

Exploiter, surveiller et assurer la maintenance des services

Module 188 (Swiss ICT, CFC informaticien)

PK@ISEIG.ch CC-BY-NC-SA

2022-10

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

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

Exploiter, surveiller et assurer la maintenance des services

Objectifs opérationnels

Sommaire

1+5 = Doc + gestion droits

2+4 = logs et monitoring

3 = updating

6...

0+6= intro

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

Domaine de compétence

Objet

System Management

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

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

Salut

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)
- [Kotté toltèque](#)
- Ce qui s'échange ici, ne sort pas d'ici...
- Pas d'insultes... (et le moins de gros mots possibles)
- Respect, de soi, des autres et sans oublier le prof.

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

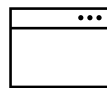
-Prendre des notes sur les points importants du cours, questions à poser ou valider.

-aller voir et compléter les infos présentées, essayer l'application exposée, et vérifier si on connaît effectivement le sujet, et 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 a 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 je suis attentif et que je clarifie au besoin, il risque d'être difficile et il sera tardif, au moment du test, de se dire «j'aurai peut-être dû faire plus attention».

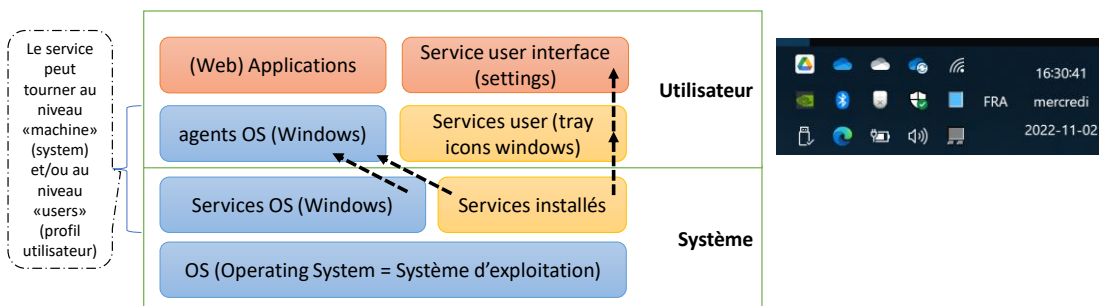
<https://medium.com/lean-design/le-5-%C3%A8me-accord-tolt%C3%A8que-a8fd2838f322>

C'est quoi un service (informatique/numérique)

Web service/serveur
Port ip Ecoute: 80/443

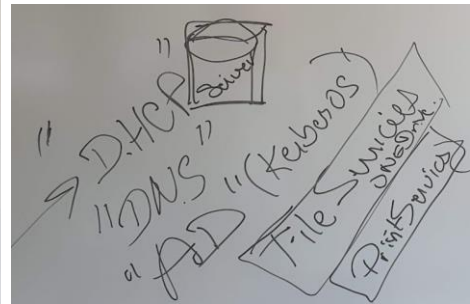
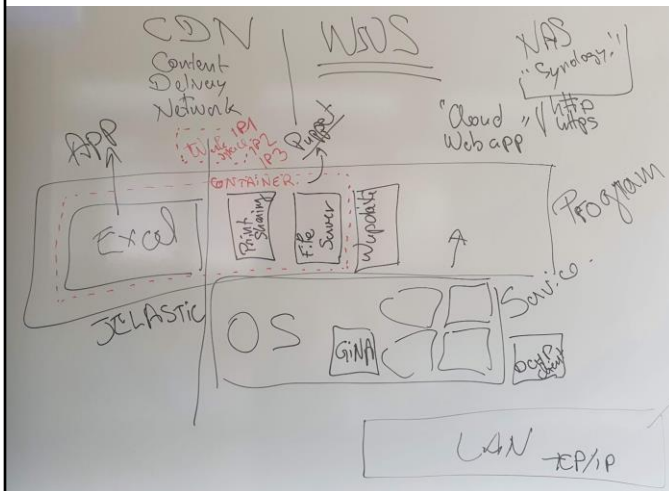


C'est un programme, qui n'est pas directement une application pour utilisateurs. Il peut tourner sur le poste de l'utilisateur, ou sur un autre appareil relié en réseau.



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

C'est quoi un service (informatique/numérique)



Un service est un ensem

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

Les services «utilisateurs» et «infras»

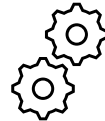


Le catalogue de services exposé aux usagers va intégrer les prestations assurées par leur département «IT» et leurs sous-traitants, ou fournisseurs: Ce sont les services finaux

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

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

- Fourniture d'une adresse IP (DHCP)
- Gestion des noms pour IP (DNS)
- identification et annuaire des utilisateurs (AD/DC)
- ...

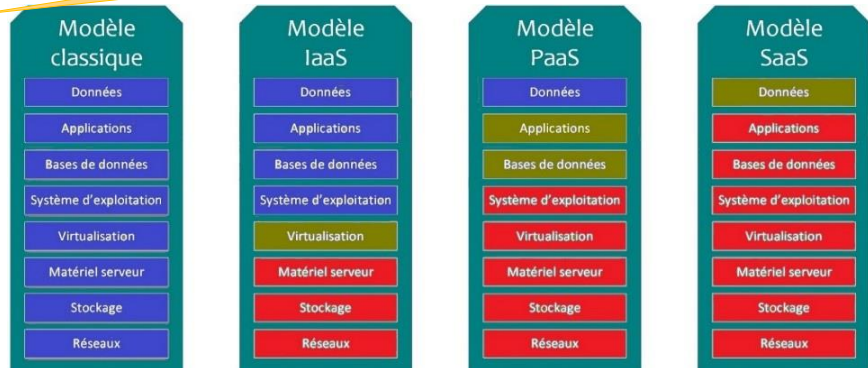


Les services dans le Cloud

GAFAM
BATX

- 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)

