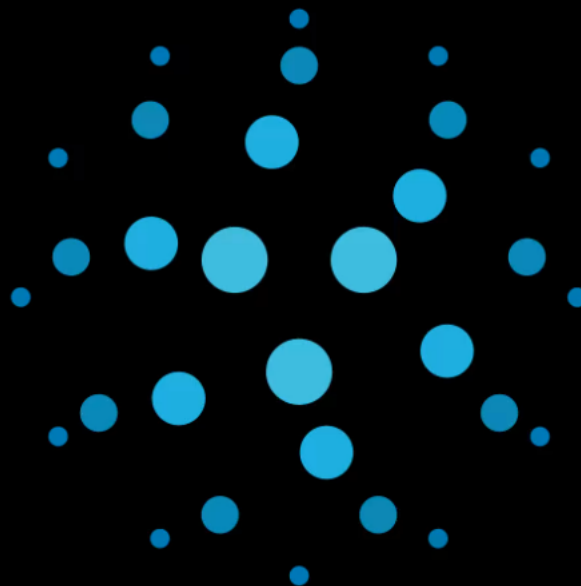




ANSIBLE



gcoop
cooperativa + software libre



DebConf '26
SANTA FE | ARGENTINA

How to Provision, Install, Configure, and Keep Thousands of Debian and Debian-Based Systems Updated

