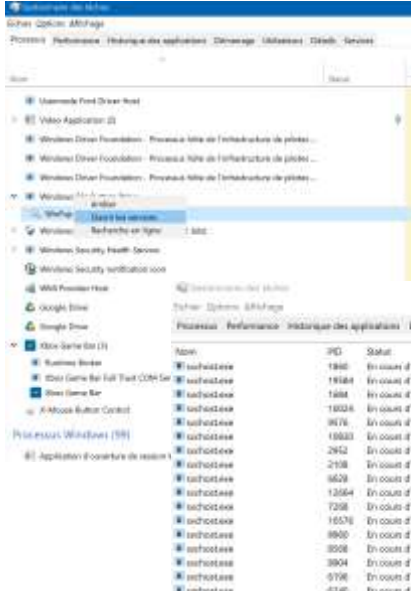
<https://medium.com/quicklearn/ccleaner-de-piriform-b54351a49fa>

- IOBit !! => PUP (<https://www.malwarebytes.com/blog/detections/pup-optional-cacaoweb>) Pas recommandé

6



# 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.



# 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



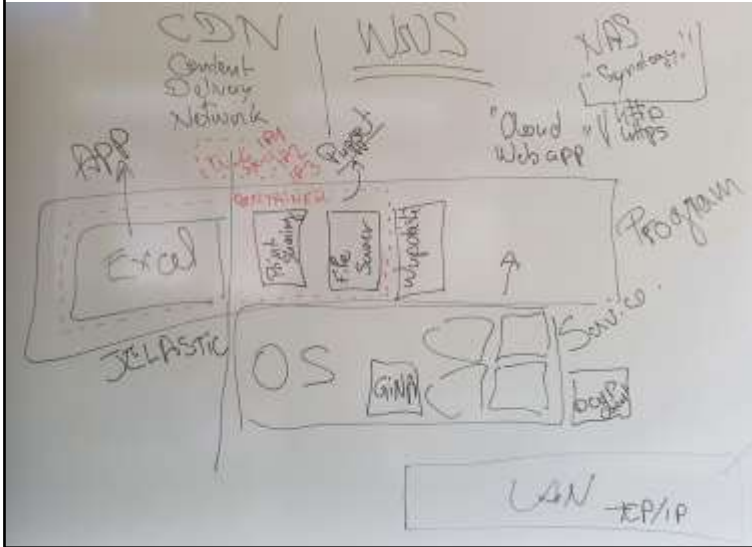
Cette photo par Auteur inconnu est soumise à la licence CC BY-SA

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](#)

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



DHCP, DNS, AD (Kerberos)  
Autres exemples...  
CDN, NAS, WSUS, Vmware

Discussions et échanges sur les services numériques d'infrastructures réseaux et systèmes, connus par les apprentis, ou pas...

## 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
- Fourniture et maintenance d'un réseau avec accès Internet
- Mise à disposition d'imprimantes, emails, espaces de stockage backupés
- Fourniture des informations aux usagers pour utiliser l'IT
- Déploiement d'un logiciel sur les bons postes
- ...

Et il y a ceux que les utilisateurs ne voient pas, ou peu:

- 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.



## 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.

**Cela sert à quoi  
l'IT?**

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

<http://pascal.kotte.net>

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).

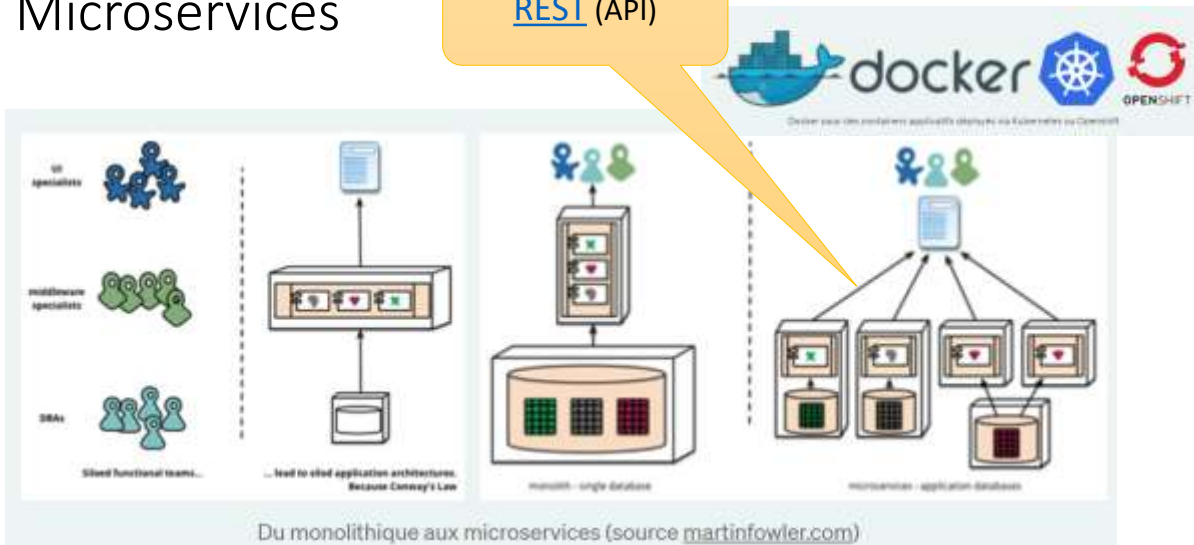
<https://www.capital.fr/votre-carriere/esn-entreprise-de-services-numeriques-definition-et-fonctionnement-1405805>

<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>  
iPaaS ? C'est quoi ?. Si je dis IFTTT, Zapier, Workato ... | by Pascal Kotté | CloudReady CH | Medium

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

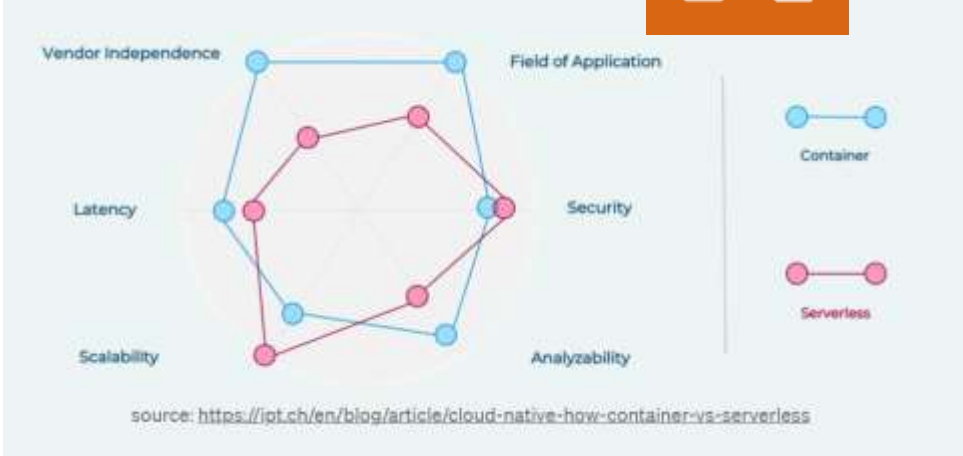
[https://fr.wikipedia.org/wiki/Representational\\_state\\_transfer](https://fr.wikipedia.org/wiki/Representational_state_transfer)

Google Cloud

Serverless computing



# DEVOPS to NoOPS



The diagram illustrates the trade-offs between Container and Serverless architectures. It features a central hexagonal network of nodes connected by lines. The nodes are color-coded: blue for Container and pink for Serverless. The metrics being compared are: Vendor Independence, Field of Application, Latency, Security, Scalability, and Analyzability. To the right, a legend shows a blue line for 'Container' and a pink line for 'Serverless'. The source is cited as: <https://igt.ch/en/blog/article/cloud-native-how-container-vs-serverless>

Les micros-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](#)

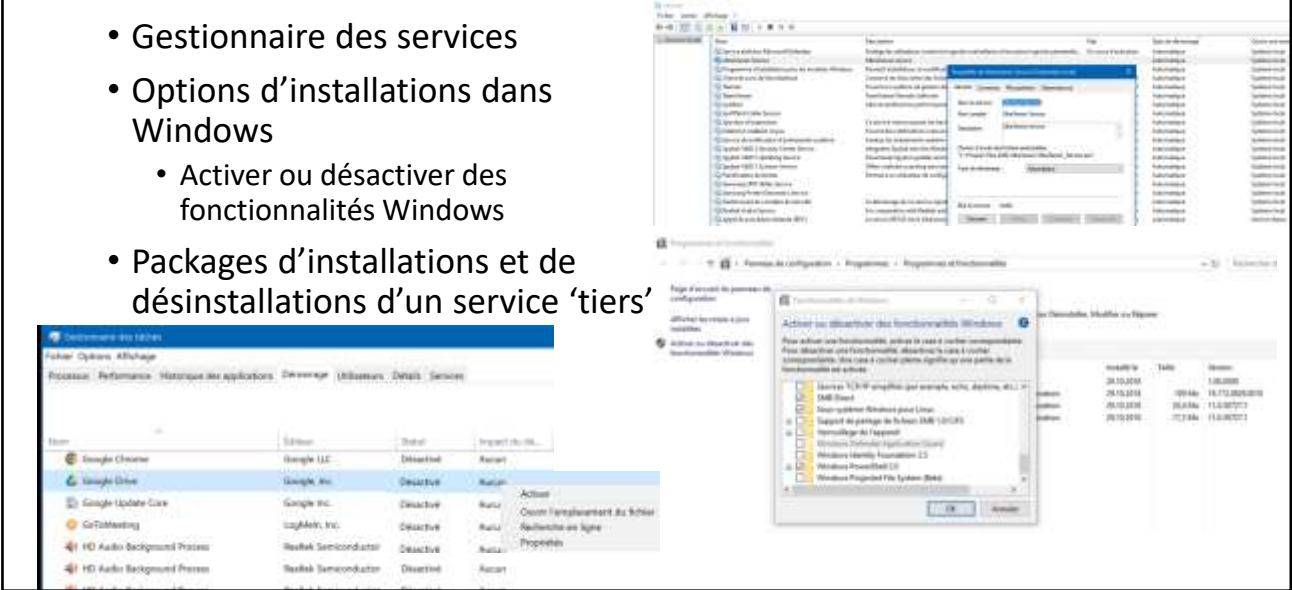


Avec OpenStreetMap - <https://www.openstreetmap.org/#map=18/46.53552/6.66660>

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>

# Activer/désactiver un service

- Gestionnaire des services
- Options d'installations dans Windows
  - Activer ou désactiver des fonctionnalités Windows
- Packages d'installations et de désinstallations d'un service 'tiers'



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/>

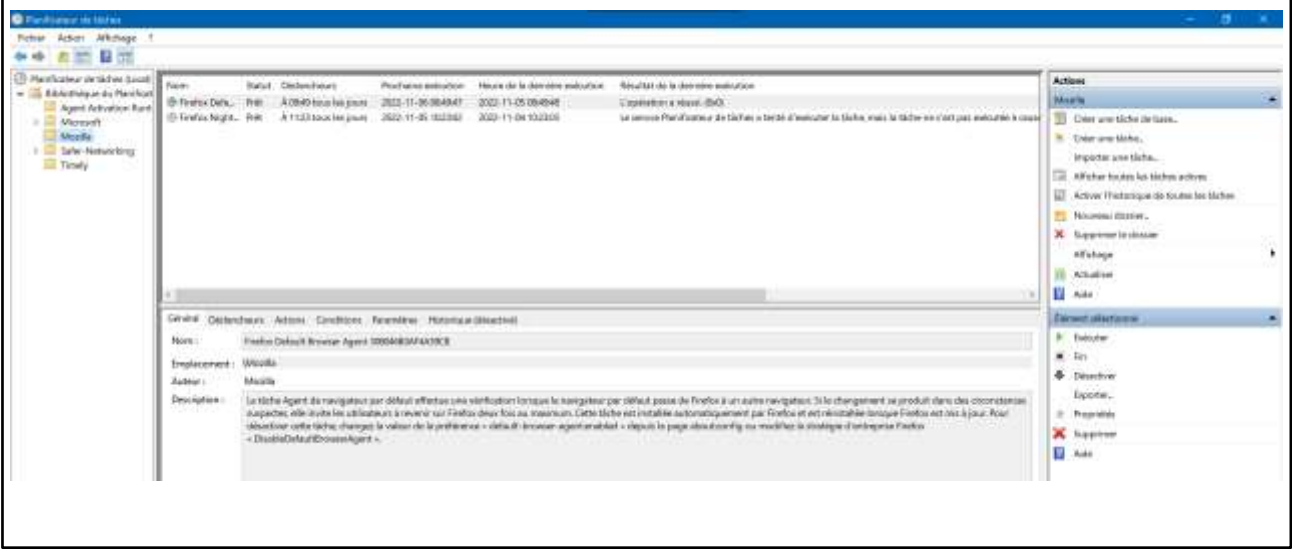
Propose de déployer des applications sans installations.