L'entreprise a le contrôle

Le fournisseur a le contrôle

<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>

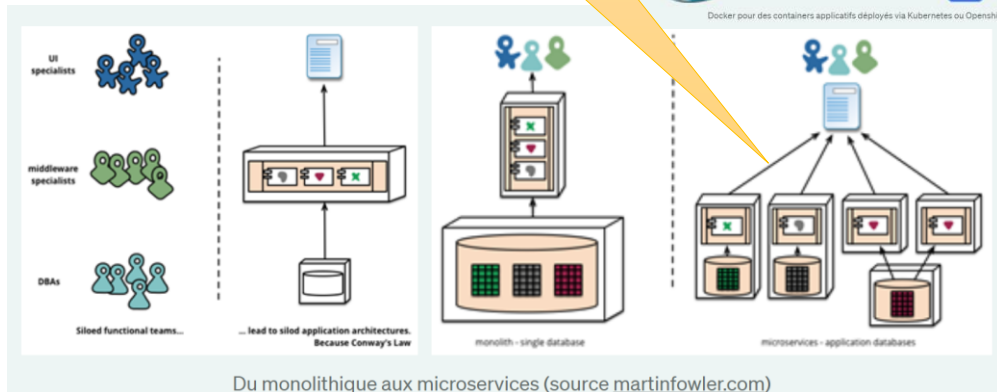
Option; **Ethique numérique, durable et responsable?**

C'est quoi? Et comment on peut faire?

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

Microservices

REST (API)



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

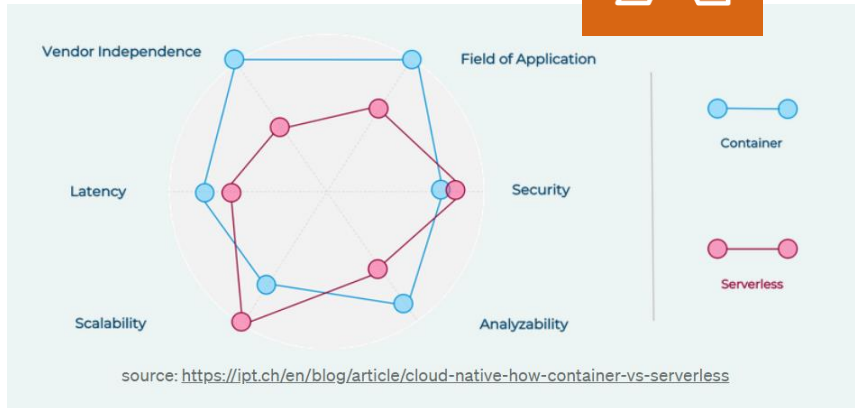
<https://medium.com/cloudready-ch/microservices-cest-quoi-f73d9ac48d94>

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>

SSII ou SS2I, vs ESN

- SSII – Sociétés de services et ingénierie en informatique
- => ESN (Entreprise de Services Numériques)

[Entreprise de services du numérique — Wikipédia \(wikipedia.org\)](https://fr.wikipedia.org/wiki/Entreprise_de_services_du_num%C3%A9rique)

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>

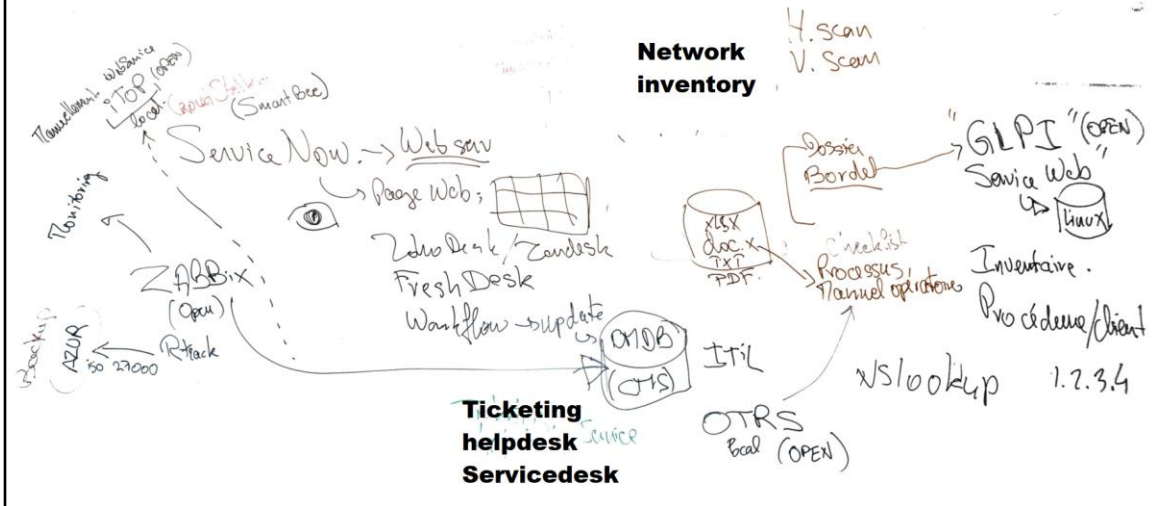
<https://www.capital.fr/votre-carriere/esn-entreprise-de-services-numeriques-definition-et-fonctionnement-1405805>

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

1. Documentation

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

Documentation d'exploitation



<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/>

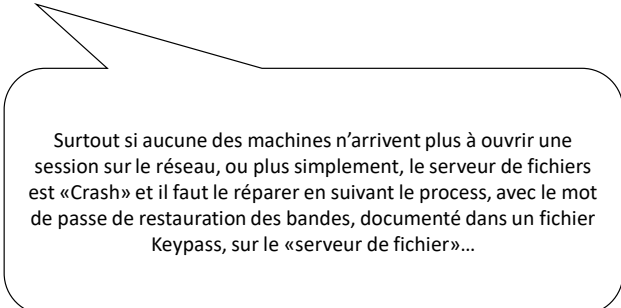
Autres exemples

Directement utiliser des modules de « Learning platform »

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

En cas de crash, la doc est où?