<https://filiales-gnu-linux.g.coop.ar/>

osiris@g.coop.ar

OSiUX



VPN



PVE



VMs



WST



IPA



ADs



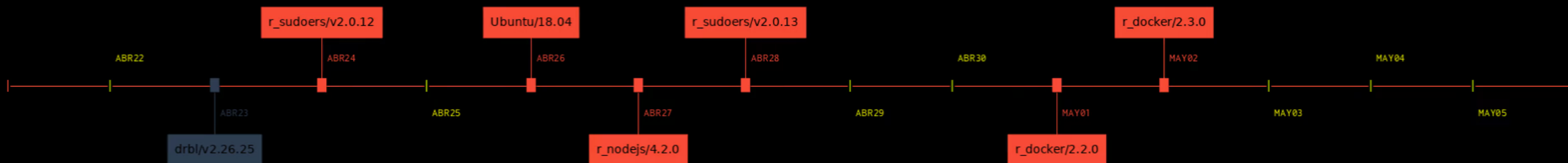
Ansible



git



AWX



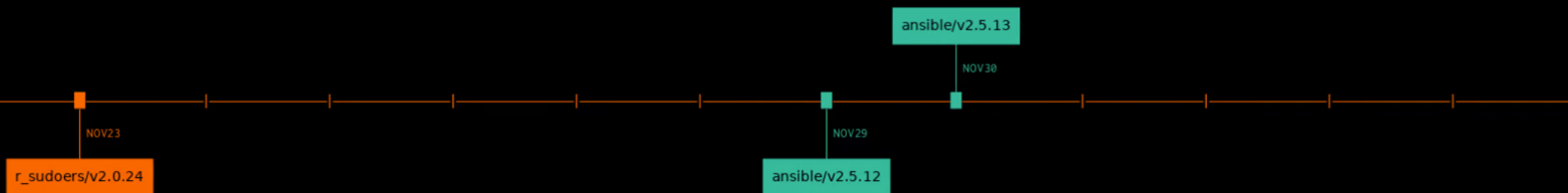
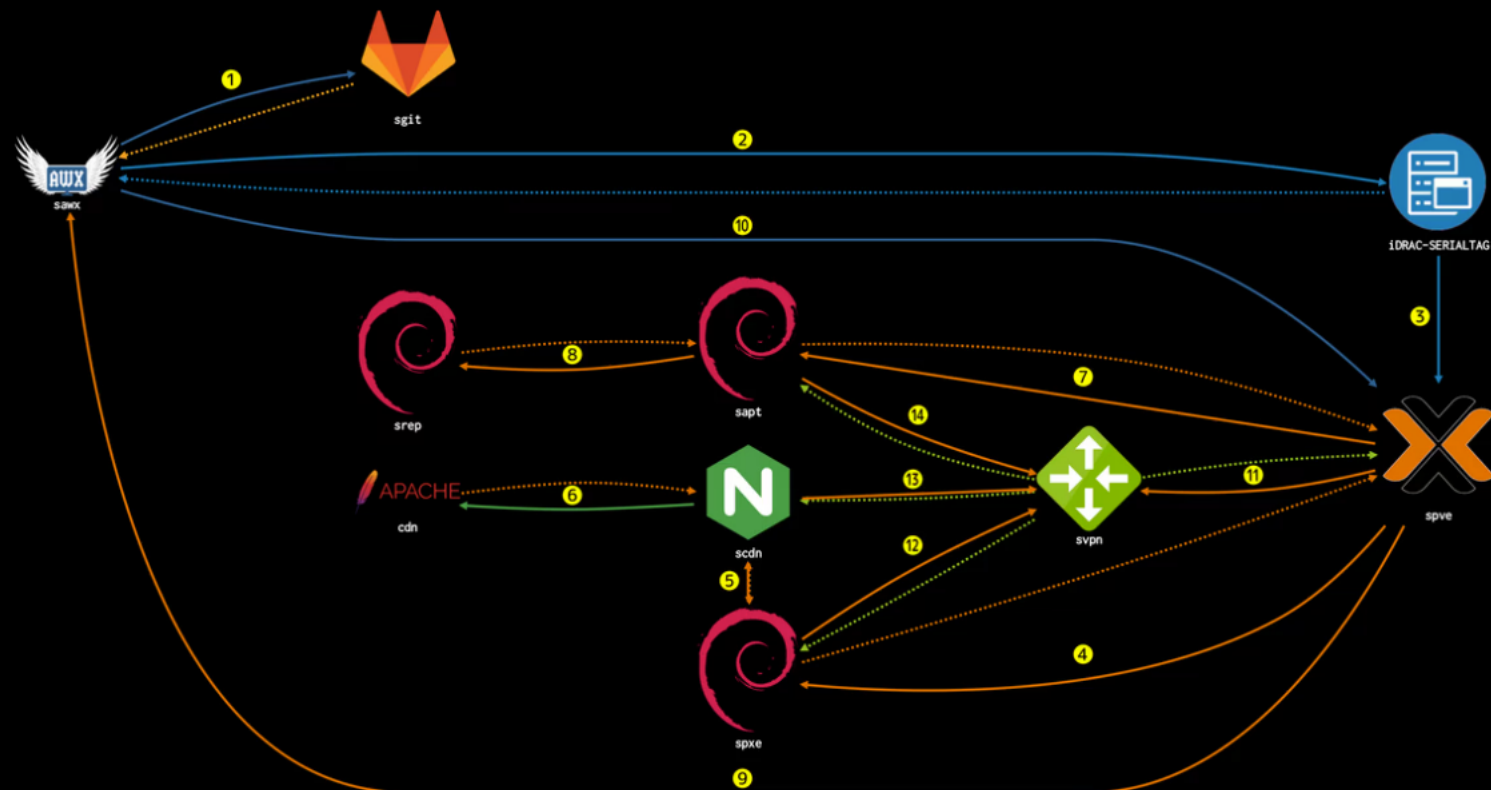
DebConf '26
SANTA FE | ARGENTINA

How to Provision, Install, Configure, and Keep Thousands of Debian and Debian-Based Systems Updated

<https://filiales-gnu-linux.g.coop.ar/>

osiris@g.coop.ar

©©© 0SiUX



DebConf '26
SANTA FE | ARGENTINA

How to Provision, Install, Configure, and Keep Thousands of Debian and Debian-Based Systems Updated

