Exploiter, surveiller et assurer la maintenance des services

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

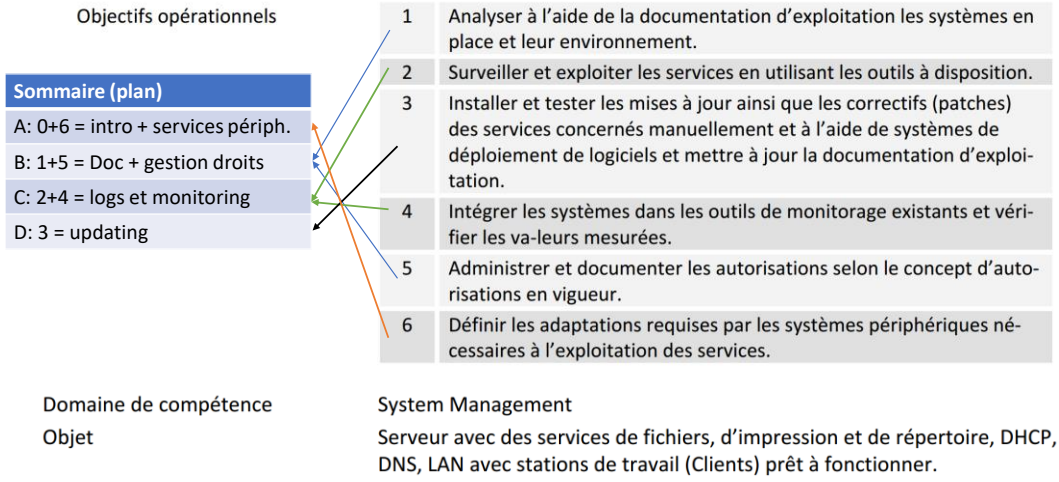
PK@ISEIG.ch

2022-10 > v2022-11-10

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



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 me-sures 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 acti-ver 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 parefeu). 6.2 Connaître des possibilités pour décrire les exigences posées aux systèmes périphé-riques 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.

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.

Salut

Tour classe

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

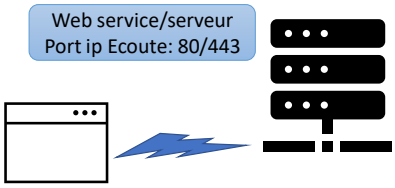
Cadre de bienveillance

- 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... (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)

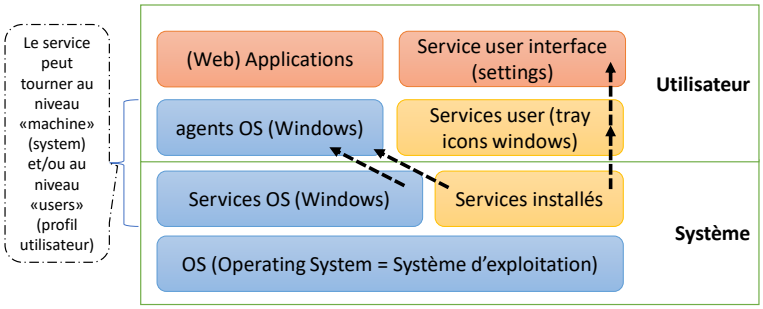
Warning: Il est supposé que lorsque vous tapotez vos claviers en cours de formation, c'est pour
-Prendre des notes sur les points importants du cours, questions à poser ou valider.
-aller voir et compléter les infos présentées, essayer l'application exposée, et vérifier si on connaît effectivement le 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 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

C’est quoi un service (informatique/numérique)

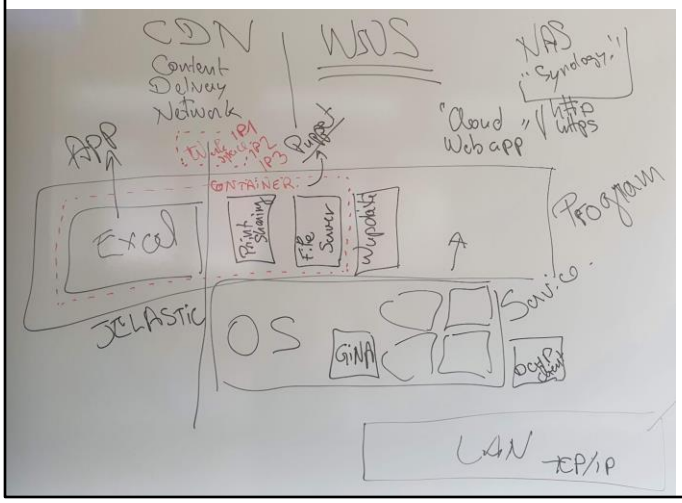


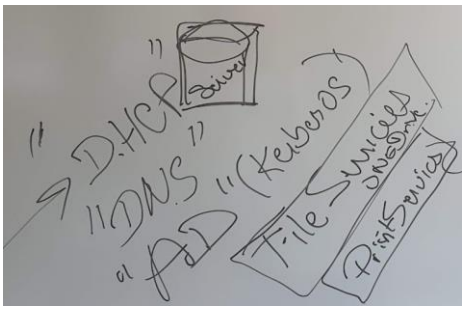
C’est un programme, qui n’est pas directement une application pour utilisateurs. Il peut tourner sur le poste de l’utilisateur, ou sur un autre appareil relié en réseau.



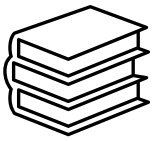
Un navigateur web, est la partie cliente d’un service numérique hébergé sur un serveur web, qui génère les codes html 5 nécessaires pour «simuler» une application locale, en réutilisant les ressources locales au maximum, afin de minimiser l’impact sur le serveur.

C’est quoi un service (informatique/numérique)





Les services «utilisateurs» et «infras»

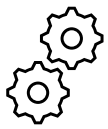


Le catalogue de services exposé aux usagers va intégrer les prestations assurées par leur département «IT» et leurs sous-traitants, ou fournisseurs: Ce sont les services finaux