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



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, sur le «serveur de fichier»...

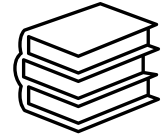
Les types de documentations

- 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
- Pour les intervenants externes des installations informatiques
- Pour les gestionnaires organisationnels des services numériques
 - A usage interne à l'entreprise
 - A usages avec prestataires

Les contenus

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

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?

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

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 (TK)

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

On a évoqué: GLPI, iTOP, ServiceNow, Zabbix, SCCM...

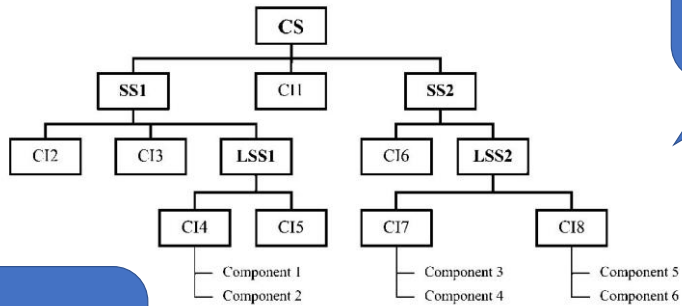
Mais on a une profusion de solutions...

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...

(ISO 10007)
ITIL (ISO 20000)
CDBB => CMS

COBIT (ISO9000)

ISO 27000 (39p)

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

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

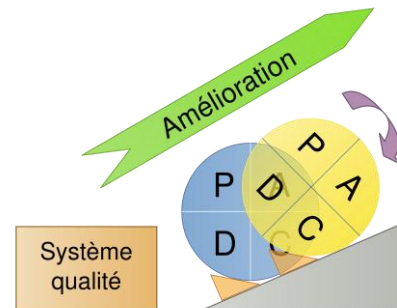
Organisation – ITIL - https://fr.wikipedia.org/wiki/ISO/CEI_20000

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

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

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...)*



[ITIL]
 'inadvis.' (H. Schme.)
 No. 1 755.255 1906
 STC
 , alloca.
 1/1000
 1/1000

- 20

Exemple de services, quelles docs?

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

127.0.1.1 local host
Cloudflare 1.1.1.1 Net.DNS
8.8.8.8 Google DNS

<http://dns.quicklearn.ch>

Azure private DNS Zone



DHCP
SERVER



Azure
Active Directory



<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/>

<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/>

1+(5). Administrer les droits d'accès

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

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.

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...

Liste des Autorisations

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

Question:

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

La réponse est NON

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

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

Et les mots de passe?

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

Gestion des comptes «machines»

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

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

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

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

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

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

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

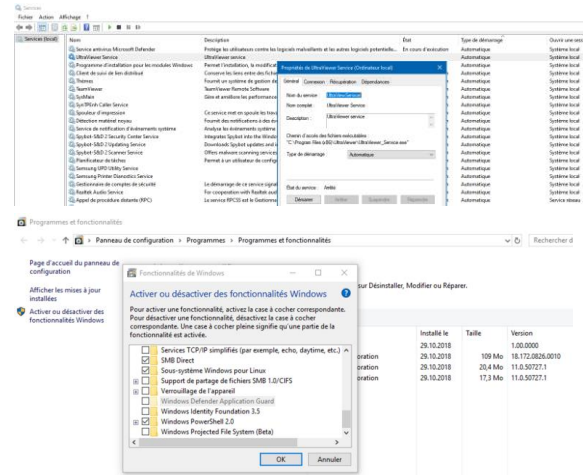
2+4. Monitoring, add counters

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

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

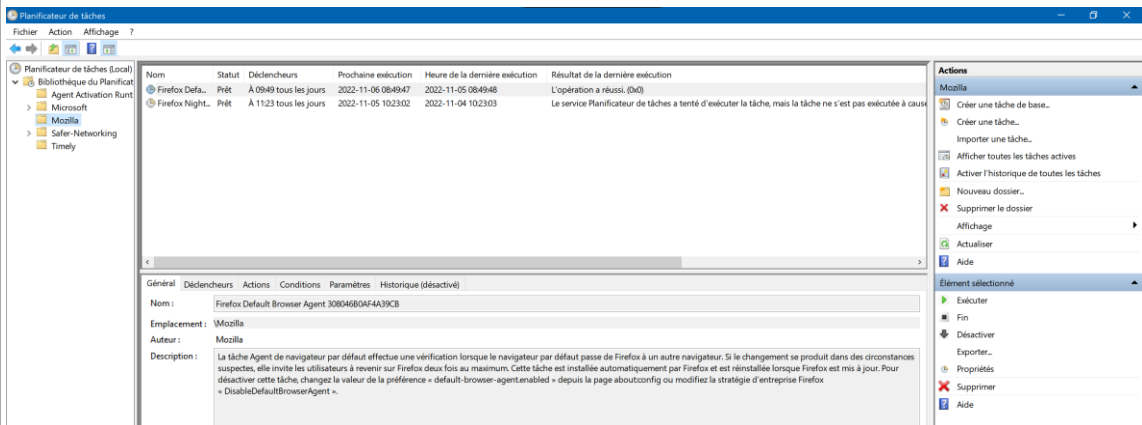
Activer/désactiver un service

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



C'est avec le gestionnaire des Services, que les services inutilisés sont désactivés, et

Tâches planifiées, crontab sous Unix



Outils de mesure des performances

Systèmes (windows)

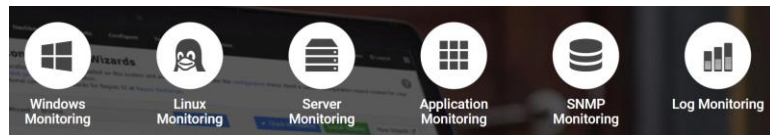
- Task manager
- Perfmon
- Analyseur de performances

Réseaux ([NMS](#))

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

Supervision

- Ex. Nagios
- Zabbix (Linux)



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

Standards réseaux, monitoring

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

Service

- [ARP](#) (identifier MAC adrs)
- DNS
- DHCP
- NAT et ip privées et ip publiques (ipv4)
 - <https://www.myip.com/>
- [ipv6](#)

Settings ▾ Discovery and Inventory ▾ SNMP Settings ▾ SNMP Device Classification

Snmp Device Classification
Classify devices by SNMP object ID

+ Add ✎ ✕ ?