Mais un programme « non déclaré » s'il se lance tout seul, devient « un service »:

Par exemple, un troyen...

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>

## 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.

Pour fonctionner, un client qui affiche une page web, va avoir besoin de quels services ?

- Un matériel numérique (smartphone/tablet/pc) avec interface Ether.
- OS, pour héberger les services clients – Même chose côté serveur
- DHCP pour récupérer une ip (Et donc: un service DHCP serveur)
- Une connectivité Internet (Et donc tous les routeurs/switchs traversés)
- DNS pour récupérer l'ip d'un nom (le host www du domaine ciblé)
- Un routeur NAT ou un Firewall pour sécuriser son terminal/client.
- Une App traducteur html sur le client: Navigateur, à jour, sans faille/bug...



Exercice collectif, lister tous les services numériques nécessaires opérés pour permettre l'affichage d'une page simple page web.

CF. <http://dns.quicklearn.ch> Pour explorer et comprendre DNS

[https://fr.wikipedia.org/wiki/Network\\_address\\_translation](https://fr.wikipedia.org/wiki/Network_address_translation)

[https://fr.wikipedia.org/wiki/Hypertext\\_Markup\\_Language](https://fr.wikipedia.org/wiki/Hypertext_Markup_Language)

[https://fr.wikipedia.org/wiki/World\\_Wide\\_Web](https://fr.wikipedia.org/wiki/World_Wide_Web)

# Exemple des services d'impressions

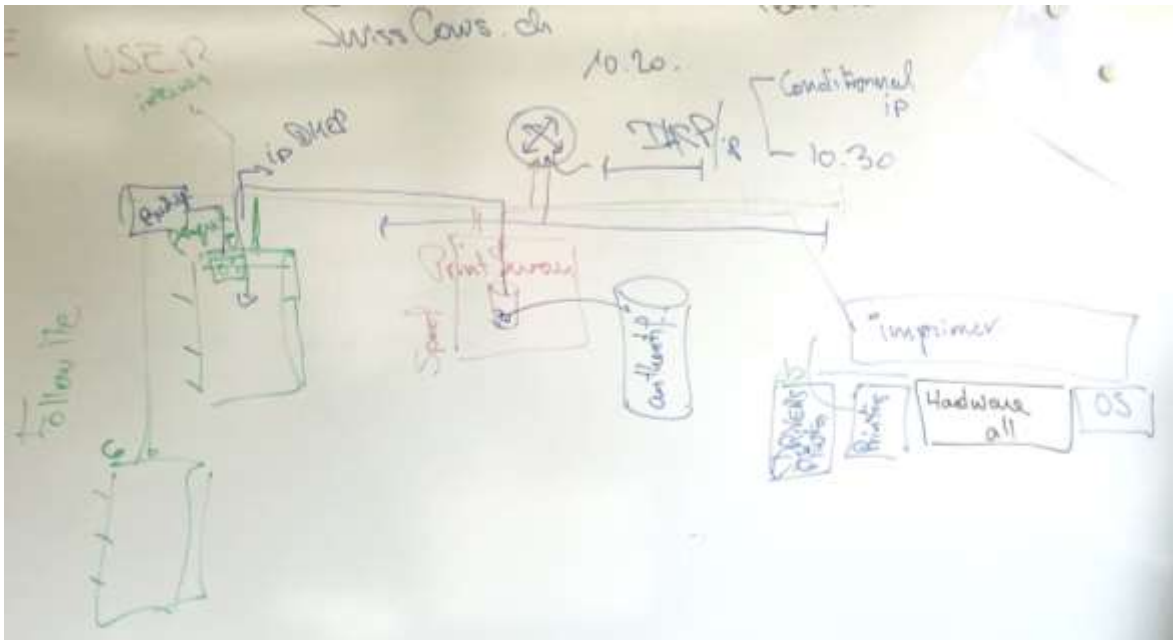
Avec la fonction «follow me»

The diagram illustrates a network setup for printing services. It includes a DHCP server, a DNS server, a print server, and various clients like PCs and printers. A green box highlights the 'follow me' function.

- DHCP Server:** Labeled 'DHCP' and 'IP Dyn. DHCP'. It has a '70' and a triangle symbol next to it.
- DNS Server:** Labeled 'DNS' and '58' with a triangle symbol. It has a '10.1.1.255' and 'broadcast' label.
- Print Server:** Labeled 'Service d'impression'. It has a 'Print Server' label and a 'Ganon x 3' label.
- Clients:** Includes 'PC', 'S1', 'S2', and 'Printer'.
- Network:** Labeled 'interne'.
- External Network:** Labeled 'Internet'.
- Other Labels:** 'S1', 'S2', 'PC', 'Printer', 'Ganon x 3', 'L4P x 5', 'L4P x 5', 'Shop (photocop)', 'Agnt (M1)', 'file d'attente', 'on-demand', '1. Priorité - général - décentralisation', '2. Sécurité - confidentialité', '3. Décompte', 'auto alloue'.

21

Service d'impression, schéma 2



Autre travail fait en classe.



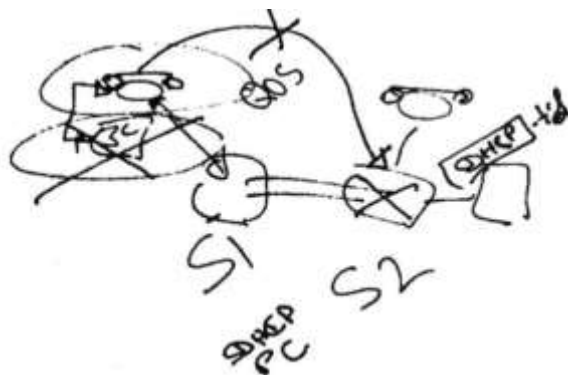
## Sans une doc Adhoc et du monitoring

- 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.

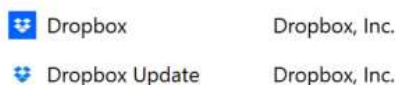
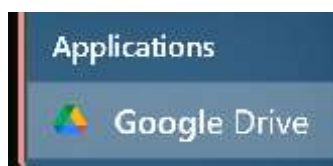
Lister les bonnes pratiques collectivement (si assez de temps dispo).

- Sera repris par la suite dans le § suivant.

## Exemple de service: OneDrive

**Avec Cryptolocker  
detection (\$)**

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




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?
- ...

## Exemple de services

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



Azure Active Directory


<http://dns.quicklearn.ch>

Handwritten notes:


127.0.1.1 local host  
Cloudflare 1.1.1.1 Net.DNS  
8.8.8.8 Google DNS

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.

### Azure private DNS Zone



**DHCP DISCOVER**



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

**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.

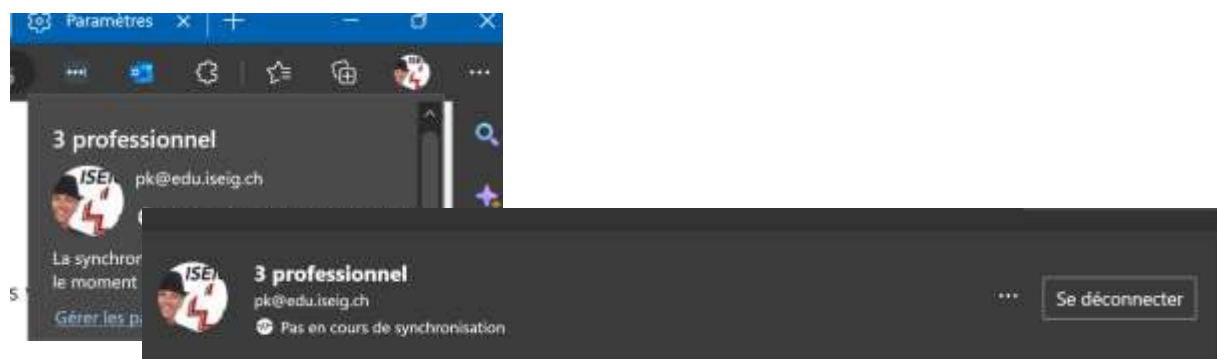
Recommandation à tout apprenti informaticien: Se prendre un domaine DNS pour son propre usage,

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.

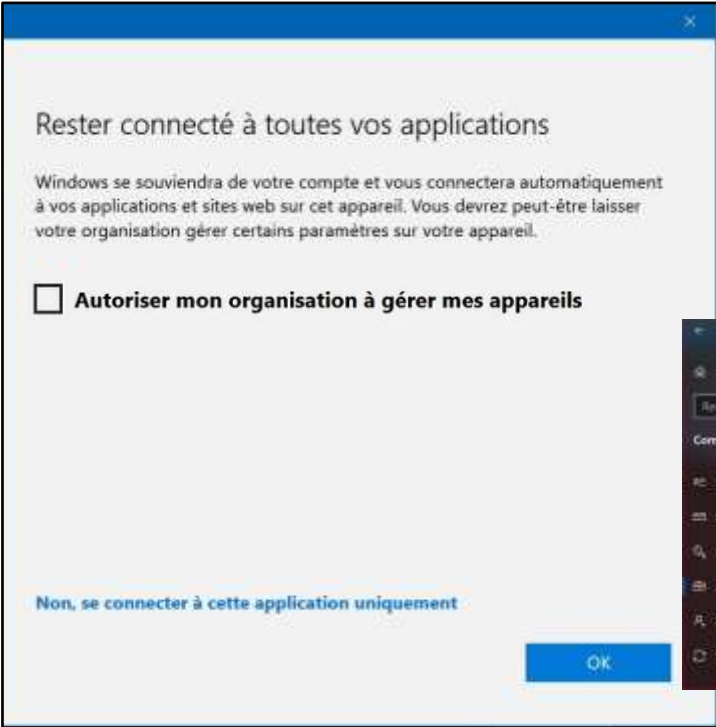
Petite exploration sur le nettoyage des Cookies, des Notifications, et usage du profil...

