

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

<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>

Salut et bienvenue à l'ISEIG

Tour classe

- ? nom, prénom, surnom, pseudo de guerre, jeux vidéo, Discord, Github, passions, horreurs/peurs, rêves

Cadre de bienveillance

- JE pas TU (pas de jugement, nous sommes tous des croyants détenir le savoir), par contre «Tu» est OK.

Kotté tolèque

- 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)

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...

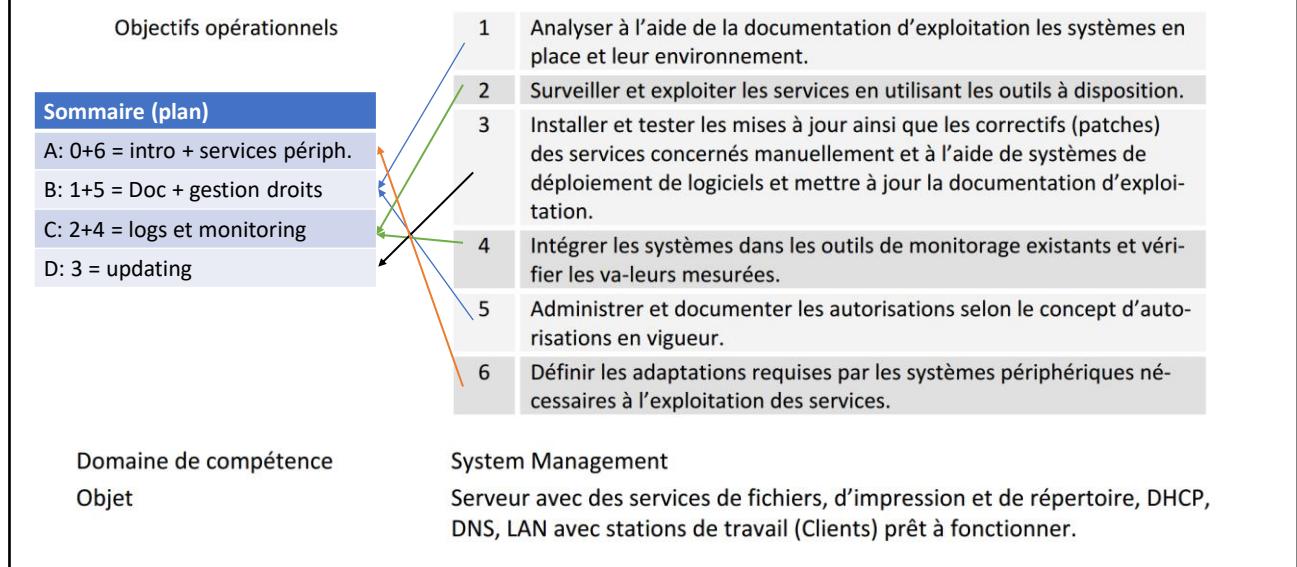
Or si l'attention en cours est réduite, et la moitié du temps utilisé à autres choses, et que du coup, les questions de compréhension ne sont pas posées à l'enseignant. Alors, bien que cette formation ne nécessite aucun travail «hors de la classe» si attentif, il risque d'être difficile et il sera tardif,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

<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



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

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.

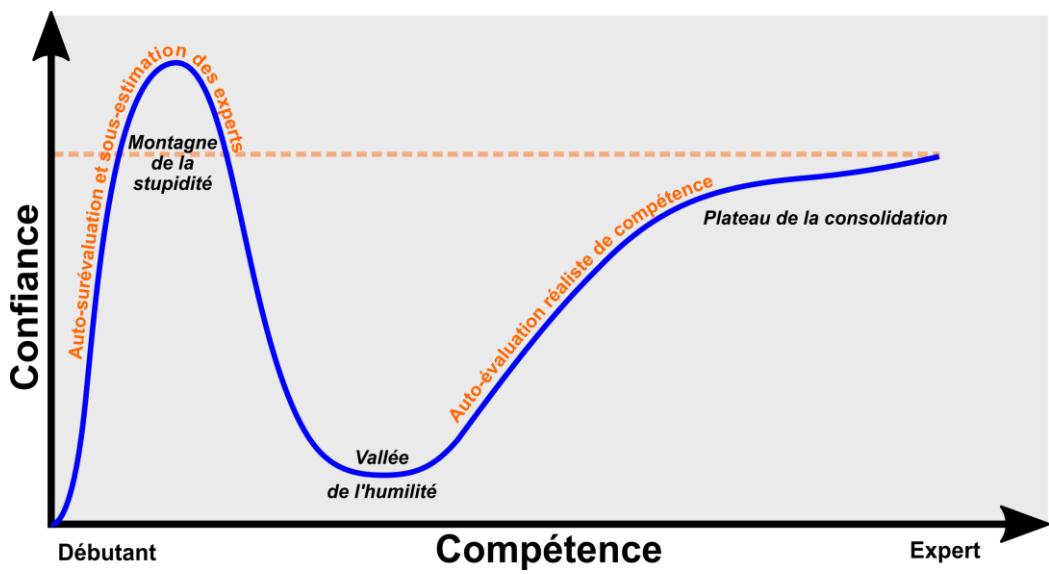
5.1 Connaître le contenu, la structure et l'application d'un concept d'autorisations. 5.2 Connaître les

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



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.

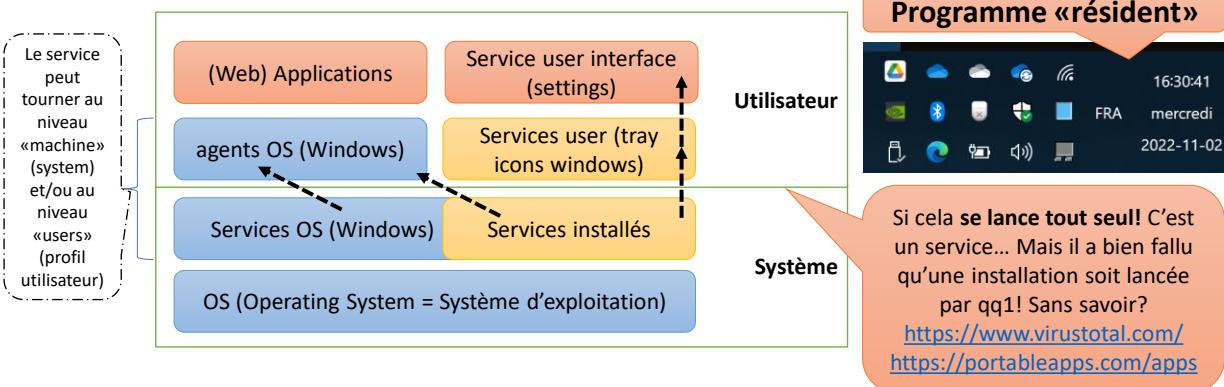
6.3 Connaître des possibilités pour tester les adaptations apportées aux systèmes périphériques.

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.

Beaucoup d'applications vont installer des « services » qui vont assurer des fonctions plus ou moins utiles, souvent leur 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.

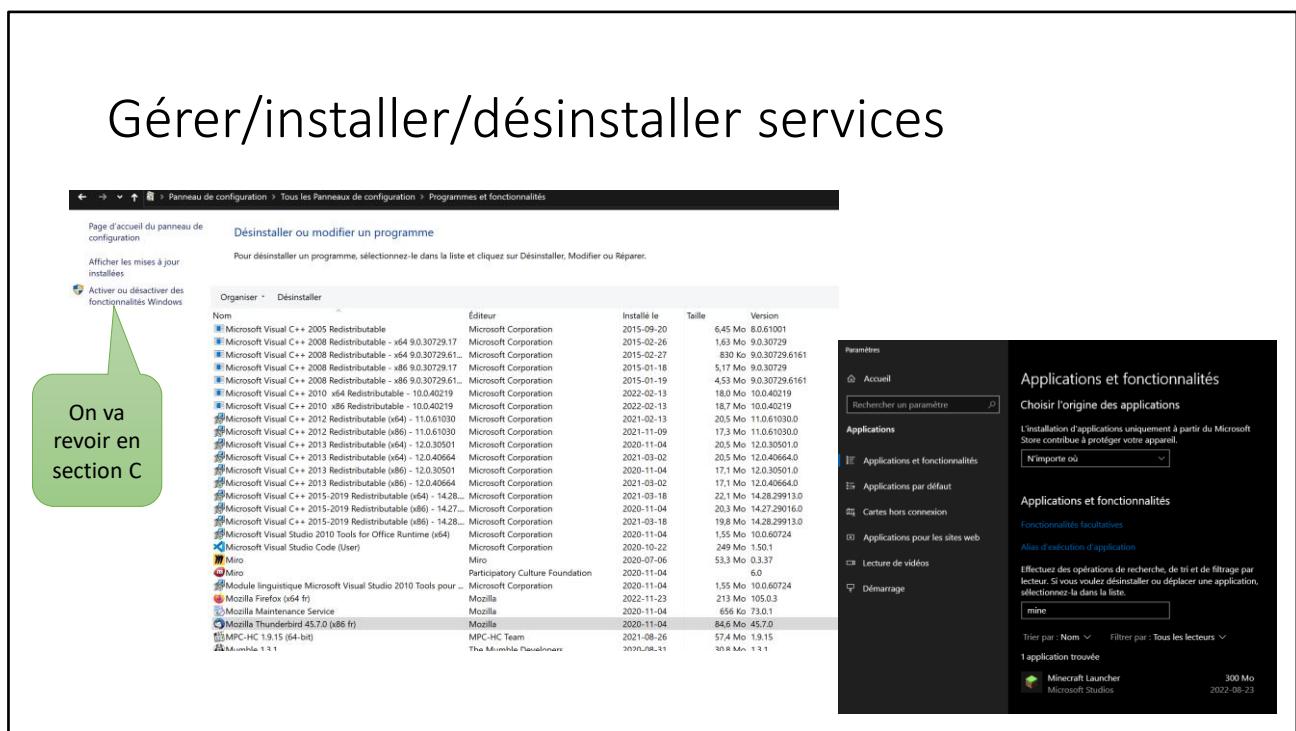
Désactivation au démarrage et nettoyage du PC:

- Piriform Ccleaner (mais gaffe avant de l'installer)

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

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

Gérer/installer/désinstaller services



On va revoir en section C

Panneau de configuration > Tous les Panneaux de configuration > Programmes et fonctionnalités

Désinstaller ou modifier un programme

Organiser : Désinstaller

Nom Editeur Installé le Taille Version

Nom	Editeur	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)	Miro	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	60,9 Ko	73,0,1
Mozilla Thunderbird 45,7,0 (x86 fr)	Mozilla	2020-09-04	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
MonoDevelop 1,2,1	The MonoDevelop Team	2020-08-21	29,9 Mo	1,2,1

Paramètres

Accueil

Rechercher un paramètre

Applications

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

Allez 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

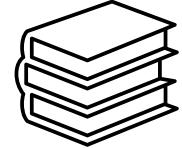
Minecraft Launcher Microsoft Studios 300 Mo 2022-08-23

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)

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

Les services «utilisateurs» et «infras»

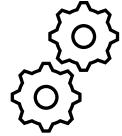


Le catalogue de services exposé aux usagers va intégrer les prestations assurées par leur département «IT» et leurs sous-traitants, ou fournisseurs: Ce sont les services finaux

- 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)
- ...



Le contenu des objectifs de cette formation, fait visiblement plus un focus sur les services infras.

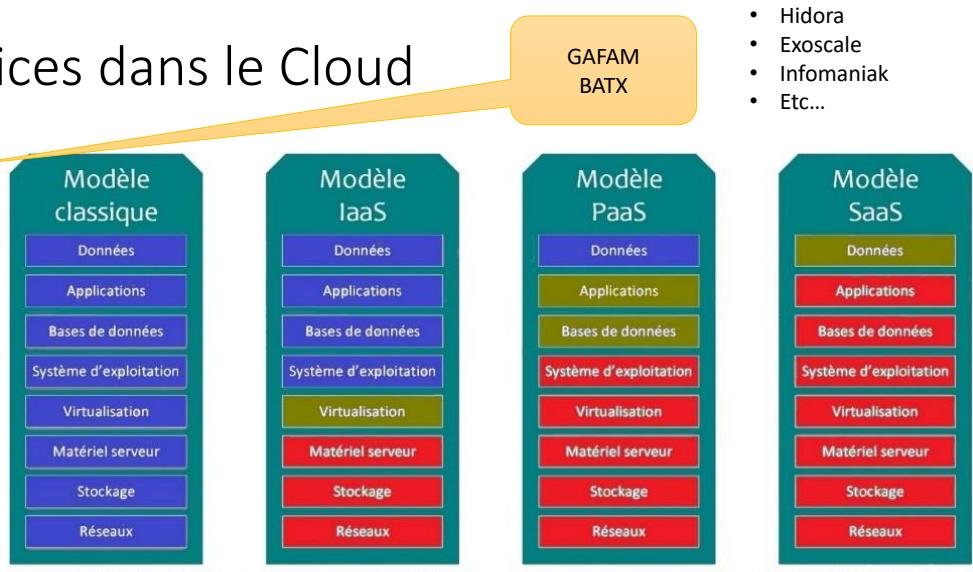
Les services dans le Cloud

- Hidora
- Exoscale
- Infomaniak
- Etc...

- Amazon
- Google
- Azure

3 Clouds

- IaaS
- PaaS
- SaaS



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

Pascal@rezolution.ch (CC-BY-SA 2016)

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

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

Option; Ethique numérique, durable et responsable?

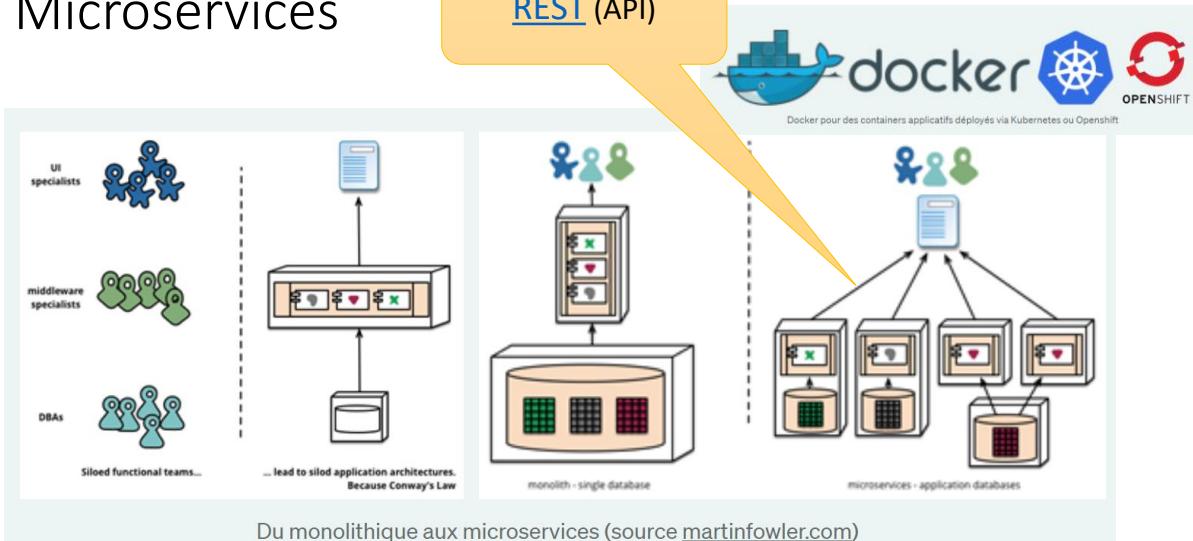
C'est quoi? Et comment on peut faire?

<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.

Microservices

REST (API)



<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/microservices-cest-quoi-f73d9ac48d94)

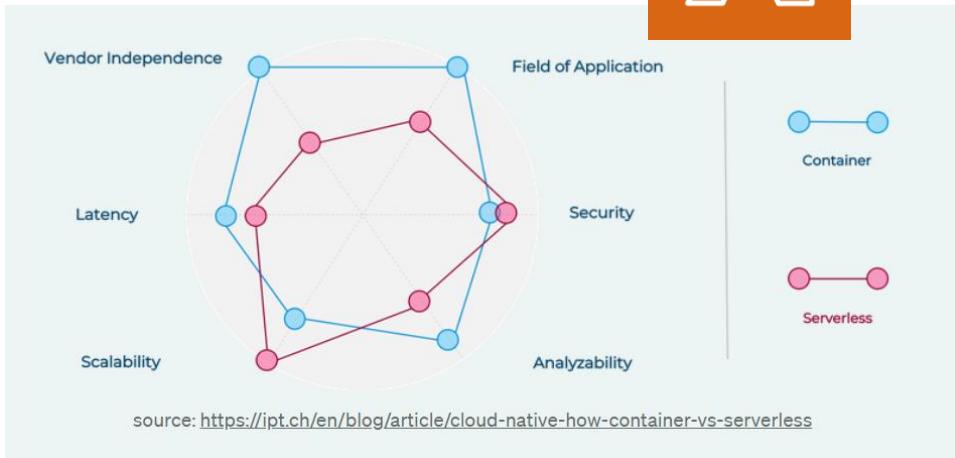
<https://medium.com/cloudready-ch/ipaas-cest-quoi-3f4b8ec84924>

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

DEVOPS to NoOPS

Google Cloud

Serverless computing



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

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>

Mais c'est aussi avec du Cloud que <https://www.missingmaps.org/> est possible

[Missing Maps](#)

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

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

<http://pascal.kotte.net>

<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

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...



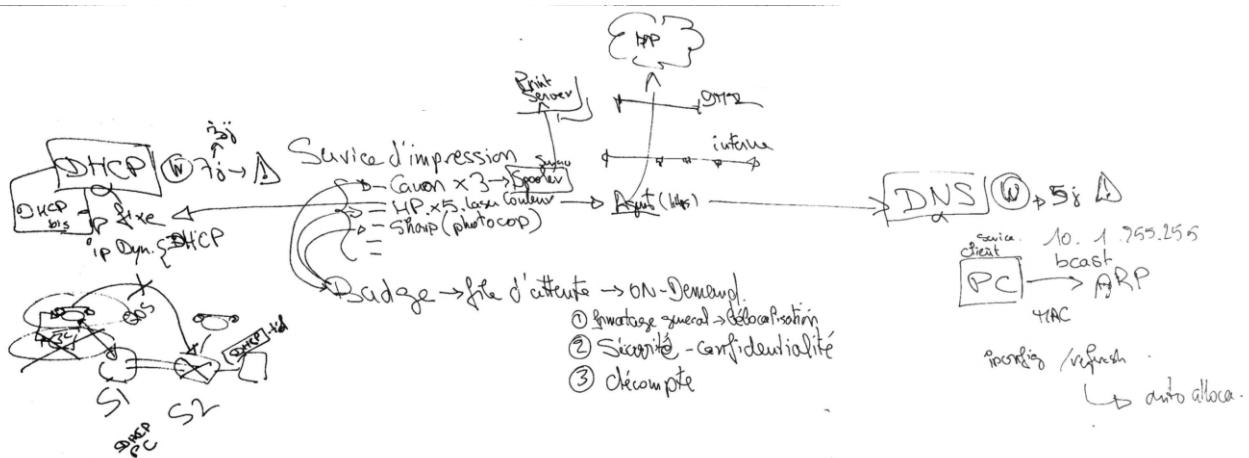
CF. <http://dns.quicklearn.ch>

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



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

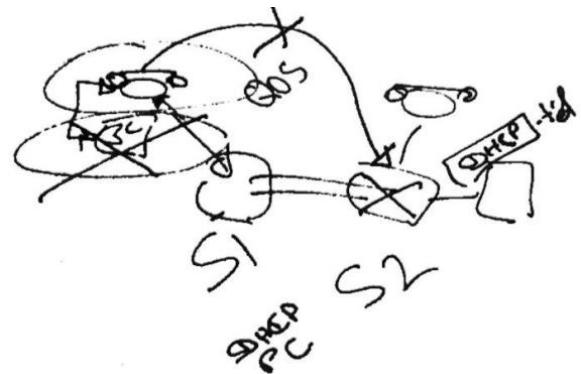
Souvent les badges nécessitent un serveur Radius:

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

Ou autre IAM serveur: (Identity and Access Management)

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.