- 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)
- …



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

Les services dans le Cloud

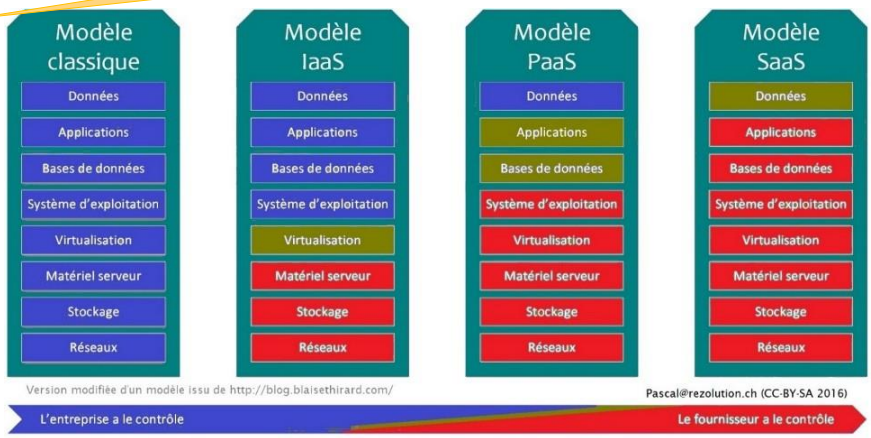
- Amazon
- Google
- Azure

<u>3 Clouds</u>

- IaaS
- PaaS
- SaaS

GAFAM
BATX

- Hidora
- Exoscale
- Infomaniak
- Etc…



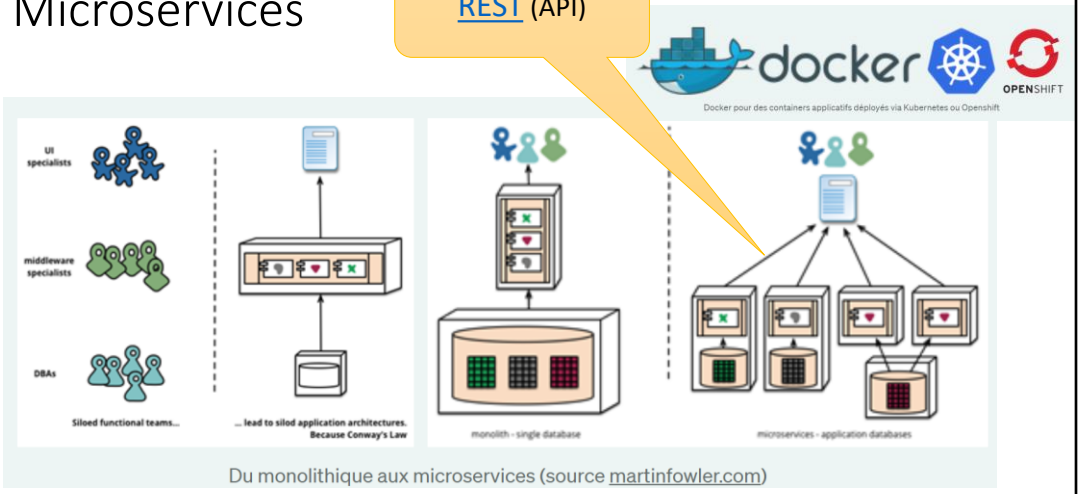
https://medium.com/cloudready-ch/cest-quoi-iaas-paas-et-saas-le-cloud-c169451d73bc

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)



Du monolithique aux microservices (source martinfowler.com)

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

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

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

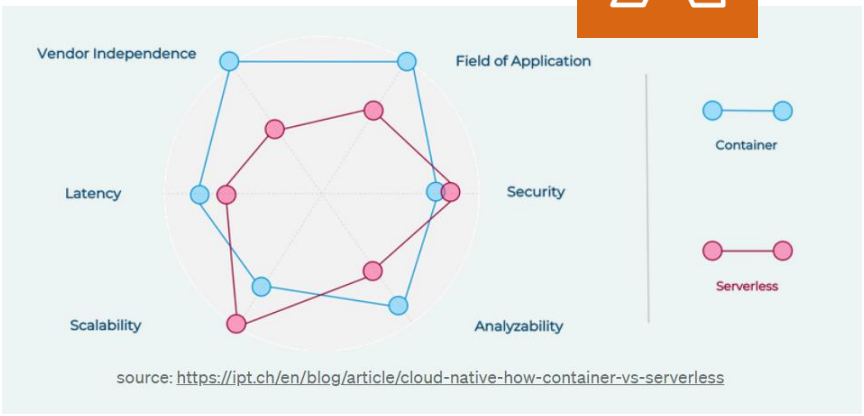
https://medium.com/cloudready-ch/ipaas-cest-quoi-3f4b8ec84924

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

DEVOPS to NoOPS

Google Cloud

Serverless computing



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, 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%A9risque

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

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

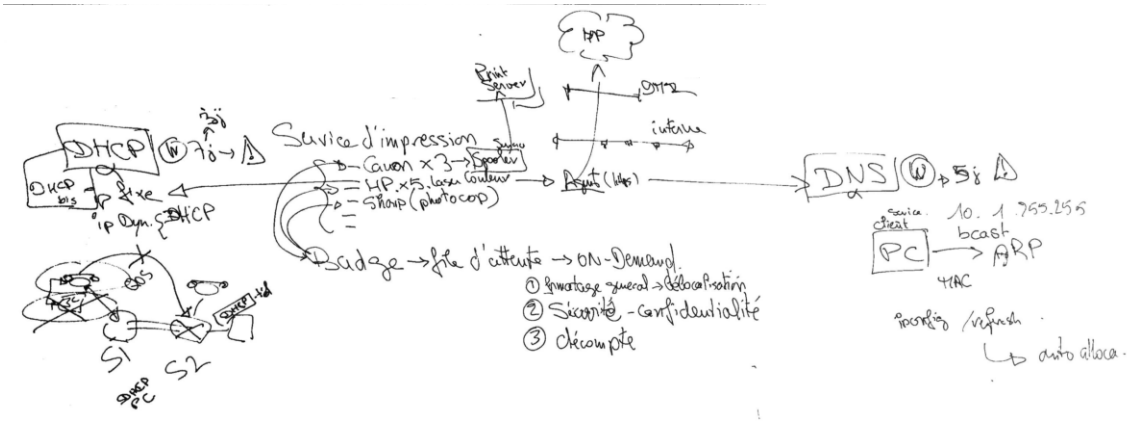
Pour fonctionner, un client qui affiche une page web, va avoir besoin de quels services ?

- 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 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 »

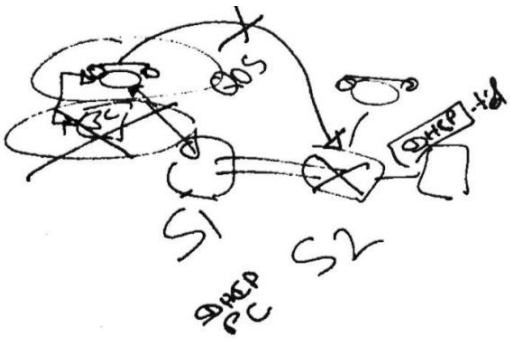
Sans une doc Adhoc et du monitoring

- 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 la 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?)