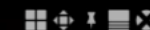
<https://filiales-gnu-linux.g.coop.ar/>

osiris@g.coop.ar

© © © 0SiUX

```
Apr 20 11:25:46 spxe05f0665 dhcpd[760]: DHCPDISCOVER from b4:96:91:65:bf:7f
Apr 20 11:25:47 spxe05f0665 dhcpd[760]: DHCPDISCOVER from b4:96:91:65:bf:7f
Apr 20 11:25:48 spxe05f0665 dhcpd[760]: DHCPDISCOVER from b4:96:91:65:bf:7f
Apr 20 11:25:49 spxe05f0665 dhcpd[760]: DHCPDISCOVER from b4:96:91:65:bf:7f
Apr 20 11:25:50 spxe05f0665 dhcpd[760]: DHCPDISCOVER from b4:96:91:65:bf:7f
Apr 20 11:25:51 spxe05f0665 dhcpd[760]: DHCPDISCOVER from b4:96:91:65:bf:7f
Apr 20 11:25:52 spxe05f0665 dhcpd[760]: DHCPDISCOVER from b4:96:91:65:bf:7f
Apr 20 11:25:53 spxe05f0665 dhcpd[760]: DHCPDISCOVER from b4:96:91:65:bf:7f
Apr 20 11:25:54 spxe05f0665 dhcpd[760]: DHCPDISCOVER from b4:96:91:65:bf:7f
Apr 20 11:26:03 spxe05f0665 dhcpd[760]: DHCPDISCOVER from b4:96:91:65:bf:7f
Apr 20 11:26:04 spxe05f0665 dhcpd[760]: DHCPREQUEST for 10.12.157.113 (10.12
```

OpenVNC - TigerVNC



Instalando el sistema base

83%

Instalando el núcleo - descargando e instalando linux-image-amd64...

```
10.12.157.113 - - [20/Apr/2022:11:26:07 -0300] "GET /preseed-pve.cfg HTTP/1.
```

```
[0] 0:~$
```

```
Ctrl + [Z] <g> LOCK [Z] <p> PANE [Z] <t> TAB [Z] <n> RESIZE [Z] <h> MOVE [Z] <s> SC
```

```
-- INTERFACE LOCKED --
```

```
— filiales — zellii [1] 01:35 |
```



DebConf '26
SANTA FE | ARGENTINA

How to Provision, Install, Configure, and Keep Thousands of Debian and Debian-Based Systems Updated

<https://filiales-gnu-linux.g.coop.ar/>

osiris@g.coop.ar

OSIUX

Almacenamiento

Descripción general



Resumen



Controladoras

Discos físicos

Agrupar por

Todos los discos

Elegir

Instrucciones:

- Es posible que la operación Parpadear/Dejar de parpadear no comience de inmediato.
- Para que comience a parpadear, seleccione uno o más LED de componente y haga clic en Parpadear. Para dejar de parpadear, seleccione uno o más LED de componente y haga clic en Dejar de parpadear.

Hacer parpadear

Dejar de hacer parpadear

☐	Condición	Nombre	Estado	Número de ranura	Tamaño	Estado d	
+	☐	☒	Solid State Disk 0:1:0	En línea	0	446.63 GB	No admit
+	☐	☒	Solid State Disk 0:1:1	En línea	1	446.63 GB	No admit
+	☐	☒	Physical Disk 0:1:2	En línea	2	1862.5 GB	No admit
+	☐	☒	Physical Disk 0:1:3	En línea	3	1862.5 GB	No admit



How to Provision, Install, Configure, and Keep Thousands of Debian and Debian-Based Systems Updated

DebConf '26
SANTA FE | ARGENTINA

<https://filiales-gnu-linux.g.coop.ar/>

osiris@g.coop.ar

OSiUX



```
Apr 20 11:24:53 spxe05f0665 in.tftpd[1563]: RRQ from 10.12.157.193 filename
Apr 20 11:24:53 spxe05f0665 in.tftpd[1564]: RRQ from 10.12.157.193 filename
Apr 20 11:24:53 spxe05f0665 in.tftpd[1565]: RRQ from 10.12.157.193 filename
Apr 20 11:24:53 spxe05f0665 in.tftpd[1566]: RRQ from 10.12.157.193 filename
Apr 20 11:24:53 spxe05f0665 in.tftpd[1567]: RRQ from 10.12.157.193 filename
Apr 20 11:24:53 spxe05f0665 in.tftpd[1568]: RRQ from 10.12.157.193 filename
Apr 20 11:24:53 spxe05f0665 in.tftpd[1569]: RRQ from 10.12.157.193 filename
Apr 20 11:24:53 spxe05f0665 in.tftpd[1570]: RRQ from 10.12.157.193 filename
Apr 20 11:24:53 spxe05f0665 in.tftpd[1571]: RRQ from 10.12.157.193 filename
Apr 20 11:24:53 spxe05f0665 in.tftpd[1572]: RRQ from 10.12.157.193 filename
Apr 20 11:24:53 spxe05f0665 in.tftpd[1573]: RRQ from 10.12.157.193 filename
```

```
[0] 0:tail*
```

OpenVNC - TigerVNC

```
GNU GRUB  version 2.02+dfsg1-20+deb10u2
```

```
*PVE: NIC enp1s0f3
PVE: NIC enp3s0f1
PVE: NIC eno1
PVE: NIC enp2
```

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the commands before booting or 'c' for a command-line.
The highlighted entry will be executed automatically in 3s.