Exemple de services

- AD + Azure Active Directory
- DNS ou Azure DNS
- DHCP (pourquoi pas dans Azure?)

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.



127.0.1.1 localhost
Cloudflare 1.1.1.1 Net.DNS
8.8.8.8 Google.DNS

<http://dns.quicklearn.ch>

Azure private DNS Zone



DHCP
DISCOVER



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

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

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

[Dynamic Host Configuration Protocol — Wikipedia](#)

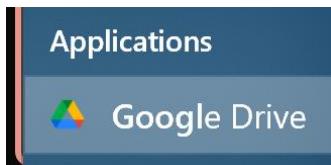
https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

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

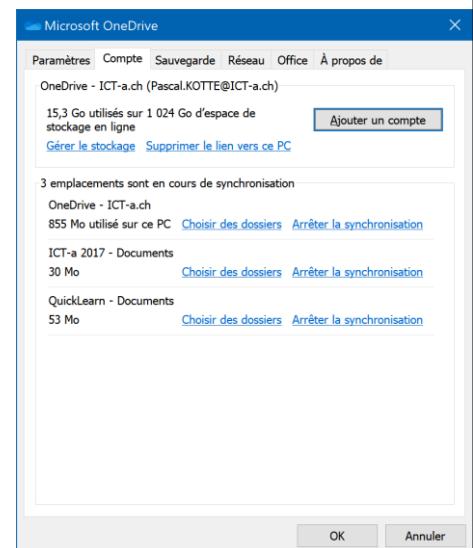
Exemple de service: OneDrive

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



Dropbox Dropbox, Inc.

Dropbox Update Dropbox, Inc.



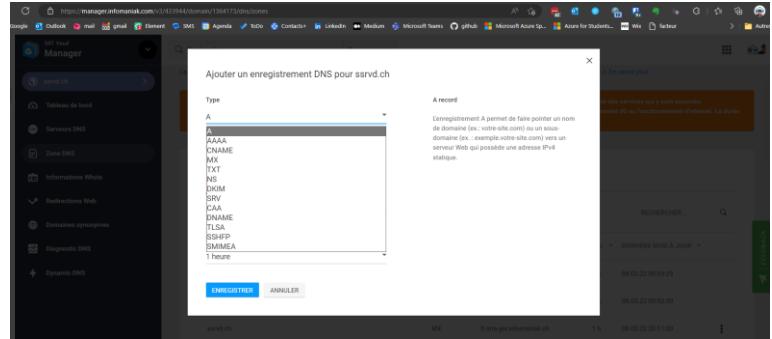
OK Annuler

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

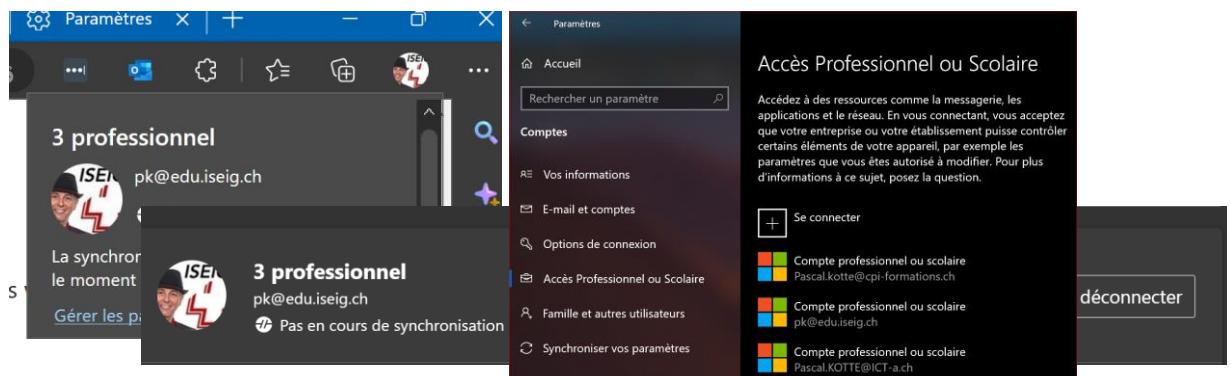
<http://dns.quicklearn.ch>



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

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»...



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

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

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/>

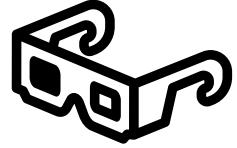
Autres exemples

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.

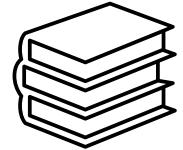
Les éléments de configurations principaux (primaires) = les attributs requis par les autres services.

- 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.

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

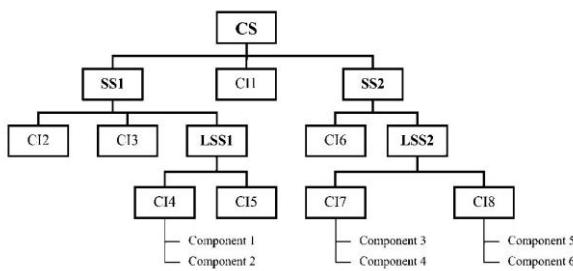
On a évoqué: GLPI, iTOP, ServiceNow, Zabbix, OTRS, SCCM... Cf aussi en annexe.
Mais on a une profusion de solutions...

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 qualificatif. 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

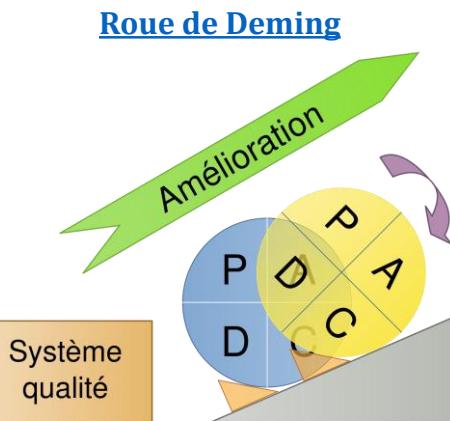
https://fr.wikipedia.org/wiki/ISO/CEI_27000

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 — Wikipédia \(wikipedia.org\)](#)

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.

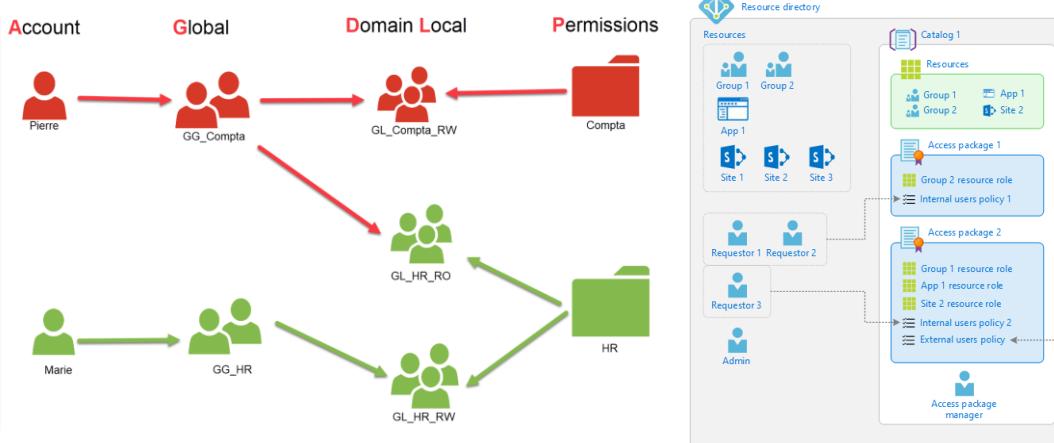
Le rôle de l'IT, sera de se donner les moyens:

- 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

AGDLP



Droits NTFS, et AGDLP...