127.0.1.1 localhos
Cloudflare 1.1.1.1 Net.DNS
8.8.8.8 Google DNS

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

http://dns.quicklearn.ch

Azure private DNS Zone

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

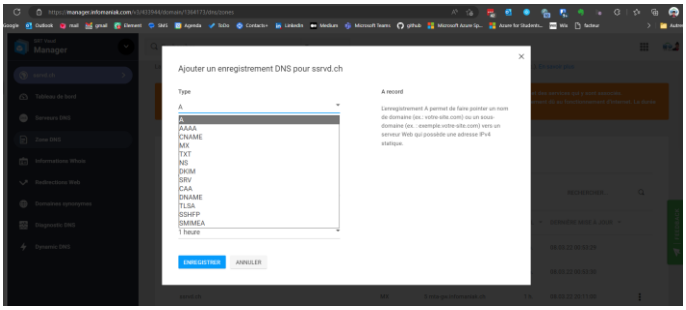
https://learn.microsoft.com/fr-fr/learn/modules/implement-windows-server-dns/
https://learn.microsoft.com/fr-fr/training/modules/host-domain-azure-dns/

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/

Présentation gestion DNS chez Infomaniak

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

Plus de détails sur le service DNS ici
http://dns.quicklearn.ch



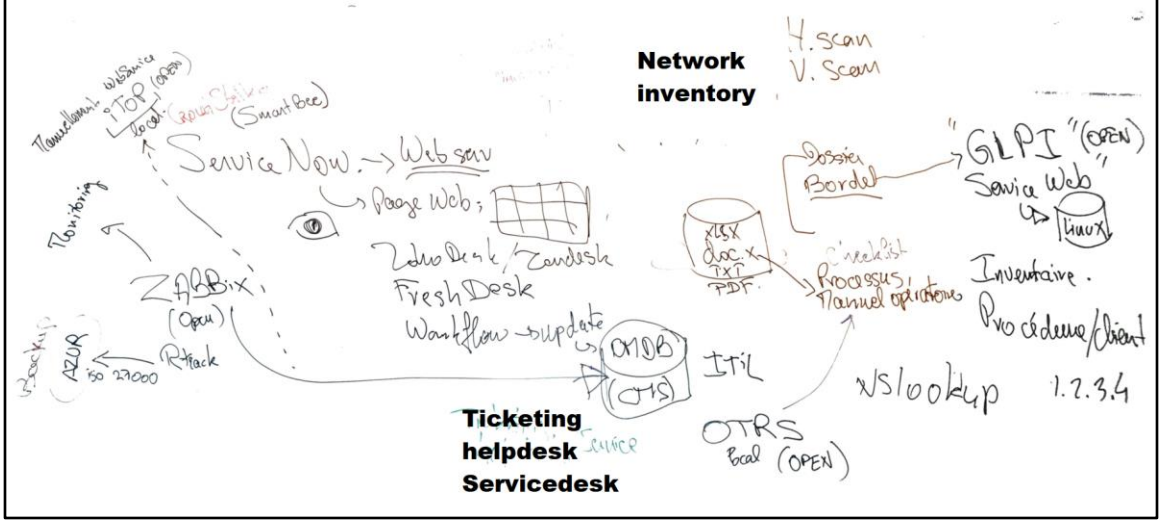
B: 1. Documentation

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

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

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»…

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/installeurs 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…)

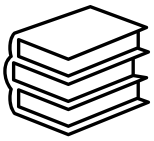
Il n'y a pas « une » doc, mais des « docs »

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
- 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)

Être lucide sur les éléments qui DOIVENT être documentés.

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?

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

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 (TK)

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.

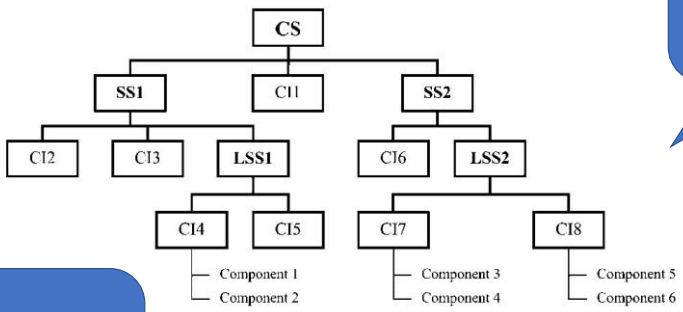
A disposition pour en causer dans vos structures, http://call.kotte.net

Gestion des configurations

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

COBIT (ISO9000)

ISO 27000 (39p)

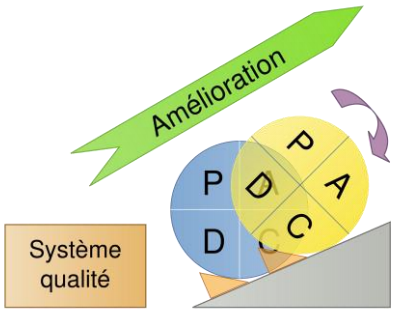


Mais pas la gestion des droits d'accès et des autorisations…

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

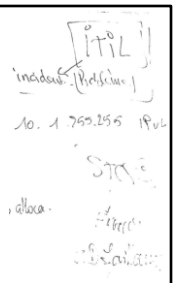
Gestion des procédures et des incidents

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…)*



Roue de Deming — Wikipédia (wikipedia.org)
https://fr.wikipedia.org/wiki/Roue_de_Deming

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.

B: (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.

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»

Création et gestion d'un fileshare dans Azure

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

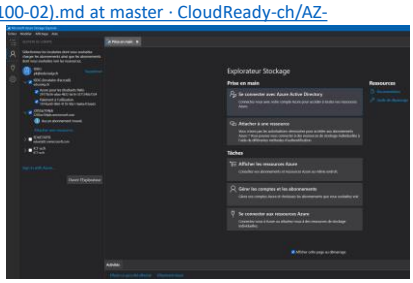
Via le compte étudiant @edu.iseig.ch et sélectionner 1 collègue pour y accéder (toujours sur son compte @edu.iseig.ch)

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



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

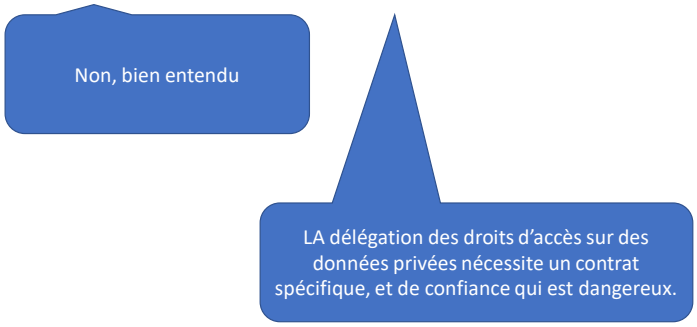
Autres docs découvertes

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 x2

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?