Ctrl + **z** **<g>** LOCK **z****z** **<p>** PANE **z****z** **<t>** TAB **z****z** **<n>** RESIZE **z****z** **<h>** MOVE **z****z** **<s>** SC

-- INTERFACE LOCKED --

filiales zellii [] 01:32 t



How to Provision, Install, Configure, and Keep Thousands of Debian and Debian-Based Systems Updated

DebConf '26
SANTA FE | ARGENTINA

<https://filiales-gnu-linux.g.coop.ar/>

osiris@g.coop.ar

© © © oSiUX

wst_wlp_v1.0.0

JUGADAS 1

TAREAS 12

SERVIDORES 1

TIEMPO TRANSCURRIDO 00:00:25

EL TRABAJO AÚN SE ESTÁ EJECUTANDO

```
79 t", "path": "/etc/dconf/db/bccl.d/00_default_org_gnome_desk
79 top_background", "size": 642, "state": "file", "uid": 0}
79 ok: [wst661f0661] => (item=00_default_org_gnome_desktop_scr
79 eensaver) => {"ansible_loop_var": "item", "changed": false,
79 "checksum": "05049b6e2c7b195e22d6d94c275516b1c6178d16", "de
79 st": "/etc/dconf/db/bccl.d/00_default_org_gnome_desktop_scr
79 eensaver", "gid": 0, "group": "root", "item": "00_default_o
79 rg_gnome_desktop_screensaver", "mode": "0755", "owner": "ro
79 ot", "path": "/etc/dconf/db/bccl.d/00_default_org_gnome_des
79 ktop_screensaver", "size": 93, "state": "file", "uid": 0}
80
80
81 RUNNING HANDLER [gcoop-libre.wallpaper : dconf updat 19:08:31
81 e] *****
82 task path: /tmp/awx_19900_g76ac_hj/requirements_roles/gc
82 oop-libre.wallpaper/handlers/main.yml:1
83
83 changed: [wst661f0661] => {"changed": true, "cmd": ["dcon
83 f", "update"], "delta": "0:00:00.009977", "end": "2022-04-1
83 9 19:08:31.398225", "rc": 0, "start": "2022-04-19 19:08:31.
83 388248", "stderr": "", "stderr_lines": [], "stdout": "", "s
83 tdout_lines": []}
84
84 META: ran handlers
85
85 META: ran handlers
```

Server View

Datacente

spve01

100

102

103

104

105

106

107

109

110

111

661

662

663

664

665

666

900

bac

dat

loc

Virtual Machine 661 (wst) on node 'spve01f0218'

Start

Shutdown

Summary

Console

Hardware

Cloud-Init

Options

Task History

Monitor

Backup

Replication

Snapshots

Firewall

Permissions

Actividades

mar, 19 de abr, 19:09

gcoop

DebConf '26
SANTA FE | ARGENTINA

How to Provision, Install, Configure, and Keep Thousands of Debian and Debian-Based Systems Updated

<https://filiales-gnu-linux.g.coop.ar/>

osiris@g.coop.ar

OSiUX

VISTAS

Panel de control

Trabajos

Programaciones

Mi vista

RECURSOS

Plantillas

Credenciales

Proyectos

Inventarios

Scripts de inventario

ACCESO

Organizaciones

Usuarios

Equipos

ADMINISTRACIÓN

Tipos de credencial

Notificación

Trabajos de gestión

Grupos de instancias

INVENTARIOS / wst / SERVIDORES / wst661f0661

wst661f0661

DETALLES

EVENTOS

GRUPOS

TAREAS COMPLETADAS

* NOMBRE DE HOST ?