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
1.3.6.1.4.1.1672	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	StoreEdge	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
1.3.6.1.4.1.6072.3.2.10	Linux			Computer

Done

Local intranet 100%

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

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

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

WMIC & commandes Windows

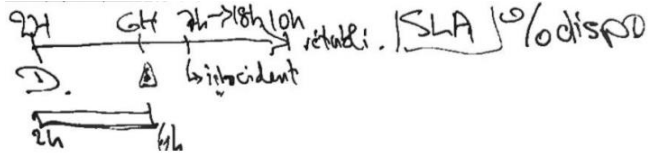
- [WMIC](#)
- Net
- Nbtstat (Netbios infos)
- Netstat -abn (IP infos)
- Arp
 - Gère les MAC adresses Ethernet
- Ping (utilise ICMP)
 - Souvent désactivé par sécurité
- Ipconfig (dhcp actions)
 - Identification des
- Nslookup (dns actions)
- Tracert (traceroute)
- ...

ping (ICMP) *Stop*
DDoS

```
C:\Windows\system32\cmd.exe
C:\Users\VincentPC>wmic service get name,processid,startmode,state,status,pathname /format:csv
Name,Name,PathName,ProcessId,StartMode,State,Status
WIN-C98ULFR9QG0,ALG,C:\Windows\System32\alg.exe,0,Manual,Stopped,OK
WIN-C98ULFR9QG0,AppIDSvc,C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation,0,Manual,Stopped,OK
WIN-C98ULFR9QG0,AppInfo,C:\Windows\system32\svchost.exe -k netsvcs,924,Manual,Running,OK
WIN-C98ULFR9QG0,aspnet_state,C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_state.exe,0,Manual,Stopped,OK
WIN-C98ULFR9QG0,AudioEndpointBuilder,C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted,876,Auto,Running,OK
WIN-C98ULFR9QG0,Audiosrv,C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted,768,Auto,Running,OK
WIN-C98ULFR9QG0,AxInstSV,C:\Windows\system32\svchost.exe -k AxInstSVGroup,0,Manual,Stopped,OK
WIN-C98ULFR9QG0,BDESVC,C:\Windows\System32\svchost.exe -k netsvcs,0,Manual,Stopped,OK
WIN-C98ULFR9QG0,BFE,C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork,130,Auto,Running,OK
WIN-C98ULFR9QG0,BITS,C:\Windows\System32\svchost.exe -k netsvcs,924,Manual,Running,OK
WIN-C98ULFR9QG0,Browser,C:\Windows\system32\svchost.exe -k netsvcs,0,Manual,Stopped,OK
WIN-C98ULFR9QG0,bthserv,C:\Windows\system32\svchost.exe -k bthservs,0,Manual,Stopped,OK
WIN-C98ULFR9QG0,CertPropSvc,C:\Windows\system32\svchost.exe -k netsvcs,0,Manual,Stopped,OK
WIN-C98ULFR9QG0,clr_optimization_v2.0.50727_32,C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.exe,0,Disabled,Stopped,OK
WIN-C98ULFR9QG0,clr_optimization_v4.0.30319_32,C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorlib.exe,0,Auto,Stopped,OK
WIN-C98ULFR9QG0,COSysApp,C:\Windows\system32\dlhhost.exe /ProcessId:{02D4B3F1-F600-11D1-9E00-00805F7923E},0,Manual,Stopped,OK
WIN-C98ULFR9QG0,CryptSvc,C:\Windows\system32\svchost.exe -k NetworkService,1184,Auto,Running,OK
WIN-C98ULFR9QG0,DeconLaunch,C:\Windows\system32\svchost.exe -k DeconLaunch,644,Auto,Running,OK
WIN-C98ULFR9QG0,defragsvc,C:\Windows\system32\svchost.exe -k defragsvc,0,Manual,Stopped,OK
WIN-C98ULFR9QG0,Dhcp,C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted,768,Auto,Running,OK
WIN-C98ULFR9QG0,Dnscache,C:\Windows\system32\svchost.exe -k NetworkService,0,Auto,Stopped,OK
WIN-C98ULFR9QG0,dot3svc,C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted,0,Manual,Stopped,OK
WIN-C98ULFR9QG0,DFS,C:\Windows\System32\svchost.exe -k LocalServiceNoNetwork,130,Auto,Running,OK
```

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

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 monitorer et alerter, pour réparer avant 7h!

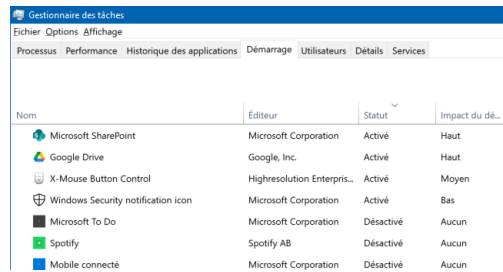
Le RTO (Recovery Time Objective) : il est important de déterminer en combien de temps un service dégradé et un retour à la normal seront effectifs.

