

**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 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/)

<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 inexiste 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 tolèteque

- 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»...

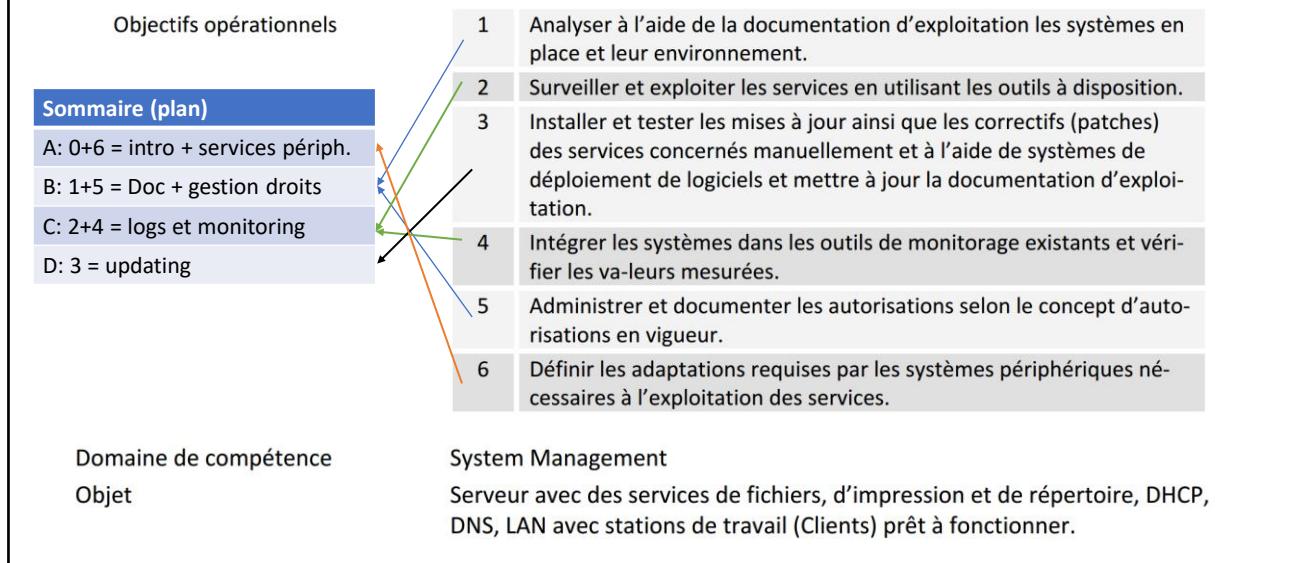
Les accords tolèques

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

Et Blackcoach

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.

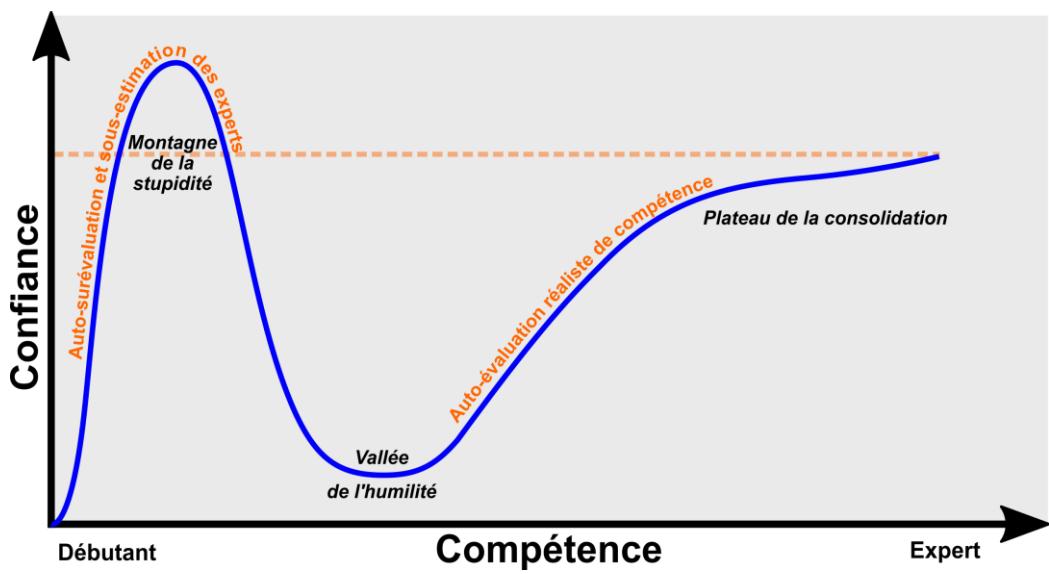
4.1 Connaître des techniques possibles (p. ex. SNMP, WMI) pour la saisie centralisée des données de performance et leurs mécanismes de sécurité. 4.2 Connaître les étapes de configuration à effectuer sur un système de serveur pour activer les mesures de performance (p. ex. SNMP, WMI). 4.3 Connaître les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

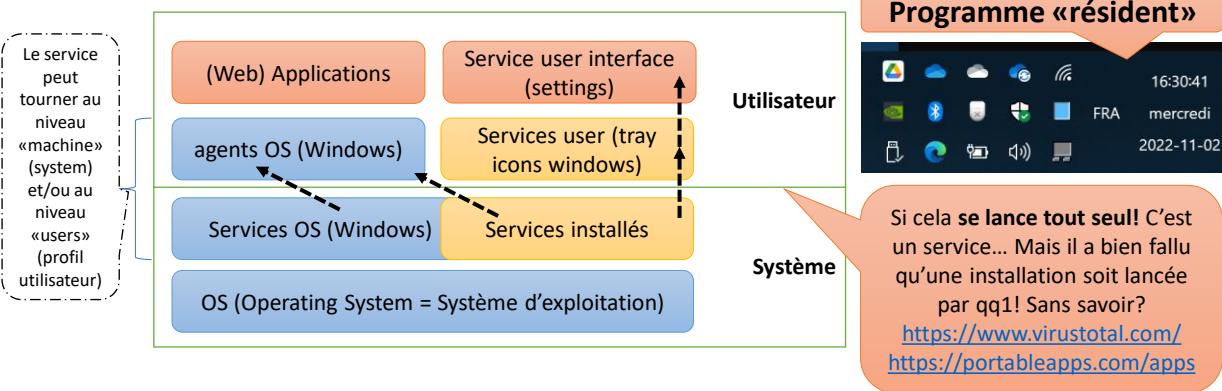
6.3 Connaître des possibilités pour tester les adaptations apportées aux systèmes périphériques.

C'est quoi un service (informatique/numérique)

Web service/serveur
Port ip Ecoute: 80/443



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.



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).

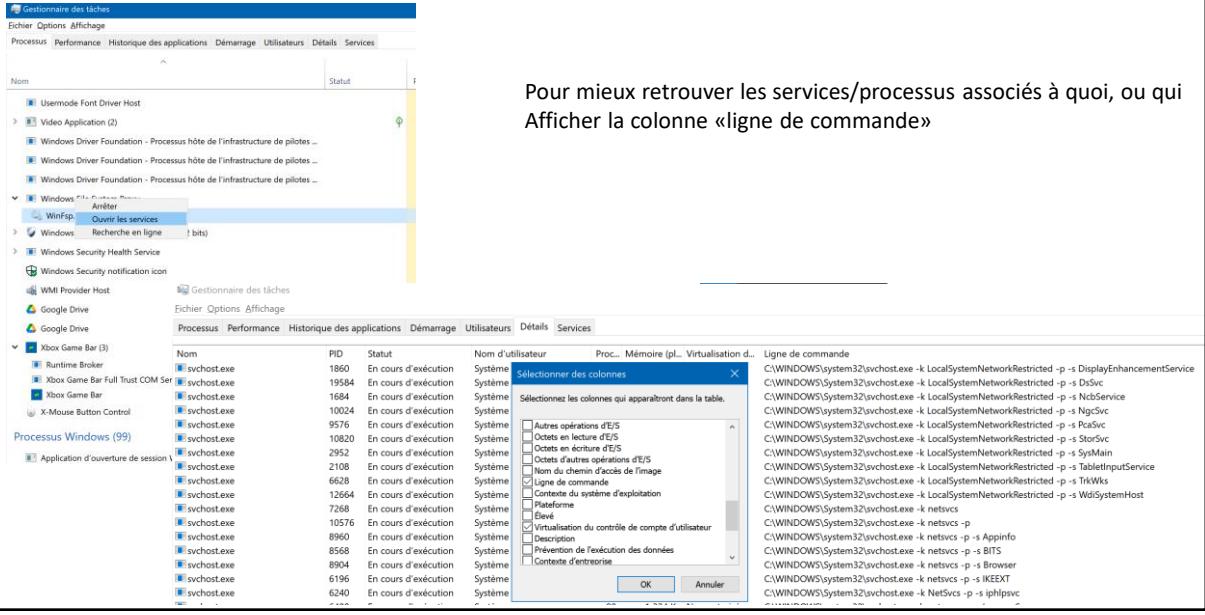
Désactivation au démarrage et nettoyage du PC:

- 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

Task manager (gestionnaire de tâches)



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

Explorations ensemble 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

Contrôle des connaissances de base les réseaux et révisions

<http://Network.quicklearn.ch>

[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-suisses-romands/cybercriminalit%C3%A9-ce-que-votre-banque-oublie-de-vous-dire-9f6fcfbdb242>

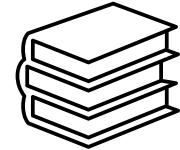
<https://medium.com/conseillers-num%C3%A9riques-suisses-romands/antivirus-sur-mac-linux-android-iphone-ou-pas-plus-que-pour-windows-9d022ff1ddbd>

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

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

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

Les services «utilisateurs» et «infras»

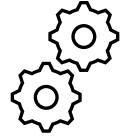


Le catalogue de services exposé aux usagers va intégrer les prestations assurées par leur département «IT» et leurs sous-traitants, ou fournisseurs: Ce sont les services finaux

- 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.

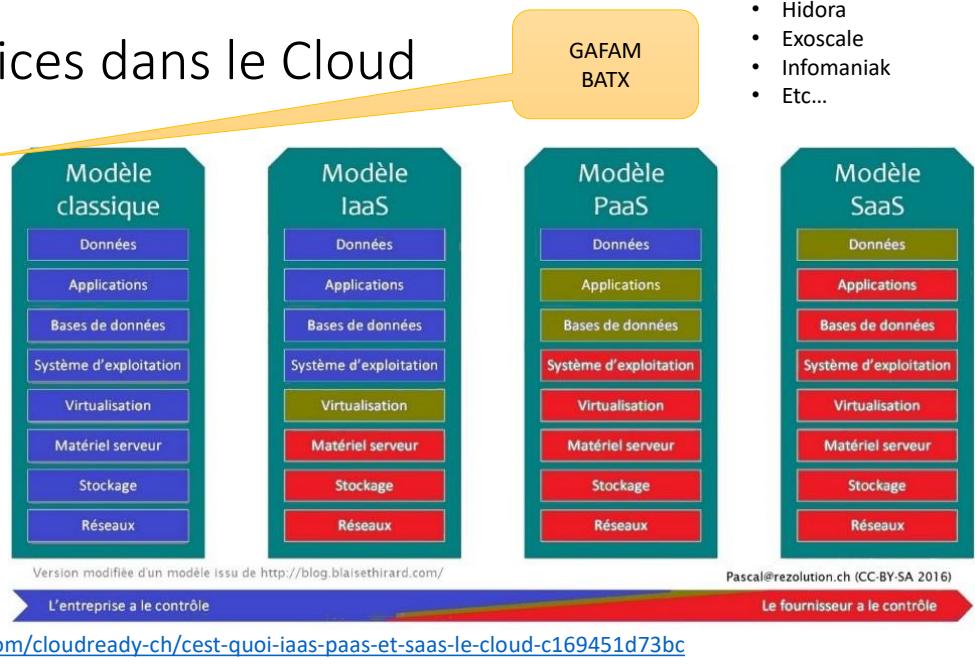
Le contenu des objectifs de cette formation, fait plus un focus sur les services infras. Mais maintenir en fonctionnement les services utilisateurs proposé dans le « catalogue des services » assurés par l'IT est la réelle finalité de l'infrastructure ICT.

Les services dans le Cloud

- Amazon
- Google
- Azure

3 Clouds

- IaaS
- PaaS
- SaaS



Explications complémentaires disponibles en ligne sur cet article:

Les services numériques déportés dans le nuage, deviennent très nombreux:

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

Option; **Ethique numérique, durable et responsable?**

C'est quoi? Et comment on peut faire?

<https://medium.com/cloudready-ch/ethique-num%C3%A9rique-durable-et-responsable-89083a6a5789>

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

- Hidora
- Exoscale
- Infomaniak
- Etc...

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 \(wikipedia.org\)](#)
- 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).

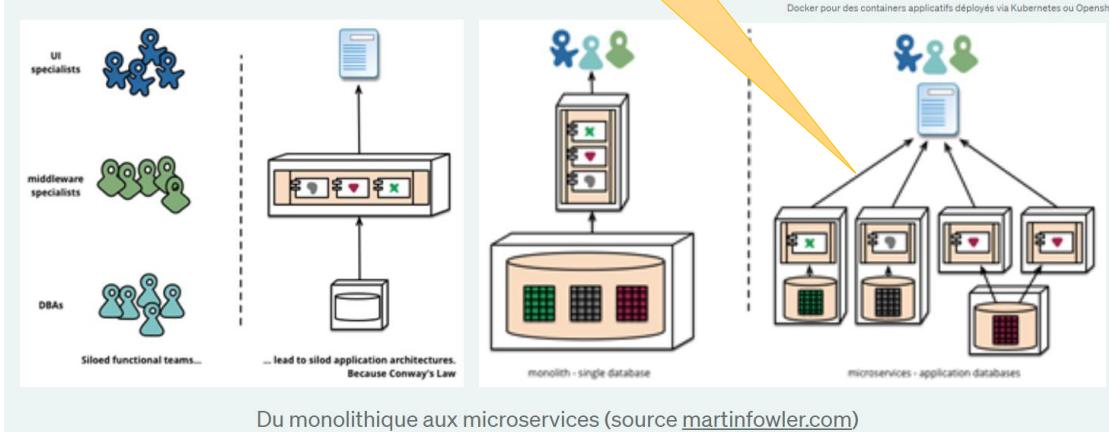
<https://www.capital.fr/votre-carriere/esn-entreprise-de-services-numeriques-definition-et-fonctionnement-1405805>

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

https://fr.wikipedia.org/wiki/Entreprise_de_services_du_num%C3%A9rique

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

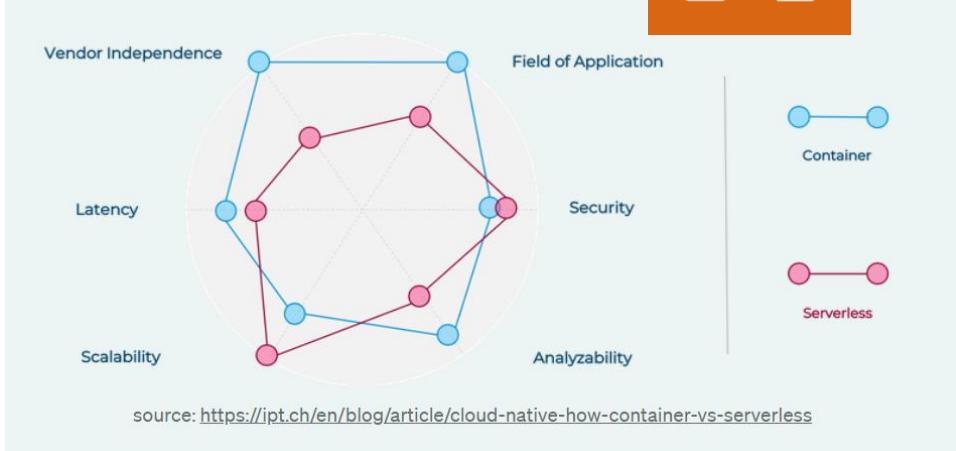
<https://medium.com/cloudready-ch/ipaas-cest-quoi-3f4b8ec84924>

https://fr.wikipedia.org/wiki/Representational_state_transfer

DEVOPS to NoOPS

Google Cloud

Serverless computing



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 faîte 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/AWS_Lambda
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

Exploiter, surveiller et assurer la maintenance des services

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

Gérer/installer/désinstaller services

The screenshot shows two windows side-by-side. On the left is the 'Programs and Features' window, which lists various installed programs from Microsoft Corporation, such as Microsoft Visual C++ Redistributables and Mozilla Firefox. On the right is the 'Applications and Features' window, which shows a single application: 'Minecraft Launcher' by Microsoft Studios.

