



université
de BORDEAUX

INRAE



Séminaire Active Directory - Proxmox

Réseau de métier ASR RAISIN / membres des GT AD et Proxmox
(Retour des travaux des Groupes de Travail)

13 juin 2024



Séminaire Active Directory - Proxmox

Réseau de métier ASR RAISIN / membres des GT AD et Proxmox
(Retour des travaux des Groupes de Travail)

13 juin 2024



Présentation des groupes de travail du réseau RAISIN en Aquitaine

Programme des présentations de l'évènement RAISIN du 13 juin 2024

Présentation des retours des travaux des GT Active Directory et Proxmox

Focus sur la documentation en ligne



Les GT et activités du réseau RAISIN



CARTOGRAPHIE DES GROUPES DE TRAVAIL (GT) du RÉSEAU RAISIN - Millésime 2023

F-Secure	Proxmox	Active Directory	Cahier de Laboratoire Electronique	Sobriété Numérique
animateurs : Axel Cattouillart Philippe Hortolland	animateurs : Alain Blück Fabrice Forlini	animateurs : Richard Ferrere Jean-Marc Sibaud	animateurs : Richard Ferrere Karine Viaud	animateurs : Edouard Kleinpeter



Les membres des GT AD (11) et Proxmox (10) - RAISIN

Active Directory

Liste de diffusion : gt-ad-raisin@services.cnrs.fr

Date de première réunion : 20 juin 2023

Richard Ferrere



Animateurs :

Jean-Marc Sibaud



Participants : 11

Jonathan Di Vita - Yann Legallais - Jean-Marc Sibaud
 David Cigrand - Marc Leforestier - Hervé Lemaître
 Michel Goillandeau - Zeneida Tucsnak - Catherine Seznec
 Gaëtan Corle - Roderick Braconneau

Proxmox

Liste de diffusion : gt-proxmox-raisin@services.cnrs.fr

Date de première réunion : 04 juillet 2023

Alain Blüch



Animateurs :

Fabrice Forlini



Participants : 10

Philippe Hortolland - Sandrine Maillet - Jean-Luc Laborde
 Julien Desenfant - Hervé Lemaître - Simon Paries
 Karine Viaud - Pascal Ung - Axel Cattouillart
 Éric Pastor



Les travaux sur Active Directory

- ▶ **Présentation des GT AD et Proxmox, et des enjeux de la sécurité de Active Directory et de Proxmox dans nos SI** par Jean-Marc SIBAUD, Richard FERRERE Alain BLUCK, Fabrice FORLINI (de 13h45 à 14h)
- ▶ **Présentation de la sécurité Active Directory**, par Cédric MULLER de l'IPHC/IN2P3 de Strasbourg en VISIO (de 14h à 14h40)
- ▶ **Retour d'expérience et bonnes pratiques suite à un incident de sécurité**, par Marc LEFORESTIER del'IUT de Bordeaux (de 14h40 à 15h10)
- ▶ **Présentation de l'outil PingCastle et quelles actions et priorités ? autres outils ForestDruid et Oradad**, par Gaëtan CORLE, Richard FERRERE et Michel GOILLANDEAU (de 15h10 à 16h00)



Les travaux sur Proxmox

- ▶ **Pause et café** (de 16h à 16h15)
- ▶ **Présentation et retour des travaux Proxmox : migration Vxrail/Vmware vers Proxmox hyperconvergé avec CEPH** par Alain BLUCK & Christophe DELMON (de 16h15 à 17h)
- ▶ **Clôture de la session** 17h

 Vos idées pour nos futurs Groupes de Travail ! 

- ▶ La sécurité / cybersécurité
- ▶ La supervision / SIEM
- ▶ Une informatique Eco-responsable / sobriété numérique
- ▶ ...



Active Directory Domain Services (AD DS), Késako ?