DESCRIPCIÓN

wst661f0661

Standard PC (i440FX + PIIX)

VARIABLES ?

YAML

JSON

EXPANDIR

1 ansible_host: 10.12.153.114

2 macaddress: '1a:fd:cf:c6:a7:cb'

3 hostname: wst661f0661

4

CANCELAR

GUARDAR

wst

DETALLES

PERMISOS

GRUPOS

SERVIDORES

FUENTES

TAREAS COMPLETADAS

BUSCAR

Q

CLAVE

EJECUTAR COMANDOS

+

wst66

LIMPIAR TODO

Server View

Datacenter

spve01

100

102

103

104

105

106

107

109

110

111

661

662

663

664

665

666

900

bac

dat

loc

Virtual Machine 661 (wst) on node 'spve01f0218'

Start

Shutdown

Summary

Console

Hardware

Cloud-Init

Options

Task History

Monitor

Backup

Replication

Snapshots

Firewall

Permissions

Actividades

mar, 19 de abr, 19:03

conky (wst661f0661.filiales.bancocredicoop.coop)

Usuario: adminws

Nombre de maquina: wst661f0661.filiales.bancocredicoop.coop

Filial: 661

Puesto: 661

Domnio: credicoop

Num. serie:

Procesador: Common KVM processor

Memoria RAM: 1,94GiB

Direccion IP: 10.12.153.114

Printer API: active

Scanner API: 1.25

Version Info:

project revision: 8d3ac1b3d2d4d98fab3680c8c96ab045d16f08fc

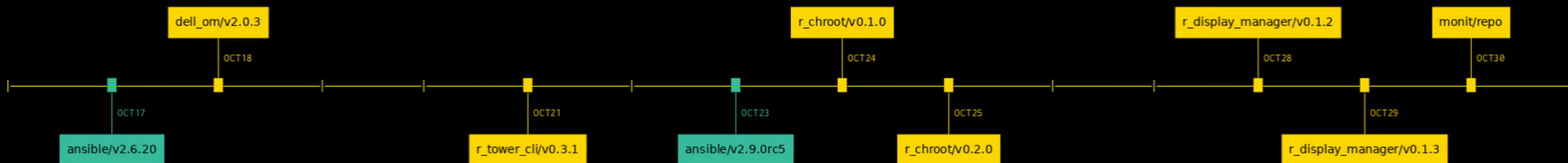
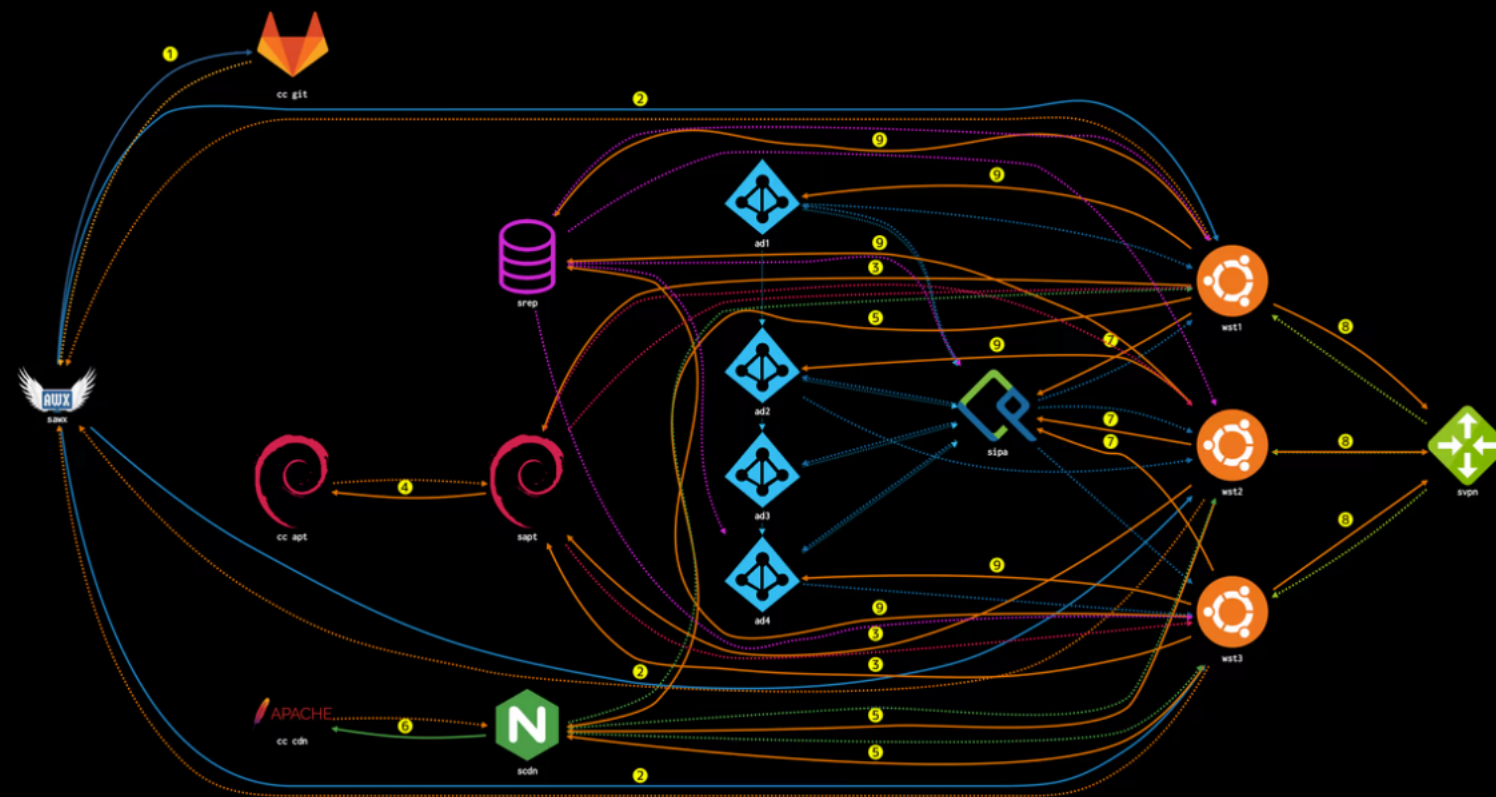
awx_job: 27952

