Retour d'expérience sur l'installation de F-Secure à l'I2M

I2M BORDEAUX INSTITUT DE MÉCANIQUE ET D'INGÉNIERIE

cnrs université de BORDEAUX Arts et Métiers Institute of Technology BORDEAUX INP INRAE

Contexte ayant mené à la bascule de l'antivirus

Questions autour de l'utilisation de Kaspersky dans l'ESR suite au contexte géopolitique depuis le 24 février 2022

❑ Quel impact pour le laboratoire ?

- Interrogations, d'inquiétude, théorie en tout genre …
- Premières conclusions :

- Renforcer la communication auprès des personnels du laboratoire (mails, CoInst, AG …)
- Objectif : rassurer les utilisateurs, insister pour qu'ils ne désactivent surtout pas leur antivirus

Contexte ayant mené à la bascule de l'antivirus

MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA RELANCE

Liberté
Égalité
Fraternité

Fiche technique

Mise en œuvre de l'interdiction d'attribuer ou d'exécuter des contrats de la commande publique avec la Russie

Le règlement (UE) n°2022/576 du Conseil du 8 avril 2022 modifiant le règlement (UE) n°833/2014 concernant des mesures restrictives eu égard aux actions de la Russie déstabilisant la situation en Ukraine prévoit, au 23 de l'article 3 terdecies, des mesures applicables aux marchés publics et aux concessions. La présente fiche a pour objet d'expliciter la nature, le champ d'application et les conséquences de ces mesures.

III. Résiliation des contrats en cours

Tout contrat en cours au 9 avril 2022, soit à la date d'entrée en vigueur du règlement (UE) 2022/576, qui ne serait pas échu au 10 octobre 2022[5], doit être résilié avant cette date.

- Informations publiées au JO du 8 avril 2022
- Conclusion : Pas de renouvellement de contrat avec l'entreprise Kaspersky pour le marché antivirus négocié chaque année en juin
- Conséquence : il deviendra impossible de mettre à jour les définitions virales à terme (07/2002)

Prises de décisions des tutelles (CNRS & UB)

- Jusqu'en mai 2022, incertitude concernant le choix de la nouvelle solution d'antivirus (plusieurs rumeurs Trend Micro ?)
- Fin mai 2022, le CNRS et l'Université nous informent qu'ils ont porté leurs choix sur le même produit. (F-Secure - WithSecure)

F-Secure Corporation

F-Secure

WITH secure

Le siège de F-Secure dans le quartier de Ruoholahti à Helsinki.

Reste à définir la solution à mettre en place à l'I2M

Que fait-on à l'I2M ?

- Contexte avant bascule :
  - Un serveur d'antivirus KASPERSKY en interne + un parc d’environ 400 postes (Windows, Linux et Mac Os) sous licence Kaspersky (Licences CNRS)

- Quelles solutions s’offrent à nous vis-à-vis de nos tutelles ?
  - Se tourner vers le CNRS ? (solution interne WithSecure)
  - Se tourner vers l’UB ? (solution externe WithSecure)
  - Autre possibilité : ENSAM ? Solution Windows Defender

Première piste : Solution WithSecure proposée par le CNRS (1/2)

- Début Juin 2022 : La DSI du CNRS organise une réunion en **visioconférence** pour aider les laboratoires à installer la nouvelle solution d'antivirus WithSecure. (enregistrement disponible si besoin*)

- Quelques points à retenir :

- 2 types de serveurs possibles : serveur Windows, **serveur Linux (recommandé)**

- Compatible avec de nombreuses distributions Linux (cas de la Debian 11)

- Une précaution lors de l'installation du serveur Linux : activer le mode « Multiarch »
*https://help.f-secure.com/product.html#business/policy-manager/15.30/fr/installing_pm_linux-15.30-fr

- Linux (seules les versions 64 bits de toutes les distributions répertoriées sont prises en charge) :
  - AlmaLinux 8.5
  - CentOS 7, 8
  - Flux CentOS 8
  - Debian GNU Linux 9, 10
  - openSUSE Leap 43, 15
  - Oracle Linux 8
  - Red Hat Enterprise Linux 6 , 7 et 8
  - SUSE Linux Enterprise Server 11, 12 et 15
  - SUSE Linux Enterprise Desktop 11, 12 et 15
  - Ubuntu 16.04, 18.04, 20.04

