RESINFO - Groupe SWMB

David Gras / Gabriel Moreau - Coordinateurs

14-16 décembre 2021 / Visio-conférence

Resinfo

SWMB

Bilan depuis l'origine

Comité de pilotage

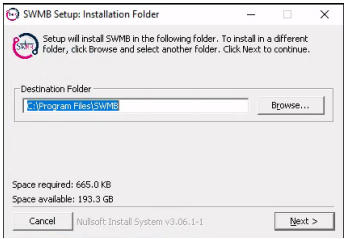
- David Gras (DR11 / Grenoble)
- Gabriel Moreau (LEGI / Grenoble)
- **Olivier de Marchi** (LEGI / Grenoble)
- Clément Deiber (DR11 / Grenoble)

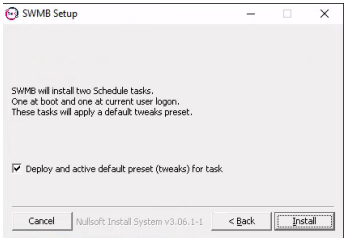
SWMB (Secure Windows Mode Batch)

- Besoin de sécuriser Microsoft Windows 10
- Fiches ANSSI que chacun doit s'approprier et refaire
- Beaucoup d'unités sans AD (mais avec Windows en client...)
- Possibilité de capitaliser, de mutualiser au sein de l'ESR
- Paramétrage existant de GPO dans AD (DR11 par ex.)
- Des scripts déjà existants (LEGI par ex.)
- Une suite logique à l'ANF SIARSv2 concernant la partie Windows

Première bêta 2021

- Mise en place d'un projet fonctionnel
- Projet modulaire, lisible, simple, extensible basé sur un projet amont archivé
- 556 règles à ce jour dont 86 RESINFO (enable / disable. . . - 50 l'an passé)
- Élargissement du groupe / 22 abonnés sur la liste de diffusion `swmb-gt` (11 l'an passé)
- 16 réunions de travail de 1h en plus du travail sur l'article JRES (arrêt depuis mi-novembre)
- Pad de travail + cloud + chat IN2P3 (`#resinfo-gt-ftto`)
- Installateur graphique et silencieux Setup.exe





Bilan 2021

- Deux tâches planifiées actives par défaut avec un minimum de règles effectives
- Intégration de Bitlocker / TPM !
- Une mini interface graphique
- Paquet OCS Inventory, WAPT et PDQ Deploy
- Documentation en anglais
- 421 commit sur la forge de l'IN2P3
- Une proposition JRES

URL du projet `https://gitlab.in2p3.fr/resinfo-gt/swmb/resinfo-swmb`

Projets 2022

- Plus de sites en production avec SWMB
- Plus de règles actives par défaut
- Être plus réactif sur les alertes de sécurité (groupe plus élargi)
- Intégration du pare-feu Windows
- Ajout de règles Kaspersky / Windows Defender ?
- Une meilleure documentation pour utiliser et comprendre SWMB (voir article des JRES)
- Finaliser le poster pour les JRES 2021

Licence

Merci à toutes les personnes et entités
nous ayant aidés ou ayant participé depuis le début

Cette présentation est sous : Licence Art Libre

http://artlibre.org/