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

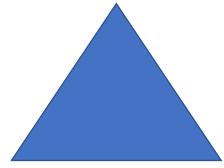
Ce qu'il faut retenir, c'est

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

Mode étendu et advanced:

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

Liste des Autorisations



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

Question:

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

La réponse est NON

Car même si les assignations dans une 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 \(github.com\)](#)

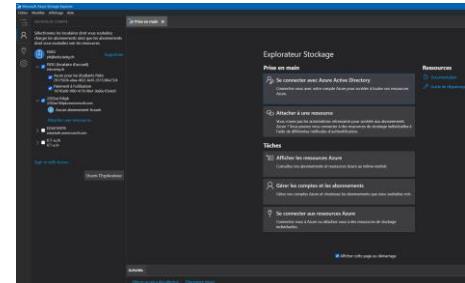
<https://azure.microsoft.com/en-us/features/storage-explorer/>

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

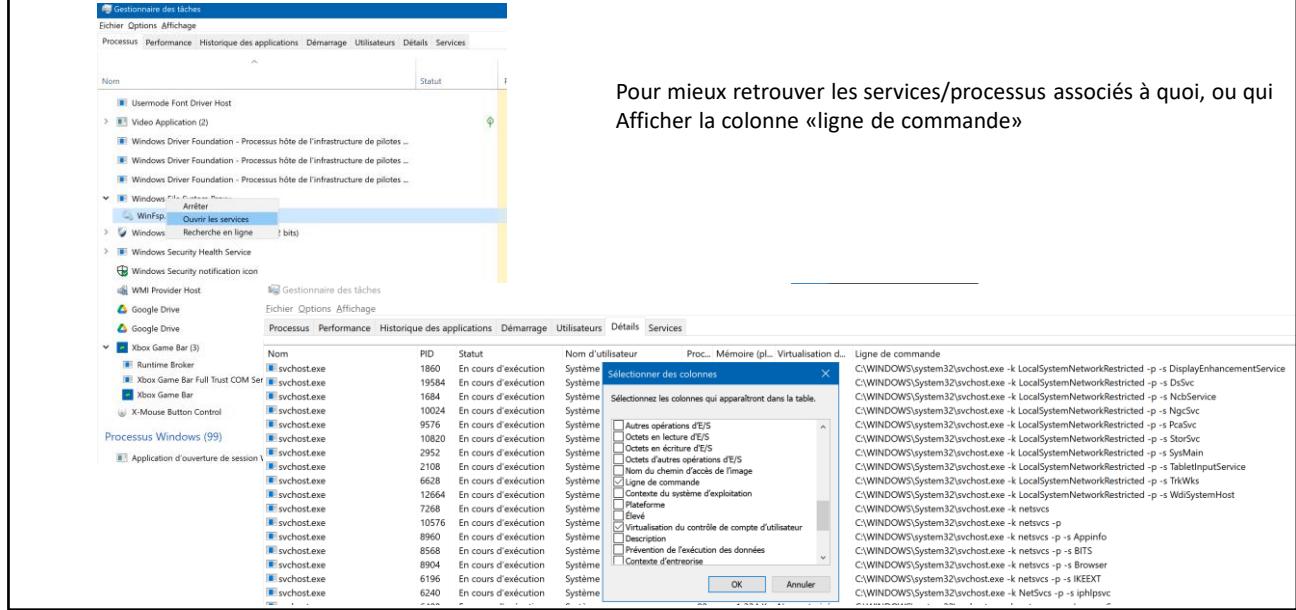
4.1 Connaître des techniques possibles (p. ex. SNMP, WMI) pour la saisie centralisée des données de performance et leurs mécanismes de sécurité.

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.

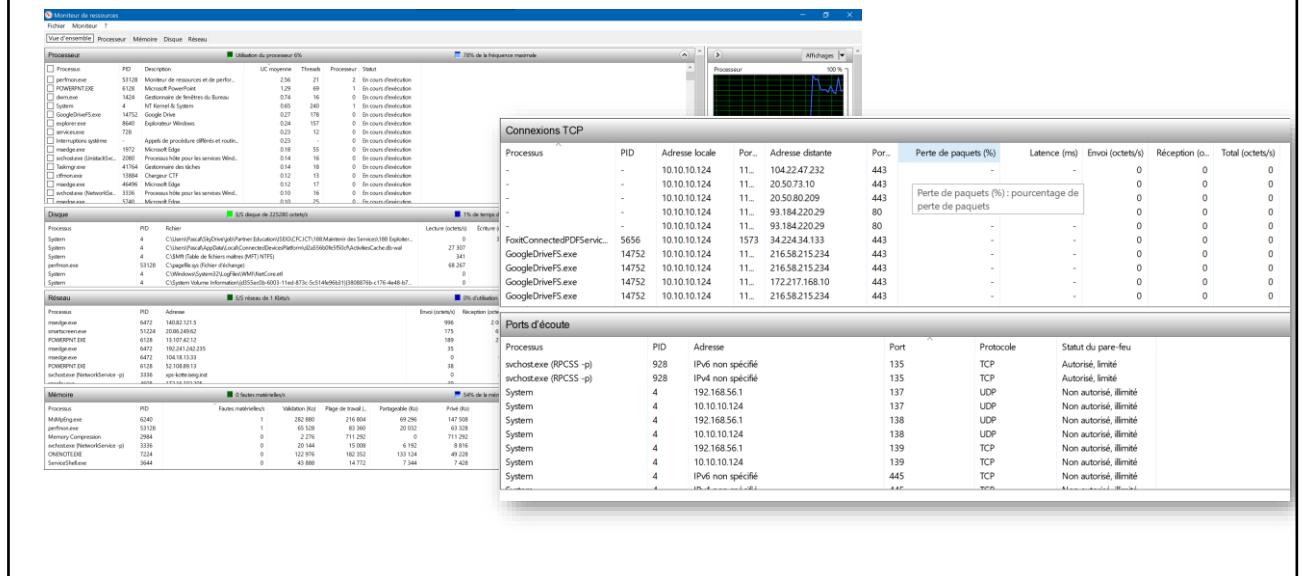
4.4 Connaître des possibilités pour définir des valeurs seuils judicieuses et installer une alarme.

Task manager (gestionnaire de tâches)



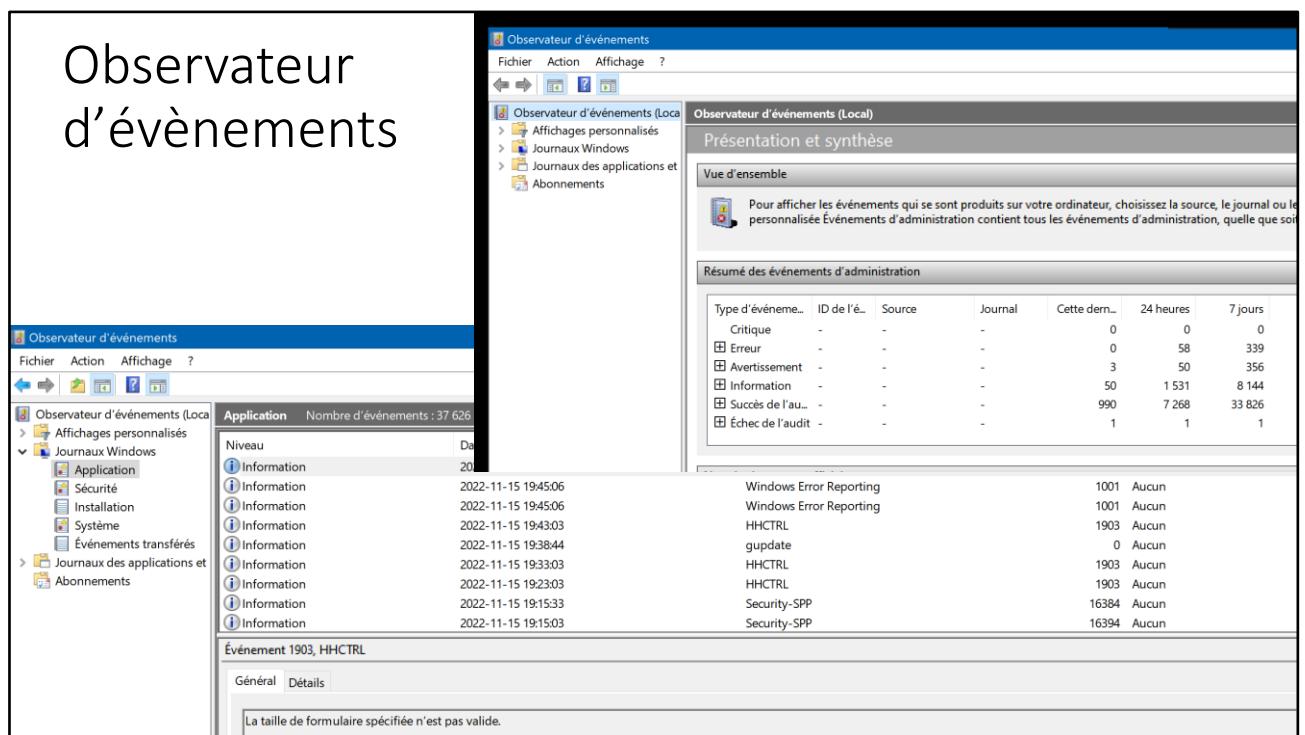
Ctrl-alt.-del > Task manager, ou clic droit sur la barre des tâches: Il permet «Gestionnaire de tâches»

Moniteur de ressources (perfmon)