Nom	Éditeur	Installé le	Taille	Version
Microsoft Visual C++ 2005 Redistributable	Microsoft Corporation	2015-09-20	6,45 Mo	9,0,61001
Microsoft Visual C++ 2008 Redistributable - x64 9,0,30729,17	Microsoft Corporation	2015-02-26	1,63 Mo	9,0,30729
Microsoft Visual C++ 2008 Redistributable - x64 9,0,30729,6161	Microsoft Corporation	2015-02-27	830 Ko	9,0,30729,6161
Microsoft Visual C++ 2008 Redistributable - x86 9,0,30729,17	Microsoft Corporation	2015-01-18	5,17 Mo	9,0,30729
Microsoft Visual C++ 2008 Redistributable - x86 9,0,30729,6161	Microsoft Corporation	2015-01-19	4,53 Mo	9,0,30729,6161
Microsoft Visual C++ 2010 x64 Redistributable - 10,0,40219	Microsoft Corporation	2022-02-13	18,0 Mo	10,0,40219
Microsoft Visual C++ 2010 x86 Redistributable - 10,0,40219	Microsoft Corporation	2022-02-13	18,7 Mo	10,0,40219
Microsoft Visual C++ 2012 Redistributable (x64) - 11,0,61030	Microsoft Corporation	2021-02-13	20,5 Mo	11,0,61030
Microsoft Visual C++ 2012 Redistributable (x86) - 11,0,61030	Microsoft Corporation	2021-11-09	17,3 Mo	11,0,61030
Microsoft Visual C++ 2013 Redistributable (x64) - 12,0,30501	Microsoft Corporation	2020-11-04	20,5 Mo	12,0,30501
Microsoft Visual C++ 2013 Redistributable (x86) - 12,0,30501	Microsoft Corporation	2020-11-02	20,5 Mo	12,0,30501
Microsoft Visual C++ 2013 Redistributable (x86) - 12,0,40564	Microsoft Corporation	2020-11-04	17,1 Mo	12,0,30501,0
Microsoft Visual C++ 2013 Redistributable (x86) - 12,0,40564	Microsoft Corporation	2021-03-02	17,1 Mo	12,0,40564,0
Microsoft Visual C++ 2015 Redistributable (x64) - 14,28...	Microsoft Corporation	2021-03-18	22,1 Mo	14,28,29913,0
Microsoft Visual C++ 2015 Redistributable (x64) - 14,27...	Microsoft Corporation	2020-11-04	20,3 Mo	14,27,29016,0
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14,28...	Microsoft Corporation	2021-03-18	19,8 Mo	14,28,29913,0
Microsoft Visual Studio 2010 Tools for Office Runtime (x64)	Microsoft Corporation	2020-11-04	1,55 Mo	10,0,60724
Microsoft Visual Studio Code (User)	Microsoft Corporation	2020-10-22	249 Mo	1,50,1
Miro	Miro	2020-07-06	53,3 Mo	0,33,7
Modèle linguistique Microsoft Visual Studio 2010 Tools pour ...	Microsoft Corporation	2020-11-04	6,0	
Mozilla Firefox (x64 fr)	Mozilla	2022-11-23	213 Mo	105,0,3
Mozilla Maintenance Service	Mozilla	2020-11-04	604 Ko	73,0,1
Mozilla Thunderbird 45,7,0 (x86 fr)	Mozilla	2020-04-04	84,6 Mo	45,7,0
MPC-HC 1,0,15 (64-bit)	MPC-HC Team	2021-08-26	57,4 Mo	1,9,15
Ubuntu 12.10	The Ubuntu Foundation	2020-08-21	29,9 Mo	1,10,1

Paramètres

- Accueil
- Rechercher un paramètre

Applications et fonctionnalités

Choisir l'origine des applications
L'installation d'applications uniquement à partir du Microsoft Store contribue à protéger votre appareil.
N'importe où

Applications et fonctionnalités

Fonctionnalités facultatives
Aide d'exécution d'application
Effectuer des opérations de recherche, de tri et de filtrage par lecteur. Si vous voulez désinstaller ou déplacer une application, sélectionnez-la dans la liste.
mine

Trier par : Nom ▾ Filtrer par : Tous les lecteurs ▾
1 application trouvée

Minecraft Launcher
Microsoft Studios
300 Mo
2022-08-23

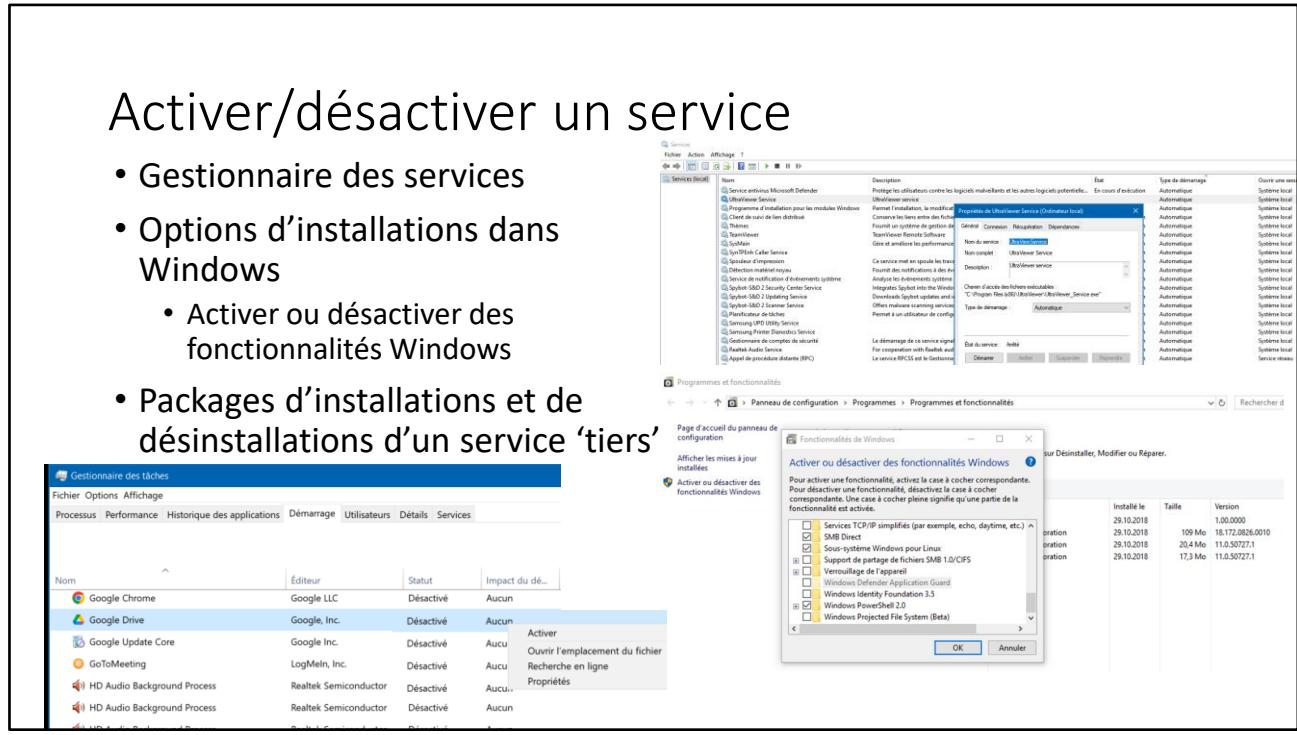
Exemple: sous-système Linux pour Windows

[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>

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/>

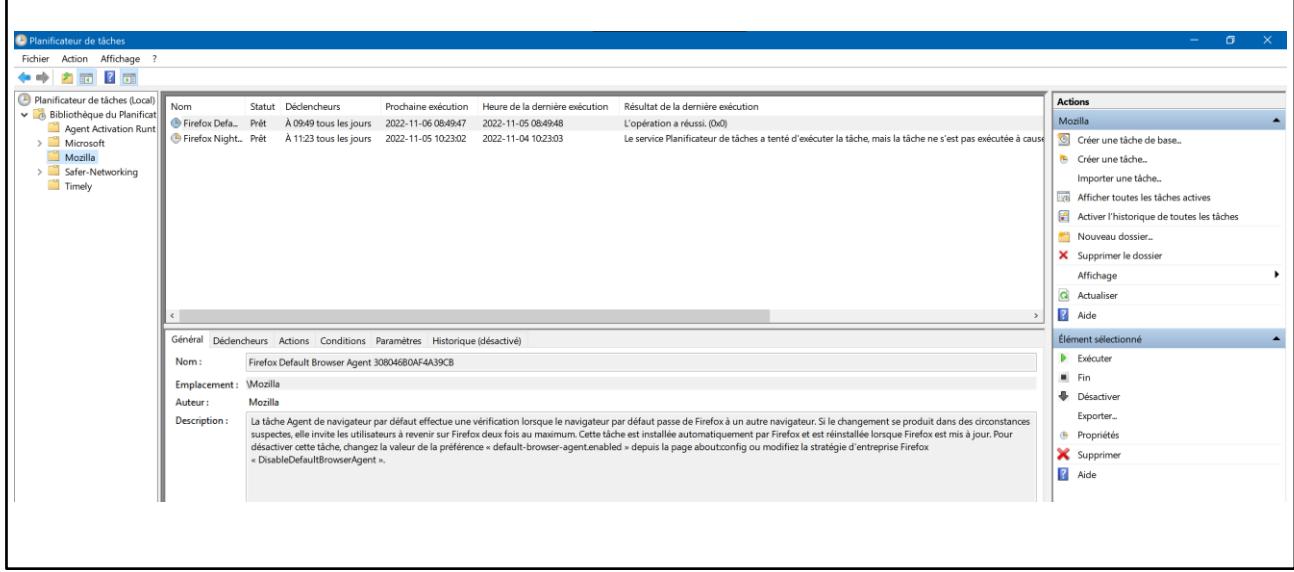
Propose de déployer des applications sans installations.

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

Par exemple, un troyen...

Tâches planifiées, crontab 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 simple page web.

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

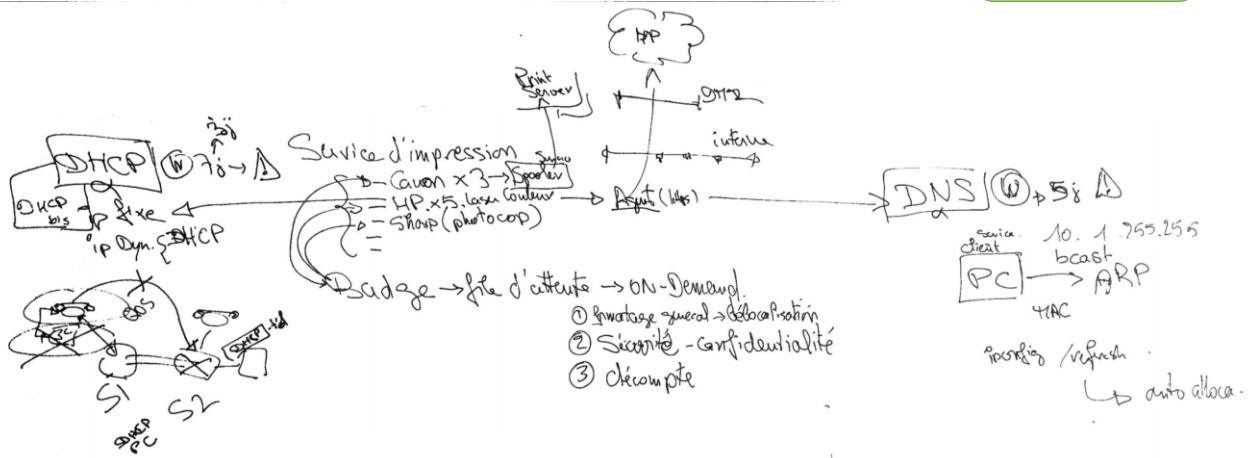
https://fr.wikipedia.org/wiki/Network_address_translation

https://fr.wikipedia.org/wiki/Hypertext_Markup_Language

https://fr.wikipedia.org/wiki/World_Wide_Web

Exemple des services d'impressions

Avec la fonction «follow me»



Présentation et illustration du fonctionnement devenu extrêmement sophistiqué des services d'impressions dans une entreprises avec l'option « Follow me »

Souvent les badges nécessitent un serveur Radius:

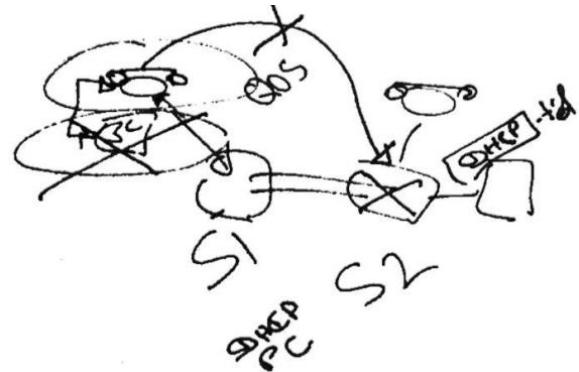
https://fr.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Service

Ou autre IAM serveur: (Identity and Access Management)

Exercice collectif en classe.