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>



## Auto-login SSO via service machine Windows

Pas bonne idée si PC partagé avec d'autres, ou pas le sien propre...



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

## 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.

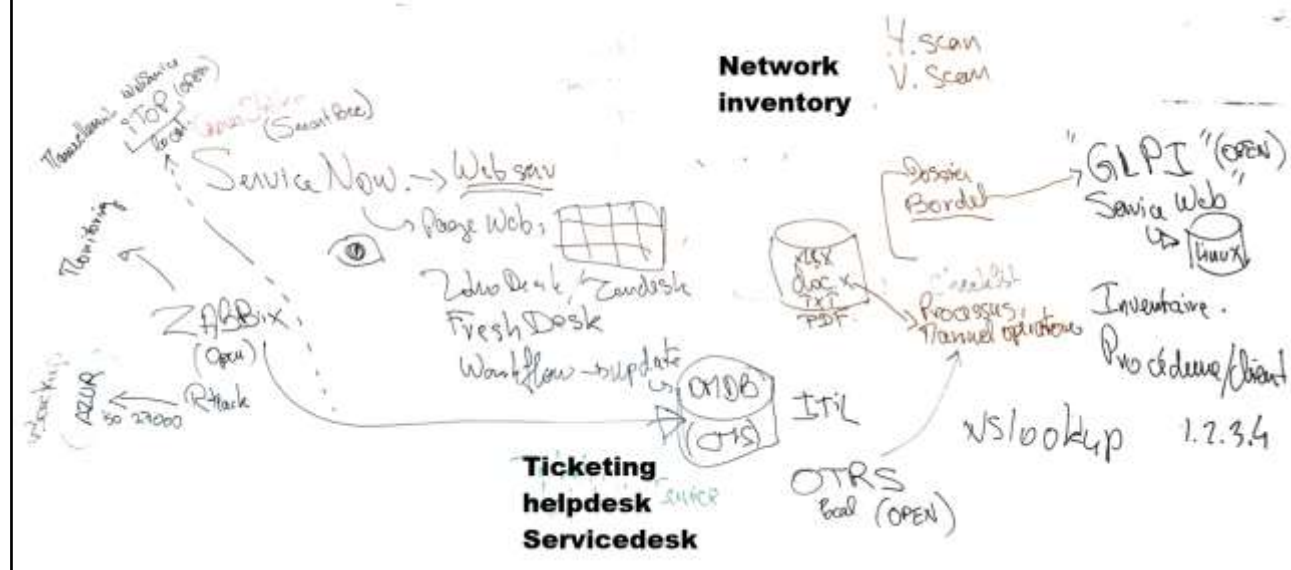
1.1 Connaître le contenu, la structure et l'application d'une documentation d'exploitation.

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.





<https://www.atlassian.com/fr/itsm/knowledge-management/what-is-a-knowledge-base>  
<https://www.ninjaone.com/fr/gestion-de-la-documentation-informatique/>

- Excel sheet (liste de paramètres de configurations, en format checklist)

## 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](#)



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'orthographe, 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

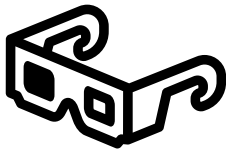
Directement utiliser des modules de « Learning platform »

- 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?

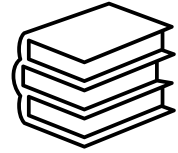
Être lucide sur les éléments qui DOIVENT être documentés.

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)

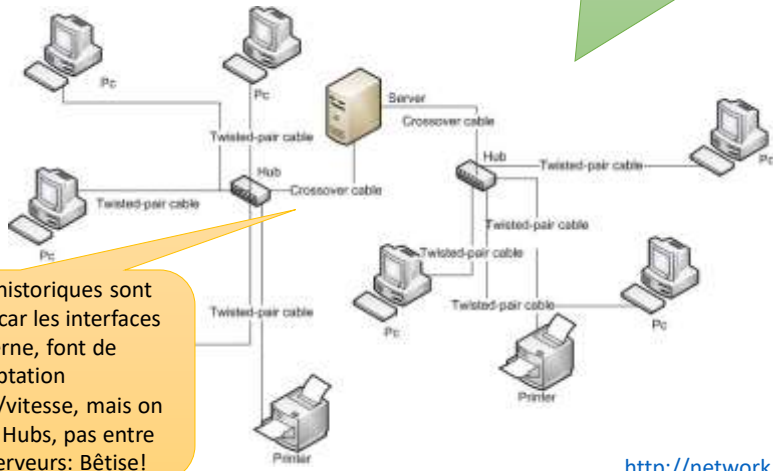
### RECOMMANDATION:

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 \(wikipedia.org\)](#)



<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 ?

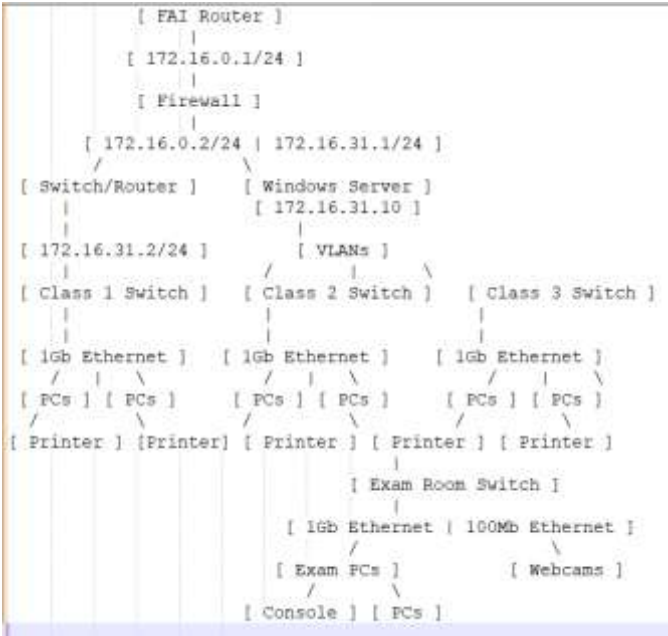
## Exercice – Dessiner et documenter le réseau ci-dessous

- 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





## 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...

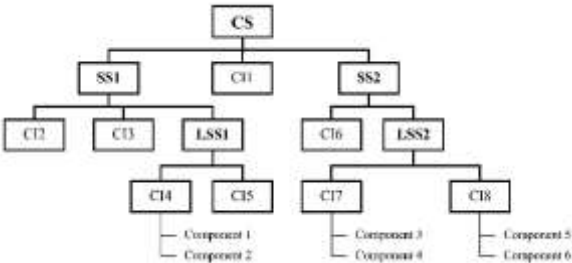
Parfois, plusieurs simples, peuvent paraître plus facile à mettre en œuvre qu'une grosse intégrée, et s'avérer requérir des redondances opérationnelles,

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

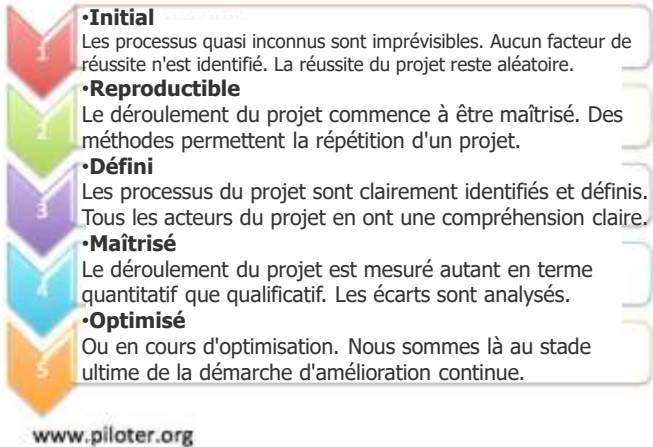
(ISO 10007) = qualité  
ITIL (ISO 20000)  
CDMB => CMS  
COBIT (ISO9000) = ISACA  
ISO 27000 (39p) = sécurité



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



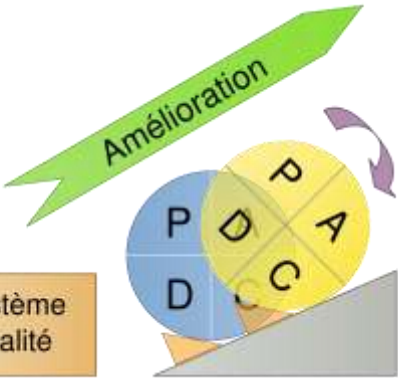
Ces éléments sont du ressort de l'IT manager, des ingénieurs, pas des opérateurs/techniciens – Mais c'est important d'avoir un aperçu des éléments qui conditionnent les organisations IT et leurs documentations.

[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

Système qualité

- 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/Roue_de_Deming)  
<https://fr.wikipedia.org/wiki/QQQQCCP>  
[https://fr.wikipedia.org/wiki/D%C3%A9coupage\\_de\\_l'information\\_pour\\_priorit%C3%A9](https://fr.wikipedia.org/wiki/D%C3%A9coupage_de_l'information_pour_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».
    - 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/criticite%C3%A9-3da6955752a9>

## 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.

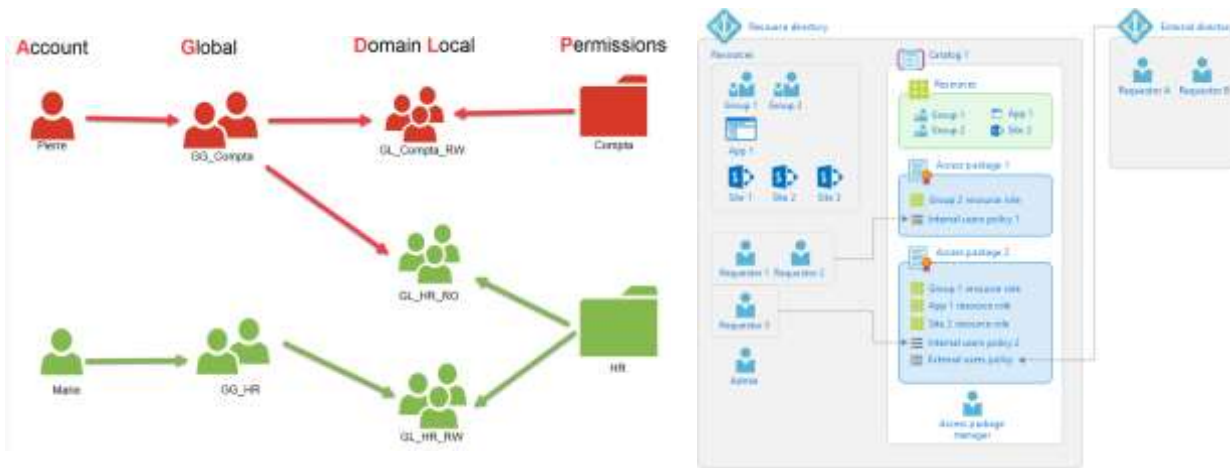
Le rôle de l'IT, sera de se donner les moyens:

- 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



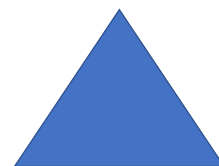
Droits NTFS, et AGDLP...  
<https://rdr-it.com/blog/agdpl-agudlp-comment-bien-gérer-les-droits-sur-un-serveur-de-fichiers-windows-serveur/>

- 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 sécurités 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.