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

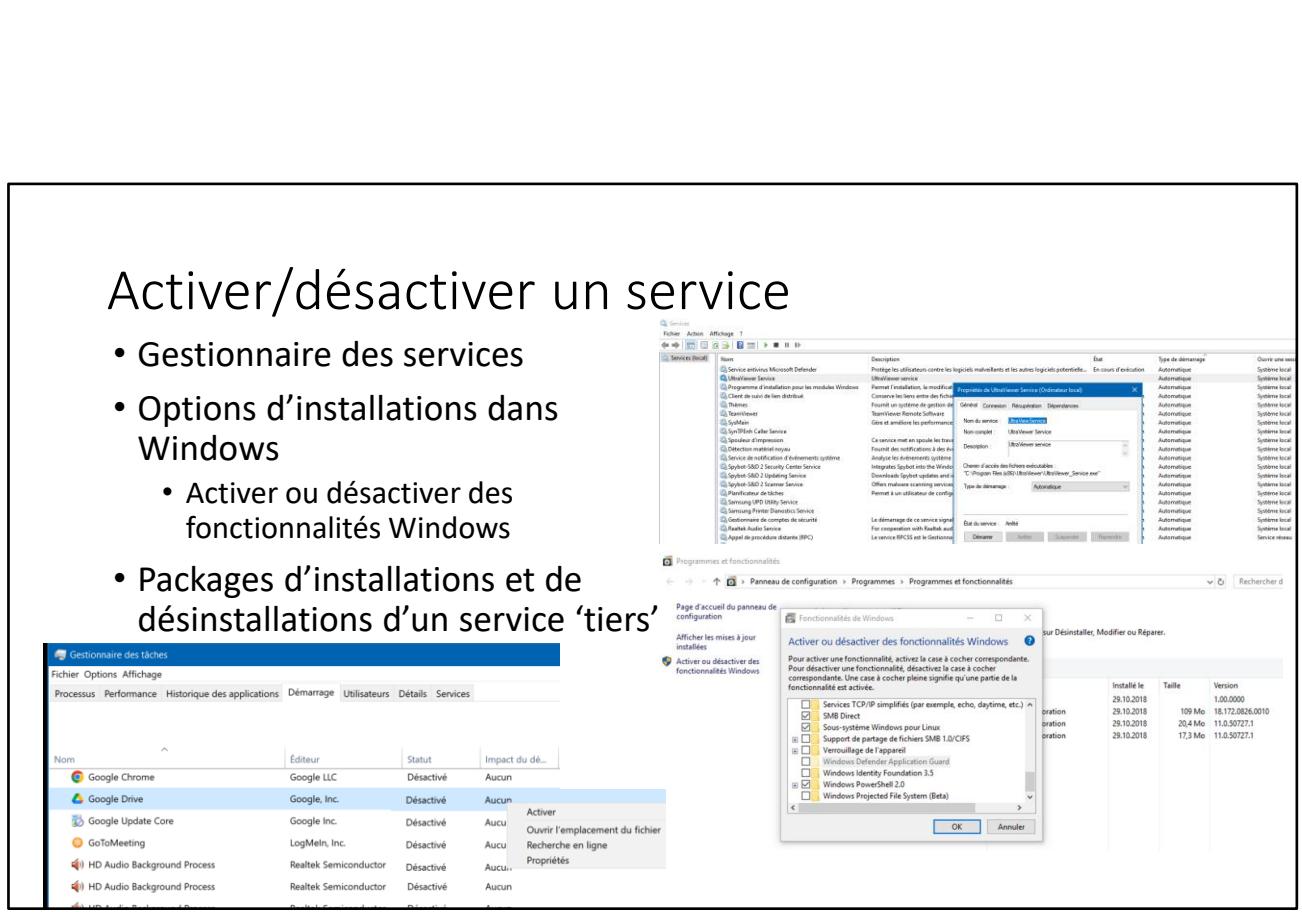
Observateur d'événements



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

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.

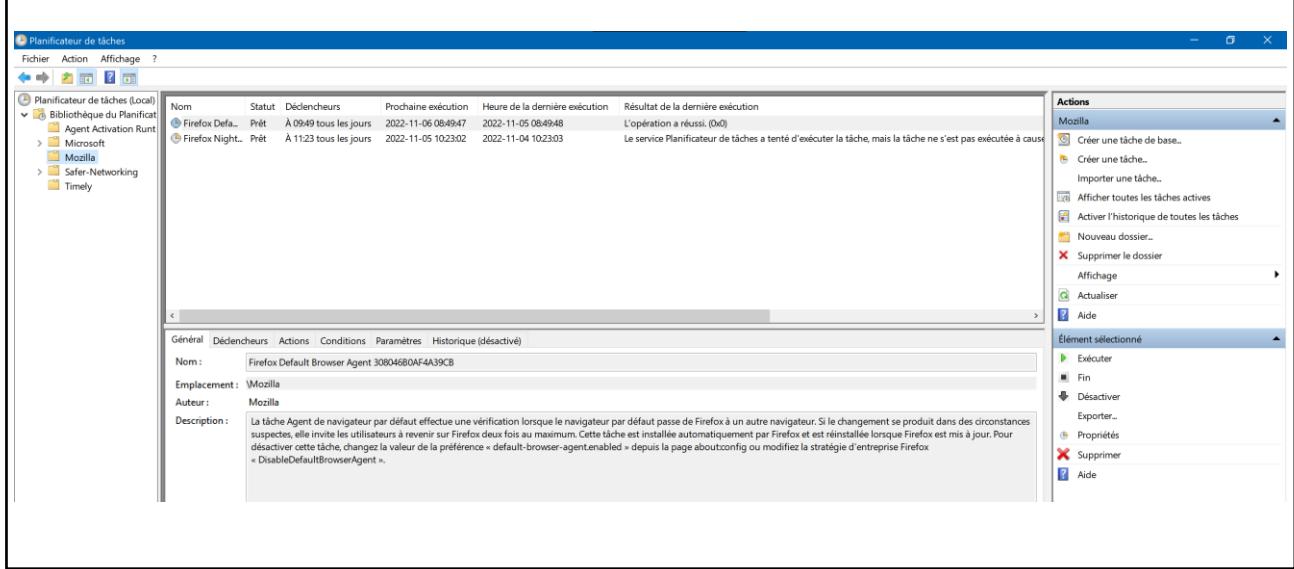
Mais tous les services ne tournent pas nécessairement dans l'onglet « Services » de Windows. Certains se présentent sous la forme d'applications « portables » lancée au démarrage automatiquement, sans même être visible dans la liste des applications installées.

<https://portableapps.com/>

Par exemple, un troyen...

Tâches planifiées, crontab sous Unix

Run Once
[Active Setup](#)



<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>

Outils de mesure des performances

Systèmes (windows)

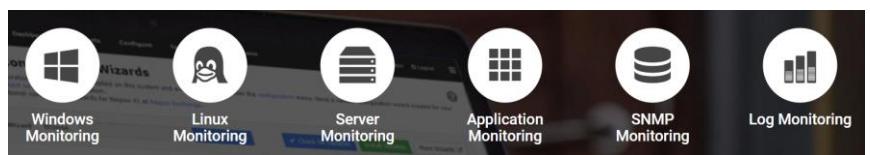
- Task manager
- Perfmon
- Analyseur de performances

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>

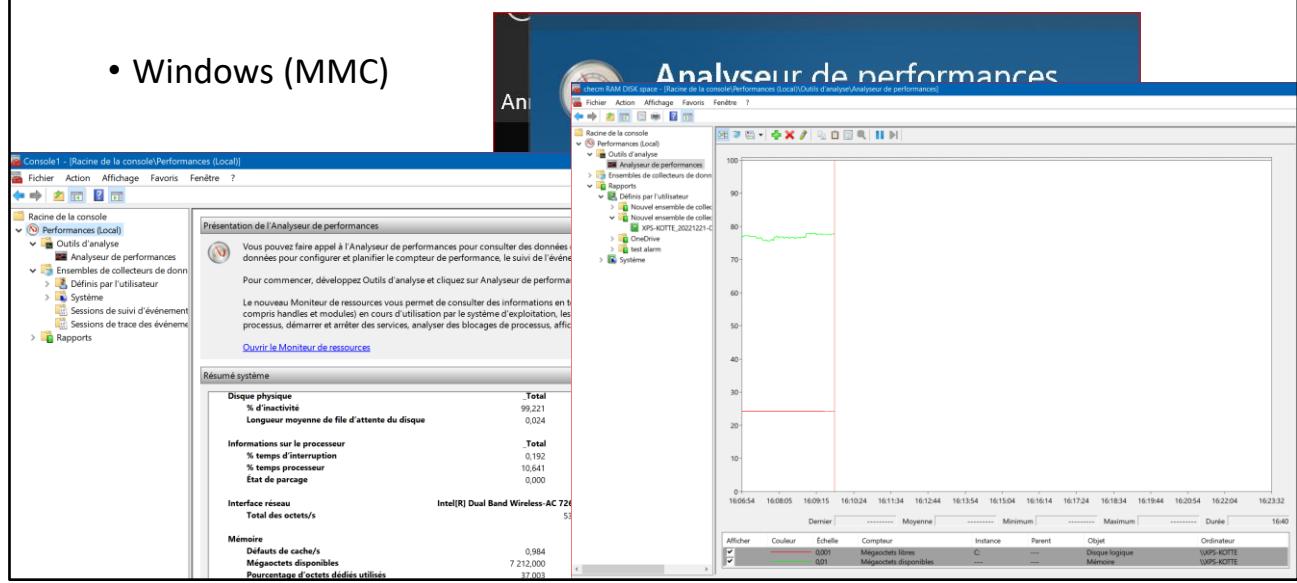
[https://fr.wikipedia.org/wiki/Supervision_\(informatique\)](https://fr.wikipedia.org/wiki/Supervision_(informatique))

<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)