Prise en charge du multiarch dans Debian

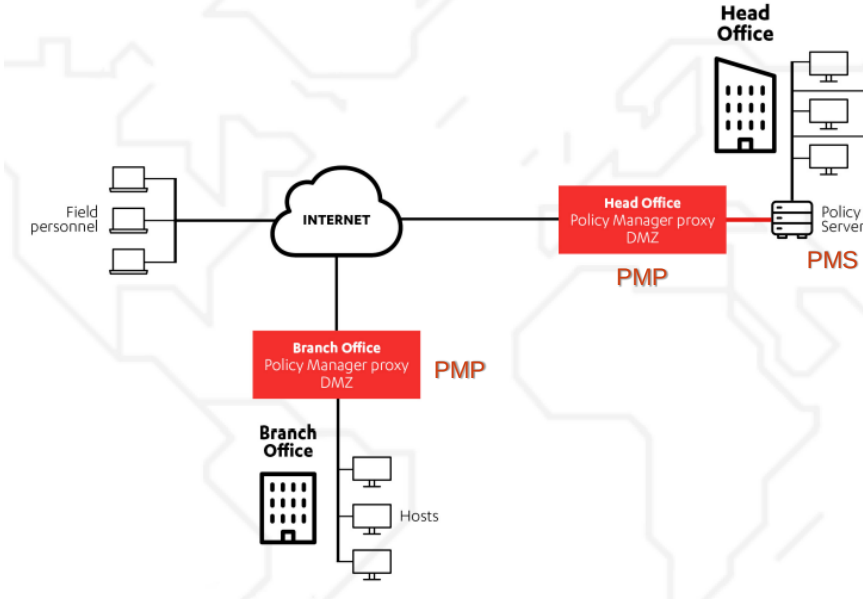
À propos

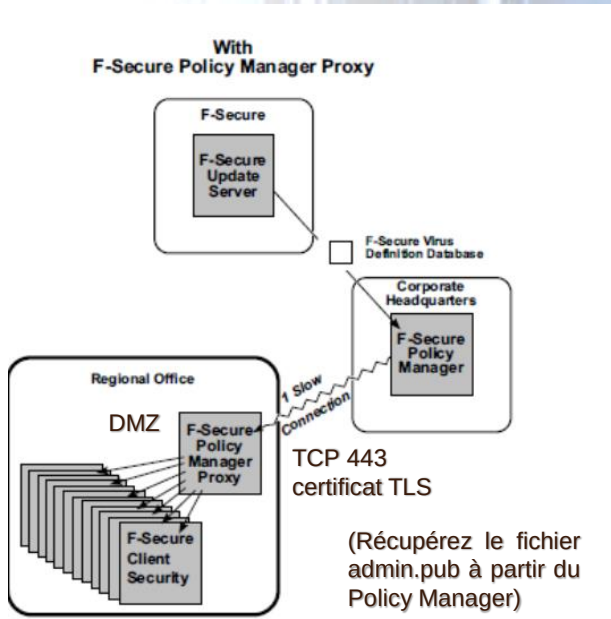
« Multiarch » est le terme utilisé pour désigner la capacité d'un système à installer et à exécuter des applications de plusieurs cibles binaires différentes sur le même système. Par exemple, exécuter une application i386-linux-gnu sur un système amd64-linux-gnu. Cet exemple est le cas le plus courant, mais de nombreuses autres combinaisons d'usages sont possibles, comme armel et armhf.

Première piste : Solution WithSecure proposée par le CNRS (2/2)

- Quelques points à retenir :

  - Une recommandation : utiliser F-Secure Policy Manager Proxy (pmp) associé au serveur (pms) . *https://help.f-secure.com/data/pdf/fspm-proxy-15.30-adminguide-fra.pdf





Mise en place des serveurs à l'I2M

- **Travail réalisé à l'I2M**

  - Installation de 2 serveurs (**Policy Manager Server et Policy Manager Proxy**) : 2 VMs de type Ubuntu Serveur 20.04 LTS sur hyperviseur PROXMOX

  - Demande d'ouverture de port à l'UB pour autoriser les flux vers le serveur proxy

  - Installation de la console d'administration (PMC) sur les postes des ASR du labo - application Windows à récupérer sur le site de WithSecure

  - Dernière étape (avortée) demande de licences auprès du SI de la délégation du CNRS (Similitude avec la solution Kaspersky)

- **Puis… rebondissement …**

Nouvelle piste : Solution WithSecure proposée par l'UB

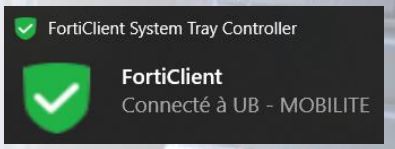
- **On change de cap !** réorientation vers la solution mise en place par l'UB

❑ Pourquoi ?