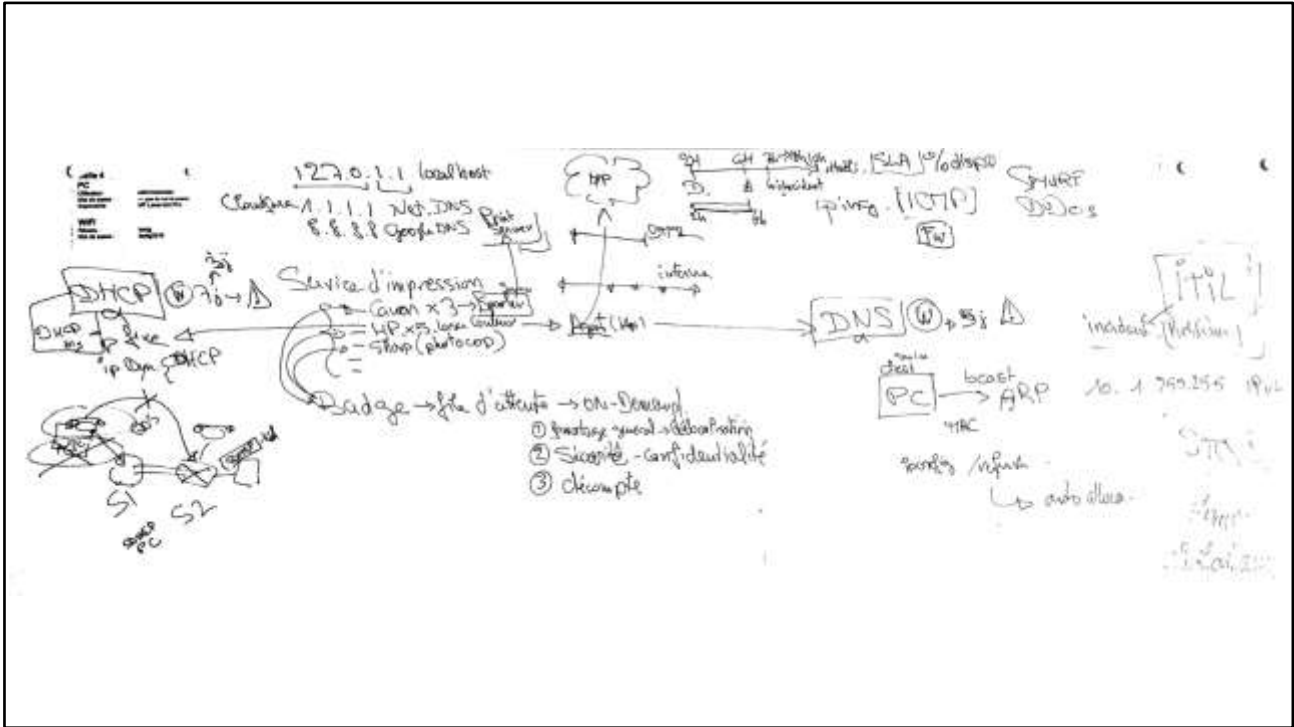


<https://learn.microsoft.com/fr-fr/troubleshoot/windows-server/identity/troubleshoot-errors-join-computer-to-domain>

<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>



Exemple de dessin fait au tableau pour faire un travail d'analyse de l'ensemble des services nécessaire pour faire fonctionner une application réseau sur un PC.

Travaux collectif en classe.

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.

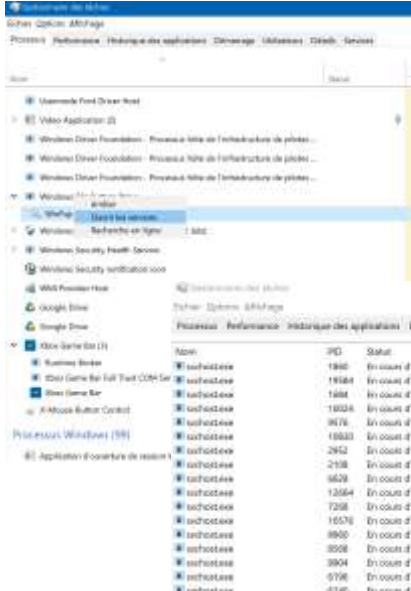
4.1 Connaître des techniques possibles (p. ex. SNMP, WMI) pour la saisie centralisée des données de performance et leurs mécanismes de sécurité.

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

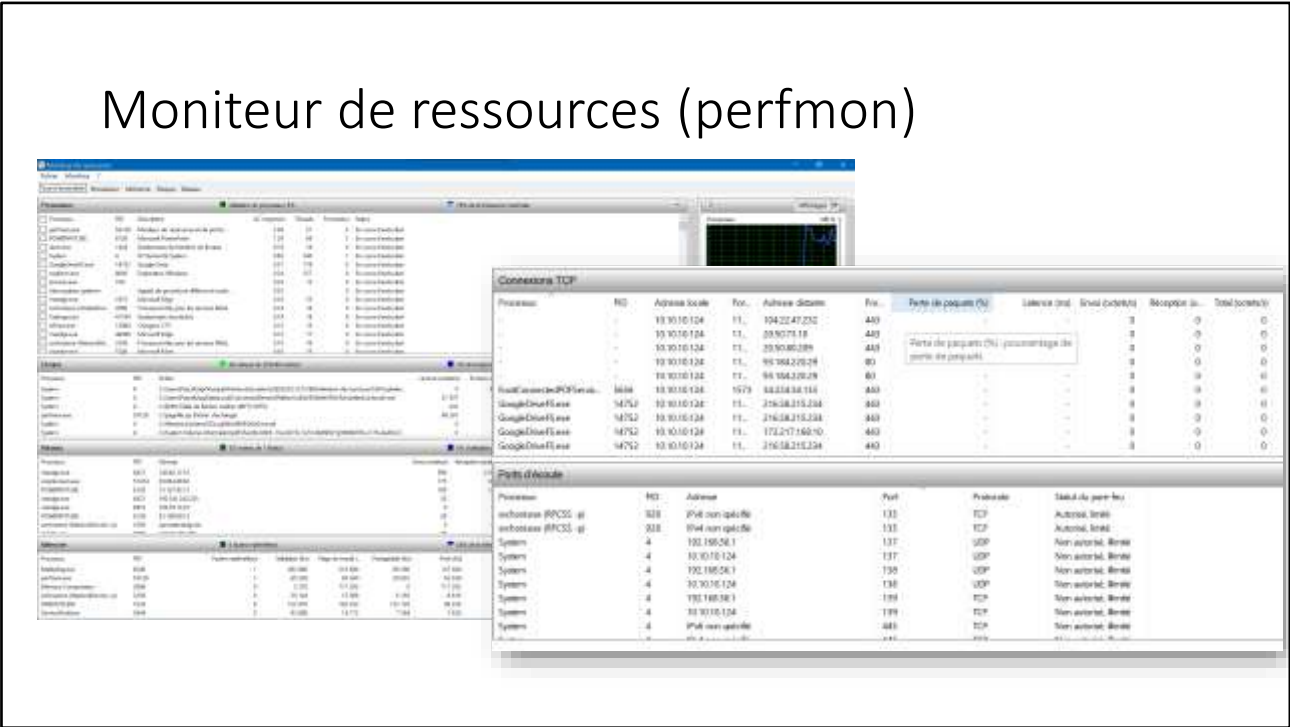


Pour mieux retrouver les services/processus associés à quoi, ou qui  
Afficher la colonne « ligne de commande »

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

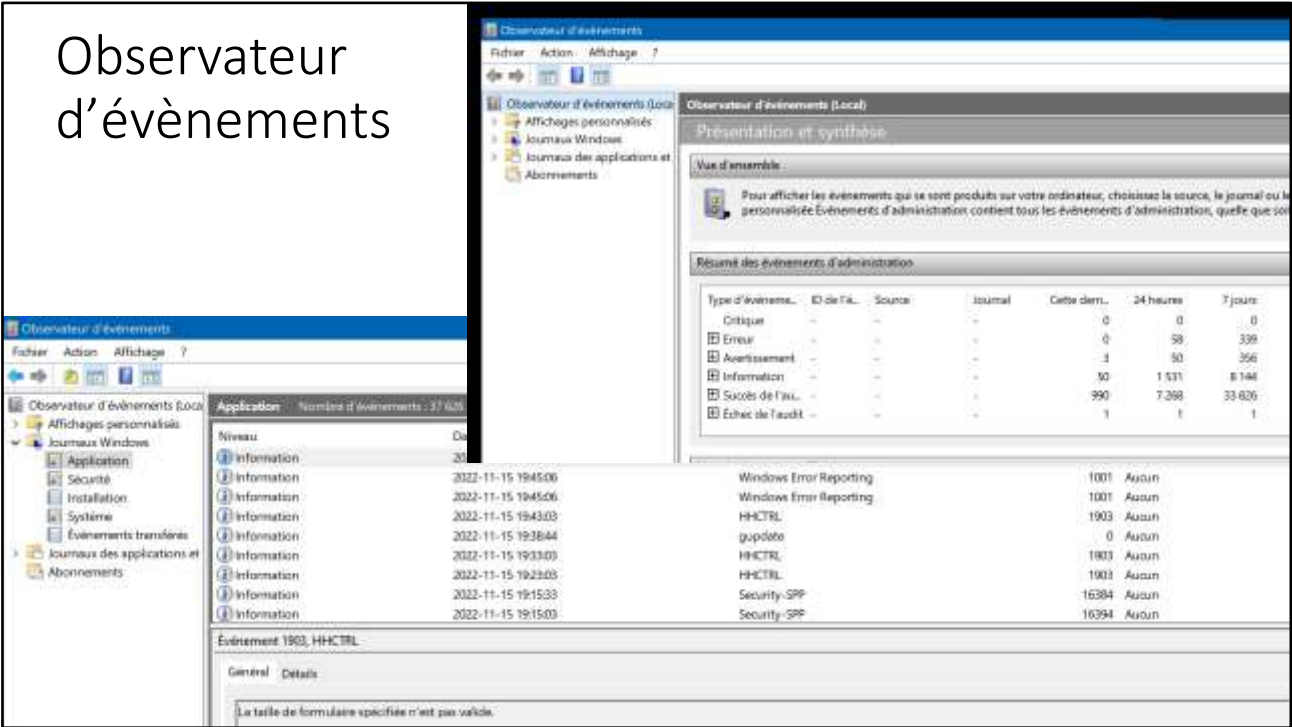


# Moniteur de ressources (perfmon)



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

# Observateur d'évènements



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

# Outils de mesure des performances

## Systèmes (windows)

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

On va voir cela  
juste après

## Réseaux ([NMS](#))

- [MRTG](#) (perl multiOS)
- [Cacti](#)