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

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

Reboot time

- Task manager, démarrage – limiter au strict nécessaire



The screenshot shows the Windows Task Manager 'Démarrage' (Startup) tab. It lists several applications that start with Windows, including Microsoft SharePoint, Google Drive, X-Mouse Button Control, Windows Security notification icon, Microsoft To Do, Spotify, and Mobile connecté. Each entry shows the publisher, status (Active or Disabled), and impact on startup time (High, Medium, Low, or None).

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



- Task manager, Performance – last reboot

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

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.

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>

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

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

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».

Sous quelle forme se présente un update Windows?

- .cab
- .msu
- .msi
- .exe
- ...

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

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

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

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

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

Patch (EXE) de Windows

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

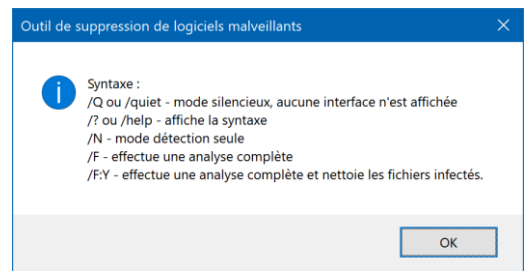
- [KB890830](#)

Un update qui va scanner les malwares identifiés via une application qui va faire un scan rapide: MSRT

Qui peut être utilisée manuellement pour approfondir. (Plusieurs heures, voir jours sur un file server)

Log: **%WINDIR%\debug folder**

Mrt.log



```
Microsoft Windows Malicious Software Removal Tool v5.96, (build 5.96.18853.1)
Started On Wed Dec 15 15:18:11 2021

Engine: 1.1.18700.4
Signatures: 1.353.1477.0
Hypervisor: 1.1.16130.1
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
Hypervisor: 1.1.16130.1
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/Zlob
MSIL/Zloader
PDF/Emotet
PowerShell/Banload
PowerShell/Bazarldr

PowerShell/Zloader
Python/Banker
Python/CVE-2021-16855
Python/CVE-2021-26855
Python/Exmann
Python/IRCBot
Script/CobaltStrike
Script/CVE-2021-26855

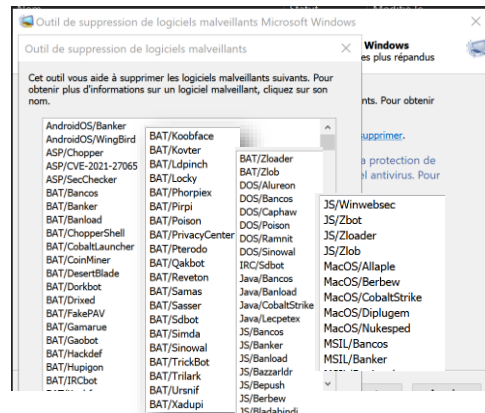
Script/Qakbot
SH/Nukesped
VBA/Emotet
VBA/Fareit
VBS/Bagle
VBS/Bancos
VBS/Banker
VBS/Banload
VBS/Bladabindi

VBS/Zlob
W97M/Emotet
W97M/Gamarue
W97M/Jenxus
W97M/Rovnix
W97M/Ursnif
W97M/Vavtrak
W97M/Zbot
Win32/Adposhel
Win32/Alcore

Win32/Zlob
Win32/Zonebac
Win32/Zuten
Win64/Alureon
Win64/AnchorBot
Win64/AnchorDNS
Win64/Badaxis

Win64/Winnit
Win64/Zbot
Win64/Zloader
WinNT/Alureon
WinNT/Bagle
WinNT/Bancos

WinNT/Zuten
X97M/Emotet
X97M/Qakbot
XML/CobaltStrike
XML/Emotet



<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>

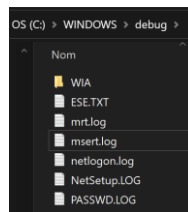
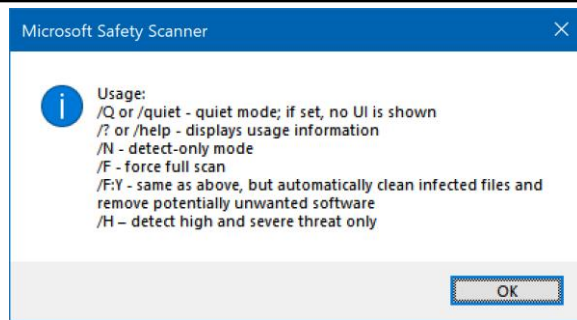
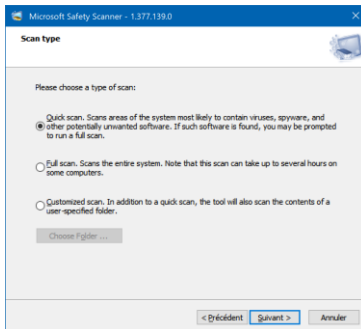
<https://support.microsoft.com/fr-fr/topic/comment-faire-pour-r%C3%A9soudre-une-erreur-lorsque-vous-ex%C3%A9cutez-le-scanner-de-s%C3%A9curit%C3%A9-microsoft-6cd5faa1-f7b4-afd2-85c7-9bed02860f1c>

MSERT

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

Un grand frère de MSRT...

- Log = msert.log



```
Microsoft Safety Scanner v1.377, (build 1.377.139.0)
Started On Thu Oct 13 00:27:12 2022

Engine: 1.1.19780.3
Signatures: 1.377.139.0
Metadata: 1.1.16330.1
Run Mode: Interactive Graphical Mode