- Échanges avec la DR15 sur le sujet (Roland Dirlewanger et Jimmy Labejof)
- Conclusion : Dans le contexte, c'est la tutelle qui gère la **PPST** qui devrait offrir la solution d'antivirus pour les UMR

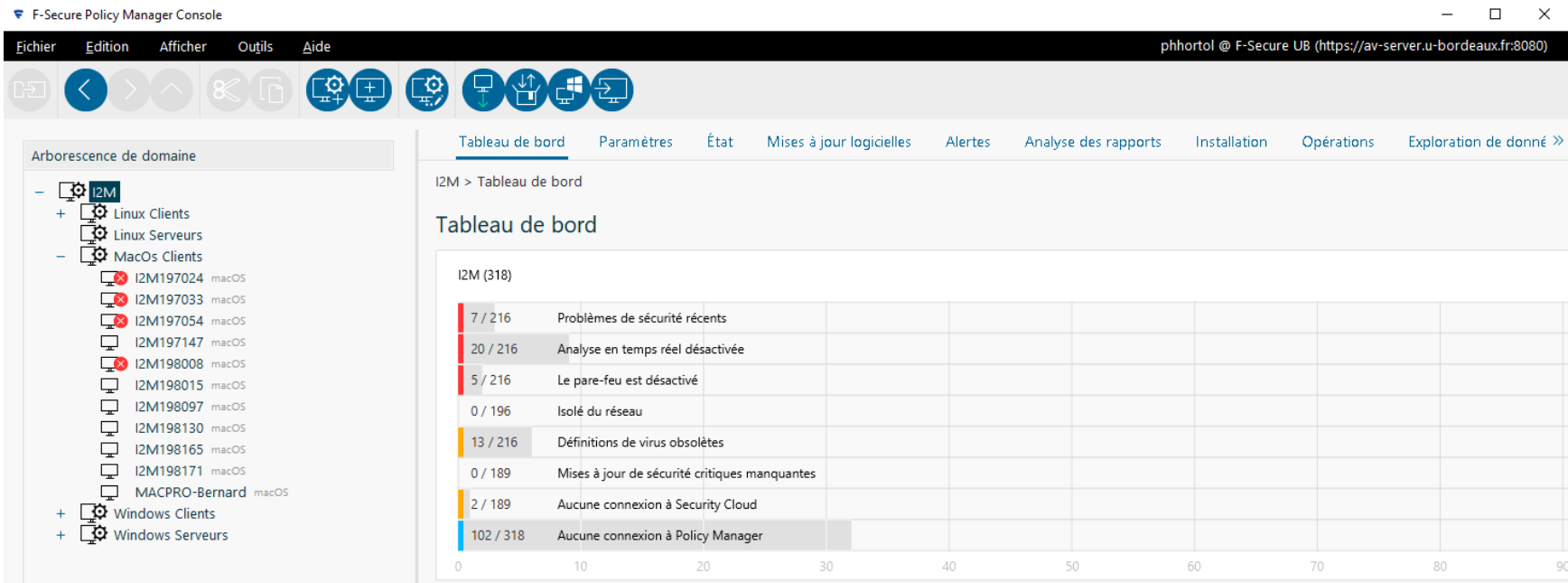
❑ Comment ?

- Adresser une demande au pôle sécurité de l'UB – (Saisie d'une demande sur le site d'assistance GLPI de l'UB) - https://assistance.u-bordeaux.fr/
- L'UB crée un accès au serveur d'antivirus UB, ce qui permet de disposer d'une console dédiée pour la gestion des postes (ATTENTION : accessible via VPN UB uniquement)
- Une précaution à prendre : Ouvrir les ports dans le pare-feu (LAN - I2M) pour autoriser les postes à communiquer avec le serveur F-Secure UB



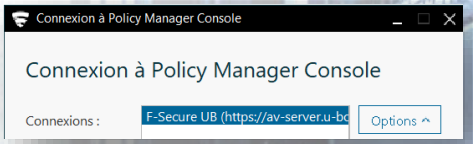
Connexion à la console d'administration de WithSecure

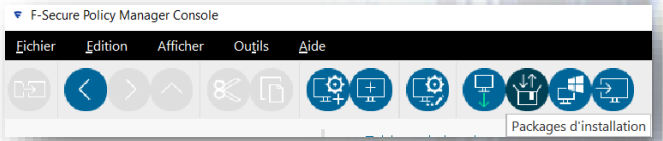
- **Vue sur la console - domaine de stratégie**