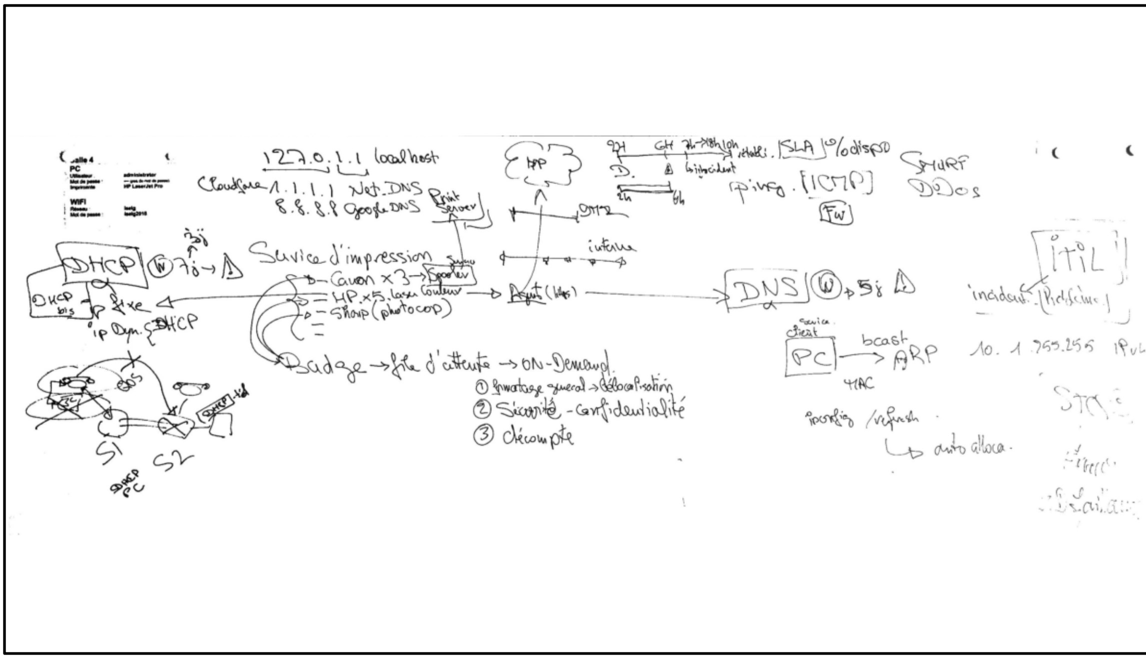


Gestion des comptes «machines»

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-controleur-de-domaine


127.0.1.1 localhost
Cloudflare 1.1.1.1 Net. DNS
8.8.8.8 Google DNS
Print Server
DHCP
ip fixe
ip Dyn. DHCP
Service d'impression
Canon x3
HP x5
Badge → file d'attente → ON-Demand
① formatage général
② Sécurité - confidentialité
③ décompte
S1
S2
APP
DNS
SLA
%dispo
ping . ICMP
FW
SMURF
DDos
ITIL
incident
PC
bcast
ARP
MAC
10. 1. 255.255
auto alloca.

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.

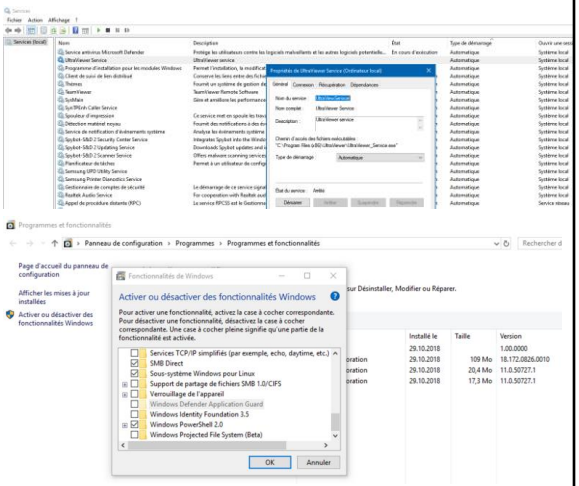
C: 2+4. Monitoring, add counters

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.

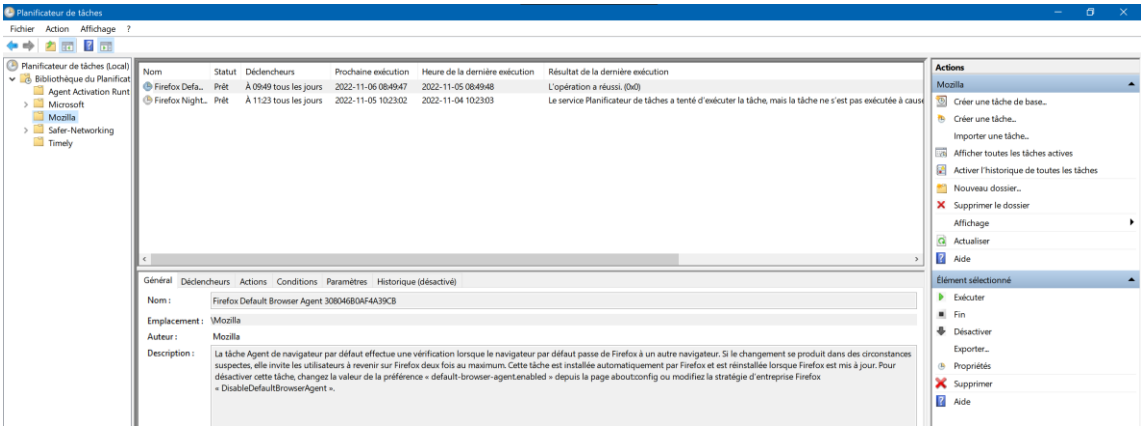
Activer/désactiver un service

- 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, ou automatiquement lancés au démarrage, voir relancer en cas d'arrêt.