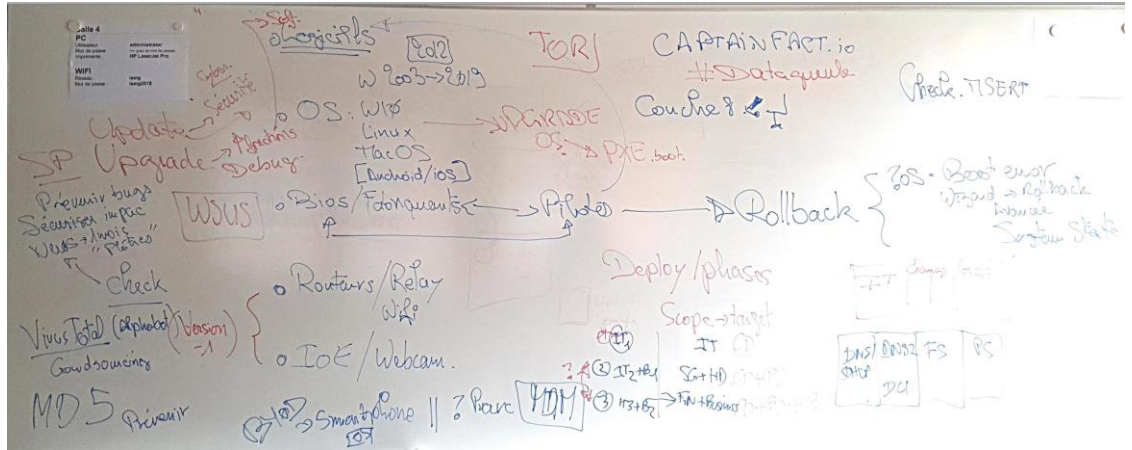
Full Scan Results:
-----
Threat Detected: Trojan:HTN/Phish, not removed.
Action: NoAction, Result: 0x00000000
File: //C:/ProgramData/Calibre Library/Chance/Karen/
Signature: R000045298215143
File: //C:/ProgramData/Calibre Library/Chance/Karen/
Signature: R000045298215143
File: //C:/ProgramData/Calibre Library/Chance/Karen/
Signature: R000045298215143
File: //C:/ProgramData/Calibre Library/Chance/Karen/
Signature: R000045298215143
File: //C:/ProgramData/Calibre Library/Chance/Karen/
Signature: R000045298215143
File: //C:/ProgramData/Calibre Library/Chance/Karen/
Signature: R000045298215143
ContainerFile: //C:/ProgramData/Calibre Library/Chance/Karen/

Results Summary:
-----
Found Trojan:HTN/Phish, not removed.
Successfully Submitted RPS Report
Successfully Submitted Infection Report
Microsoft Safety Scanner Finished On Thu Oct 13 00:04:16 2022

Return code: 7 (WU)
```

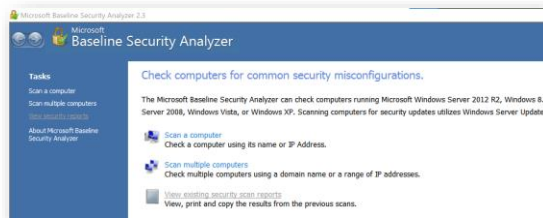
<https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/safety-scanner-download>

Les mises à jour

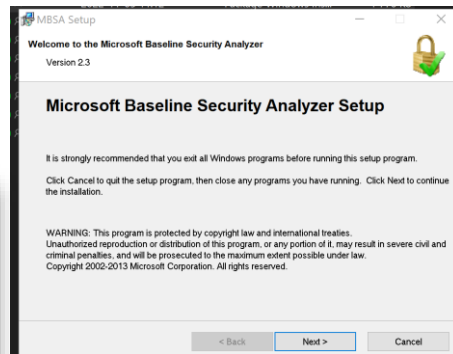


Scan vulnérabilité vs Removal!

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



[Microsoft Baseline Security Analyzer - Wikipedia](#)



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

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

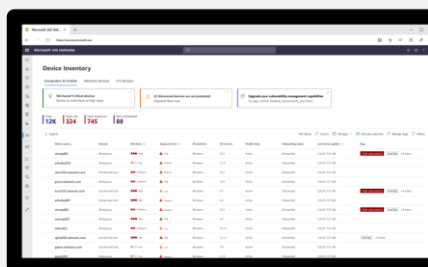
Evaluer les vulnérabilités

Comparez les offres en préversion



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.



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

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

https://learn.microsoft.com/en-us/windows/win32/wua_sdk/other-sources-of-windows-update-agent-information

Jusqu'en 2017...

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

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

Windows update

Wuauoserv

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

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

Optimisation de la distribution

Certains de ces paramètres sont masqués ou gérés par votre organisation.

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, autoriser 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 téléchargés 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

☒ Désactivé

☐ PC sur mon réseau local

☐ PC sur mon réseau local, et PC sur Internet

Paramètres

Accueil

Rechercher un paramètre

Mise à jour et sécurité

Windows Update

Optimisation de la distribution

Sécurité Windows

Sauvegarde

Résolution des problèmes

Recupération

Activation

Localiser mon appareil

Espace développeurs

Programme Windows Insider

Windows Update

Redémarrage nécessaire

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

2022-10 Aperçu de la mise à jour cumulative de .NET Framework 3.5, 4.8 et 4.8.1 Windows 10 Version 22H2 pour x64 (KB5018858)

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

Actuallement 07:00 à 01:00

☒ Afficher l'historique des mises à jour

Voit 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

☒ Actif

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

☐ Désactivé

Redémarrer cet appareil dès que possible lorsqu'un redémarrage est nécessaire pour installer une mise à jour

☐ Désactivé

Notifications de mise à jour

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

☒ Actif

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

Obtenez 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](#)

Windows Update

Votre appareil va redémarrer pour être mis à jour en dehors des heures d'activité

Laissez-le allumé et branché. Ouvrez Paramètres pour afficher vos heures d'activité et si vous voulez des rapports.

[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

Spécifique pour antivirus Windows

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

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

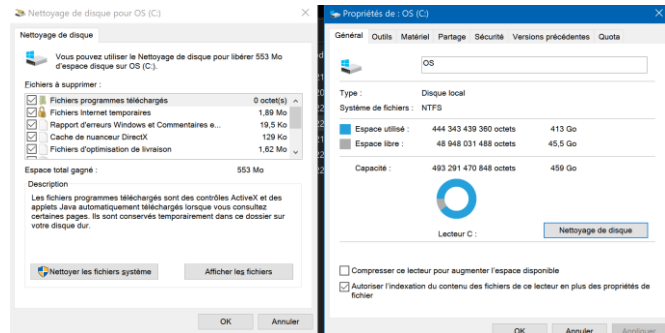
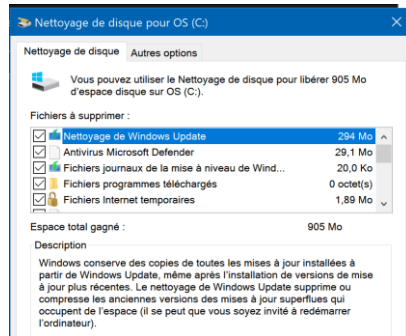
Enterprise administrators can also push updates to devices in their network. To clear the current cache and trigger an update, use a batch script that runs the following commands as an administrator:

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

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

Windows, comment on fait le ménage après?

- cleanmgr



Et Linux ? Mac OS ? Et les smartphones ?

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

Des plateformes MDM (Mobile Device Management) permettent:

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

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

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

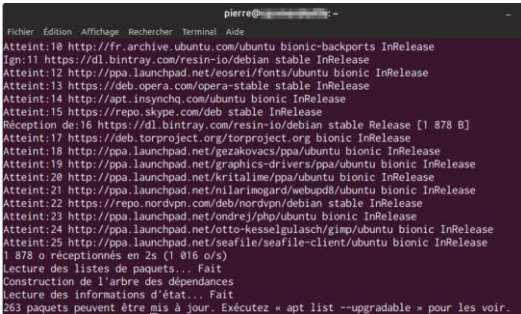
<https://medium.com/lesenfantsdu-net/passer-de-win10-%C3%A0-linux-5799c79d33f7>

Linux (selon la distribution, mais similaires)

- `sudo apt update`
- `apt list --upgradable`
- `'sudo apt upgrade'`
Ou bien `'sudo apt full-upgrade'`

Faire le ménage

- `sudo apt autoremove`
- `sudo apt autoclean`