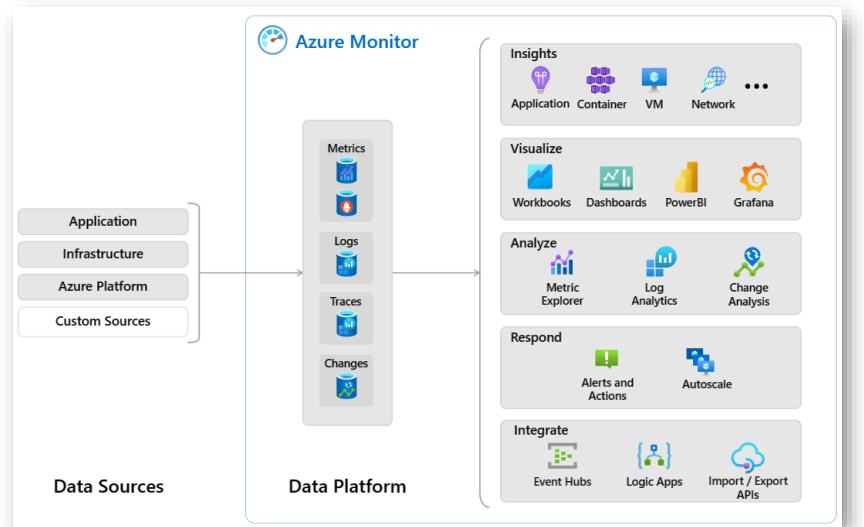


Analyseur de performances

- 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](#)

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

<https://www.myip.com/>

<https://fr.wikipedia.org/wiki/IPv6>

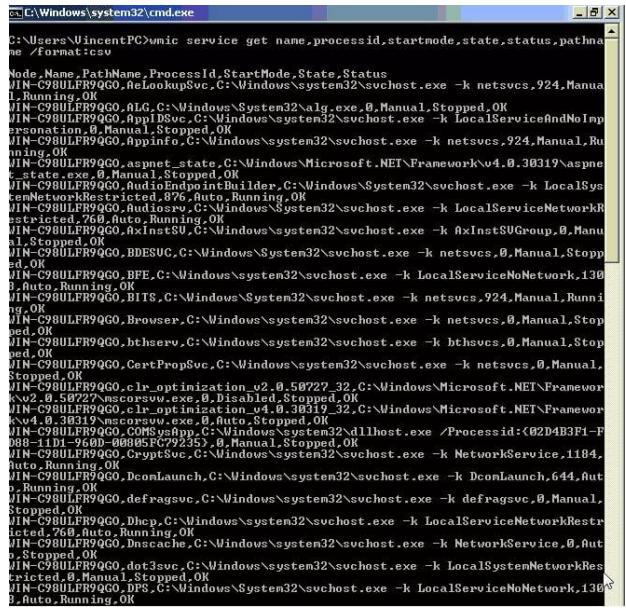
<http://www.ipv6-test.ch/>

WMIC & commandes Windows

SHARP
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
- Ipcfg (dhcpc actions)
 - Identification des DNS, DHCP, Routeur
- Nslookup (dns actions)
- Tracert (traceroute) lister les réseaux (hop)
- ...

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



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

<https://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/>

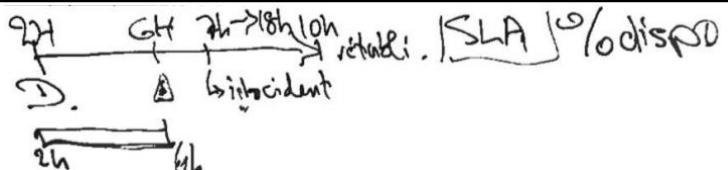
A noter que getmac ne permet que d'avoir les MAC locales à la machine (ipconfig /all le fait aussi bien)

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)

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 ont souvent recours 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 monter 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

The screenshot shows the Windows Task Manager interface. On the left, a list of processes is displayed with columns for Nom, Éditeur, Statut, and Impact du dé... . Processes listed include Microsoft SharePoint, Google Drive, X-Mouse Button Control, Windows Security notification icon, Microsoft To Do, Spotify, and Mobile connecté. On the right, system status information is shown: 'Dernier temps de démarrage du BIOS: 35.3 secondes', battery level (15:23:27), location (FRA), date (mercredi), and system date (2022-11-02). At the bottom left, system statistics show 'Durée de fonctionnement' as 0:06:43:31 and cache sizes: Cache de niveau 1: 256 Ko, Cache de niveau 2: 1,0 Mo, Cache de niveau 3: 6,0 Mo.

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

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

Dernier temps de démarrage du BIOS: 35.3 secondes

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

- Task manager, Performance – last reboot

Eventlog – exercice pratique

- Fournir la liste des reboot de la dernière semaine sur ce PC (ou le tien)

TK

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.

Que doit-on mettre à jour ?

- Les OS
 - Windows, légende urbaine: Linux, Mac pas besoin?
 - Android/iOS
- Les firmwares
 - Bios, mais aussi flashprom des appareils iOE/iOT (webcam,NAS...)
- Les Relais
 - Routeurs, Switchs (Flash)
- Les logiciels eux-mêmes

[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>

Pourquoi ?



- Pour des raisons de sécurité
- Pour corriger des bugs
- Pour ajouter des fonctions

Sauf que ce n'est plus des «updates»
dans ce cas, mais des UPGRADE...

Comme les services Packs.

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

- Certains updates spécifiques vont « nettoyer » un bonet existant
- Mais la plupart servent à éviter de conserver exposé une faille de sécurité
- Ou à stabiliser des dysfonctionnement...

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

Sous quelle forme se présente un update Windows?

- .cab
- .msu
- .msi
- .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 ? \(lojiciels.com\)](https://www.lojiciels.com/comment-installer-manuellement-un-fichier-CAB-dans-Windows-10-.html)

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

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, two command-line logs from the MSRT tool, and an "OK" button.

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

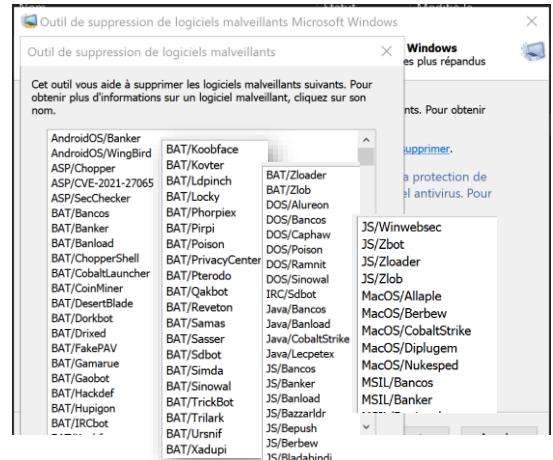
<https://support.microsoft.com/fr-fr/topic/supprimer-des-logiciels-malveillants-sp%C3%A9cifiques-et-r%C3%A9pandus-%C3%A0-l-aide-de-l-outil-de-suppression-de-logiciels-malveillants-windows-kb890830-ba51b71f-39cd-cdec-73eb-61979b0661e0>

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



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

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

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

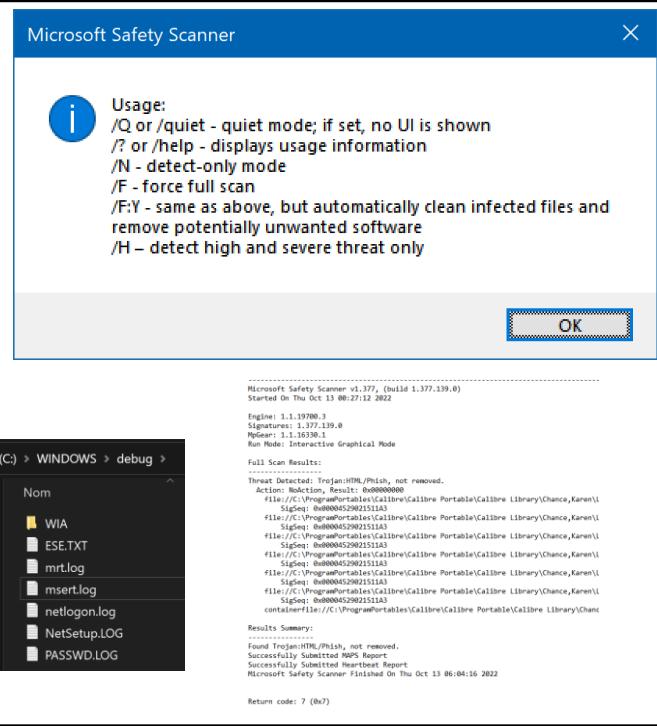
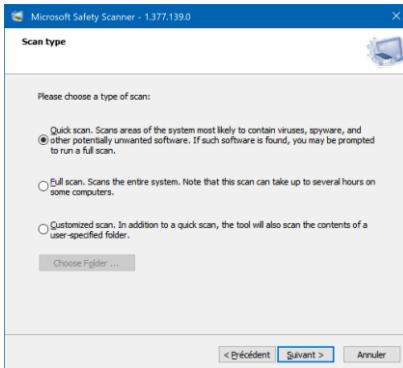
<https://support.microsoft.com/fr-fr/topic/comment-faire-pour-r%C3%A9soudre-une-erreur-lorsque-vous-ex%C3%A9cutez-le-scanner-de-s%C3%A9curit%C3%A9-microsoft-6cd5faa1-f7b4-afd2-85c7-9bed02860f1c>

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>

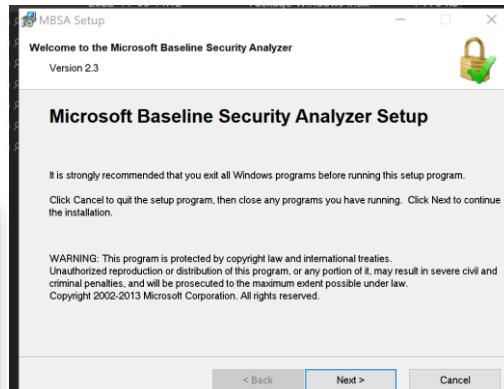
Scan vulnérabilité vs Removal!