Sans une doc Adhoc et du monitoring

- Pas de vision claire de ce qu'il se passe en cas de problèmes
- Histoire vécue et réelle
La mise hors-service de plus 100 postes, sur une erreur de procédure de reprise...
Sans un diagnostic du problème.



La documentation et le monitoring nécessaire et indispensable.

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

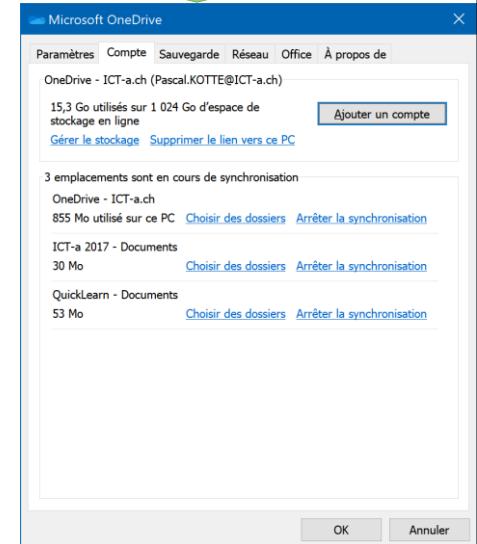
Lister les bonnes pratiques collectivement (si assez de temps dispo).

- Sera repris par la suite dans le § suivant.

Exemple de service: OneDrive

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

Avec Cryptolocker
detection



Applications

Google Drive

Dropbox Dropbox, Inc.

Dropbox Update Dropbox, Inc.

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

127.0.1.1 localhos

Cloudflare 1.1.1.1 Net.DNS

8.8.8.8 Google.DNS

<http://dns.quicklearn.ch>

Azure private DNS Zone



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



DHCP
DISCOVER

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

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://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:

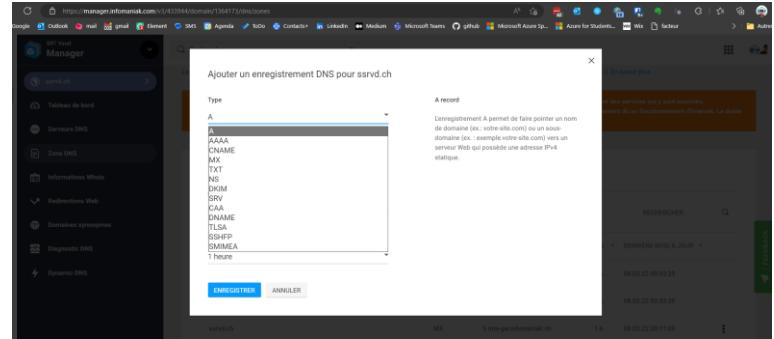
<https://rdr-it.com/windows-serveur-configuration-du-basculement-dhcp/>

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.

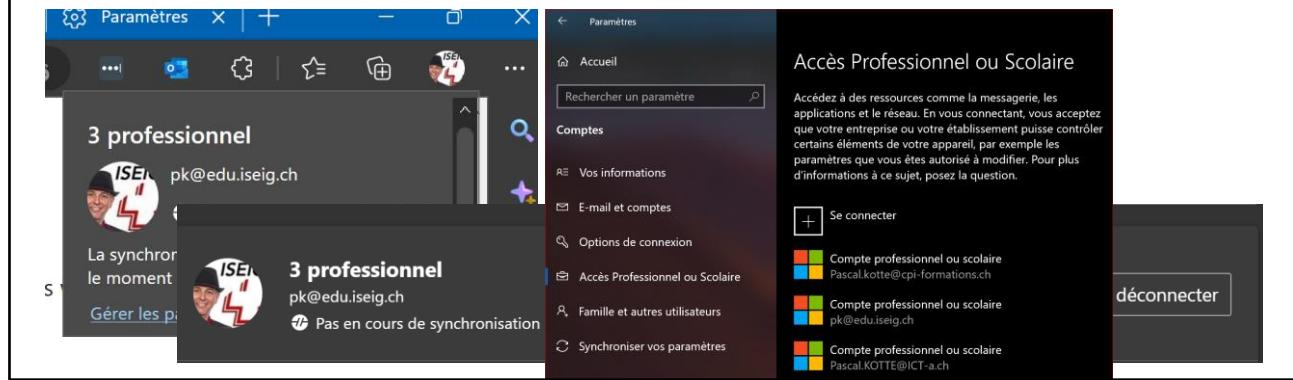
Recommandation à tout apprenti informaticien: Se prendre un domaine DNS pour son propre usage,

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 maîtriser 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>

B: 1(+5). Documentation

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

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

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

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

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

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

En cas de crash, la doc est où?

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

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

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

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



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'orthographies, 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/>

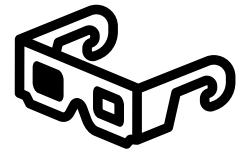
Autres exemples

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
- **Eléments de configurations**
 - Comment et où sont installés les composants d'un service
 - Procédure de rollback et de réinstallation «from scratch»
 - Liste des paramètres spécifiques
- **Eléments 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)
- **Eléments de sécurité**
 - Données sensibles, et ayants-droits: Méthodes et outils de sécurisations (Mots de passe services)

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

Être lucide sur les éléments qui DOIVENT être documentés.

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

- IP du serveur DNS

Les éléments de configurations pour restaurations ou contrôles:

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

Les outils pour documenter



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

Et pour maintenir à jour des données massives et complexes?

=> **Inventaires !!**

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

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

RECOMMANDATION:

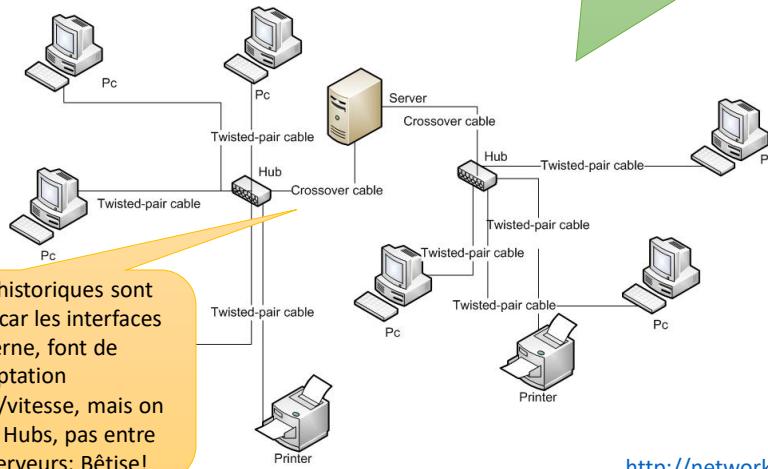
Se familiariser brièvement avec VISIO, version « online » fournie avec le compte
@edu.iseig.ch

Utilisation de draw.io (EPSIC)

Schémas de réseaux

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

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



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

<http://network.quicklearn.ch>

Source: Wikipedia

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

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

REVISION SUR LES RESEAUX:

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

EXERCICE EN CLASSE:

Comment représentez-vous les couches 3, et 7 ?

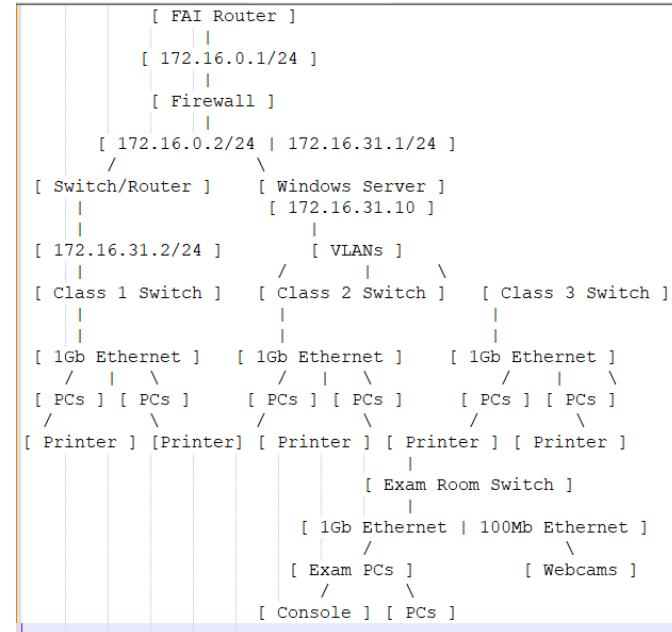
Exercice – Dessiner et documenter le réseau ci-dessous

- 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^{ème} 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

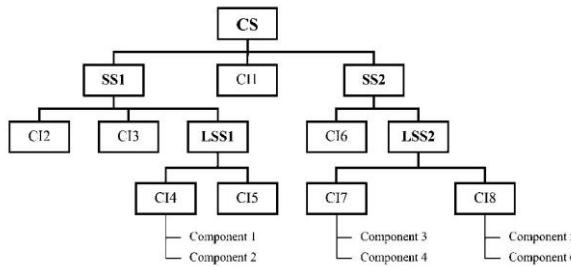
On a évoqué: GLPI, iTOP, ServiceNow, Zabbix, OTRS, SCCM... Cf aussi en annexe.
Mais on a une profusion de solutions...

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



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

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

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

Les 5 niveaux de maturité du modèle CMMI



Initial

Les processus quasi inconnus sont imprévisibles. Aucun facteur de réussite n'est identifié. La réussite du projet reste aléatoire.

Reproductible

Le déroulement du projet commence à être maîtrisé. Des méthodes permettent la répétition d'un projet.

Défini

Les processus du projet sont clairement identifiés et définis. Tous les acteurs du projet en ont une compréhension claire.

Maîtrisé

Le déroulement du projet est mesuré autant en terme quantitatif que qualitatif. Les écarts sont analysés.

Optimisé

Ou en cours d'optimisation. Nous sommes là au stade ultime de la démarche d'amélioration continue.

www.piloter.org

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

Qualité - https://fr.wikipedia.org/wiki/ISO_10007

Organisation – ITIL - https://fr.wikipedia.org/wiki/ISO/CEI_20000

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

https://www.piloter.org/gouvernance/CMMI_gouvernance_SI.htm

<https://cmmiinstitute.com/company> = ISACA

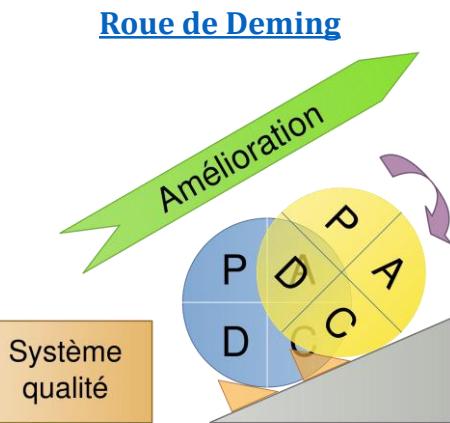
https://fr.wikipedia.org/wiki/ISO/CEI_27000 = Sécurité

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...)

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

2 = Test + Prod



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

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

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

https://fr.wikipedia.org/wiki/Roue_de_Deming

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

https://fr.wikipedia.org/wiki/D%C3%A9coupage_de_l%27information_pour_priorit%C3%A9

<https://medium.com/conseillers-num%C3%A9riques-suisses-romands/criticit%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-suisses-romands/criticit%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»



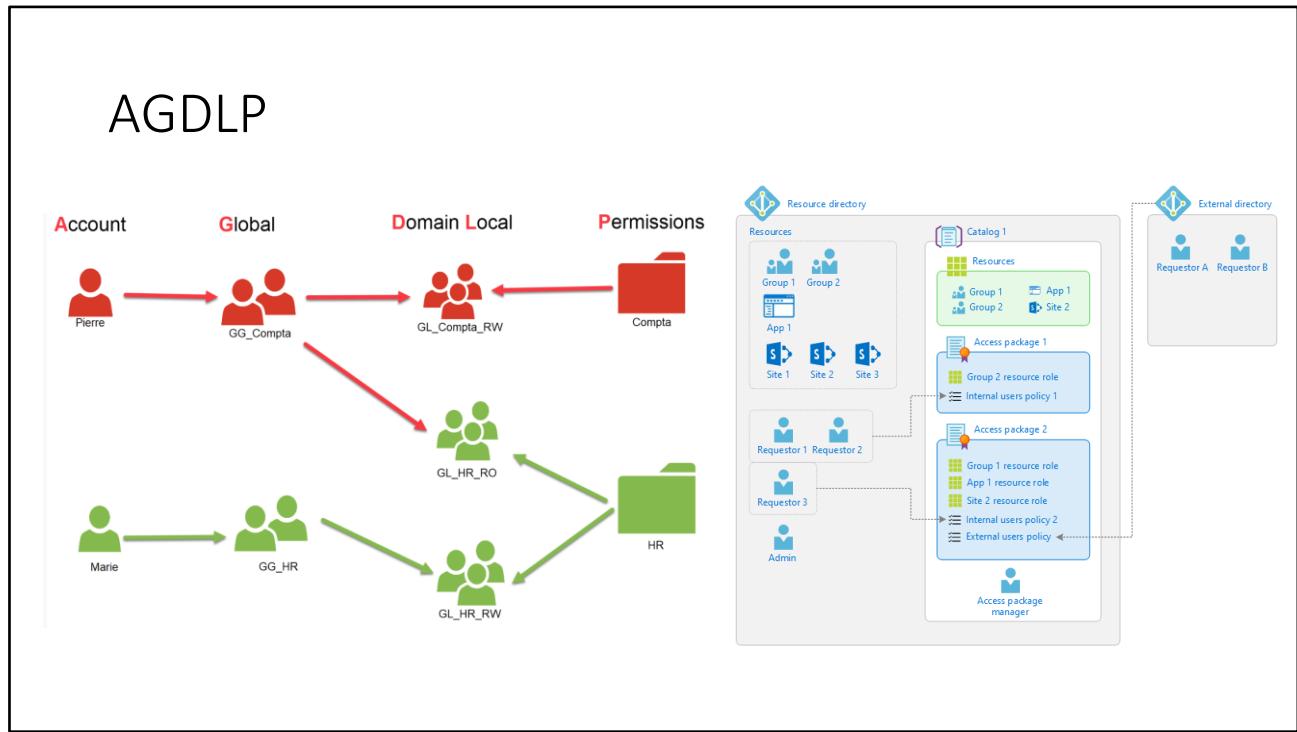
Pour une application métier, comme une «comptabilité», ce n'est pas à l'IT d'attribuer les «règles d'accès», mais au responsable métier (chef comptable, CFO) de déterminer quelles règles existent, et doivent être attribuées à qui.

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



Droits NTFS, et AGDLP...