Tâches planifiées, crontab sous Unix



Mais tous les services ne tournent pas nécessairement dans l'onglet « Services » de Windows. Certains se présentent sous la forme d'applications « portable »

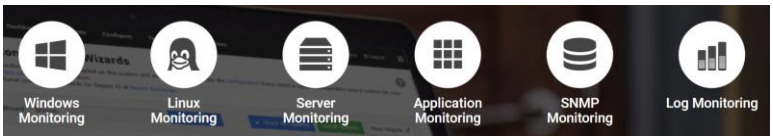
https://portableapps.com/

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

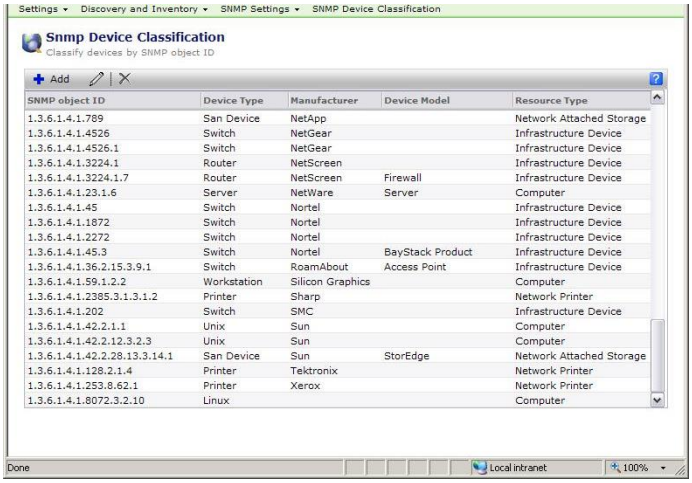
https://fr.wikipedia.org/wiki/Supervision_(informatique)

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



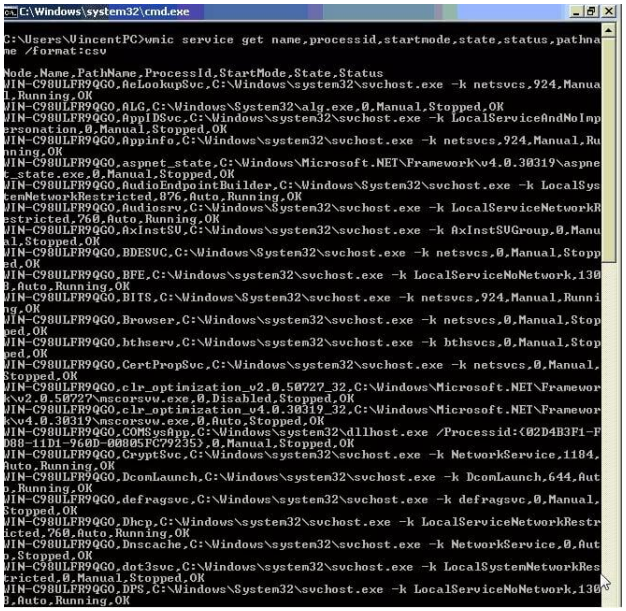
SNMP object ID	Device Type	Manufacturer	Device Model	Resource Type
1.3.6.1.4.1.789	San Device	NetApp		Network Attached Storage
1.3.6.1.4.1.4526	Switch	NetGear		Infrastructure Device
1.3.6.1.4.1.4526.1	Switch	NetGear		Infrastructure Device
1.3.6.1.4.1.3224.1	Router	NetScreen		Infrastructure Device
1.3.6.1.4.1.3224.1.7	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/Simple_Network_Management_Protocol
https://fr.wikipedia.org/wiki/Internet_Control_Message_Protocol_V6
https://fr.wikipedia.org/wiki/IPv6

WMIC & commandes Windows

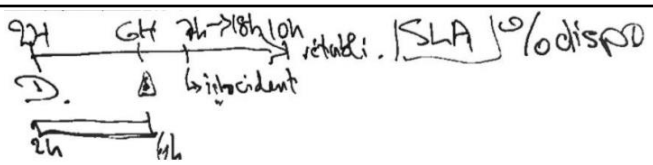
- WMIC
- Net
- Nbtstat (Netbios infos)
- Netstat –abn (IP infos)
- Arp
  - Gère les MAC adresses Ethernet
- Ping (utilise ICMP)
  - Souvent désactivé par sécurité
- Ipconfig (dhcp actions)
  - Identification des
- Nslookup (dns actions)
- Tracert (traceroute)
- …

ping. [ICMP] SMURF DDoS



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.

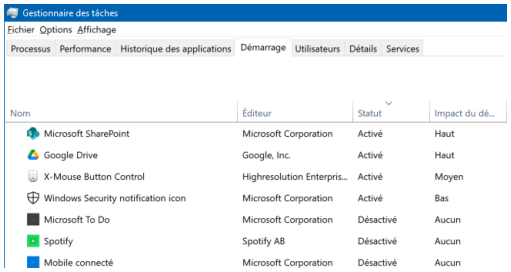
D'où l'intérêt de monitorer et alerter, pour réparer avant 7h!

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 ?

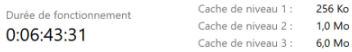
Sont des notions qui seront exploitées par les PRI/PRA (cf. plus loin)

Reboot time

- Task manager, démarrage – limiter au strict nécessaire



- Task manager, Performance – last reboot



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.

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

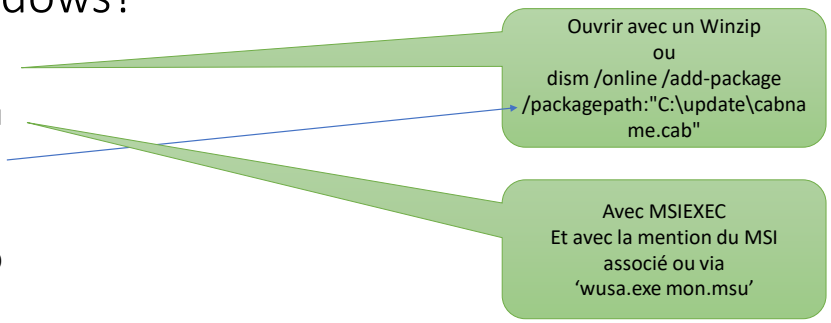
Pourquoi ?

- 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
- .msp
- …



Comment installer manuellement un fichier CAB dans Windows 10 ? (lojiciels.com)
https://www.lojiciels.com/comment-installer-manuellement-un-fichier-cab-dans-windows-10/ (Bof cet article à trouver mieux!)
http://www.easy-pc.org/2017/01/comment-installer-les-mises-a-jour-cab-et-msu-dans-windows-10.html

Patch (EXE) de Windows

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

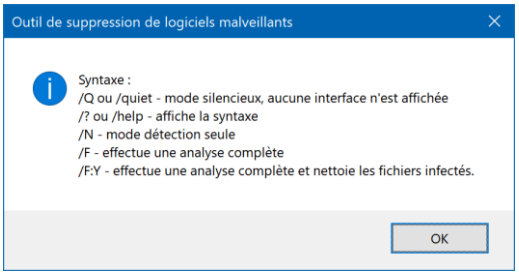
- KB890830

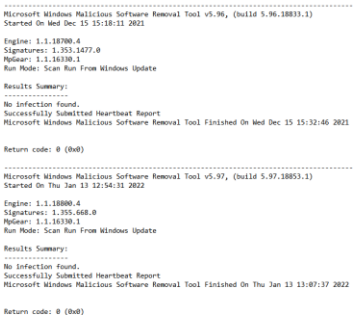
Un update qui va scanner les malwares identifiés via une application qui va faire un scan rapide: MSRT

