DebConf '26
SANTA FE | ARGENTINA

# *PVE Promox* Virtualization Platform

## DevOps Milestones in Branch Virtual Infrastructure

*Ansible-driven Promox VE cluster automation across 285+ branch locations*

`2022-10-22` -> `2026-07-07`

# Platform Overview

| Metric | Value |
|---|---|
| Total Releases (since 2022-10-22) | `17` |
| Playbooks | box-all / box-pve / box-vms / pve-update / vms-* |
| Target Hypervisor | *Promox* VE (Debian-based) |
| Key Roles | *Promox* / *ACSI* / auditd / nut / cloud-init |

## *FreeIPA* Server Migration Automation

Automating srep host migration between *FreeIPA* domains with zero downtime:

- `v0.9.1` (`2026-06`): Full playbook to migrate a srep from old -> new *FreeIPA* server
- `v0.9.0` (`2026-05`): `cloud-init` configuration for new *FreeIPA* domain bootstrap
- Fix vulnerabilities detected in **"Copy Fail"** and **"Dirty Tags"** compliance scans
- Automated *DNS* record updates during *IPA* migration lifecycle

# *ACSI* Compliance & Security Auditing

Continuous security compliance automation for *Promox* hosts:

- `v0.8.2` (`2026-04`): Updated *ACSI* role + auditd integration for security auditing
- `v0.8.1` (`2025-07`): Bumped *ACSI* role to v0.4.14 -- latest compliance ruleset
- `v0.6.1` (`2025-05`): *ACSI* role v0.4.9 deployment across *PVE* cluster
- `v0.5.5/4`: *ACSI* `v0.4.2` + auditd role name fix for requirements.yml
- Automatic audit rule generation and compliance report pipeline

# Kernel & Boot Stack Management

Automated kernel updates with safe initramfs regeneration:

- **initramfs regeneration**: Added task for safe initramfs rebuild after kernel updates
- Fix lint errors in regenerate-initramfs -- ensures idempotent execution
- Control flow added to skip regenerate on lint failures -- prevents broken boot images
- Safe upgrade path for *PVE* kernel without manual intervention per host

# *PVE* Box Image & Repository Infrastructure

Building and maintaining standardized *PVE* base images with correct repositories:

- **box-pve playbook**: Creates standardized *PVE* box images for *VM* deployment
- **box-all / box-vms**: Unified image generation across all *PVE* cluster nodes
- **tower-cli fix** (v0.5.4): Corrected *Promox* repository source in box-pve config
- **box wfw playbook** (v0.5.3): Implemented workflow for automated box creation pipeline
- Repository pinning ensures consistent *PVE* package versions across deployments

# *VM* Lifecycle & Cluster Management Playbooks

Comprehensive virtual machine management automation:

- **vms-delete-sans** (v0.7.0/v0.8.0): Automated *VM* cleanup -- delete sans VMs without git tracking
- **vms-delete-sgit**: Git-safe *VM* removal with automated resource reclamation
- **vms-backup-disk**: Cross-node *VM* backup disk orchestration
- **vms-startup-order**: Configurable *VM* startup sequence for cluster boot ordering
- **pve-kvm-state**: Real-time KVM *VM* state monitoring and reporting
- **pve-update**: Main playbook -- *PVE* host updates with NUT (UPS) integration

## Hardware Compatibility & Network Infrastructure

Expanding supported hardware and network stack automation:

- *Dell* `R350` compatibility( `v0.2.3/v0.5.2` ): Full support for *Dell PowerEdge* `R350` servers
- **Nut role integration** ( `v0.5.1` ): *UPS* monitoring and graceful shutdown automation
- **Cloud-init roles**: Automated *VM* provisioning with cloud-init metadata injection
- Network stack hardening alongside *Promox* package updates

# APT Source Configuration & Maintenance

Ensuring reliable package management across all *PVE* hosts:

- **Valid-Until fix** (v0.5.7): Handled apt indexes with Valid-Until attributes
- **Release info change** (v0.5.6): Fixed apt update to allow --allow-releaseinfo-change
- **Backports fix**: Corrected backports apt source in box-pve -- prevents package pinning issues
- Ensures *PVE* hosts stay updated without manual apt configuration intervention

# Timeline at a Glance

| Period | Version Range | Key Achievements |
|---|---|---|
| Mid 2023 | `v0.2.3-v0.5.1` | *Dell* `R350` compat, *Nut UPS* integration, `cloud-init` roles |
| Early 2024 | `v0.5.2-v0.5.7` | Box image pipeline, `apt` Valid-Until fix, `tower-cli` correction |
| Mid 2025 | `v0.6.0-v0.8.1` | *ACSI* compliance chain, backports fix, *VM* delete playbooks |
| 2026 | `v0.8.2-v0.9.1` | `initramfs` mgmt, `auditd` integration, *FreeIPA* migration automation |

# Core Playbook Modules (ansible_proxmox)

| Playbook | Purpose |
|---|---|
| `box-pve` | Create standardized *PVE* base box image |
| `box-all` | Generate box images across all cluster nodes |
| `box-vms` | *VM* template generation from *PVE* box |
| `pve-update` | Main *PVE* host update with NUT *UPS* integration |
| `vms-backup-disk` | Cross-node *VM* backup disk orchestration |
| `vms-delete-sans` | Automated sans *VM* cleanup (no git tracking) |
| `vms-delete-sgit` | Git-safe *VM* removal with resource reclamation |
| `vms-ipa-migrate` | Proxmox-side *FreeIPA* server migration |
| `vms-startup-order` | *VM* startup sequence configuration |
| `pve-kvm-state` | Real-time KVM *VM* state monitoring |

## References & Resources

- Site: https://filiales-gnu-linux.g.coop.ar/
- Code: https://gitlab.com/gcoop-libre | https://github.com/gcoop-libre
- Story: https://www.gcoop.coop/experiencia-exitosa/infraestructura-como-codigo-en-el-banco-credicoop

## 2026-07-21 How to Provision, Install, Configure, and Keep Thousands of Debian and Debian-Based Systems Updated

- Video: https://debconf26.debconf.org/talks/63-como-aprovisionar-instalar-configurar-y-mantener-actualizados-miles-de-sistemas-debian-y-basados-en-debian/
- Transcription: https://osiux.com/2026-07-21-debconf26-how-to-provision-install-configure-and-keep-thousands-of-debian-and-debian-based-systems-updated.html

## 2022-10-20 HowTo Migrate 6300 hosts to GNU/Linux using Ansible and AWX

- Video: https://www.youtube.com/embed/3hjQwbqCUP4
- Transcription: https://osiux.com/2022-10-20-howto-migrate-6300-hosts-to-gnu-linux-using-ansible-and-awx.html