<https://rdr-it.com/blog/agdlp-agudlp-comment-bien-gerer-les-droits-sur-un-serveur-de-fichiers-windows-serveur/>

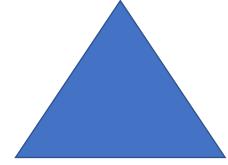
Ce qu'il faut retenir, c'est

- la nécessaire création de groupes globaux, explicites, pour gérer les «profils»:
 - Qui est censé avoir droit, à faire quoi?
- Des groupes et settings de sécurité doivent alors être mis en œuvre pour appliquer correctement les droits aux membres de ces groupes.
- 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 comptabilité 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-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)

[AZ-103-MicrosoftAzureAdministrator/03 - Implement and Manage Storage \(az-100-02\).md at master · CloudReady-ch/AZ-103-MicrosoftAzureAdministrator \(github.com\)](#)

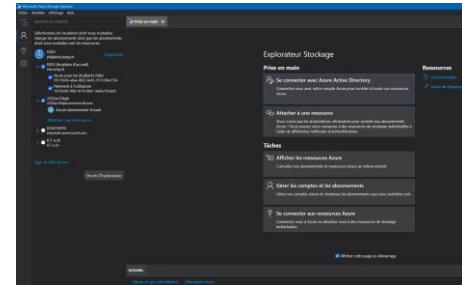
<https://azure.microsoft.com/en-us/features/storage-explorer/>

Cf. Microsoft Virtual Training Days <https://mvtd.events.microsoft.com/>

<https://mvtd.events.microsoft.com/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-LAB/blob/faddabe644708d6a0808e5755af75d39c7740a0a/AZ-103/01.AzurAdmin.md>

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

Nouvelle version

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://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.commentcamarache.net/forum/affich-1650439-probleme-connexion-controleur-de-domaine>



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

C: 2+4. Monitoring, add counters

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

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

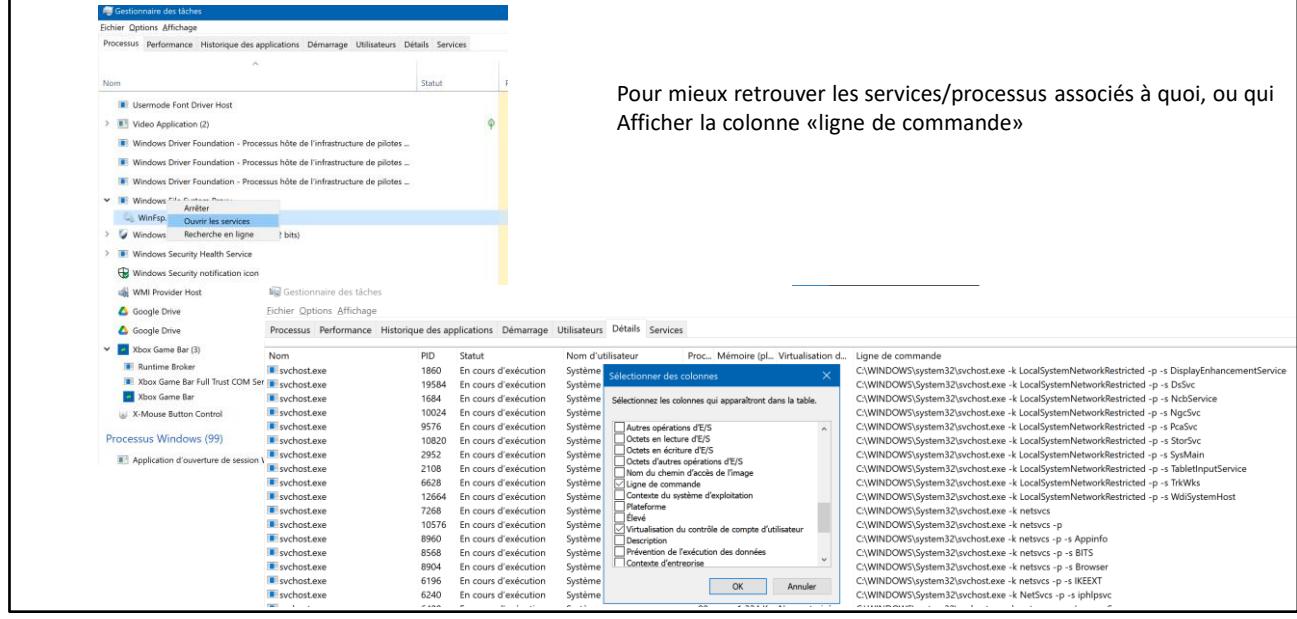
4.1 Connaître des techniques possibles (p. ex. SNMP, WMI) pour la saisie centralisée des données de performance et leurs mécanismes de sécurité.

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 monitorage existant.

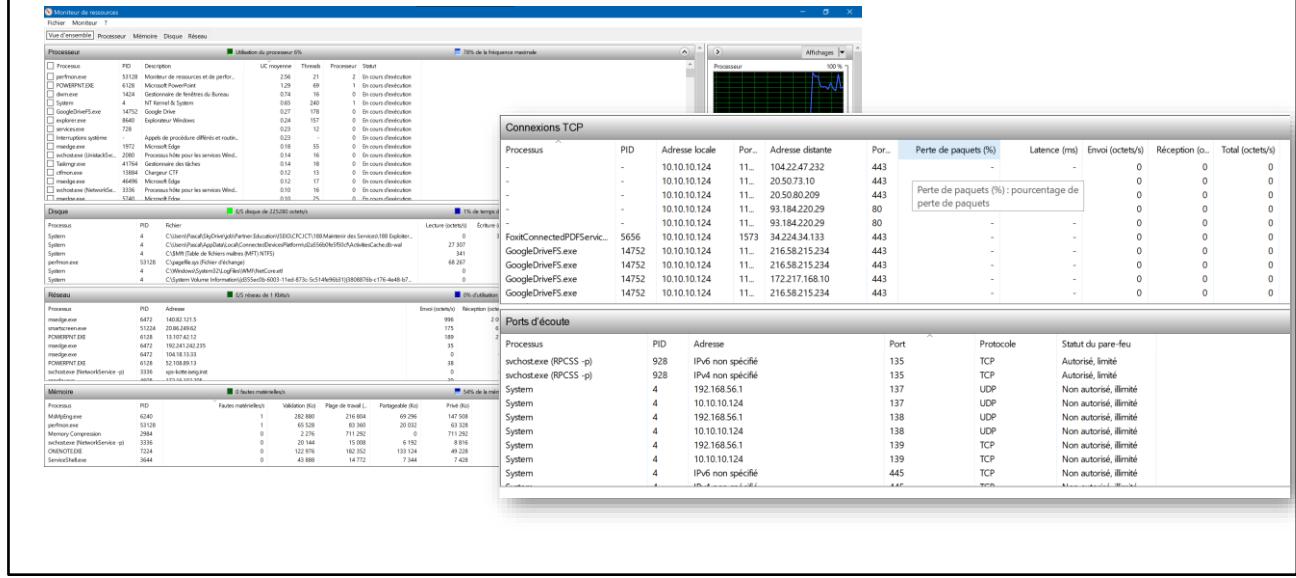
4.4 Connaître des possibilités pour définir des valeurs seuils judicieuses et installer une alarme.

Task manager (gestionnaire de tâches) - AGAIN



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'événements

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Observateur d'événements (Local), Affichages personnalisés, Journaux Windows (selected), Système, Installation, Sécurité, Applications transférées, Journaux des applications et Avertissements. The right pane has tabs for Présentation et synthèse and Vue d'ensemble. The Vue d'ensemble tab is active, showing a summary of events. Below it is a table titled "Résumé des événements d'administration".

Type d'événement	ID de l'événement	Source	Journal	Cette dernière heure	24 heures	7 jours
Critique	-	-	-	0	0	0
Erreur	-	-	-	0	58	339
Avertissement	-	-	-	3	50	356
Information	-	-	-	50	1 531	8 144
Succès de l'authentification	-	-	-	990	7 268	33 826
Échec de l'audit	-	-	-	1	1	1

The main pane shows the "Application" journal with 37 626 events. A detailed view of event 1903 (HHCTRL) is shown in the bottom right, with tabs for Général and Détails. A message at the bottom states: "La taille de formulaire spécifiée n'est pas valide."

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 (Speccy,

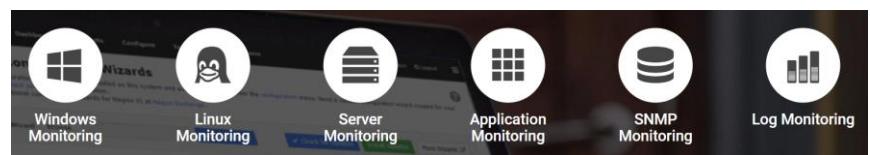
On va voir cela
juste après

Réseaux (NMS)

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

Supervision

- Ex. Nagios
- Zabbix (Linux)



https://fr.wikipedia.org/wiki/Network_management_station

https://fr.wikipedia.org/wiki/Multi_Router_Traffic_Grapher

<https://github.com/oetiker/mrtg>

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

<https://github.com/Cacti/cacti>

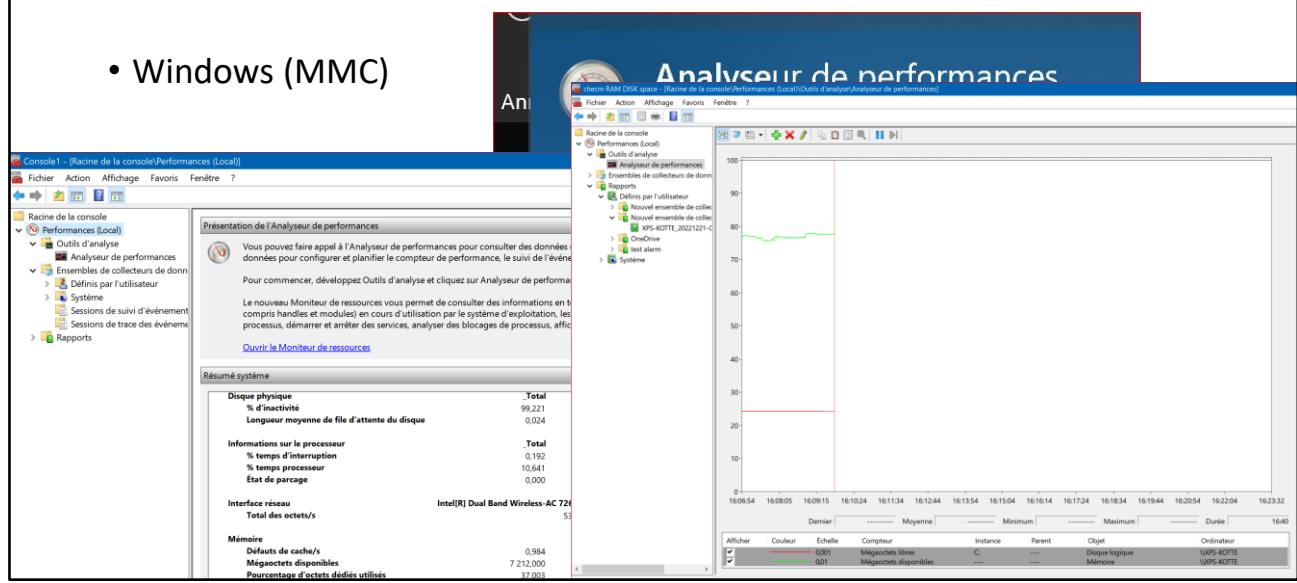
[https://fr.wikipedia.org/wiki/Supervision_\(informatique\)](https://fr.wikipedia.org/wiki/Supervision_(informatique))

<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)

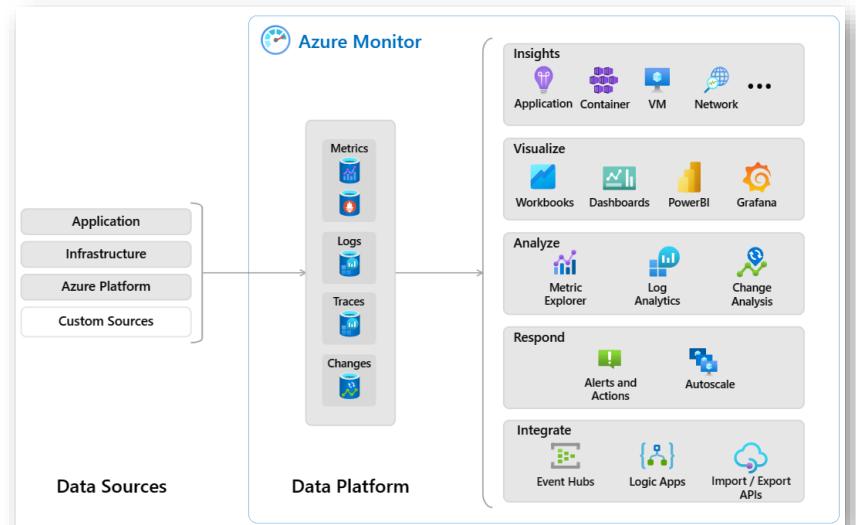


Analyseur de performances

- 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](#)
- ...