```
pierre@pierre:~$ apt list --upgradable
Fichier Édition Affichage Recherche 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:16 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/nilarimogard/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-kesselgulasch/gimp/ubuntu bionic InRelease
Atteint:25 http://ppa.launchpad.net/seafire/seafire-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
263 paquets 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



Avoir fait des tests avant pour éviter de devoir corriger partout...
Mais comment peut-on tester ?

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...

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...

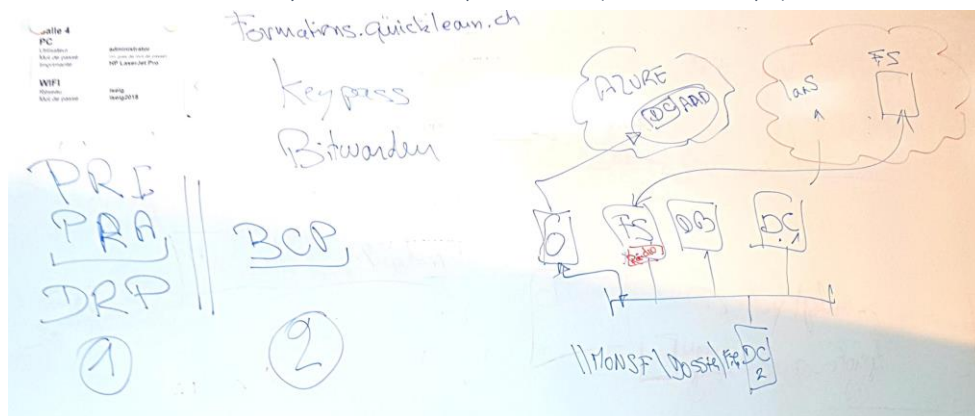
Déployer uniquement les éléments nécessaires

- 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.

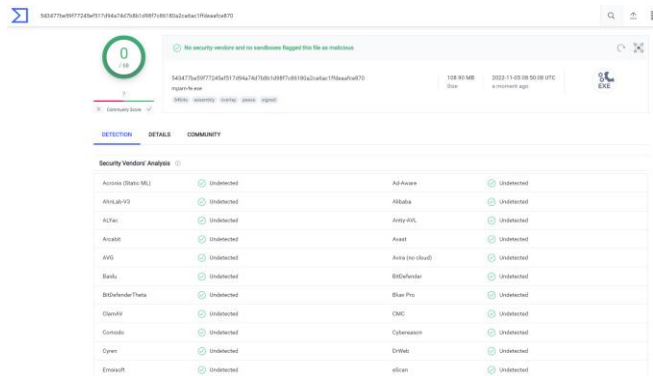
PRI ou PRA = Disaster Recovery Plan ou Plan de Reprise d'Activité

<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)



6. Services sous-jacents/infra

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

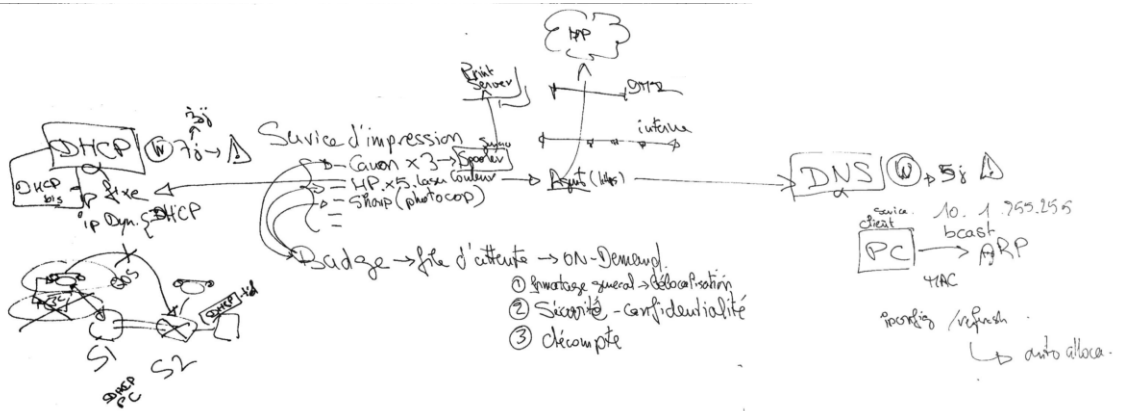
Pour fonctionner, un client qui affiche une page web, va avoir besoin de quels services ?