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

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

Mrt.log



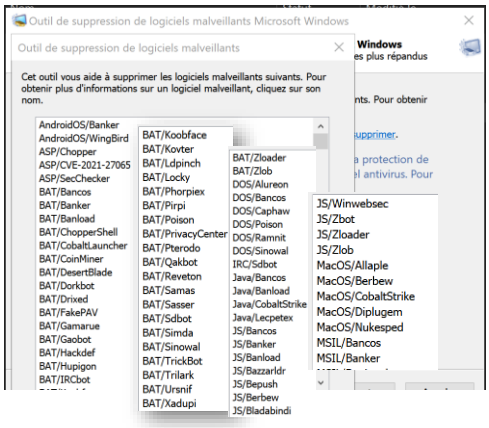


Exemple avec: KB890830 - MSRT
https://support.microsoft.com/fr-fr/topic/supprimer-des-logiciels-malveillants-sp%C3%A9cifiques-et-r%C3%A9pandus-%C3%A0-l-aide-de-l-outil-de-suppression-de-logiciels-malveillants-windows-kb890830-ba51b71f-39cd-cdec-73eb-61979b0661e0

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



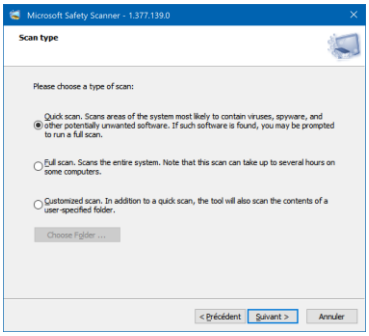
https://medium.com/cloudready-ch/botnet-c-est-quoi-89710901de99
https://medium.com/cloudready-ch/internet-et-la-s%C3%A9curit%C3%A9-f0cd27a14408
https://www.microsoft.com/en-us/download/details.aspx?id=9905
https://support.microsoft.com/fr-fr/topic/comment-faire-pour-r%C3%A9soudre-une-erreur-lorsque-vous-ex%C3%A9cutez-le-scanner-de-s%C3%A9curit%C3%A9-microsoft-6cd5faa1-f7b4-afd2-85c7-9bed02860f1c

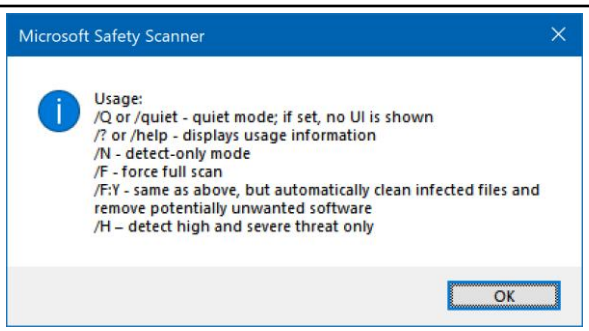
MSERT

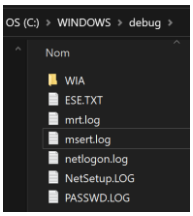
[Microsoft Safety Scanner Download | Microsoft Learn]

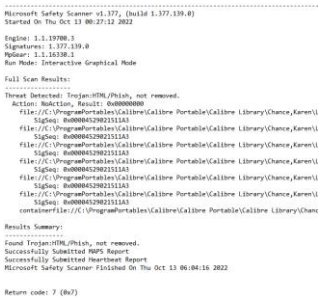
Un grand frère de MSRT…

- Log = msert.log



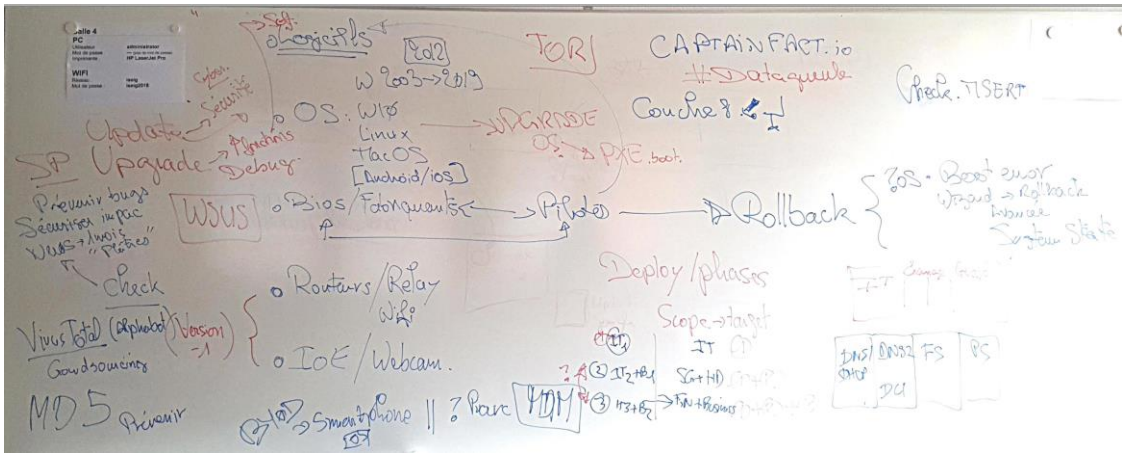






https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/safety-scanner-download

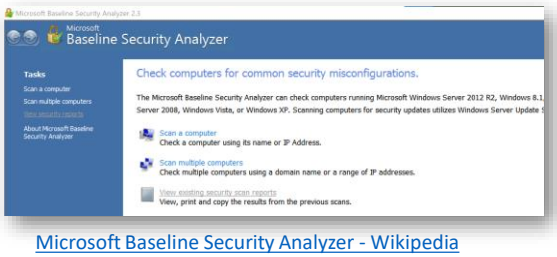
Les mises à jour

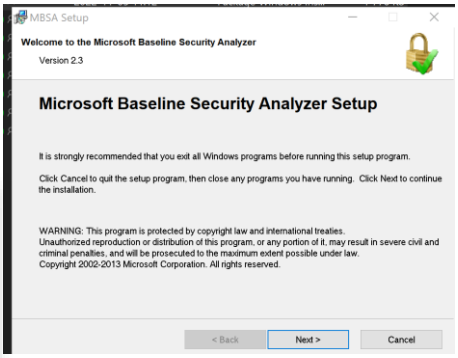


Scan vulnérabilité vs Removal!