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
1.3.6.1.4.1.4526	Switch	NetGear		Infrastructure Device
1.3.6.1.4.1.4526.1	Switch	NetGear		Infrastructure Device
1.3.6.1.4.1.3224.1	Router	NetScreen		Infrastructure Device
1.3.6.1.4.1.3224.1.7	Router	NetScreen	Firewall	Infrastructure Device
1.3.6.1.4.1.23.1.6	Server	NetWare	Server	Computer
1.3.6.1.4.1.45	Switch	Nortel		Infrastructure Device
1.3.6.1.4.1.1872	Switch	Nortel		Infrastructure Device
1.3.6.1.4.1.2272	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
1.3.6.1.4.1.59.1.2.2	Workstation	Silicon Graphics		Computer
1.3.6.1.4.1.2385.3.1.3.1.2	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	Unix	Sun		Computer
1.3.6.1.4.1.42.2.12.3.2.3	Unix	Sun		Computer
1.3.6.1.4.1.42.2.28.13.3.14.1	San Device	Sun	StorEdge	Network Attached Storage
1.3.6.1.4.1.128.2.1.4	Printer	Tektronix		Network Printer
1.3.6.1.4.1.253.8.62.1	Printer	Xerox		Network Printer
1.3.6.1.4.1.8072.3.2.10	Linux			Computer

https://fr.wikipedia.org/wiki/Internet_Control_Message_Protocol_V6

https://fr.wikipedia.org/wiki/Simple_Network_Management_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

Adresse IP privées: 10.*.*.*, 172.16-31.*.*, 192.168.*.*

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/>

WMIC & commandes Windows

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

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

```
C:\Windows\system32\cmd.exe
C:\Users\VincentPC>wmic service get name,processid,startmode,state,status,pathname /format:csv
Node_Name,PathName,ProcessId,StartMode,State,Status
$IN-098ULFR9QGO_reLookupSvc,C:\Windows\System32\svchost.exe -k netsvcs,924,Manual,Running,OK
$IN-098ULFR9QGO_ALG,C:\Windows\System32\alg.exe,0,Manual,Stopped,OK
$IN-098ULFR9QGO_AppIDsvc,C:\Windows\System32\svchost.exe -k LocalServiceAndNoImpersonation,0,Manual,Stopped,OK
$IN-098ULFR9QGO_AppInfo,C:\Windows\System32\svchost.exe -k netsvcs,924,Manual,Running,OK
$IN-098ULFR9QGO_aspnets_state,C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnets_state.exe,0,Manual,Stopped,OK
$IN-098ULFR9QGO_AudioEndpointBuilder,C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted,768,Auto,Running,OK
$IN-098ULFR9QGO_BDESVU,C:\Windows\System32\svchost.exe -k BDESVUGroup,0,Manual,Stopped,OK
$IN-098ULFR9QGO_BFE,C:\Windows\System32\svchost.exe -k netsvcs,0,Manual,Stopped,OK
$IN-098ULFR9QGO_BITS,C:\Windows\System32\svchost.exe -k netsvcs,924,Manual,Running,OK
$IN-098ULFR9QGO_Browser,C:\Windows\System32\svchost.exe -k netsvcs,0,Manual,Stopped,OK
$IN-098ULFR9QGO_bthserv,C:\Windows\System32\svchost.exe -k bthservs,0,Manual,Stopped,OK
$IN-098ULFR9QGO_CertPropSvc,C:\Windows\System32\svchost.exe -k netsvcs,0,Manual,Stopped,OK
$IN-098ULFR9QGO_c1r_optimization_v2_0_50722_32,C:\Windows\Microsoft.NET\Framework\v2.0.50722\ncorsrv.exe,0,Disabled,Stopped,OK
$IN-098ULFR9QGO_c1r_optimization_v4_0_30319_32,C:\Windows\Microsoft.NET\Framework\v4.0.30319\ncorsrv.exe,0,Auto,Stopped,OK
$IN-098ULFR9QGO_d3dumdl,C:\Windows\System32\dllhost.exe /ProcessId:{02D4B3F1-FD88-41D1-9E09-008A5FC9235},0,Manual,Stopped,OK
$IN-098ULFR9QGO_CryptSvc,C:\Windows\System32\svchost.exe -k NetworkService,1184,Auto,Running,OK
$IN-098ULFR9QGO_DcomLaunch,C:\Windows\System32\svchost.exe -k DcomLaunch,644,Auto,Running,OK
$IN-098ULFR9QGO_defragsvc,C:\Windows\System32\svchost.exe -k defragsvc,0,Manual,Stopped,OK
$IN-098ULFR9QGO_Dhcp,C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted,768,Auto,Running,OK
$IN-098ULFR9QGO_DnsCache,C:\Windows\System32\svchost.exe -k NetworkService,0,Manual,Stopped,OK
$IN-098ULFR9QGO_dot3svc,C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted,0,Manual,Stopped,OK
$IN-098ULFR9QGO_DPS,C:\Windows\System32\svchost.exe -k LocalServiceNoNetwork,1304,Auto,Running,OK
```

https://fr.wikipedia.org/wiki/Windows_Management_Instrumentation

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

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

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

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

getmac /v /fo list

netsh interface ipv6 show int

netsh interface ipv6 show neighbors interface=43
(ou remplacer 43 par le bon index de l'interface souhaitée)

Exercice: tracert

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

```
C:\Users\pasca>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  internethbox.home [192.168.1.1]
 2  63 ms  34 ms  4 ms  100.85.192.1
 3  8 ms  4 ms  3 ms  ae22-1150.ipc-lss690-m-pe-48.bluewin.ch [213.3.220.253]
 4  5 ms  3 ms  3 ms  etht22-1150.lssic20p-cgn001.bluewin.ch [213.3.220.254]
 5  5 ms  5 ms  4 ms  213.3.220.169
 6  5 ms  4 ms  3 ms  i69lsp-015-aell.bb.ip-plus.net [193.134.95.64]
 7  *   *   *   * Déjà d'attente de la demande dépassé.
 8  *   *   *   * Déjà d'attente de la demande dépassé.
 9  *   *   *   * Déjà d'attente de la demande dépassé.
10  *   *   *   * Déjà d'attente de la demande dépassé.
11  *   *   *   * Déjà d'attente de la demande dépassé.
12  11 ms  11 ms  11 ms  ae-15.r00.frnkge13.de.bb.gin.ntt.net [129.250.66.57]
13  69 ms  39 ms  63 ms  ae-2.r22.frnkge13.de.bb.gin.ntt.net [129.256.6.13]
14  12 ms  11 ms  11 ms  ae-0.a02.frnkge07.de.bb.gin.ntt.net [129.256.5.34]
15  101 ms  49 ms  59 ms  ae-0.f5-networks.frnkge07.de.bb.gin.ntt.net [128.241.10.17]
16  *   *   *   * Déjà d'attente de la demande dépassé.
17  47 ms  88 ms  78 ms  107.162.251.254
18  111 ms  89 ms  61 ms  107.162.248.163
19  102 ms  101 ms  101 ms  107.162.249.4
20  *   *   *   * Déjà d'attente de la demande dépassé.
21  64 ms  52 ms  75 ms  te0-0-1-0.er01.lyo02.fr.ip-max.net [46.20.254.2]
22  17 ms  19 ms  17 ms  be1.er01.lyo01.fr.ip-max.net [46.20.254.114]
23  19 ms  22 ms  18 ms  te0-1-0-3.er01.pva09.ch.ip-max.net [46.20.247.168]
24  23 ms  37 ms  83 ms  te0-0-1-0.er01.pva09.ch.ip-max.net [46.20.253.15]
25  53 ms  98 ms  46 ms  te0-2-0-4.er01.pva20.ch.ip-max.net [46.20.253.21]
26  96 ms  18 ms  24 ms  be20.er02.pva20.ch.ip-max.net [46.20.254.89]
27  17 ms  16 ms  18 ms  46.20.248.147
28  100 ms  97 ms  38 ms  160.53.249.22
29  *   *   *   * Déjà d'attente de la demande dépassé.
30  17 ms  16 ms  17 ms  webaccess.ville-geneve.ch [193.134.176.29]
```

```
C:\Users\pasca>tracert paris.fr
```

```
Détermination de l'itinéraire vers paris.fr [194.153.110.192]
avec un maximum de 30 sauts :

 1  1 ms  1 ms  1 ms  internethbox.home [192.168.1.1]
 2  4 ms  4 ms  4 ms  100.85.192.1
 3  45 ms  110 ms  89 ms  ae22-1150.ipc-lss690-m-pe-48.bluewin.ch [213.3.220.253]
 4  49 ms  74 ms  91 ms  etht22-1150.lssic20p-cgn001.bluewin.ch [213.3.220.254]
 5  28 ms  87 ms  82 ms  213.3.220.169
 6  6 ms  10 ms  9 ms  i69lsp-015-aell.bb.ip-plus.net [193.5.72.24]
 7  *   *   *   * Déjà d'attente de la demande dépassé.
 8  *   *   *   * Déjà d'attente de la demande dépassé.
 9  *   *   *   * Déjà d'attente de la demande dépassé.
10  55 ms  64 ms  102 ms  il5-lef01-t2-62-34-3-223.ft.lns.abo.bbox.fr [62.34.3.223]
11  107 ms  55 ms  95 ms  be5.cbr01-cro.net.bbox.fr [212.194.171.141]
12  17 ms  17 ms  17 ms  0.lal15.bsr01-th2.net.bbox.fr [212.194.171.93]
13  *   *   *   * Déjà d'attente de la demande dépassé.
14  *   *   *   * Déjà d'attente de la demande dépassé.
15  87 ms  53 ms  71 ms  89.81.78.217
16  17 ms  17 ms  17 ms  31.32.73.146
17  *   *   *   * Déjà d'attente de la demande dépassé.
18  *   *   *   * Déjà d'attente de la demande dépassé.
19  *   *   *   * Déjà d'attente de la demande dépassé.
20  *   *   *   * Déjà d'attente de la demande dépassé.
21  *   *   *   * Déjà d'attente de la demande dépassé.
22  *   *   *   * Déjà d'attente de la demande dépassé.
23  *   *   *   * Déjà d'attente de la demande dépassé.
24  *   *   *   * Déjà d'attente de la demande dépassé.
25  *   *   *   * Déjà d'attente de la demande dépassé.
26  *   *   *   * Déjà d'attente de la demande dépassé.
27  *   *   *   * Déjà d'attente de la demande dépassé.
28  *   *   *   * Déjà d'attente de la demande dépassé.
29  *   *   *   * Déjà d'attente de la demande dépassé.
30  *   *   *   * Déjà d'attente de la demande dépassé.
```

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

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

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

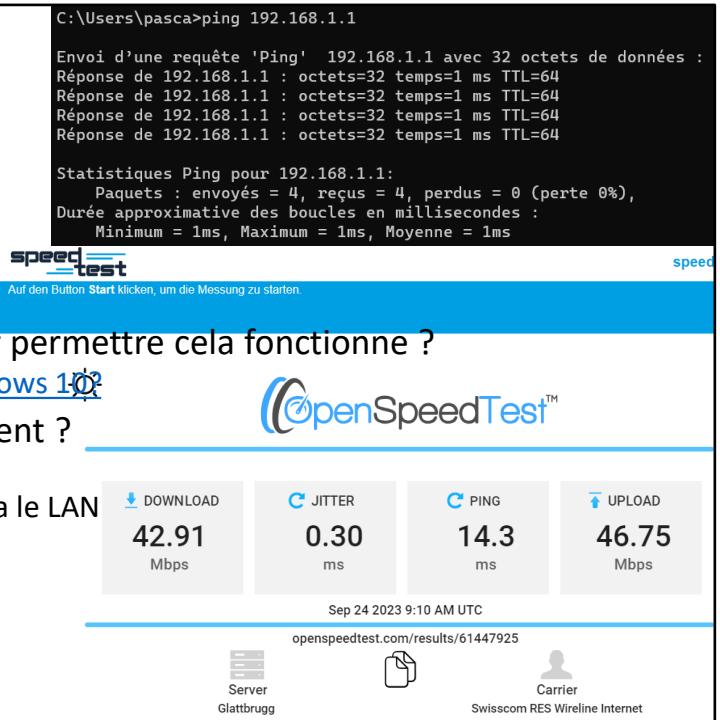
<https://trouver-ip.info/localiser-ip/>

Exercice - ping

- Faire un Ping du voisin
 - Est-ce que cela fonctionne ?
 - Pourquoi ?
- Quelle action nécessaire pour permettre cela fonctionne ?
 - [Comment faire ping vers Windows 10?](#)
- Que cela mesure-t-il exactement ?

Et pour un accès Internet ?

 - Présence et connectivité OK via le LAN
 - Débit (speed)
 - [Latence](#) (Latency)
 - [Gigue](#) (Jitter)



Comment autoriser Ping, entre 2 W10/11?

<https://medium.com/conseillers-num%C3%A9riques-suisses-romands/comment-faire-ping-sous-windows-10-4123cbb32787>

Voir aussi tests performances de l'accès Internet

Best

<https://www.nperf.com/fr/>

Avec Jitter:

<https://www.speedtest.ch/> (Germain)

<https://openspeedtest.com/about-speed-test>

<https://test-debit-internet.fr/test-ping/>

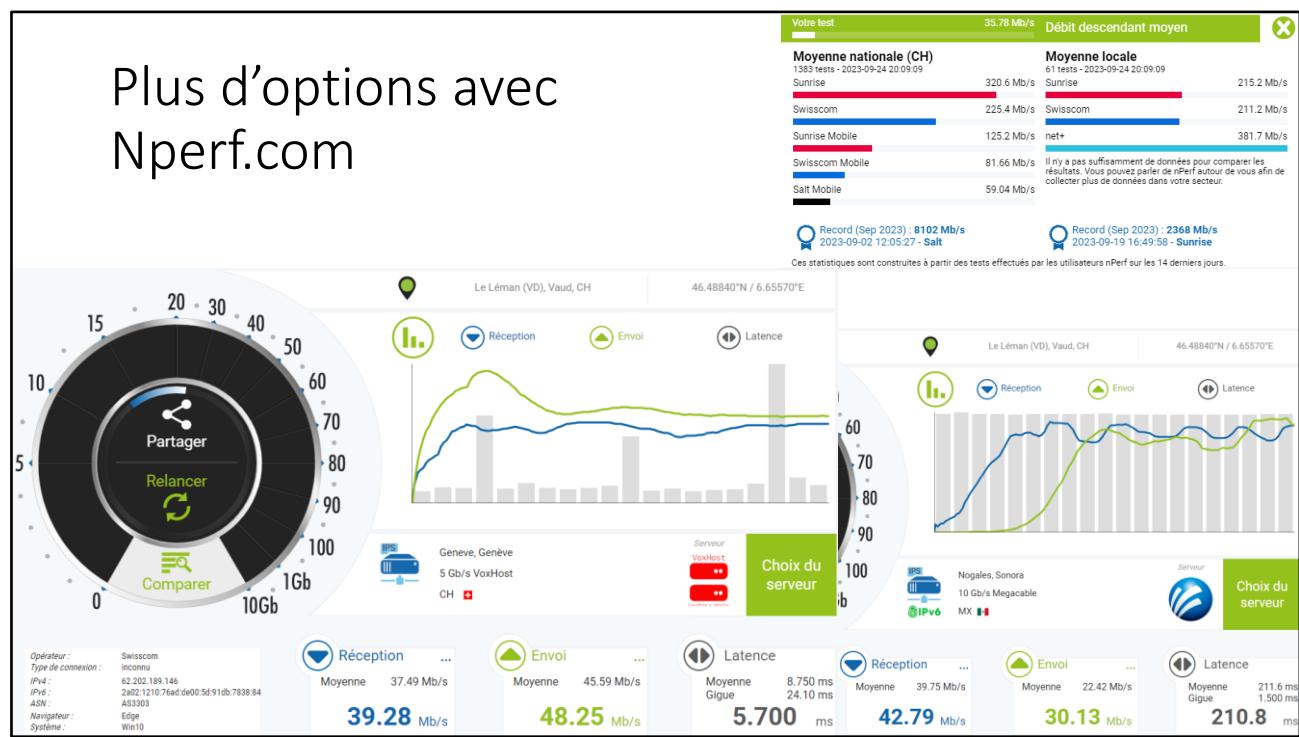
<https://www.speedtest.net/fr>

Alternative: slide suivante et

<https://www.cnlab.ch/fr/speedtest>

Version Web: <https://speedtest.cnlab.ch/fr/>

<https://ux.cnlab.ch/benchmarking/home>



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

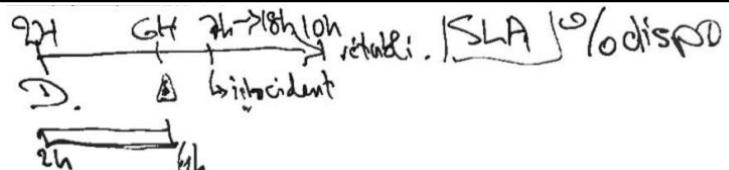
[A propos - nPerf.com](https://www.nperf.com/fr/about-us/) <https://www.nperf.com/fr/about-us/>

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 moniter 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/Indicateur_clé_de_performance](https://fr.wikipedia.org/wiki/Indicateur_cl%C3%A9_de_performance)

[https://fr.wikipedia.org/wiki/Disponibilité](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 Début Utilisateurs Détails Services

Nom	Éditeur	Statut	Impact du dé...
Microsoft SharePoint	Microsoft Corporation	Activé	Haut
Google Drive	Google, Inc.	Activé	Haut
X-Mouse Button Control	Highresolution Enterpris...	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

15:23:27
FRA mercredi
2022-11-02

Durée de fonctionnement
0:06:43:31

Cache de niveau 1 : 256 Ko
Cache de niveau 2 : 1,0 Mo
Cache de niveau 3 : 6,0 Mo

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

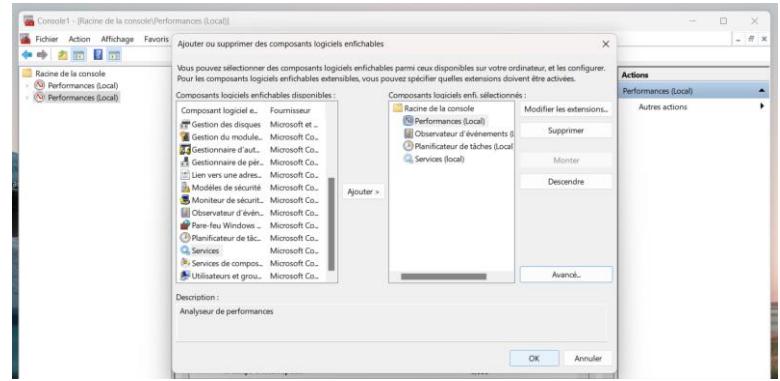
Exercice: Repérer comment lister l'historique de tous les (re)démarrages enregistrés par une machine Windows.