Ensemble de services proposé par Microsoft depuis 2000 :

- ▶ d'authentification et d'autorisation (NTLM, LDAP et Kerberos)
- ▶ d'accès à un annuaire LDAP (RFC4511 Lightweight Directory Access Protocol)
- ▶ dédiés avec intégration DNS, DHCP, réplication, stratégies GPO

Quels enjeux et risques ? nos pratiques une fois installé !

- ▶ Primordial et en 1ere ligne sur nos systèmes d'information (SI)
- ▶ Cibles les plus attaquées et attaquables (techniques évoluées)
- ▶ Malwares et attaques sur les protocoles SMB, NTLM et parfois faiblesse de Kerberos
- ▶ Reconsidérer l'architecture et sa sécurité (bonnes pratiques, outils), Groupe de travail (GT AD)



Proxmox VE (Virtual Environment), Késako ?

Solution de virtualisation libre et Open Source (Allemande) depuis 2008


- ▶ hyperviseur baremetal (de type 1) sur 1 serveur physique dédié
- ▶ déployer des images de machines virtuelles KVM ou de conteneurs LXC
- ▶ flexibilité et isolation des VM et conteneurs
- ▶ prise en charge de EXT4, XFS, ZFS et CEPH


Les possibilités ?

- ▶ Très utilisé pour nos systèmes d'information (SI)
- ▶ Hyperconvergence (HCI) pour les calculs, le stockage et les réseaux
- ▶ Face à des solutions coûteuses (VMware vSphere/VSAN, Dell VxRail, Nutanix/AOS)
- ▶ Con/Reconsidérer l'architecture avec Proxmox et Ceph !



Livrable en ligne documentation des Groupes de Travail

 **ACTIVITES et DOCUMENTATION RAISIN**



Accueil
Fonctionnement des GT
F-SECURE
PROXMOX
CAHIER DE LABORATOIRE ELECTRONIQUE
ACTIVE DIRECTORY
SOBRIETE NUMERIQUE


ACTIVE DIRECTORY

Rappels

- Microsoft Active Directory (AD), qu'est-ce que c'est ?
- Structurer l'Active Directory
- Sécuriser l'Active Directory
 - les règles de bonnes pratiques
 - les outils d'audit et de supervision
- Sauvegarder l'AD
- Créer et gérer des GPO
- Créer et gérer des GPO avec filtres WMI
- Comment sauvegarder et restaurer l'AD
- Comment remonter les clés BITLOCKER dans l'AD
- Comment joindre un poste Linux au domaine AD
- Implémenter la séparation des tiers dans l'AD avec LAPS
- Gérer la sécurité au sein de l'AD
- Les outils d'audit et de sécurité de l'AD

Rappels sur Active Directory et travaux du GT

Microsoft Active Directory (AD), qu'est-ce que c'est ?


 Selon l'ANSSI, l'AD est un service d'annuaire introduit par Microsoft sous Windows 2000 Serveur. Il permet de centraliser des informations relatives aux utilisateurs et aux ressources d'un SI.


L'AD permet de déclarer et de gérer des comptes et des groupes d'utilisateurs ayant accès au SI ainsi que d'autres ressources comme les serveurs, les postes de travail, les imprimantes, les domaines, ...

Par conséquent, l'AD permet aux utilisateurs d'accéder aux ressources avec des mécanismes d'identification, d'authentification et d'autorisation. Pour que les ordinateurs puissent être gérés par l'AD et bénéficier des stratégies GPO, ils doivent être intégrés à un "DOMAINE" AD.

Des services AD comme l'authentification, l'annuaire, la réplication sont portés par des contrôleurs de domaine AD.

Structurer l'Active Directory

 1. Structure cohérente de l'AD avec le regroupement logique en OU = Unités d'Organisation (groupes d'ordinateurs, d'utilisateurs).

 2. Création de GPO en fonction de la structure de l'AD afin de lier une stratégie de groupe à une unité d'organisation, à un domaine ou à un site.



Fin

- ▶ Merci pour votre attention !

AVEZ-VOUS DES QUESTIONS ?