- 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>

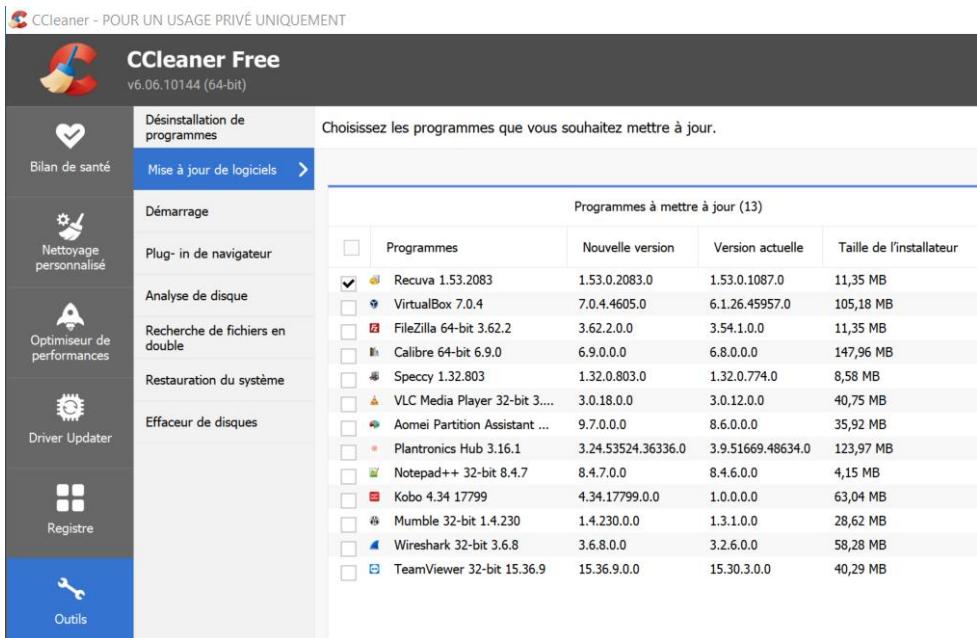
<https://learn.microsoft.com/en-us/windows/security/threat-protection/mbsa-removal-and-guidance>

<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/>

Mise à jour des logiciels



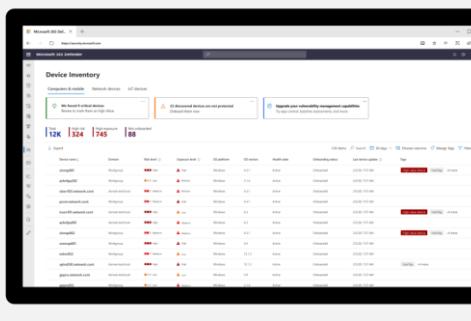
[10 Best Free Software Updater Programs \(December 2022\) \(lifewire.com\)](https://www.lifewire.com/free-software-updater-programs-2625200)

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

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...

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>

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.

Si cette fonction est activée, votre PC peut également envoyer des éléments de mises à jour et applications Windows précédemment téléchargées vers des PC sur votre réseau local ou sur Internet. Votre PC ne chargera pas de contenu vers les autres PC sur Internet lorsque votre connexion réseau est limitée.

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 ?

Options avancées

Options de mise à jour

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

Activé

Désactivé

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'appareil est allumé et branché.

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

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

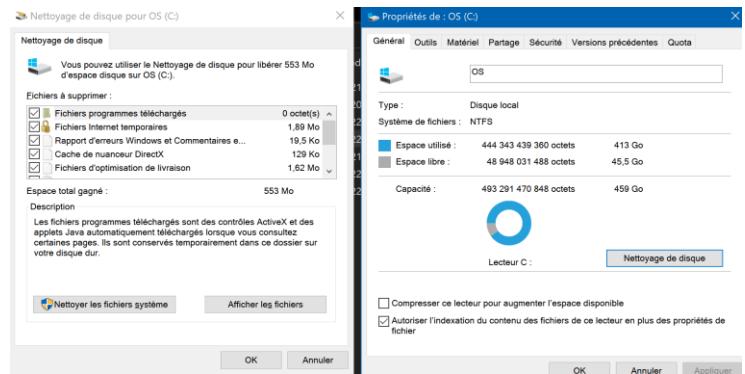
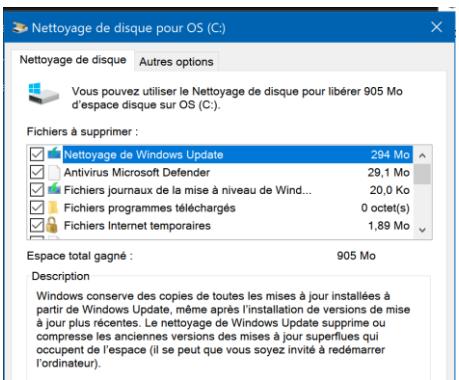
<https://www.microsoft.com/en-us/wdsi/defenderupdates>

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

Windows, comment on fait le ménage après?

- Cleanmgr (Windows)



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

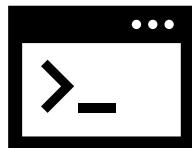
Cela fonctionne aussi sur des OS serveurs, sauf qu'il faut ajouter la fonctionnalité
[Windows Server 2008 nettoyage de disque - comment activer / installer / exécuter. \(hdd-tool.com\)](#)

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

<https://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>

Et pour les applications ?



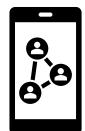
- Microsoft/Windows ne propose pas de solutions...
- Il est nécessaire de passer par les éditeurs de ces solutions
- Ou bien par des outils «partenaires», exemple: Ccleaner...
- Quelles sont les applications critiques ?
 - Les navigateurs web... (lecteurs html)
 - Les anti-virus (et de second passage...)
 - Les lecteurs PDF...
 - Les lecteurs JPEG...
 - Les pilotes (mais ceux-là sont normalement intégrés Windows update)
 - ...

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

<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>

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 fournit des services similaires pour les Macintosh

Des plateformes MDM (Mobile Device Management) permettent:

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

[Comment installer les mises à jour sous Linux ? \(lojicieux.com\)](#)

<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)

Equivalent du cleanmgr

```
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.
```

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

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

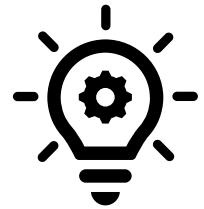
The screenshot shows a web browser window for OneDrive at the URL <https://onedrive.live.com/?v=restore>. The left sidebar has a 'Restaurer votre espace OneD...' option highlighted. The right panel is titled 'Restaurer votre OneDrive' and contains a note about restoring OneDrive space if problems occur. It features a dropdown menu labeled 'Sélectionnez une date' (Select a date) with options: 'Hier' (Yesterday), 'Il y a une semaine' (A week ago), 'Il y a trois semaines' (Three weeks ago), and 'Date et heure personnalisées' (Custom date and time). There is also a 'Tout rechercher' (Search everything) button.

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...

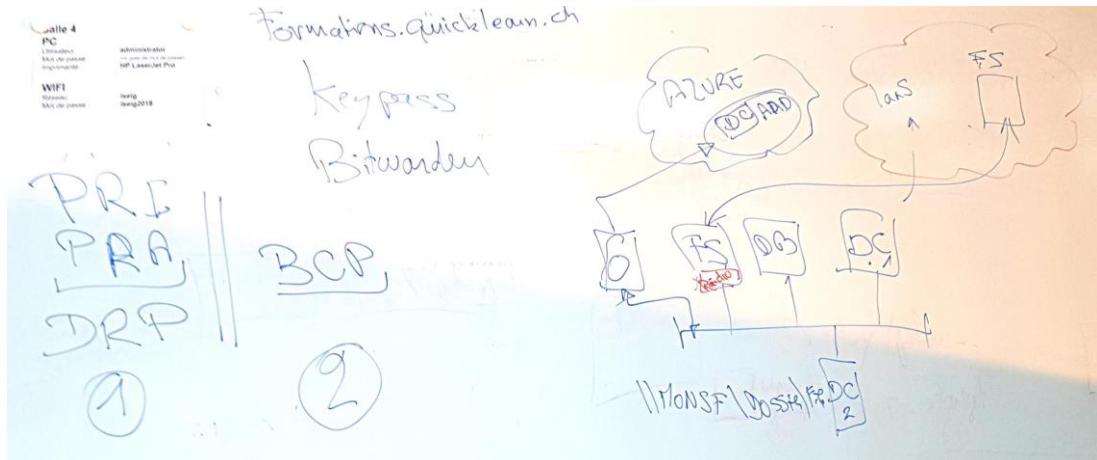
Déployer uniquement les éléments nécessaires

- 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

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.

The screenshot shows the VirusTotal analysis interface. At the top, there's a search bar and a file upload area. Below that is a summary card with a green icon, the file hash (5434771a59f77245ef517d94a74d7db1d98f7c81f5a2cafa1f1beaaf4e77), and the message "No security vendors and no sandboxes flagged this file as malicious". To the right, it shows the file size (108.90 MB) and last update (2022-11-05 08:50:08 UTC). A "Community Score" section follows. Below these are tabs for DETECTION, DETAILS, and COMMUNITY. The DETECTION tab is selected, showing a table titled "Security Vendors' Analysis". The table lists various antivirus engines and their detection status (Undetected or Green checkmark). The table includes columns for vendor name, detection status, and a third column that appears to be a status indicator.