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 processus des
«patchs» pour cela, si c'est gratuit,
mais ce n'est plus du «patching».

- Certains « updates » spécifiques vont « nettoyer » un botnet existant, sans nécessairement 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](#)

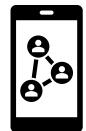
[Microsoft Update Catalog](#) <https://www.catalog.update.microsoft.com/Search.aspx?q=kb>

[Security Update Guide – Microsoft](#) <https://msrc.microsoft.com/update-guide>

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

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

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 ? \(lojicieux.com\)](#)

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

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

Linux (selon la distribution, mais similaires)

- sudo apt update
- **apt list --upgradable**
- ‘sudo apt upgrade’
Ou bien ‘sudo apt full-upgrade’

Faire le ménage (1 des 2)

- sudo apt autoremove (**light**)
- sudo apt autoclean (**deep**)

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

```
Fichier Edition Affichage Rechercher Terminal Aide
Atteint:10 http://fr.archive.ubuntu.com/ubuntu bionic-backports InRelease
Ign:11 https://dl.bintray.com/resin-io/debian stable InRelease
Atteint:12 http://ppa.launchpad.net/eosrei/fonts/ubuntu bionic InRelease
Atteint:13 https://deb.opera.com/opera-stable stable InRelease
Atteint:14 http://apt.insynchq.com/ubuntu bionic InRelease
Atteint:15 https://repo.skype.com/deb stable InRelease
Réception de:1 https://dl.bintray.com/resin-io/debian stable Release [1 878 B]
Atteint:17 https://deb.torproject.org/torproject.org bionic InRelease
Atteint:18 http://ppa.launchpad.net/gezakovacs/ppa/ubuntu bionic InRelease
Atteint:19 http://ppa.launchpad.net/graphics-drivers/ppa/ubuntu bionic InRelease
Atteint:20 http://ppa.launchpad.net/kritalime/ppa/ubuntu bionic InRelease
Atteint:21 http://ppa.launchpad.net/nilarmogard/webupd8/ubuntu bionic InRelease
Atteint:22 https://repo.nordvpn.com/deb/nordvpn/debian stable InRelease
Atteint:23 http://ppa.launchpad.net/ondrej/php/ubuntu bionic InRelease
Atteint:24 http://ppa.launchpad.net/otto-kesselgulash/gimp/ubuntu bionic InRelease
Atteint:25 http://ppa.launchpad.net/seafile/seafile-client/ubuntu bionic InRelease
1 878 o réceptionnés en 2s (1 016 o/s)
  lecture des listes de paquets... Fait
  construction de l'arbre des dépendances
  lecture des informations d'état... Fait
  1 paquet peuvent être mis à jour. Exécutez « apt list --upgradable » pour les voir.
```

Equivalent du cleanmgr

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

Windows update

Wuauserv

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

Optimisation de la distribution

*Certains de ces paramètres sont masqués ou gérés par votre opérateur.

L'optimisation de la distribution vous fournit des mises à jour de Windows et des applications du Store, et d'autres produits Microsoft de manière rapide et fiable.

Autoriser les téléchargements à partir d'autres PC

Si vous avez une connexion Internet instable ou si vous mettez plusieurs appareils à jour, autorisez les téléchargements à partir d'autres PC, peut accélérer le processus.

En savoir plus

Autoriser les téléchargements à partir d'autres PC

Désactive

PC sur mon réseau local

PC sur mon réseau local, et PC sur Internet

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

Windows Update

Redémarrage nécessaire

Votre appareil va redémarrer en dehors des heures d'activité.

Statut : Redémarrage en attente

Redémarrer Planifier le redémarrage

Afficher les mises à jour facultatives

Mise à jour de fonctionnalité vers Windows 10, version 22H2

La prochaine version de Windows est disponible avec de nouvelles fonctionnalités et des améliorations en matière de sécurité. Lorsque vous êtes prêt pour la mise à jour, sélectionnez « Télécharger et installer ».

Télécharger et installer Découvrez ce qu'il y a dans cette mise à jour

Suspendre les mises à jour pendant 7 jours Consultez les options avancées pour modifier la période de suspension.

Modifier les heures d'activité Actuellement 07:00 à 01:00

Afficher l'historique des mises à jour Voir les mises à jour installées sur votre appareil

Options avancées Paramètres et contrôles de mise à jour supplémentaires

Options avancées

Options de mise à jour

Recevoir les mises à jour d'autres produits Microsoft lorsque vous mettez à jour Windows

Activé

Télécharger les mises à jour sur des connexions limitées (des frais supplémentaires peuvent s'appliquer)

Désactivé

Redémarrez cet appareil dès que possible lorsqu'un redémarrage est nécessaire pour installer une mise à jour. Assurez-vous que l'alimentation de votre appareil doit être allumée et branchée.

Désactivé

Notifications de mise à jour

Afficher une notification lorsque votre PC nécessite un redémarrage pour terminer la mise à jour

Active

Actuellement, ce PC ne dispose pas de la configuration système minimale requise pour exécuter Windows 11

Obtenir les détails et voyez s'il y a des choses que vous pouvez faire dans l'application Bilan de santé du PC

Obtenir un bilan de santé du PC

Vous recherchez des informations sur les toutes dernières mises à jour ?

En savoir plus

Redémarrer OK

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 consister 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

Jusqu'en 2017...

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

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

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 MSIEEXEC
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 ? \(lojicieux.com\)](https://www.lojicieux.com/comment-installer-manuellement-un-fichier-CAB-dans-Windows-10-.html)

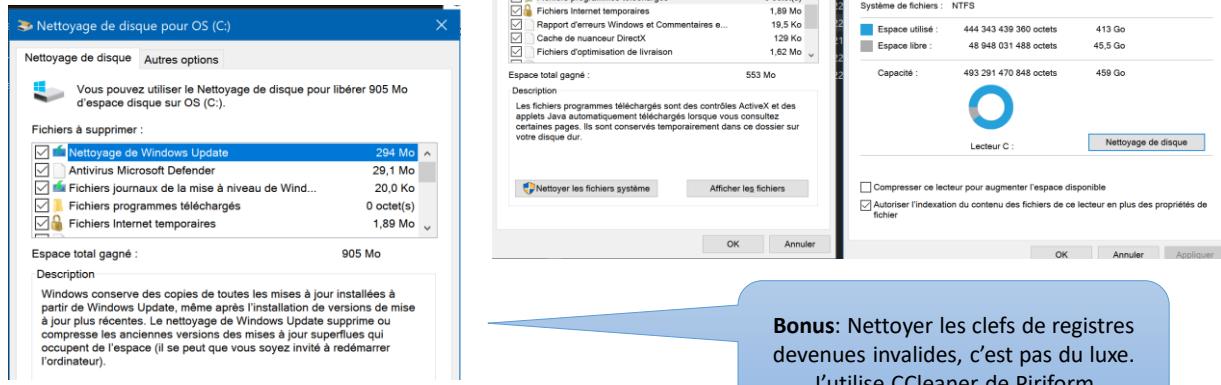
[https://www.lojicieux.com/comment-installer-manuellement-un-fichier-cab-dans-windows-10/ \(Bof cet article à trouver mieux!\)](https://www.lojicieux.com/comment-installer-manuellement-un-fichier-cab-dans-windows-10/)

<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)

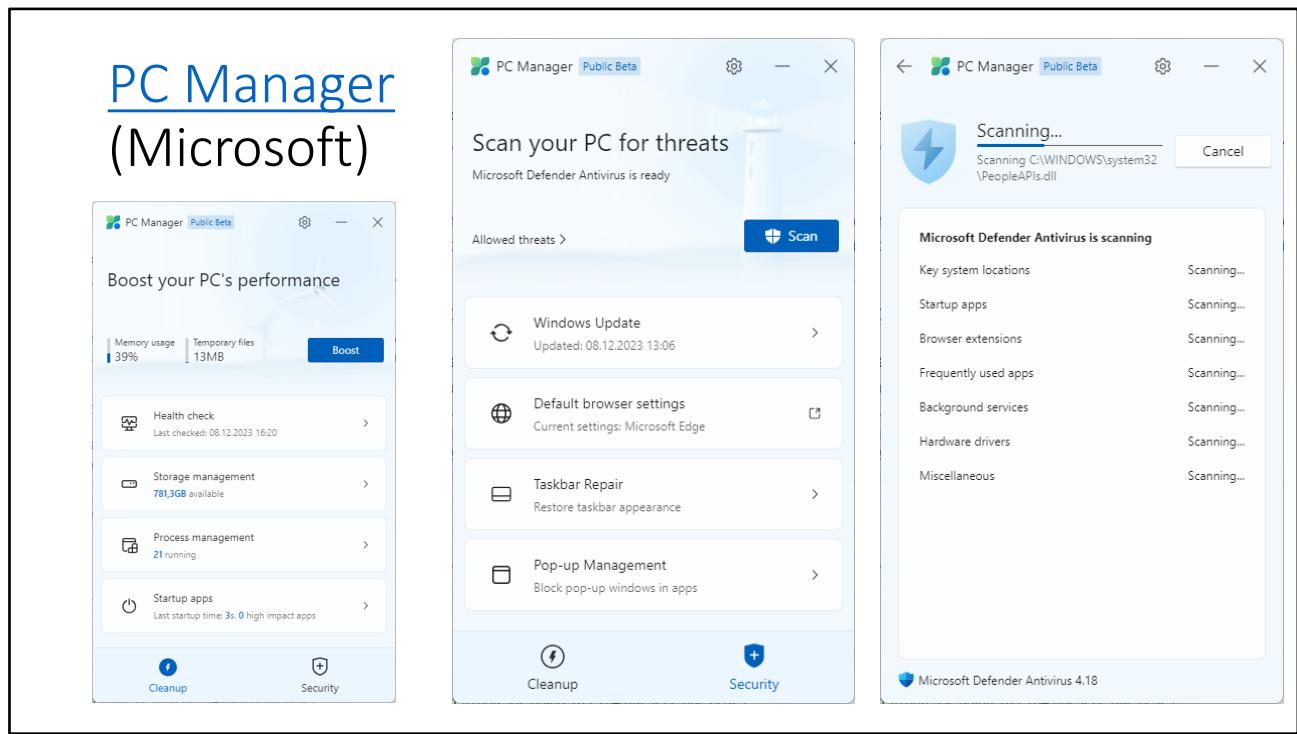


Cela fonctionne aussi sur des OS serveurs, sauf qu'il faut ajouter la fonctionnalité [Windows Server 2008 nettoyage de disque - comment activer / installer / exécuter. \(hdd-tool.com\)](#)

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

<https://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>



Merci Laeticia

<https://pcmanager.microsoft.com/en-us>

Download Beta

<https://www.bing.com/ck/a?!&&p=c822a4ba9dff34e3JmltdHM9MTcwMTk5MzYwMCZpZ3VpZD0zMmQ3YmRmYi1kOGVkLTZjMzUtMTEyNi1hZTZjZDk1NzZkOWMmaW5zaWQ9NTUwNQ&ptn=3&ver=2&hsh=3&fclid=36d7bdfb-d8ed-6c35-1126-ae6cd9576d9c&psq=PC+manager+Microsoft&u=a1aHR0cHM6Ly9ha2EubXMvUENNYW5hZ2VyT0ZMNTIwMDAx&ntb=1>

Official

<https://apps.microsoft.com/detail/9PM860492SZD?hl=en-US&gl=US>

Patch (EXE) de Windows

Certains «Patchs» 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

The screenshot shows a window titled "Outil de suppression de logiciels malveillants". It contains syntax information for the tool, followed by two log outputs from the Microsoft Malicious Software Removal Tool.

Syntaxe :

- /Q ou /quiet - mode silencieux, aucune interface n'est affichée
- /? ou /help - affiche la syntaxe
- /N - mode détection seule
- /F - effectue une analyse complète
- /FY - effectue une analyse complète et nettoie les fichiers infectés.