- 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 traducteur html sur le client: Navigateur, à jour, sans faille/bug...



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

Exemple des services d'impressions

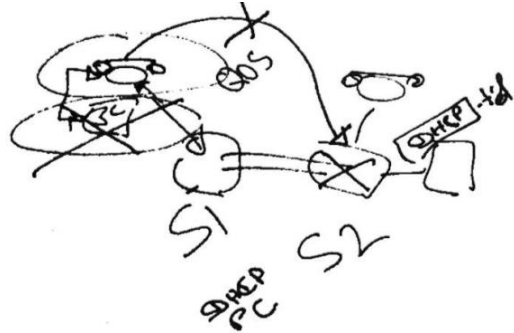


Sans une doc Adhoc et du monitoring

- 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...



X. Annexes

Bonus

Tools cools (end user)

Tuning

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

Sécurité

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

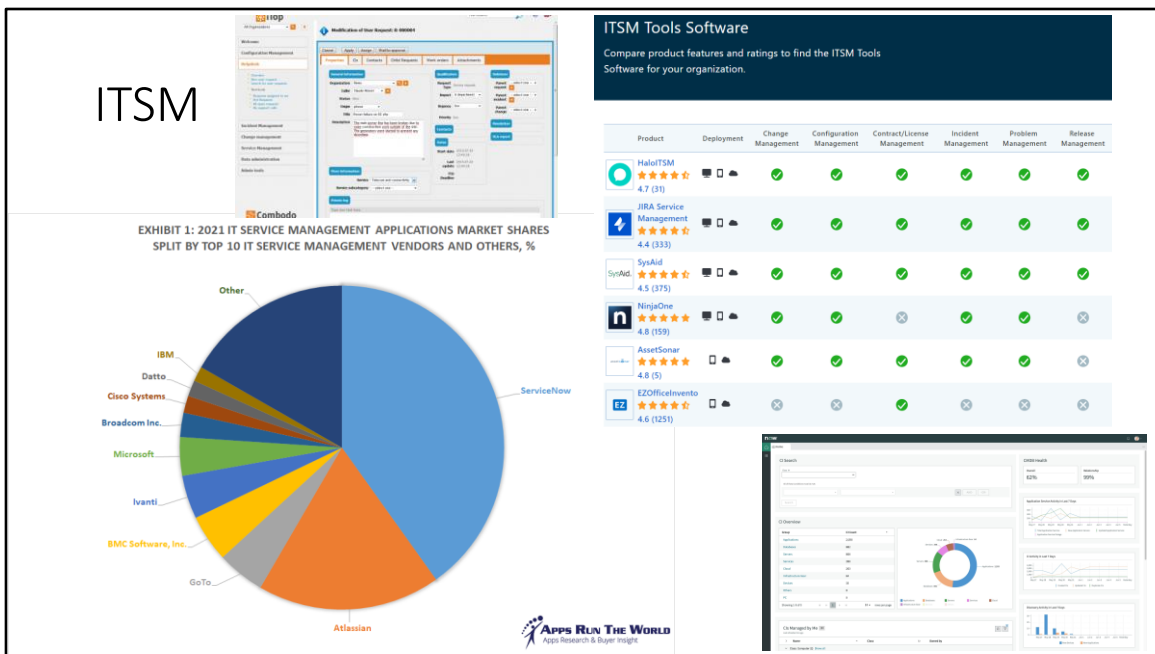
Plateformes cools (Entreprises)

ManageEngine

- Endpoint Central
- Patch Manager

		Free Edition	Edition Professionnelle	Edition Entreprise	Edition UEM
		Convient aux PME		Fonctionnalités de l'Edition Professionnelle +	Fonctionnalités de l'Edition Entreprise +
		Gérez jusqu'à 25 ordinateurs et 25 appareils mobiles	» Gestion des correctifs	» Optimisation de la Bande Passante WAN	» Gestion des Périphériques Mobiles
		» Gestion des Correctifs	» Déploiement de Logiciels	» Portail Libre-service	» Gestion Moderne des Périphériques 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 Périphériques 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				

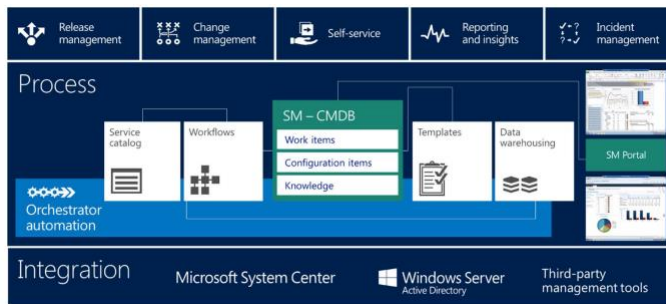
<https://www.manageengine.fr/produits/patch-management/presentation.html>
<https://www.manageengine.fr/pdf/factsheet.pdf>



<https://www.capterra.com/sem-compare/itsm-software/>
<https://www.appsruntheworld.com/top-10-it-service-management-software-vendors-and-market-forecast/>
https://fr.wikipedia.org/wiki/System_Center_Configuration_Manager
<https://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 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/>