## 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>

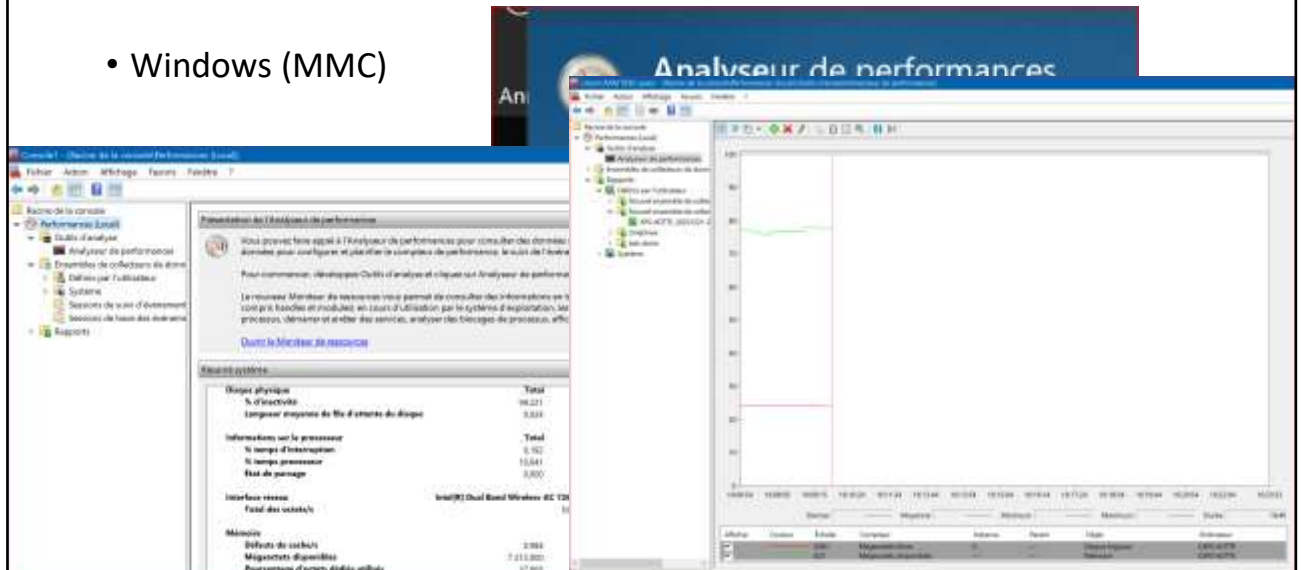
[https://fr.wikipedia.org/wiki/Supervision\\_\(informatique\)](https://fr.wikipedia.org/wiki/Supervision_(informatique))

<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)

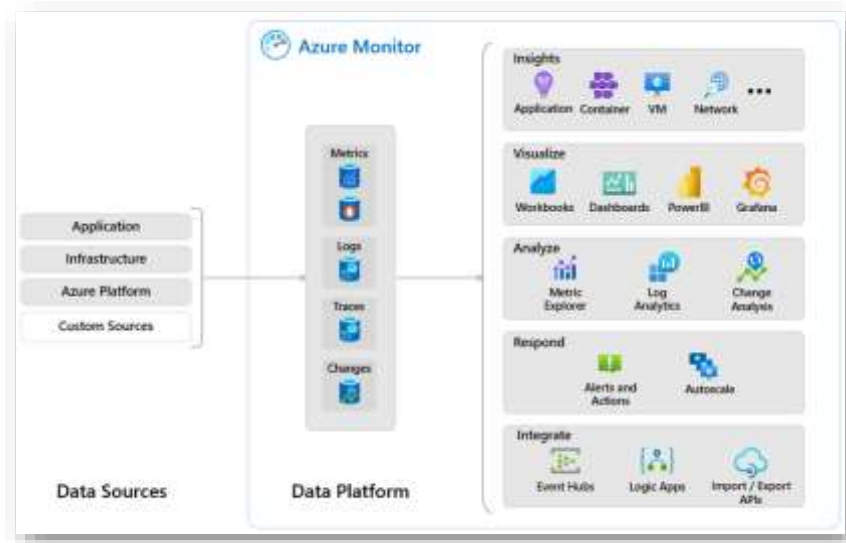


### Analyseur de performances

- 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](#)
- ...



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>

## Standards réseaux, monitoring

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

### Service

- [ARP](#) (identifier MAC adrs) ipv4
- [DNS](#)
- DHCP
- [NAT](#) et ip privées et ip publiques (ipv4)
  - <https://www.myip.com/>
- [Ipv6](#)
  - <https://ipcost.com/fr>

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
1.3.6.1.4.1.4326.1	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
1.3.6.1.4.1.255.8.42.1	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://fr.wikipedia.org/wiki/IPv6>

<http://www.ipv6-test.ch/>

Get-Command -Noun WMI\*  
Get-Command -Module CimCmdlets

[illegible]