Microsoft Windows Malicious Software Removal Tool v5.96, (build 5.96.18833.1)
Started On Wed Dec 15 15:18:11 2021
Engine: 1.1.18700.4
Signatures: 1,353,1477,0
MdGear: 1.1.16330.1
Run Mode: Scan Run From Windows Update

Results Summary:
.....
No Infection Found.
Successfully Submitted Heartbeat Report
Microsoft Windows Malicious Software Removal Tool Finished On Wed Dec 15 15:32:46 2021

Return code: 0 (0x0)

Microsoft Windows Malicious Software Removal Tool v5.97, (build 5.97.18853.1)
Started On Thu Jan 13 12:54:31 2022
Engine: 1.1.18800.4
Signatures: 1,355,668,0
MdGear: 1.1.16330.1
Run Mode: Scan Run From Windows Update

Results Summary:
.....
No Infection Found.
Successfully Submitted Heartbeat Report
Microsoft Windows Malicious Software Removal Tool Finished On Thu Jan 13 13:07:37 2022

Return code: 0 (0x0)

Exemple avec: KB890830 - MSRT

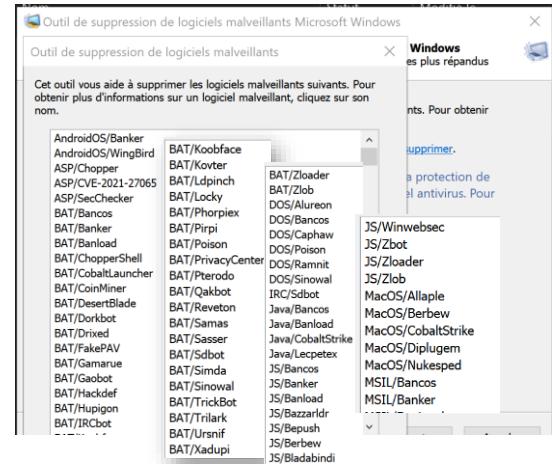
<https://support.microsoft.com/fr-fr/topic/supprimer-des-logiciels-malveillants-sp%C3%A9cifiques-et-r%C3%A9pandus-%C3%A0-l-aide-de-l-outil-de-suppression-de-logiciels-malveillants-windows-kb890830-ba51b71f-39cd-cdec-73eb-61979b0661e0>

<https://msrc.microsoft.com/> [Microsoft Security Response Center](#)

Par sécurité !! Motivation principale...

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

MSIL/Zloader	Script/Qakbot	Win32/Zlob	WinNT/Zuten
PDF/Emotet	VBA/Emotet	Win32/Zonebac	X97M/Emotet
PowerShell/Banload	VBA/Fareit	Win32/Zutem	X97M/Qakbot
PowerShell/Bazzardr	VBS/Bagle	Win64/Alureon	XML/CobaltStrike
	VBS/Bancos	Win64/AnchorBot	XML/Emotet
	VBS/Banker	Win64/AnchorDNS	
	VBS/Banload	Win64/Badaxis	
PowerShell/Zloader	VBS/Bladabindi	Win64/Winnti	
Python/Banker		Win64/Zbot	
Python/CVE-2021-16855		W97M/Emotet	Win64/Zloader
Python/CVE-2021-26855		W97M/Gamarue	X97M/Alureon
Python/Exmann		W97M/Jexnexus	WinNT/Bagle
Python/IRCBot		W97M/Rovnix	WinNT/Bancos
Script/CobaltStrike		W97M/Ursnif	
Script/CVE-2021-26855		W97M/Vawtrak	
		W97M/Zbot	
		Win32/Adposhel	
		Win32/Afore	



Pour références:

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

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

Microsoft:

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

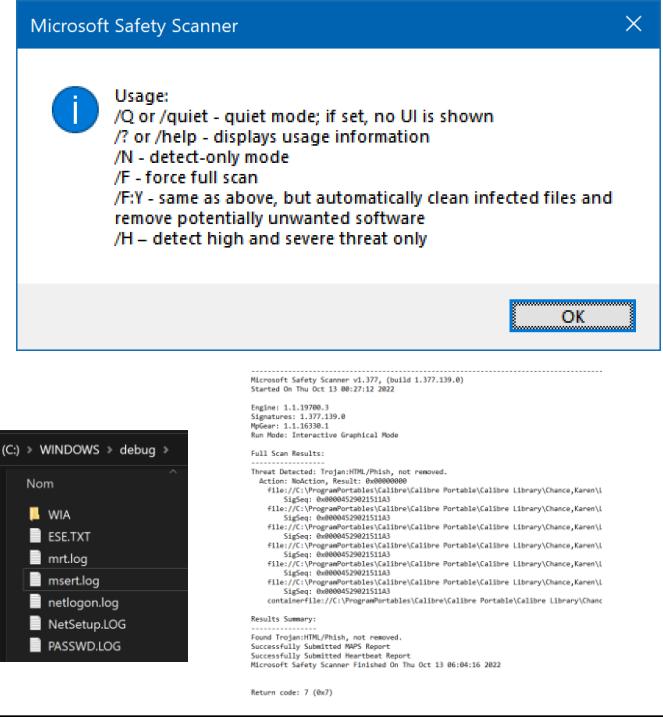
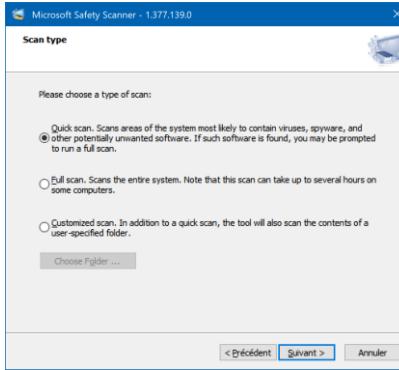
<https://support.microsoft.com/fr-fr/topic/comment-faire-pour-r%C3%A9soudre-une-erreur-lorsque-vous-ex%C3%A9cutez-le-scanner-de-s%C3%A9curit%C3%A9-microsoft-6cd5faa1-f7b4-af2-85c7-9bed02860f1c>

MSERT

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

Un grand frère de MSRT...

- Log = msert.log

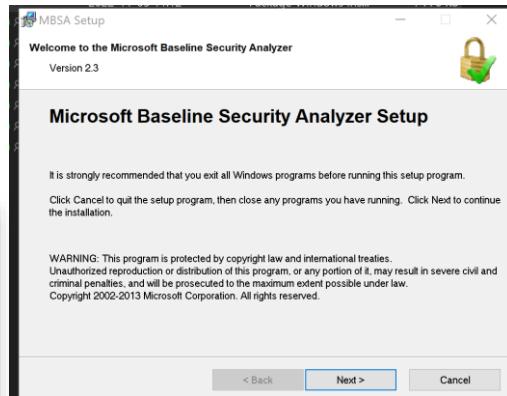


<https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/safety-scanner-download>

Scan vulnérabilité vs Removal!

- MBSA pour Windows (fini!) depuis 2013/2014

Historique: Avant W10/S2016



[Microsoft Baseline Security Analyzer - Wikipedia](#)

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

<https://learn.microsoft.com/fr-fr/security-updates/security/20196904>

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

<https://learn.microsoft.com/fr-fr/windows-server/administration/windows-server-update-services/deploy/1-install-the-wsus-server-rôle>

[Definition of a Security Vulnerability \(microsoft.com\)](https://www.microsoft.com/en-us/msrc/definition-of-a-security-vulnerability?rtc=1) <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 Plan 2 et E5 peuvent ajouter de nouveaux outils avancés de gestion des vulnérabilités à leur abonnement existant grâce au module complémentaire Gestion des vulnérabilités Microsoft Defender.

Fonctionnalités clés :

- ✓ Outils de sécurité unifiée 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
- ✓ Blocage des applications vulnérables

Disponible pour tous les clients

Gestion des vulnérabilités Microsoft Defender autonome

[Essayez gratuitement](#)

Inclut toutes les fonctionnalités du module complémentaire Gestion des vulnérabilités Microsoft Defender, PLUS :

- ✓ Évaluation des vulnérabilités
- ✓ Évaluation des configurations
- ✓ Surveillance continue
- ✓ Analytique 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>

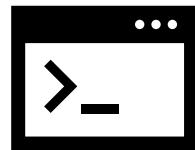
Autres solutions:

- 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 férences:

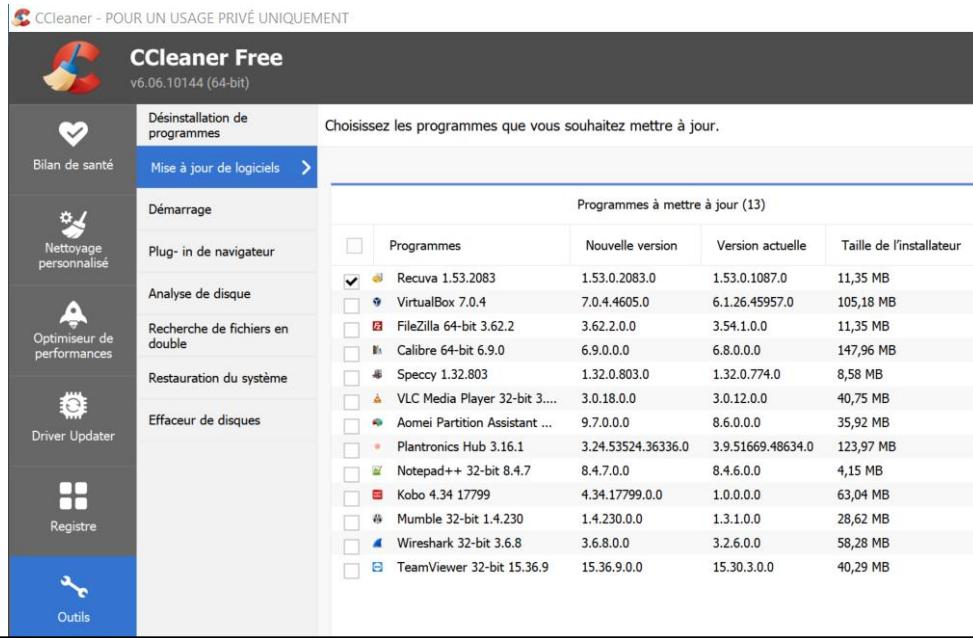
<https://www.malekal.com/installer-plusieurs-antivirus-windows-10/>

De l'auteur de ce support: PaKo

<https://medium.com/conseillers-num%C3%A9riques-suisses-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)



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

<https://www.lifewire.com/10-best-free-software-updater-programs-2625200>

winstall

Winget

- [Browse the winget repository - winstall](#)
- [Your own winget repository | winget.Pro](#)

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

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

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

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?)

Exploiter, surveiller et assurer la maintenance des services

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

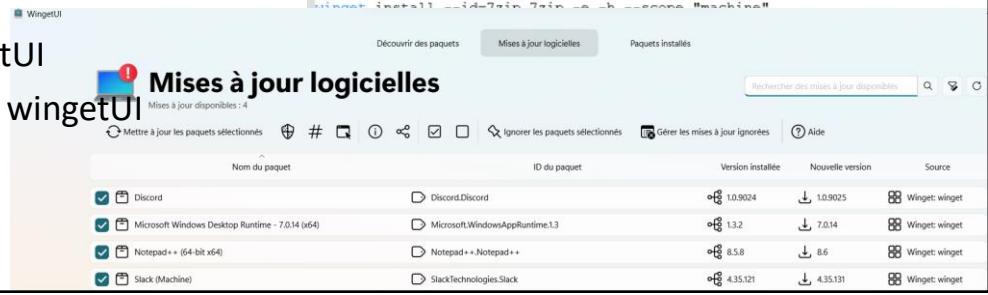
```
rem sécurité et système
winget install --id=SomePythonThings.WingetUIStore -e -h --scope "machine"
rem WingetUI - on est d'accord, c'est un nom de package assez moi si
winget install --id=Piriform.CCleaner -e -h --scope "machine"
winget install --id=Bitwarden.Bitwarden -e -h --scope "machine"
winget install --id=VirusTotal.VirusTotalUploader -e -h --scope "machine"
rem winget install --id=IObit.MalwareFighter -e -h --scope "machine"
rem bug Le code de hachage de l'installation ne correspond pas ; ceci ne peut pas être vérifié
rem winget install --id=SaferNetworking.SpybotAntiBeacon -e -h --scope "machine"

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

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

rem winget install --id=Discord.Discord -e -h --scope "machine" - bug ?
winget install --id=Discord.Discord -e -h --scope "machine"

rem outils, traducteur, pdf reader...
winget install --id=7zip.7z -e -h --scope "machine"
```

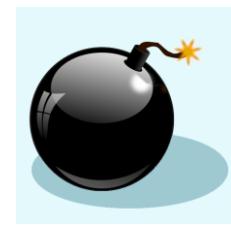


WingetUI

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

Rollback ?

- Identifier lequel des KB a posé problème,
 - et le retirer, avec la plateforme de déploiement...
- Faire un système state restore sur les postes
- Cryptolocker – utiliser OneDrive



Avoir fait des tests avant pour éviter de devoir corriger partout...

Mais comment peut-on tester ?

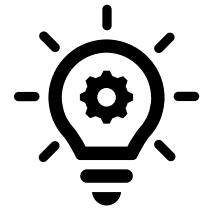
- Par phase
- Échantillons significatifs

Tester:

- Monter un LAB, un clone, et tester sur une copie...
- Si pas possible, tester sur 1 échantillon limité
- Si pas possible, faire un bon backup, et vérifier être capable de revenir rapidement dessus, effectivement...

Merci à Noha,

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...

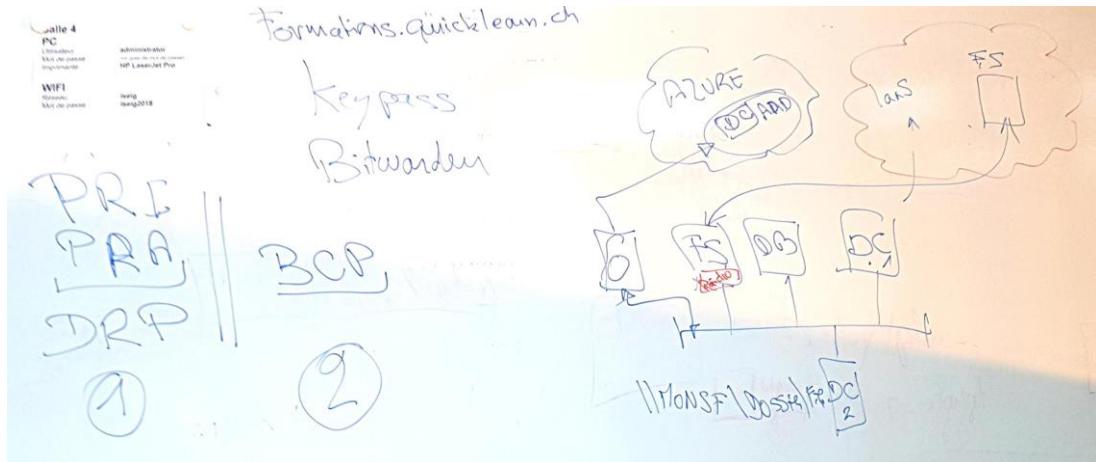
Déployer uniquement les éléments nécessaires

- 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
- * Check signatures (ex MD5 => SHA2)



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE URL SEARCH



Choose file

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the sharing of your sample submission with the security community. Please do not submit any personal information. VirusTotal is not responsible for the contents of your submission. Learn more.

Want to automate submissions? Check our API, free quota grants available for new file uploads.