Vendor	Detection	Status
Acronis (Static ML)	Undetected	Undetected
AI-Lab-V3	Undetected	Undetected
AIYac	Undetected	Undetected
Amavitz	Undetected	Undetected
AVG	Undetected	Undetected
Baidu	Undetected	Undetected
BitDefenderTheta	Undetected	Undetected
ClamAV	Undetected	Undetected
Comodo	Undetected	Undetected
Cynet	Undetected	Undetected
Emsisoft	Undetected	Undetected
Ad-Aware	Undetected	Undetected
Alibaba	Undetected	Undetected
Anti-VUL	Undetected	Undetected
Avast	Undetected	Undetected
Avira (no cloud)	Undetected	Undetected
BitDefender	Undetected	Undetected
Blar Pro	Undetected	Undetected
CMC	Undetected	Undetected
Cyberwason	Undetected	Undetected
D-Web	Undetected	Undetected
eScan	Undetected	Undetected

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



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

- L'ordinateur affecté est ouvert sur la session
 - Les supports et documentations de son choix peuvent y être téléchargée
 - Les sessions «connectées» sur autre chose que le compte @edu.iseig.ch doivent être fermées.
 - Office en ligne sera utilisé pour éditer le document posé sur le bureau.
- Préparer ses affaires comme pour partir
 - Pas droit à son ordinateur perso, ni son smartphone, docs papiers/crayons ok.
- Il n'est pas autorisé
 - De tenter de récupérer une copie du questionnaire à remplir, ni de le diffuser.
 - De «chater» avec un tiers via Internet, ni en présentiel. 1 seul à la fois aux toilettes
- A la fin du test, lever la main, laisser la session ouverte,
 - exporter le doc rempli au format PDF, et copie docx de secours: sur le bureau.

Directives: 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.

X. Annexes

Bonus

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 image shows two screenshots of web-based tools. On the left is the Fing.com interface, which displays network monitoring information for a local network. It shows 8 online devices, a speed test of 44.1 / 49.2 Mbps, and a security rating of 'Medium-Secure'. On the right is the VirusTotal interface, which allows users to upload files, URLs, or search for specific terms to analyze them against a community of security engines.

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

Plateformes ITSM (Entreprises)

IT Service Management

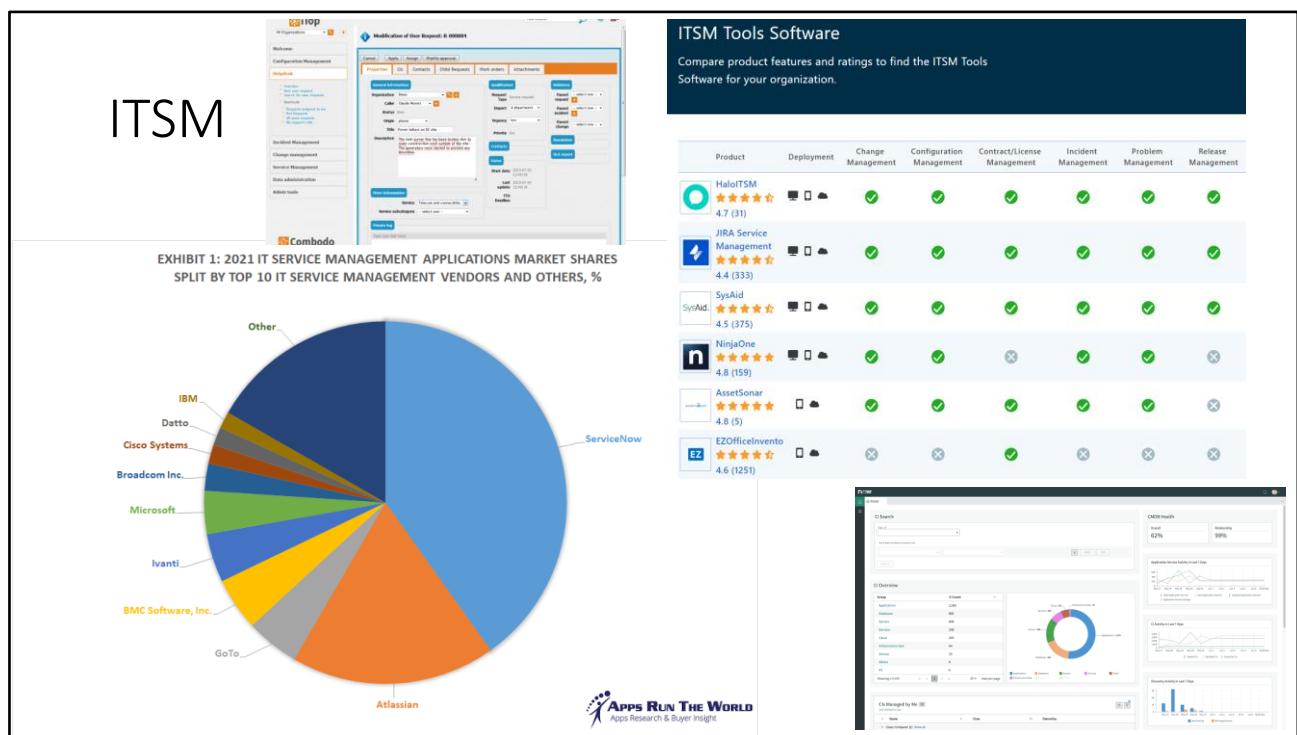
ManageEngine

- Endpoint Central
- Patch Manager

Edition Gratuite	Free Edition	Edition Professionnelle	Edition Entreprise	Edition UEM
Jusqu'à 20 ordinateurs et 5 serveurs	Convient aux PME		Fonctionnalités de l'édition Professionnelle +	Fonctionnalités de l'édition Entreprise +
Adaptée aux PME Entièrement fonctionnel Jusqu'à 20 ordinateurs et 5 serveurs	<ul style="list-style-type: none"> » Gérez jusqu'à 25 ordinateurs et 25 appareils mobiles » Gestion des Correctifs » Déploiement de Logiciels » Gestion des Assets » Configurations » Outils Système de Windows » Contrôle à Distance 	<ul style="list-style-type: none"> » Gestion des correctifs » Déploiement de Logiciels » Gestion des Ressources » Configurations » Outils Système de Windows » Contrôle à Distance » Rapports AD et de connexion des utilisateurs » Gestion des périphériques mobiles (Add-on) » Déploiement d'OS (Add-on) 	<ul style="list-style-type: none"> » Optimisation de la Bande Passante WAN » Portail Libre-service » Logiciels interdits / Blocage des EXE » Mesurage des Logiciels » Gestion des Licences » Enregistrement des Sessions à Distance » Gestion des Périphériques USB » Authentification à Deux Facteurs » Gestion des appareils mobiles (Add-on) » Déploiement d'OS (Add-on) 	<ul style="list-style-type: none"> » Gestion des Périphériques Mobiles » Gestion Moderne des Périphériques Windows 10 » Déploiement d'OS
		Convient aux ordinateurs en réseau local	Convient aux ordinateurs en WAN	
			Fonctionnalités de l'édition professionnelle + <ul style="list-style-type: none"> » Serveur de distribution pour l'optimisation de la bande passante » Mises à jour des définitions d'antivirus » Validation et approbation des correctifs » Authentification double facteurs 	

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

ITSM



<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>

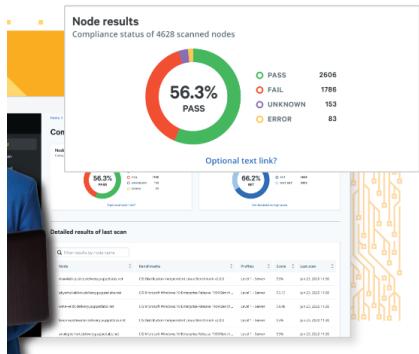
Microsoft SCCM

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



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

Outils d'automatisation, DEVOPS



Why Puppet

Innovate through infrastructure automation.

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

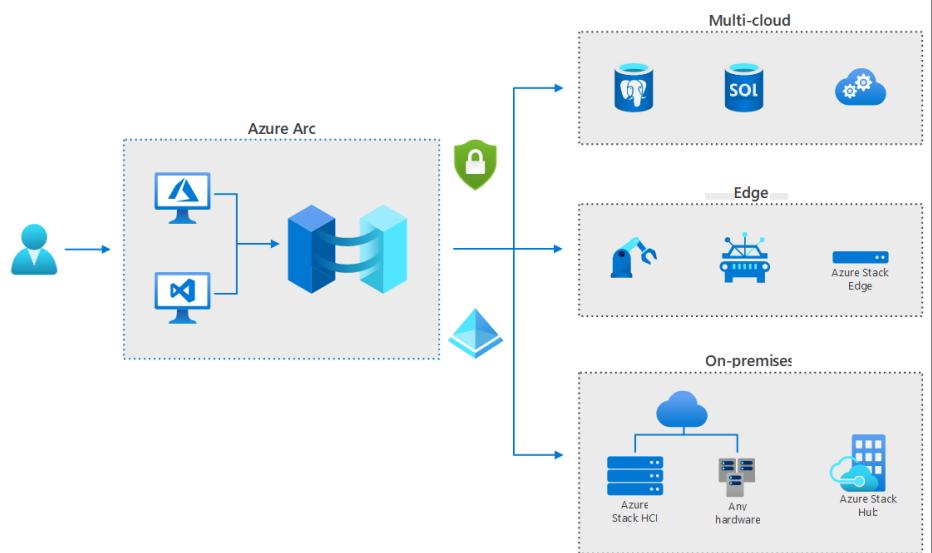
Dans l'univers Microsoft: Les Automatisations sont assurées généralement avec des Scripts en Powershell.

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

Azure ARC

Services de données et gestion Azure

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



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

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

PowerToys & Sysinternals



Sysinternals

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

[Feedback](#)

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

[Learn](#) / [Windows](#) / [Development environment](#) / [PowerToys](#) /

[+](#) [Edit](#) [⋮](#)

Microsoft PowerToys: Utilities to customize Windows

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

[Feedback](#)

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

[Install PowerToys](#)

[Microsoft PowerToys | Microsoft Learn](#)

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

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

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