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

Historique: Avant W10/S2016



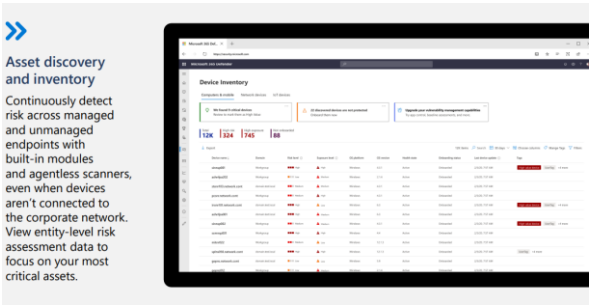


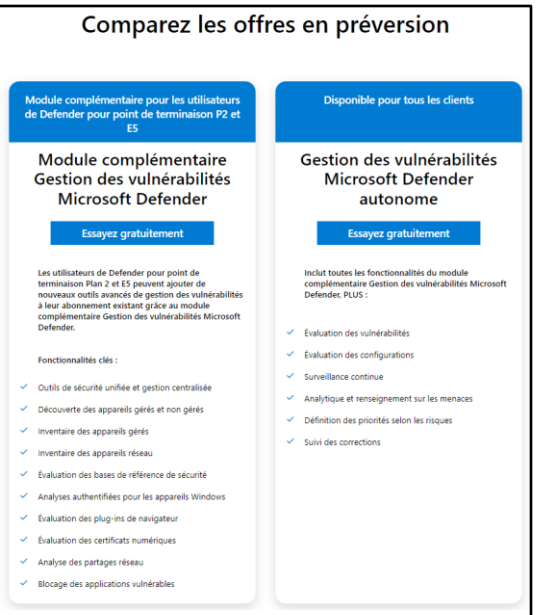
Microsoft Baseline Security Analyzer - Wikipedia

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





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

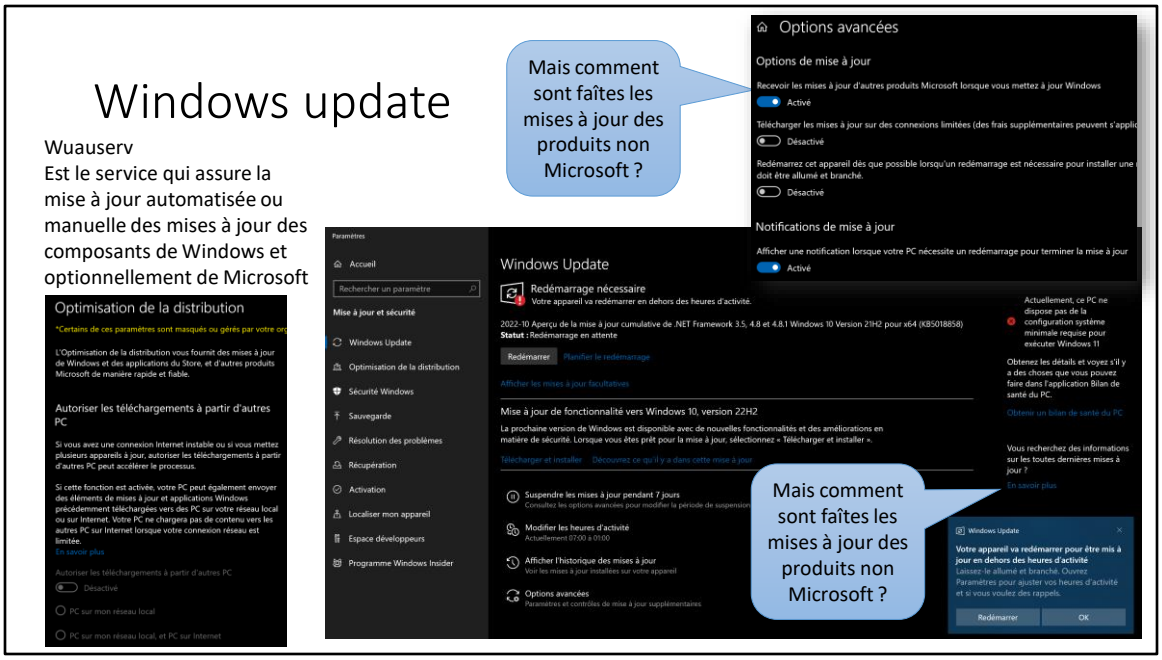
Bien que les updates de Microsoft incluent aussi un MSRT mensuel, le gros du travail consister à essayer de boucher les trous, avant agression.

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



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:

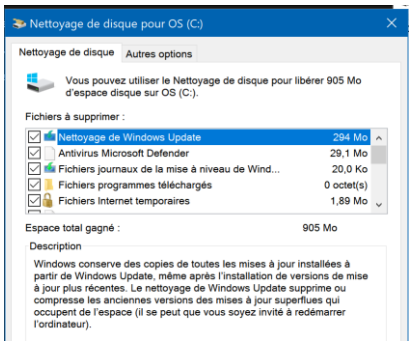
```
cd %ProgramFiles%\Windows Defender
MpCmdRun.exe -removedefinitions -dynamicsignatures
MpCmdRun.exe -SignatureUpdate
```

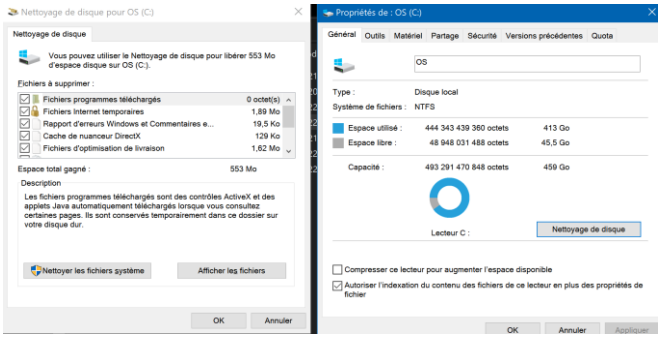
Slide masquée car hors-sujet

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

Windows, comment on fait le ménage après?

- cleanmgr





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

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 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)

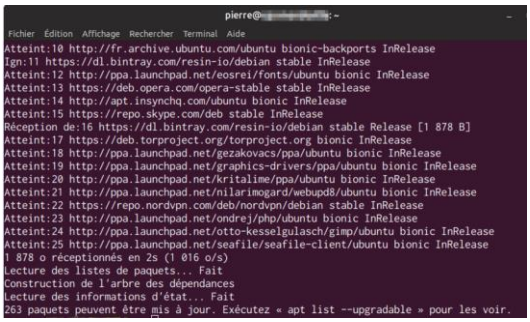
Comment installer les mises à jour sous Linux ? (lojiciels.com)
https://www.lojiciels.com/comment-installer-les-mises-a-jour-sous-linux/
https://medium.com/lesenfantsdu-net/passer-de-win10-%C3%A0-linux-5799c79d33f7

