UTOPIOS®
TRANSFORMATION DIGITALE INTELLIGENTE

Formation PCA/PRA

Outils Open Source

Programme de la Formation

- Introduction : Pourquoi l'open source
- Module 1 : Sauvegarde et restauration
  - BorgBackup
  - Restic
  - Bareos
  - Proxmox Backup Server
- Module 2 : Haute disponibilite
  - DRBD
  - Pacemaker / Corosync
  - HAProxy / Keepalived
- Module 3 : Detection et reponse
  - Wazuh (SIEM/XDR)
  - ELK / OpenSearch
  - Velociraptor
  - Outils forensic
- Module 4 : Supervision et documentation
  - Prometheus / Grafana
  - Uptime Kuma
  - Wiki.js / Netbox
- TP Final : Infrastructure complete

UTOPIOS®
TRANSFORMATION DIGITALE INTELLIGENTE

Introduction

Pourquoi l'open source pour le PCA/PRA

Avantages de l'open source

Cout

- Pas de licence a payer
- Reduction du TCO (Total Cost of Ownership)
- Budget reallouable vers expertise et formation

Flexibilite

- Personnalisation possible du code
- Integration facilitee via APIs ouvertes
- Pas de vendor lock-in

Transparence

- Code auditable (securite)
- Communaute active pour les corrections
- Documentation communautaire abondante

Inconvenients a considerer

Support

- Pas de support editeur garanti (sauf offres commerciales)
- Dependance aux competences internes
- Communaute parfois lente a repondre

Maturite variable

- Certains projets instables ou abandonnes
- Documentation parfois insuffisante
- Interface utilisateur souvent spartiate

Competences

- Necessite des equipes formees
- Courbe d'apprentissage parfois raide
- Integration a faire soi-meme

Criteres de choix d'un outil

Critere	Questions a se poser
Activite projet	Derniere release ? Frequence commits ?
Communaute	Taille ? Reactivite sur issues ?
Documentation	Complete ? A jour ? Tutoriels ?
Securite	CVE recentes ? Politique disclosure ?
Integration	APIs ? Plugins ? Compatibilite ?
Offre commerciale	Support pro disponible si besoin ?

Conseil : Verifier le projet sur GitHub avant adoption

UTOPIOS®
TRANSFORMATION DIGITALE INTELLIGENTE

Module 1

Sauvegarde et Restauration

Les fondamentaux - Regle 3-2-1-1-0

Chiffre	Signification
3	3 copies des donnees (prod + 2 sauvegardes)
2	Sur 2 types de supports differents
1	1 copie hors site (ou cloud)
1	1 copie offline/immuable (air-gapped)
0	0 erreur lors des tests de restauration

Point cle

Une sauvegarde non testee n'est pas une sauvegarde.
Planifier des tests de restauration reguliers (mensuel minimum).

Types de sauvegarde

Sauvegarde complete (Full)

- Copie integrale des donnees
- Restauration simple et rapide
- Consomme beaucoup d'espace et de temps

Sauvegarde incrementale

- Uniquement les modifications depuis derniere sauvegarde
- Rapide et econome en espace
- Restauration plus complexe (chaine de dependances)

Sauvegarde differentielle

- Modifications depuis derniere sauvegarde complete
- Compromis entre les deux approches
- Restauration : full + derniere differentielle

RTO et RPO - Rappel

RPO (Recovery Point Objective)

- Perte de donnees maximale acceptable
- Determine la frequence des sauvegardes
- Exemple : RPO 4h = sauvegarde toutes les 4h minimum

RTO (Recovery Time Objective)

- Temps maximal de restauration acceptable
- Influence le choix de la solution
- Exemple : RTO 2h = restauration complete en moins de 2h

Impact sur le choix des outils

- RPO court : replication temps reel, sauvegardes frequentes
- RTO court : infrastructure de secours, restauration automatisee

BorgBackup - Presentation

Solution de sauvegarde avec deduplication et compression.

Points forts

- Deduplication au niveau bloc (tres efficace)
- Chiffrement AES-256 cote client
- Compression (lz4, zstd, lzma)
- Verification d'integrite
- Montage FUSE des archives

Cas d'usage

- Sauvegarde de serveurs fichiers
- Sauvegarde de bases de donnees (dumps)
- Sauvegarde de configurations

BorgBackup - Installation

```
# Debian/Ubuntu
sudo apt update
sudo apt install borgbackup

# CentOS/RHEL
sudo yum install epel-release
sudo yum install borgbackup

# Via pip (version recente)
pip install borgbackup
```

Initialisation d'un depot

```
# Depot local chiffre
borg init --encryption=repokey /chemin/vers/backup

# Depot distant (SSH)
borg init --encryption=repokey ssh://user@serveur/chemin/repo
```

BorgBackup - Creer une sauvegarde

```
# Sauvegarde basique
borg create /backup::archive-{now} /donnees/a/sauvegarder

# Sauvegarde avec exclusions et stats
borg create --stats --progress \
    --exclude '*.tmp' \
    --exclude '/home/*/.cache' \
    /backup::srv-{hostname}-{now:%Y-%m-%d} \
    /etc /home /var/www

# Sauvegarde distante
borg create ssh://backup@serveur/repo::archive-{now} /donnees
```

Bonne pratique : Nommer les archives avec date et hostname

BorgBackup - Restauration

```
# Lister les archives
borg list /backup

# Voir le contenu d'une archive
borg list /backup::archive-2024-01-15

# Restaurer une archive complete
cd /restore
borg extract /backup::archive-2024-01-15

# Restaurer un fichier specifique
borg extract /backup::archive-2024-01-15 home/user/document.pdf

# Monter une archive (lecture seule)
mkdir /mnt/backup
borg mount /backup::archive-2024-01-15 /mnt/backup
```

BorgBackup - Politique de retention

```
# Appliquer une politique de retention
borg prune --stats \
    --keep-daily=7 \
    --keep-weekly=4 \
    --keep-monthly=6 \
    /backup

# Liberer l'espace disque
borg compact /backup
```

Options de retention

Option	Description
--keep-daily	Nombre de sauvegardes journalieres
--keep-weekly	Nombre de sauvegardes hebdomadaires
--keep-monthly	Nombre de sauvegardes mensuelles
--keep-yearly	Nombre de sauvegardes annuelles

BorgBackup - Script automatise

```
#!/bin/bash
# /usr/local/bin/backup-borg.sh

set -e

export BORG_REPO="ssh://backup@nas.local/volume1/backups/serveur-web"
export BORG_PASSPHRASE="MotDePasseComplexe"

BACKUP_NAME="backup-{hostname}-{now:%Y-%m-%d_%H%M%S}"

# Creer la sauvegarde
borg create --stats --compression zstd \
    --exclude '/var/cache/*' \
    --exclude '*.log' \
    ::$BACKUP_NAME /etc /home /var/www

# Appliquer la retention
borg prune --stats --keep-daily=7 --keep-weekly=4 --keep-monthly=12

# Verifier l'integrite
borg check --last 1
```

Crontab : `0 2 * * * /usr/local/bin/backup-borg.sh`