Antivirus	Result	Antivirus	Result
AegisLab	Undetected	Ad-Aware	Undetected
AI4PC	Undetected	Alibaba	Undetected
AVG	Undetected	Anti-ViL	Undetected
Baidu	Undetected	Avast	Undetected
BitDefenderTheta	Undetected	BitDefender	Undetected
ClamAV	Undetected	Blar Pro	Undetected
Comodo	Undetected	CMC	Undetected
Cynet	Undetected	Cyberseason	Undetected
Emsisoft	Undetected	D-Web	Undetected
		eScan	Undetected

<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 reformatée 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'examinateur 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

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

The screenshot displays three separate web interfaces side-by-side:

- Fing:** Shows network status for "Your dilwif2etage2.4ghz network". It indicates 8 online devices (1 found, 7 unrecognized), an internet speed of 44.1 / 49.2 Mbps, and a security rating of "Medium-Secure".
- VIRUSTOTAL:** A file analysis tool with tabs for FILE, URL, and SEARCH. It includes a note about analyzing files, domains, IPs and URLs to detect malware and other threats.
- BitWarden:** A password manager interface showing a list of saved items, including "swisscom" and "XPS 15 9530". It also shows a "Local Network" section with details like Local IP (192.168.1.10) and a "VPN - Swisscom" entry.

Quelques outils, plutôt destinés aux utilisateurs et non aux infrastructures IT.

https://www.fing.com/premium#premium_plans

Plateformes ITSM (Entreprises)

IT Service Management

IT Service Management

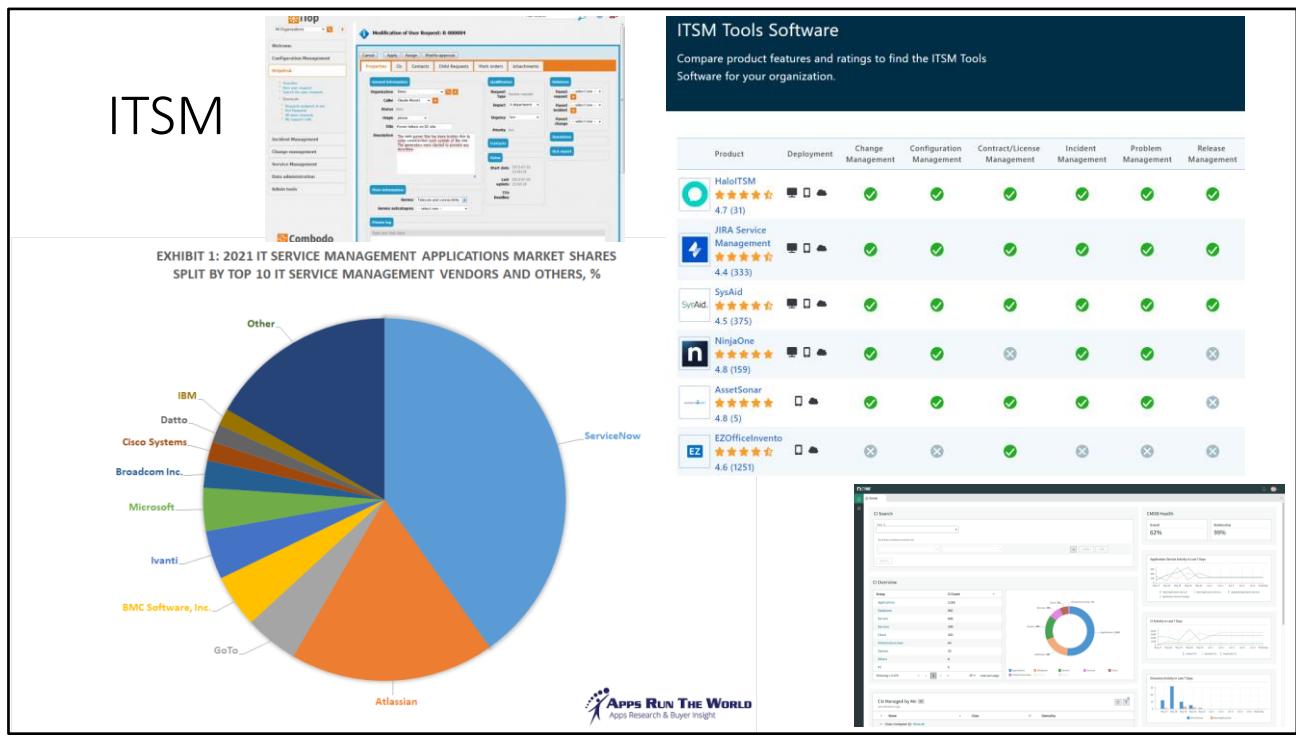
Free Edition	Edition Professionnelle	Edition Entreprise	Edition UEM
Convient aux PME		Fonctionnalités de l'édition Professionnelle +	Fonctionnalités de l'édition Entreprise +
Gérez jusqu'à 25 ordinateurs et 25 appareils mobiles	» Gestion des correctifs	» Optimisation de la Bande Passante WAN	» Gestion des Péphériques Mobiles
» Gestion des Correctifs	» Déploiement de Logiciels	» Portail Libre-service	» Gestion Moderne des Péphériques Windows 10
» Déploiement de Logiciels	» Gestion des Ressources	» Logiciels Interdits / Blocage des EXE	» Déploiement d'OS
» Gestion des Assets	» Configurations	» Mesurage 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 Péphériques USB	
	» Gestion des périphériques mobiles (Add-on)	» Authentification à Deux Facteurs	
	» Déploiement d'OS (Add-on)	» Gestion des appareils mobiles (Add-on)	
		» Déploiement d'OS (Add-on)	

Edition Gratuite	Professionnelle	Enterprise
Jusqu'à 20 ordinateurs et 5 serveurs	Convient aux ordinateurs en réseau local	Convient aux ordinateurs en WAN
Adaptée aux PME	» Correctifs pour Windows, Mac & terminaux Linux	Fonctionnalités de l'édition professionnelle +
Entièrement fonctionnel	» Gestion des correctifs tiers	» Serveur de distribution pour l'optimisation de la bande passante
Jusqu'à 20 ordinateurs et 5 serveurs	» Gestion des correctifs des applications serveur	» Mises à jour des définitions d'antivirus
	» Déploiement des Service Packs	» Validation et approbation des correctifs
	» Rapports sur la gestion des correctifs	» Authentification double 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>



Un aperçu d'autres solutions:

<https://www.capterra.com/sem-compare/itsm-software/>

<https://www.appsrunttheworld.com/top-10-it-service-management-software-vendors-and-market-forecast/>

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>

The screenshot shows the Chocolatey website with the following sections:

- Chocolatey (packaging & deploy)**
- Chocolatey for Business**: Automate your entire Windows Software Lifecycle.
- Benefits**, **Features**, **Pricing** buttons.
- About**, **Product**, **Community**, **Docs**, **Beta** buttons.
- chocolatey/VirusTotal.NET: A full implementation of the VirusTotal 2.0 API (github.com)**
- Pricing** section for Chocolatey for Business:
 - Small**: 100-499 Machines, \$16.50 /license per year, Purchase button.
 - Medium**: 500+ Machines, \$16.10 /license per year, Purchase button.
- Step 2: Choose Your Installation Method** dropdown menu:
 - Generic
 - Individual**
 - Ansbile
 - CHEF
 - PS DSC
 - puppet
- Know the Requirements:**
 - Supported Windows client and server Operating Systems (can run on older Operating Systems)
 - PowerShell v2+ (minimum is v5 for install from this website due to TLS 1.2 requirement)
 - .NET Framework 4.8 (the installation will attempt to install .NET 4.8 if you do not have it installed)
- 1. Choose How to Install Chocolatey:**
 - Generic
 - Individual**
 - Ansbile
 - CHEF
 - PS DSC
 - puppet
- Install Chocolatey for Individual Use:**
 - First, ensure that you are using an **administrative shell** - you can also install as a non-admin, check out [Non-Administrative Installation](#).
 - Install with powershell.exe

NOTE: Please inspect <http://community.chocolatey.org/install.ps1> prior to running any of these scripts to ensure safety. We already know it's safe, but you should verify the security and contents of **any** script from the internet you are not familiar with. All of these scripts download a remote PowerShell script and execute it on your machine. We take security very seriously. [Learn more about our security protocols](#).

With PowerShell, you must ensure `Get-ExecutionPolicy` is not Restricted. We suggest using `ByPass` to bypass the policy to get things installed or `AllSigned` for quite a bit more security.

Run `Get-ExecutionPolicy`, if it returns `Restricted`, then run `Set-ExecutionPolicy ByPass -Scope Process`.
- choco** GitHub repository:
 - 4 branches
 - 42 tags
 - 440 commits
 - Issues (48)
 - Pulls (10)
 - Discussions (0)
 - Actions (0)
 - Projects (0)
 - Security (0)
 - Insights (0)

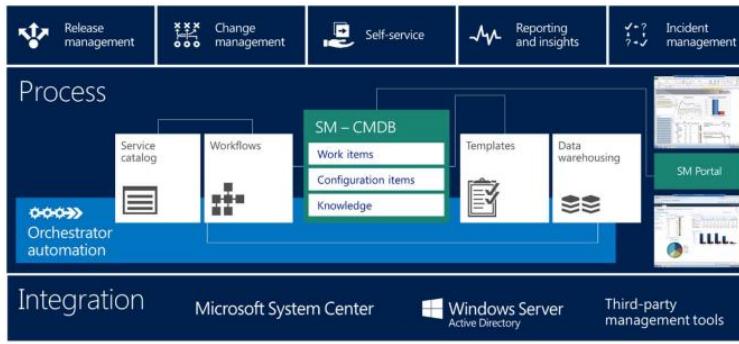
Recent commits:

 - gep13 (feat) Update to latest Chocolatey Cache Recipe [ci skip]
 - gratianWorkflow (fix) Fix unit tests only on push and PR
 - notifications (feat) Instant Remove Everyone from Discord notification
 - teamcity (fix) #2000 Adjust parameters on Docker builds
 - templates/default (feat) Spread local 'templates' with remote: https://github/GitHubActionsTemplates
 - srcode (feat) Add voice settings file
 - docker (feat) #1900 Use the Docker image as the base for the Windows image
- Chocolatey Software | Community**

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

Microsoft SCCM

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



- **System Center Operations Manager**

Monitor health, capacity, and usage across applications, workloads, and infrastructure.

- **System Center Orchestrator**

Automate your datacenter tasks; efficiently create and execute runbooks using native PowerShell scripts.

- **System Center Virtual Machine Manager**

Deploy and manage your virtualized, software-defined datacenter with a comprehensive solution for networking, storage, compute, and security.

- **System Center Service Manager**

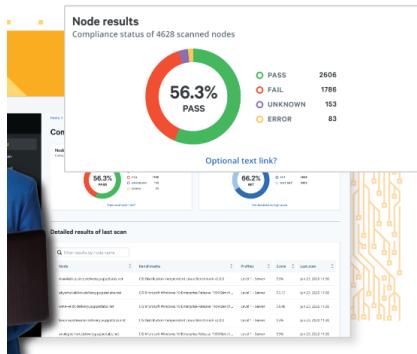
Automated service delivery tool for incident resolution, change control, and asset lifecycle management.

- **System Center Data Protection Manager**

Protect your data with backup, storage, and recovery for private cloud deployments, physical machines, clients, and server applications.

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

Outils d'automatisation, DEVOPS



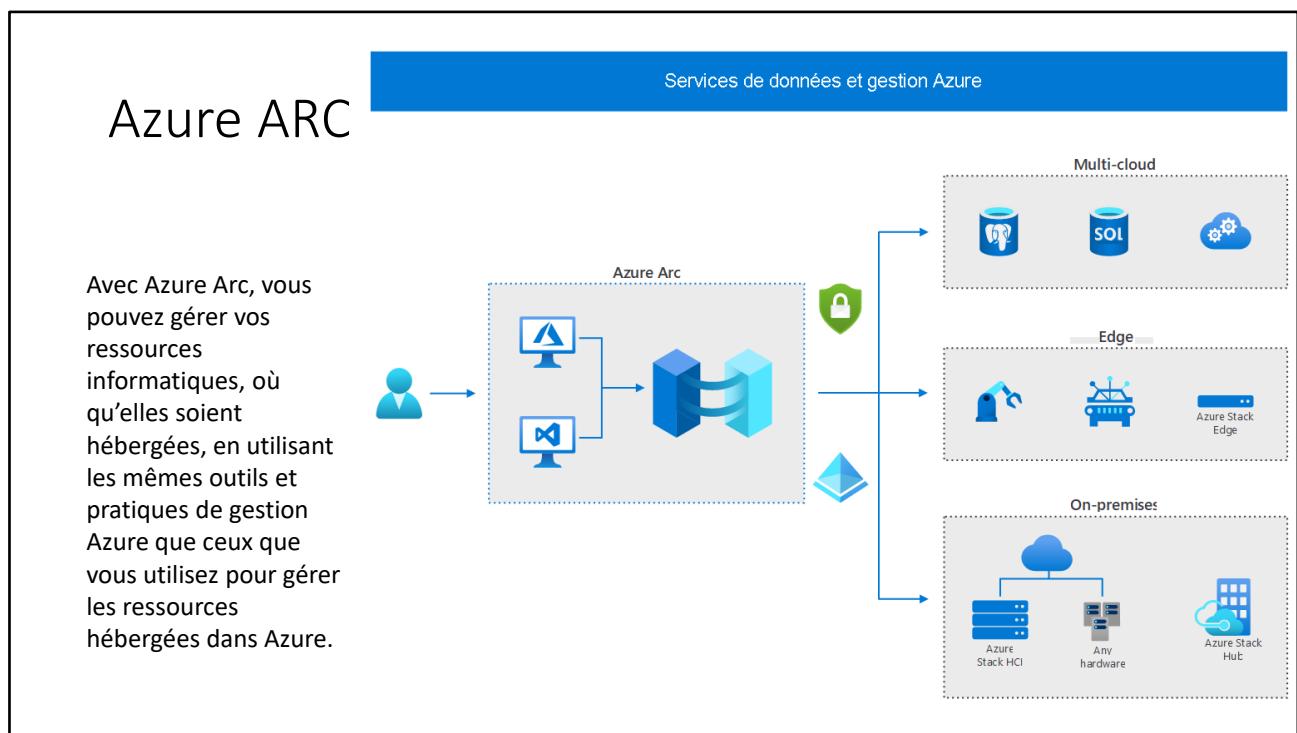
Why Puppet

Innovate through infrastructure automation.

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

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

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



[Décrire Azure Arc - Training | Microsoft Learn](#)

<https://learn.microsoft.com/fr-ch/training/modules/intro-to-azure-arc/2-describe-azure-arc>

PowerToys & Sysinternals



Microsoft PowerToys: Utilities to customize Windows

Article • 11/29/2022 • 5 minutes to read • 15 contributors [Feedback](#)

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

[Install PowerToys](#)

Article • 12/12/2022 • 2 minutes to read • 10 contributors [Feedback](#)

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

[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>