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>



# Exercice: traceret

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 6 ms 4 ms 3 ms ae22-1150.lpc-155090-s-pe-08.bluelwin.ch [213.3.220.253]  
4 6 ms 3 ms 3 ms eth12-1150.lsic20p-cps001.bluelwin.ch [213.3.220.254]  
5 5 ms 5 ms 4 ms 213.3.220.189  
6 5 ms 4 ms 3 ms 1001ip-015-as11.bb-ip-plus.net [193.134.95.84]  
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-15.rso.frikgel3.de.bb.gin.ntt.net [129.250.66.67]  
13 49 ms 19 ms 43 ms ae-2.r2b.frikgel3.de.bb.gin.ntt.net [129.250.6.13]  
14 12 ms 11 ms 11 ms ae-0.ad2.frikgel7.de.bb.gin.ntt.net [129.250.5.38]  
15 181 ms 49 ms 59 ms ae-0.f9-networks.frikgel7.de.bb.gin.ntt.net [129.241.10.17]  
16 \* \* \* Délai d'attente de la demande dépassé.  
17 47 ms 40 ms 70 ms 107.162.251.256  
18 111 ms 89 ms 41 ms 107.162.240.181  
19 162 ms 161 ms 181 ms 107.162.240.4  
20 \* \* \* Délai d'attente de la demande dépassé.  
21 64 ms 52 ms 70 ms t08-0-1-0.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 t08-0-1-0.er01.gva09.ch.ip-max.net [46.20.249.168]  
24 25 ms 17 ms 83 ms t08-0-1-0.er01.gva09.ch.ip-max.net [46.20.235.15]  
25 53 ms 98 ms 46 ms t08-2-0-0.er01.gva26.ch.ip-max.net [46.20.235.21]  
26 96 ms 58 ms 24 ms be2b.er05.gva26.ch.ip-max.net [46.20.254.59]  
27 17 ms 16 ms 18 ms 46.20.245.147  
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 webaccess.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 4 ms 4 ms 100.85.192.1  
3 45 ms 119 ms 89 ms ae22-1150.lpc-155090-s-pe-08.bluelwin.ch [213.3.220.253]  
4 49 ms 74 ms 91 ms eth12-1150.lsic20p-cps001.bluelwin.ch [213.3.220.254]  
5 28 ms 87 ms 82 ms 213.3.220.189  
6 6 ms 10 ms 9 ms 1001ip-015-as11.bb-ip-plus.net [193.134.95.84]  
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 162 ms 115-lef01-c2-02-30-3-223.fr.lnx.abo.bbox.fr [62.36.3.223]  
11 107 ms 65 ms 95 ms be5.chr01-cro.net.bbox.fr [212.184.176.161]  
12 17 ms 17 ms 17 ms 8.la16.bcr01-t03.net.bbox.fr [212.194.171.95]  
13 \* \* \* Délai d'attente de la demande dépassé.  
14 \* \* \* Délai d'attente de la demande dépassé.  
15 87 ms 51 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)

```
C:\Users\pasca>ping 192.168.1.1

Envoi d'une requête 'Ping' 192.168.1.1 avec 32 octets de données :
Réponse de 192.168.1.1 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.1.1 : octets=32 temps=1 ms TTL=64

Statistiques Ping pour 192.168.1.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

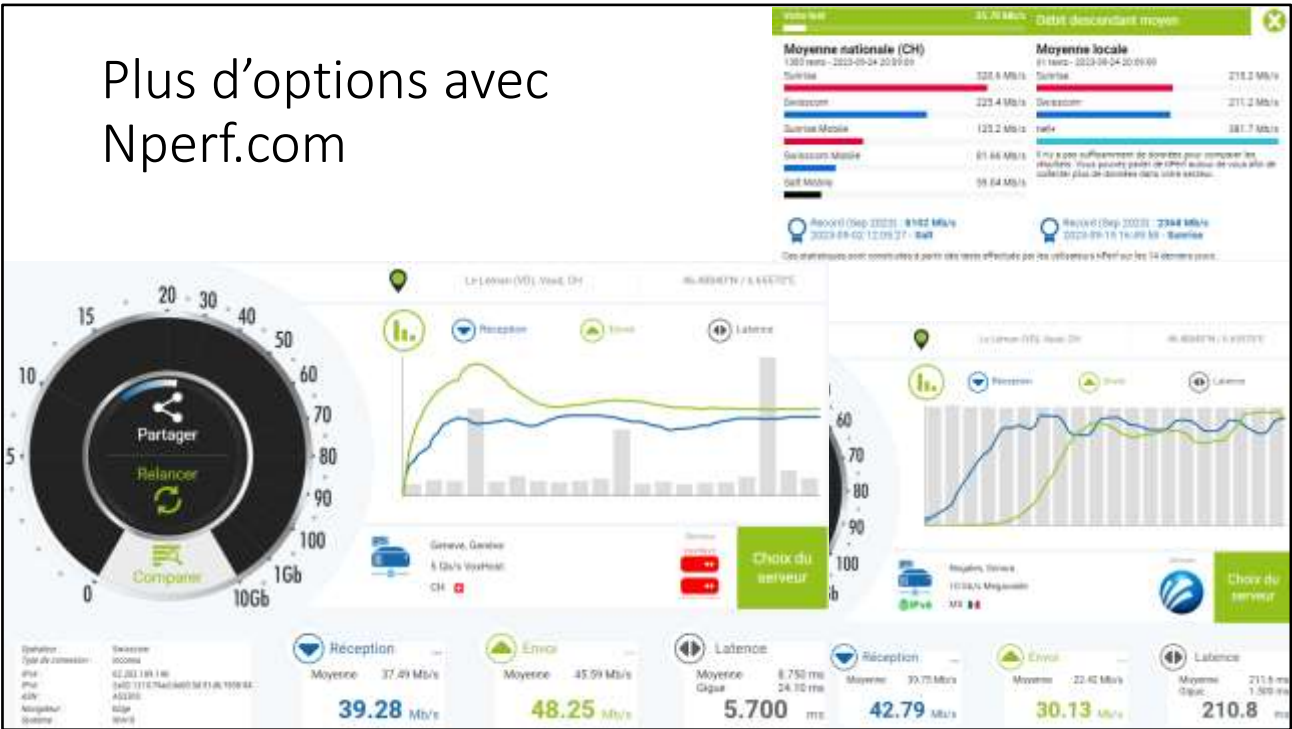


Comment autoriser Ping, entre 2 W10/11?  
<https://medium.com/conseillers-num%C3%A9riques-suisse-romands/comment-faire-ping-sous-windows-10-4123cbb32787>

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

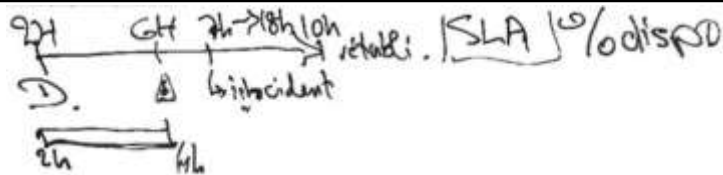


En plus de récupérer vos IPv4 et v6 publiques, on accède à des statistiques locales par opérateur: [Comparer]

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>

## Reboot time

- Task manager, démarrage – limiter au strict nécessaire

Gestionnaire des tâches			
Fichier Options Affichage			
Processus Performance Historique des applications Démarrage Utilisateurs Détails Services			
Nom	Éditeur	Statut	Impact au démarrage
Microsoft StorePain	Microsoft Corporation	Activé	Haut
Google Drive	Google, Inc.	Activé	Haut
Hi-Mouse Button Control	HighResolution Enterpr...	Activé	Moyen
Windows Security notification icon	Microsoft Corporation	Activé	Bas
Microsoft To Do	Microsoft Corporation	Désactivé	Aucun
Spotify	Spotify AB	Désactivé	Aucun
Mobile connecté	Microsoft Corporation	Désactivé	Aucun

Dernier temps de démarrage du BIOS: 35.3 secondes



- 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

Valider en classe la spécificité de Windows, de ne pas arrêter mais de faire hiberner une machine

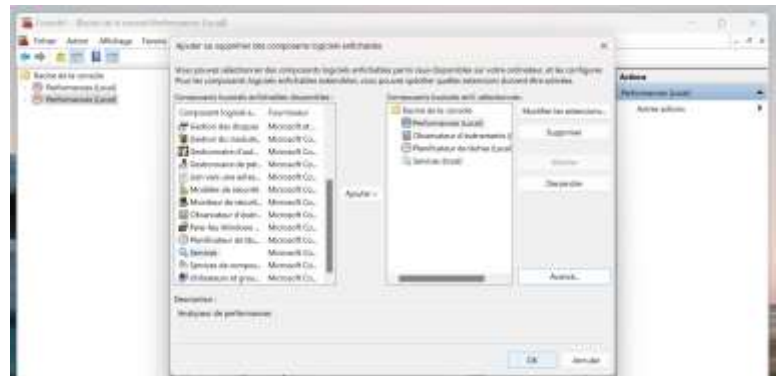
Exercice: Repérer comment lister l'historique de tous les (re)démarrages enregistrés par une machine Windows.

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>

## 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 «Boitiers» réseaux (Relais)
  - Routeurs, Switchs (Flash ROM ou EPROM)
- Les logiciels eux-mêmes
  - (option Microsoft seulement pour Windows)



[Microsoft Update Catalog](#)

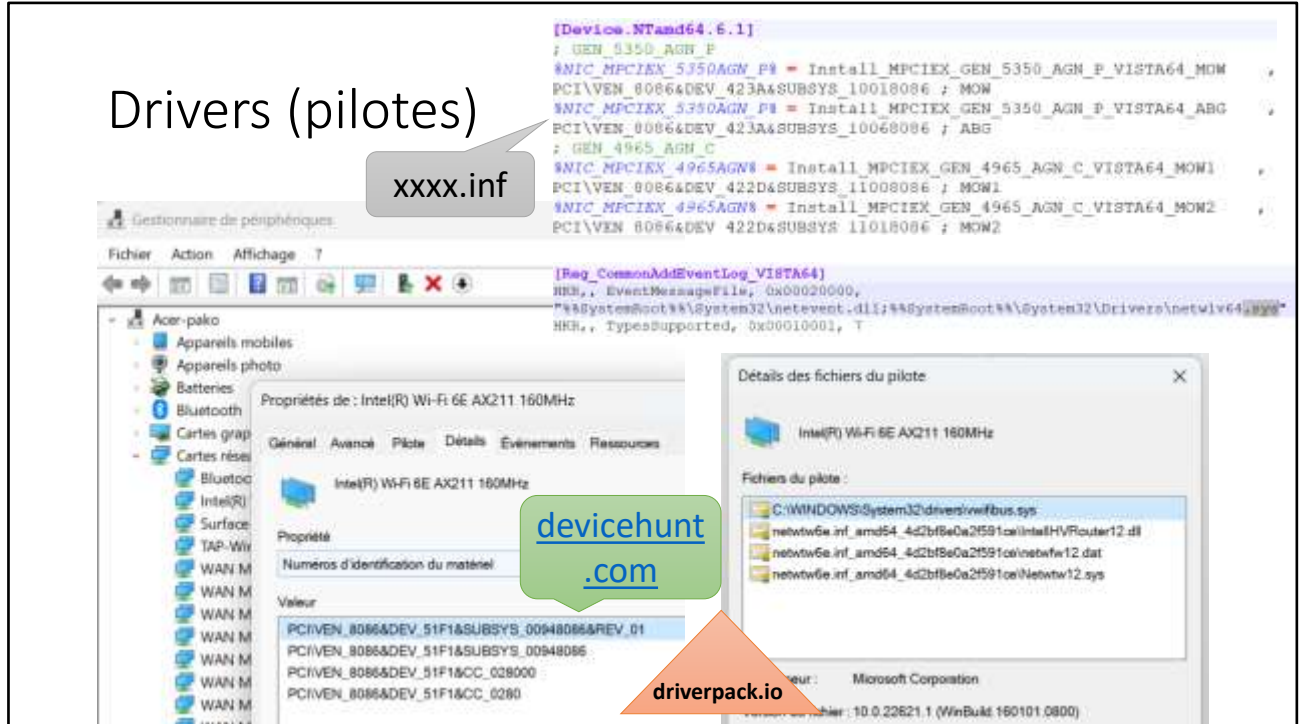
[Mises à jour de sécurité Apple - Assistance Apple \(CH\)](#)

[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/>

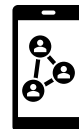
A fuir:

<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 pros 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)

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

## Faire le ménage (1 des 2)

- [illegible]

## Equivalent du cleanmgr

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

# 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 ?



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

<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.

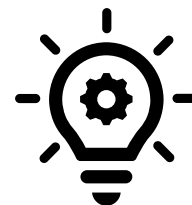
[https://learn.microsoft.com/en-us/windows/win32/wua\\_sdk/other-sources-of-windows-update-agent-information](https://learn.microsoft.com/en-us/windows/win32/wua_sdk/other-sources-of-windows-update-agent-information)

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

- 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

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

[Sandboxie — Wikipedia](https://en.wikipedia.org/wiki/Sandboxie) <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>

# 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-?)

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

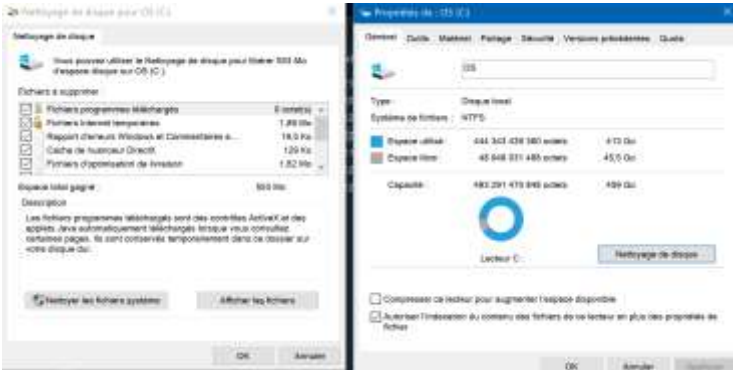
<http://www.easy-pc.org/2017/01/comment-installer-les-mises-a-jour-cab-et-msu-dans-windows-10.html>

<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

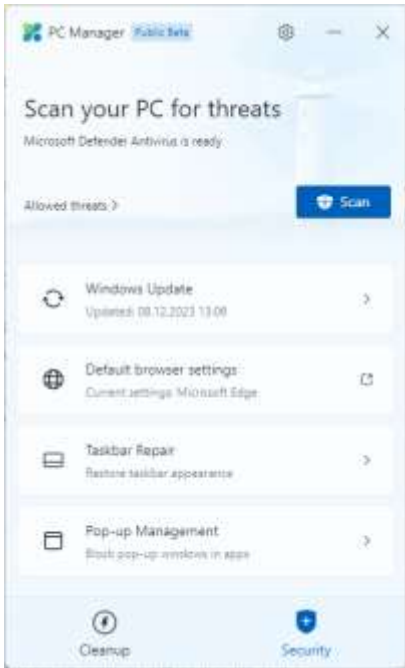
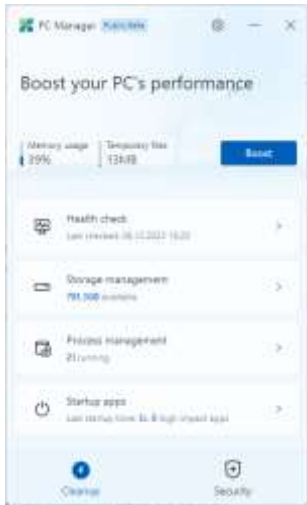
Cela fonctionne aussi sur des OS serveurs, sauf qu'il faut ajouter la fonctionnalité [Windows Server 2008 nettoyage de disque - comment activer / installer / exécuter. \(hdd-tool.com\)](https://www.hdd-tool.com/fr/windows-server-2008/disk-cleanup-server-2008.html)

<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>

PC Manager  
(Microsoft)



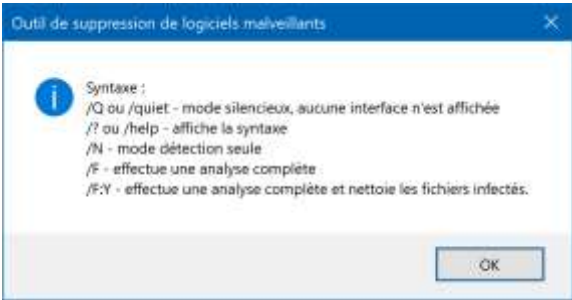
Merci Laeticia  
<https://pcmanager.microsoft.com/en-us>  
Download Beta  
<https://www.bing.com/ck/a?!&&p=c822a4ba9dff34e3JmltdHM9MTcwMTk5MzYwMCZpZ3VpZD0zNmQ3YmRmYi1kOGVklTJjMzUtMTEyNi1hZTZjZDk1NzZkOWMmaW5zaWQ9NTUwNQ&ptn=3&ver=2&hsh=3&fclid=36d7bdfb-d8ed-6c35-1126-ae6cd9576d9c&psq=PC+manager+Microsoft&u=a1aHR0cHM6Ly9ha2EubXMvUENNYW5hZ2VyT0ZMNTlwMDAx&ntb=1>  
Official  
<https://apps.microsoft.com/detail/9PM860492SZD?hl=en-US&gl=US>

# Patch (EXE) de Windows

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

- [KB890830](#)

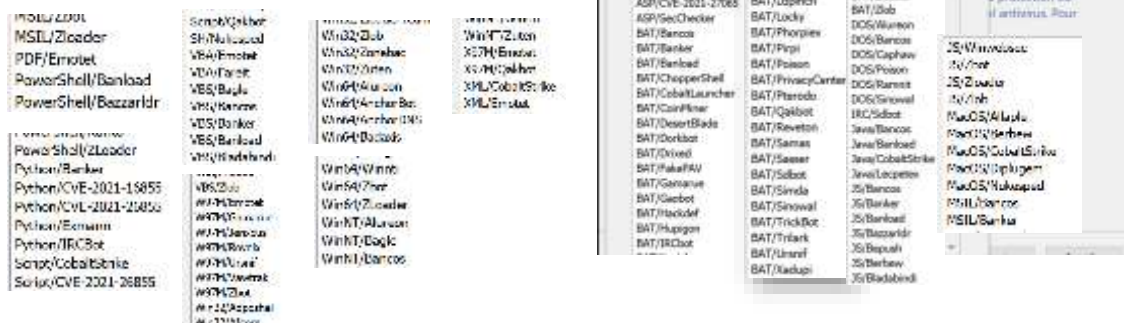
Un update qui va scanner les malwares identifiés via une application qui va faire un scan rapide: MSRT  
Qui peut être utilisée manuellement pour approfondir. (Plusieurs heures, voire jours sur un file server)  
Log: %WINDIR%\debug folder  
Mrt.log



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](#)

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



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

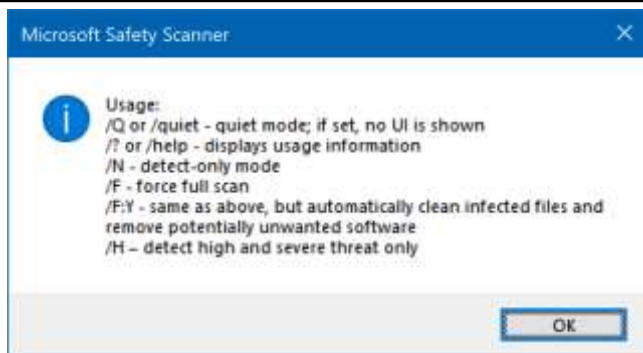
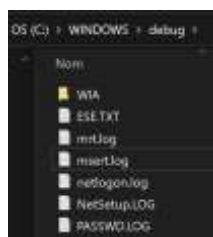
Microsoft:

<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>

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

- Log = msert.log

[illegible]

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

## Spécifique pour antivirus Windows

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

In Windows 10, select **Check for updates** in the Windows Security **Virus & threat protection** screen to check for the latest updates.

Enterprise administrators can also push updates to devices in their network. To clear the current cache and trigger an update, use a batch script that runs the following commands as an administrator:

```
cd %ProgramFiles%\Windows Defender  
MpCmdRun.exe -removedefinitions -dynamicssignatures  
MpCmdRun.exe -SignatureUpdate
```

Slide masquée car hors-sujet

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

# 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) <https://www.microsoft.com/en-us/msrc/definition-of-a-security-vulnerability?rtc=1>  
[Microsoft Security Response Center](https://msrc.microsoft.com/) <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, outils et services 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 réseau
- ✓ Évaluation des bases de référence de sécurité
- ✓ Analyses authentifiées 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:

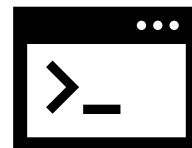
- Cf annexes, DamageEngine Patch gratuit moins de 20 ou 25 machines, multi OS (mais version payante)...

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

- Aussi: Nessus...
- Aussi: Darktrace



## 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

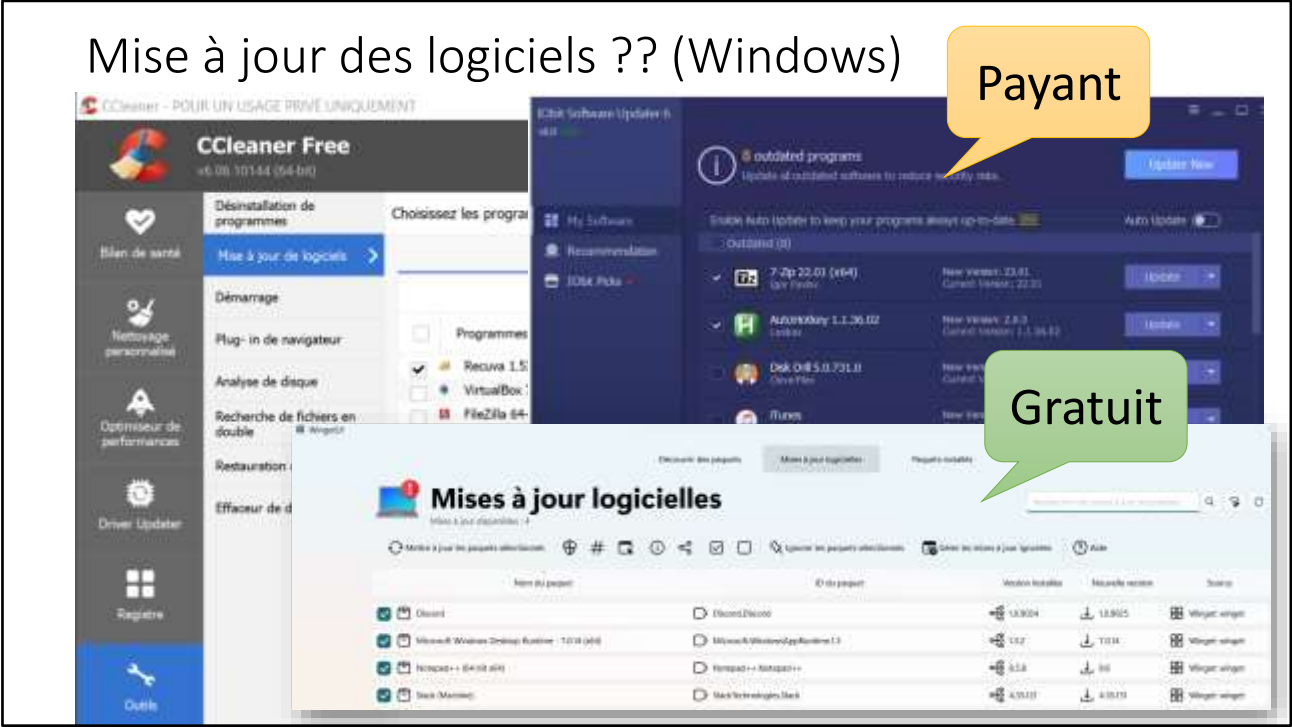
<https://medium.com/conseillers-num%C3%A9riques-suisse-romands/pourquoi-mon-pc-pourtant-sain-se-trouve-infect%C3%A9-par-un-spy-un-troyen-4507c3b4d446>

<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>

Les mises à jour





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?)

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

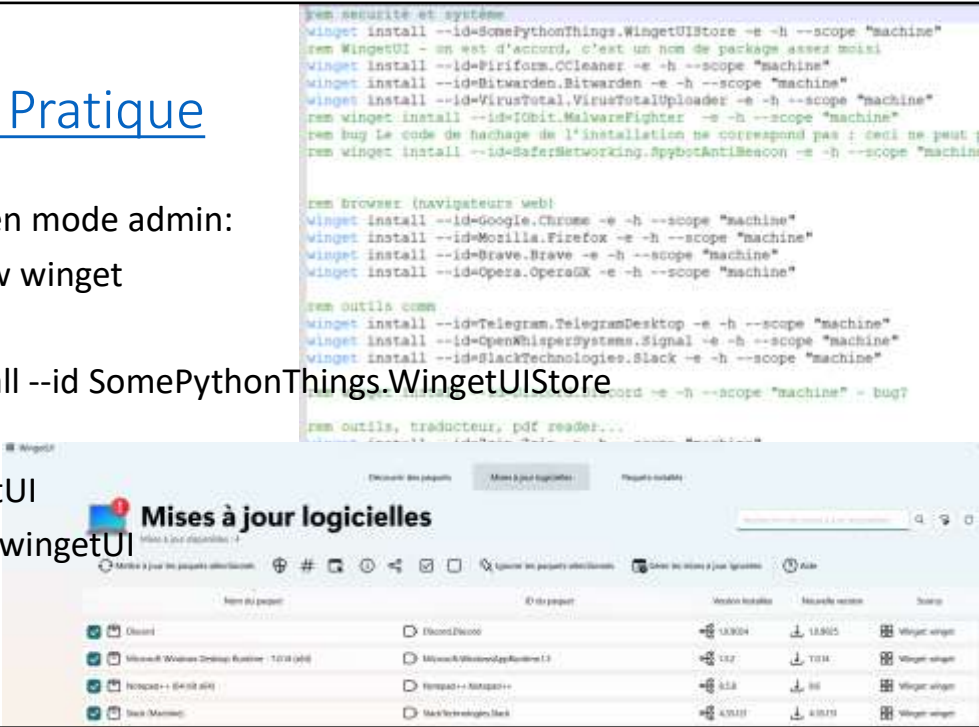
Lancer CMD en mode admin:

> winget show winget

> winget install --id SomePythonThings.WingetUIStore

Lancer wingetUI

Voir infos sur wingetUI



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.

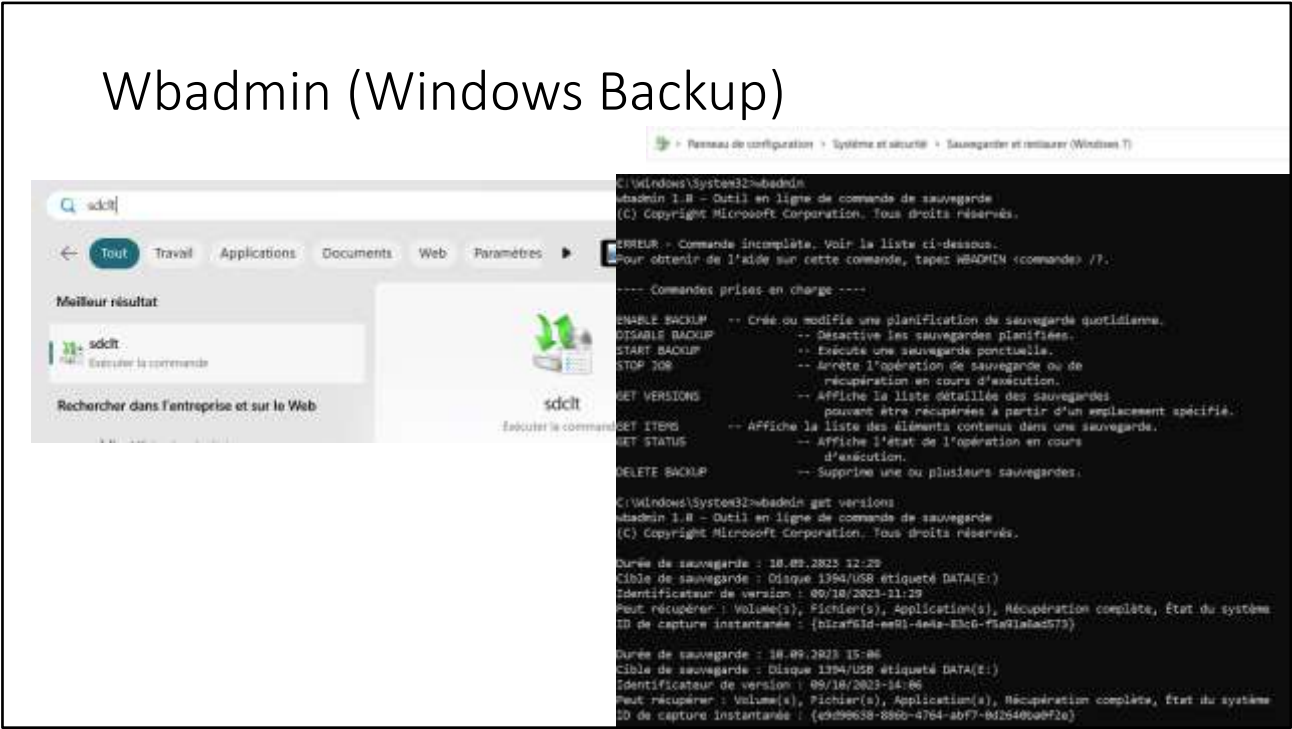


[Tutoriel sur l'activation de la touche F8 au démarrage de Windows 10 - Communauté Microsoft](https://answers.microsoft.com/fr-fr/windows/forum/all/tutoriel-sur-lactivation-de-la-touche-f8-au/7bc6d853-6dbf-421d-b185-651f2a342b24)

<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 ?

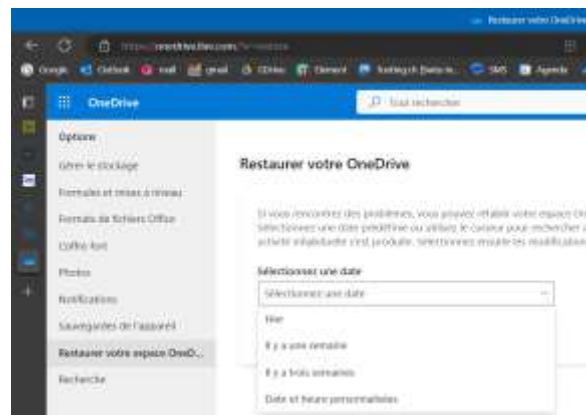


Cryptolocker – utiliser OneDrive

### ATTENTION:

Les données critiques sont-elles correctement sauvegardées ?

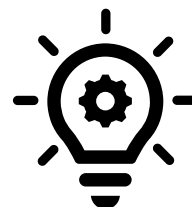
- Vaudtax2024
- Fichier PST archives locales (outlook)
- Autres...



Désormais, OneDrive détecte le chiffrement 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...)

## 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...

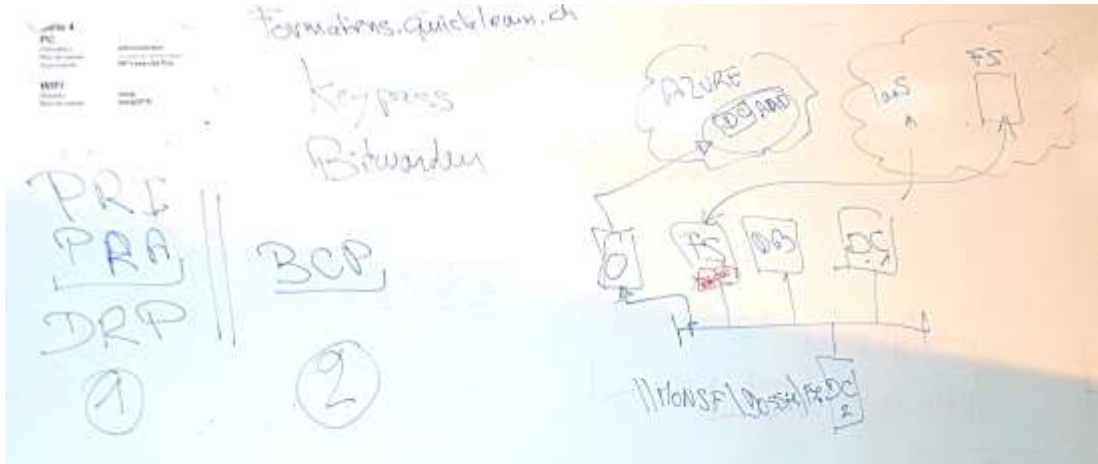
Déployer uniquement les éléments nécessaires

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

Déployer en prévention les autres, mensuellement

# 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.

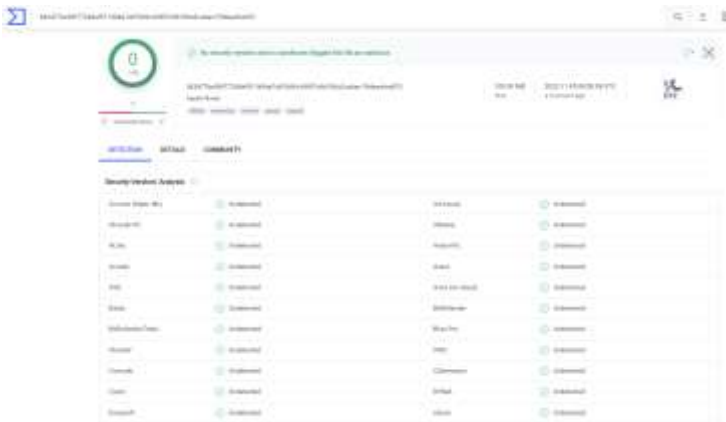
PRI ou PRA = Disaster Recovery Plan ou Plan de Reprise d'Activité  