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



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…

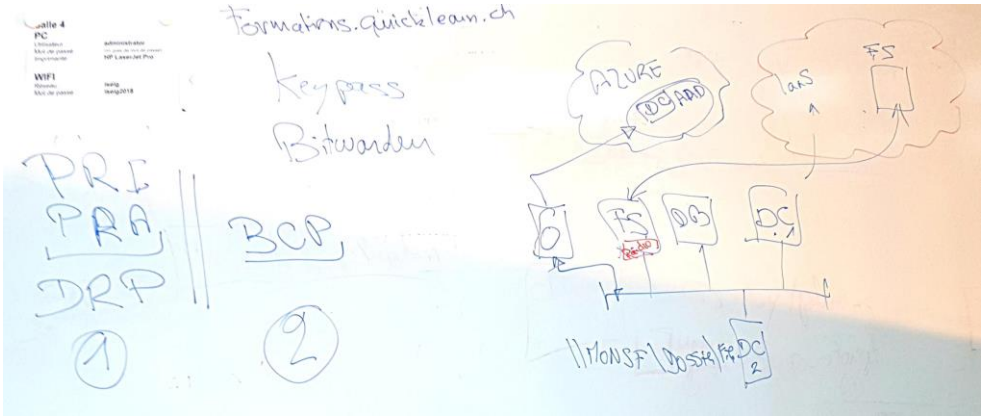
Déployer uniquement les éléments nécessaires

- 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 opérationnels.

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

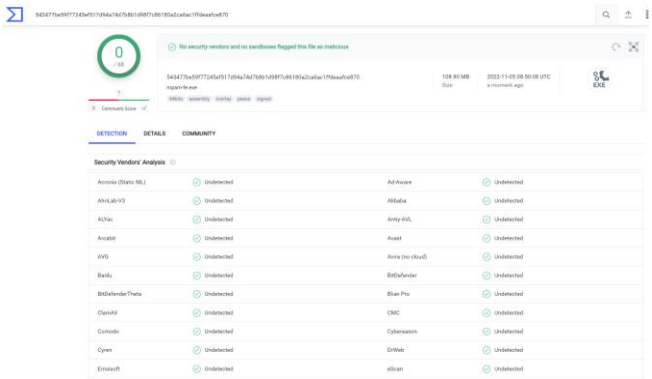
Exemple – le service Onedrive, qui permet au poste de continuer sur une copie locale sur le poste, hors connexion, et de récupérer un accès à une version enregistrée par le passé, en cas d'erreur et de suppression de données involontaires (voir un cryptage par un Malware).

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



X. Annexes

Bonus

Tools cools (end user)

Tuning

- Piriform — Wikipédia (wikipedia.org) : Ccleaner => Quoique
- …

Sécurité

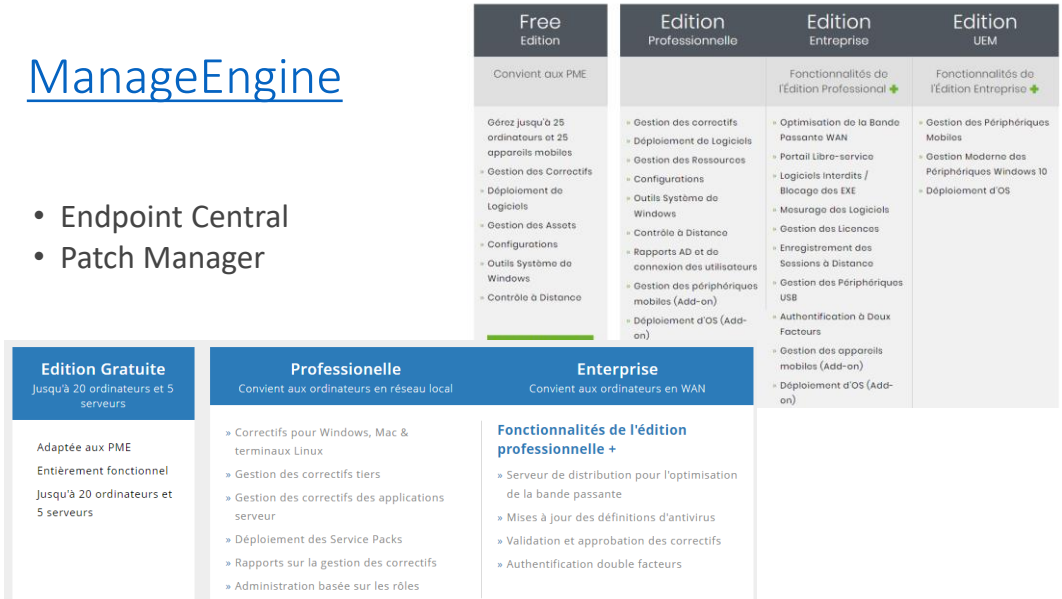
- BitWarden.com pour stocker les mots de passe
- Keypass (plus économique en entreprise)

Plateformes ITSM (Entreprises)

IT Service Management

ManageEngine

- Endpoint Central
- Patch Manager



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

ITSM

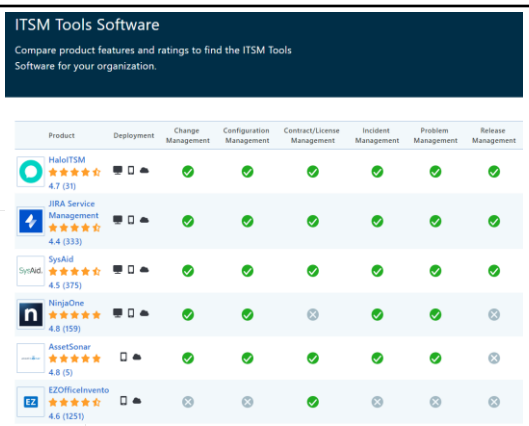
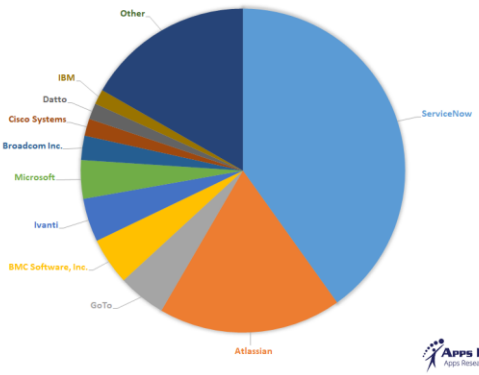
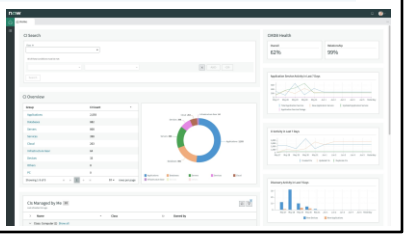


EXHIBIT 1: 2021 IT SERVICE MANAGEMENT APPLICATIONS MARKET SHARES
SPLIT BY TOP 10 IT SERVICE MANAGEMENT VENDORS AND OTHERS, %



Apps Run The World
Apps Research & Buyer Insight



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

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/