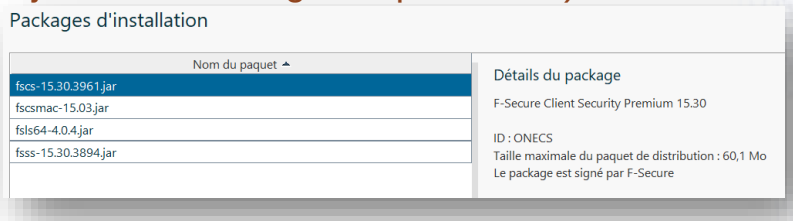
Récupération du package d'installation

- Etapes permettant de récupérer le package d'installation :





- Cliquer sur l'icône 'Package d'installation'
- Choisir le paquet au format ***.jar** approprié (4 sont disponibles) pour générer un fichier d'installation en fonction du type de poste à installer
  F-Secure **Client** Security Premium 15.30 / F-Secure Client Security for **Mac** 15.03 / F-Secure **Linux** Security 64 4.00.4 / F-Secure **Server** Security Premium 15.30
- Un assistant nous guide dans les étapes permettant de paramétrer le package (les informations sont déjà toutes renseignées par défaut)

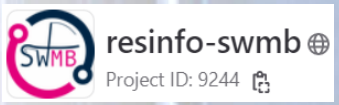


Reste à déployer l'agent sur les postes – Quelles solutions ?

- Plusieurs solutions ont été proposées par la communauté des ASR - de nombreux échanges sur les listes de diffusion
- Parmi les solutions proposées : installation par déploiement (OCS, WAPT, Console WithSecure, Console Kaspersky …)

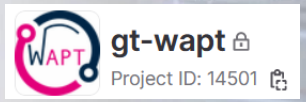
❑ Certaines configurations ont rendu la désinstallation de Kaspersky compliquée.

- Une piste intéressante a été proposée par le groupe de travail **SWMB (RESINFO)**. Proposition d'un script PowerShell qui force la suppression de Kaspersky et en supprime toute trace sur les PC (Windows)



Voir : https://resinfo.org/les-groupes-de-travail-11/groupe-de-travail-swmb/

- Dans le même ordre d'idée, le groupe de travail WAPT (RESINFO) a proposé un paquet basé sur le script SWMB pour déployer cette solution.



Voir : https://resinfo.org/les-groupes-de-travail-11/groupe-de-travail-wapt/

Reste à déployer l'agent sur les postes à l'I2M

- Retour d'expérience I2M - Pas de déploiement généralisé :
  - Les raisons : hétérogénéité du parc informatique, implémentation partielle de WAPT
  - D'autres besoins identifiés : mise à jour de l'inventaire, vérification de bitlocker, des mise à jours. Mise en place d'une checklist
  - Organisation de plusieurs phases d'installation de l'antivirus (Windows en premier, Linux et MacOS en suite) avec planification des campagnes d'installation
  - Bilan : nombre de postes visibles dans la console : Plus de 300, mais tous les postes ne remontent pas et d'autres ne sont pas compatibles avec WithSecure
  - Reste à traiter au cas par cas les postes de manip (non connectés au réseau I2M)

Un GRAND MERCI aux collègues en charge de la partie assistance/support I2M

(Gilles Gay et Jean-Marc Sibaud) pour leur investissement dans ce projet

Conclusions

- Le choix de la solution à adopter est lié au contexte :
  - Qui héberge le labo (tutelle) ? qui supervise la PPST ? (Protection du potentiel scientifique et technique)
- Pour l'I2M, le choix de la solution UB comporte plusieurs avantages :
  - Solution déportée, pas de gestion du serveur en interne (mises à jour, pannes)
  - Rapide à mettre en place, mise à disposition d'une console dédiée pour le laboratoire
- Quelques écueils rencontrés tout de même (retours d'expérience) :
  - Problèmes de remontée dans la console de certains postes Linux et MacOS
  - Pas d'interface GUI sur les postes Linux
  - Ne fonctionne pas sur toutes les distributions Linux (Ex : Linux Mint – OK pour Ubuntu)
  - Ne fonctionne pas sur toutes les distributions MacOs (que sur les distributions les plus récentes)

Merci de votre attention

Dans la deuxième partie de cette présentation,

Axel abordera le **paramétrage des options** disponibles à partir de la console d'administration de WithSecure