SFT = System Fault Tolerance => Capacité de ne pas tomber en panne.

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](https://www.virustotal.com)
- \* Check signatures (ex MD5 => SHA2



<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 (sans mot de passe) une session 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)
- 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 reformaté et vos sessions mémorisées avec.  
**Pas de risque sécuritaire** pour votre compte @edu.iseig.ch

### 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 (mieux de le fixer au PC)
  - Les supports et documentations de son choix doivent y être copié 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,
  - 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

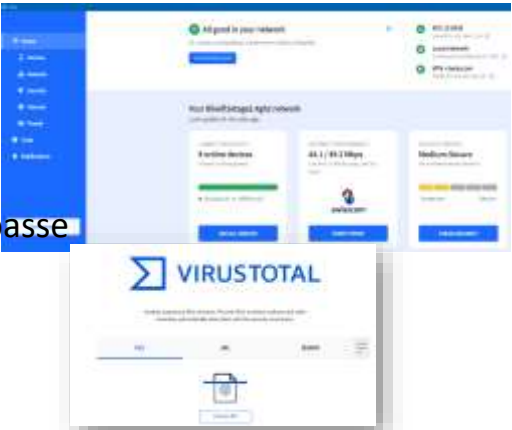
- [Piriform — Wikipédia \(wikipedia.org\)](#) : Ccleaner => [Quoique](#)
- ...

## 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

# ManageEngine

- Endpoint Central
- Patch Manager

		Free Edition	Edition Professionnelle	Edition Entreprise	Edition UEM
		Convient aux PME	Fonctionnalités de l'Edition Professionnelle +		Fonctionnalités de l'Edition Entreprise +
		Gère jusqu'à 25 ordinateurs et 25 appareils mobiles	Gestion des correctifs	Optimisation de la bande passante WAN	Gestion des périphériques Mobiles
		Restion des correctifs	Déploiement de logiciels	Portail Ultra-service	Gestion des périphériques Windows 10
		Déploiement de logiciels	Gestion des Ressources	Logiciels Intégrés / 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 Sessions 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 filars		» 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 facteurs	
		» 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>

# 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 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

Advanced Email Security

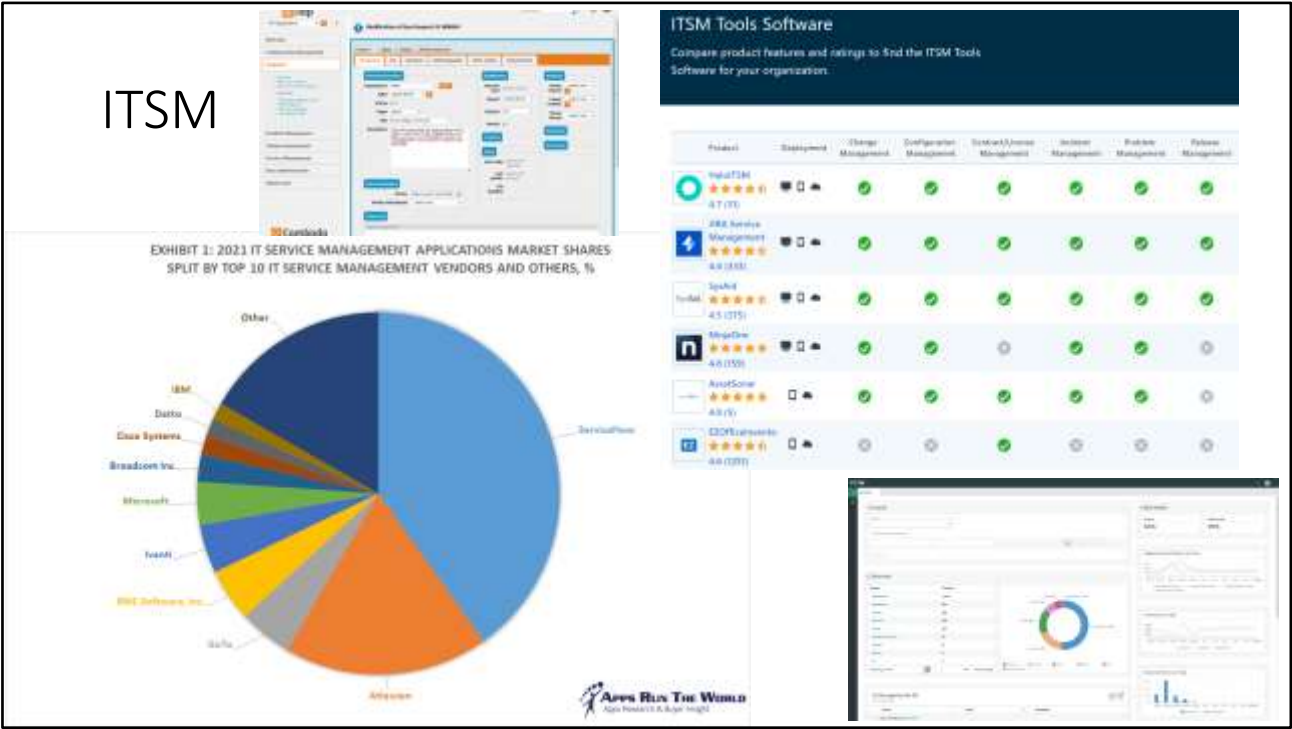
Advanced Email Security permet la protection en temps réel pour vos boîtes aux lettres Microsoft 365 et Gmail :

- 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



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>

[Chocolatey Software | Community](#)

105

# 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.

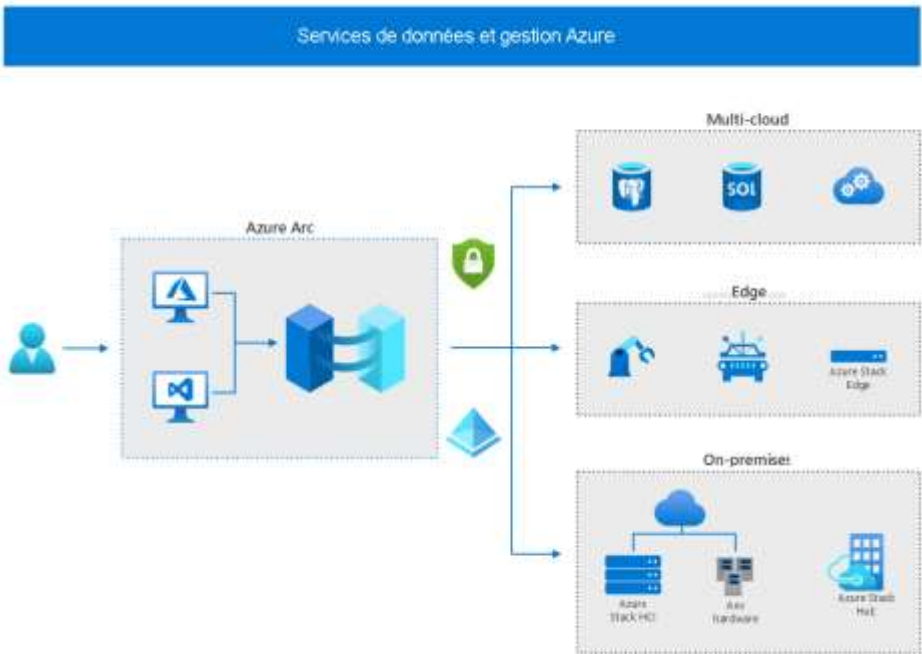
Dans l'univers Microsoft: Les Automatisations sont assurées généralement avec des Scripts en Powershell.

<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

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 /

Microsoft PowerToys: Utilities to customize Windows

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

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

Feedback

Install PowerToys

Feedback

[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>

109