awx_template: 1232 - wst_nip_v1.4.0

awx_inventory: 22 - wst

awx_user: admin





DebConf '26
SANTA FE | ARGENTINA

How to Provision, Install, Configure, and Keep Thousands of Debian and Debian-Based Systems Updated

<https://filiales-gnu-linux.g.coop.ar/>

osiris@g.coop.ar



CC BY-SA



<https://g.coop.ar/>

<https://github.com/gcoop-libre/ansible-role-deploy-git-repos>

<https://github.com/gcoop-libre/ansible-role-git-bare-repos>

<https://github.com/gcoop-libre/ansible-role-pure-ftpd>

https://github.com/gcoop-libre/ansible_role_sssd_conf

https://github.com/gcoop-libre/ansible_role_test_users

https://github.com/gcoop-libre/ansible_sudoers

https://gitlab.com/gcoop-libre/ansible_role_apt_pin

https://gitlab.com/gcoop-libre/ansible_role_freeipa_sssd_tools

https://gitlab.com/gcoop-libre/ansible_role_hp_linux_tools

https://gitlab.com/gcoop-libre/ansible_tools

<https://gitlab.com/gcoop-libre/freeipa-sssd-tools>





hardware

3000 wst HP ProDesk 400 G5

300 pve Dell PowerEdge R340

3000 vms Debian KVM Proxmox

6300 hosts



time / devops

180d	lab	2018-03-15	2018-09-17	2p
350d	dev	2018-09-17	2019-09-02	3p
365d	dep	2019-09-02	2020-09-01	4p
087d	stg	2020-09-01	2020-11-27	4p
347d	prd	2020-11-27	2021-11-09	5p
052d	sup	2021-11-09	2021-12-31	5p
292d	nxt	2022-01-01	2022-10-20	5p





3581 Peripherals

1460 Lexmark MS610 Printer

500 CTS-150 Scanner/Check

300 Samsung M4370 Scanner/Printer

500 Epson TM-U220D Ticket/Printer

275 TAT Self Service Terminal

546 VDB LCD Videos/Dolar/Queuing

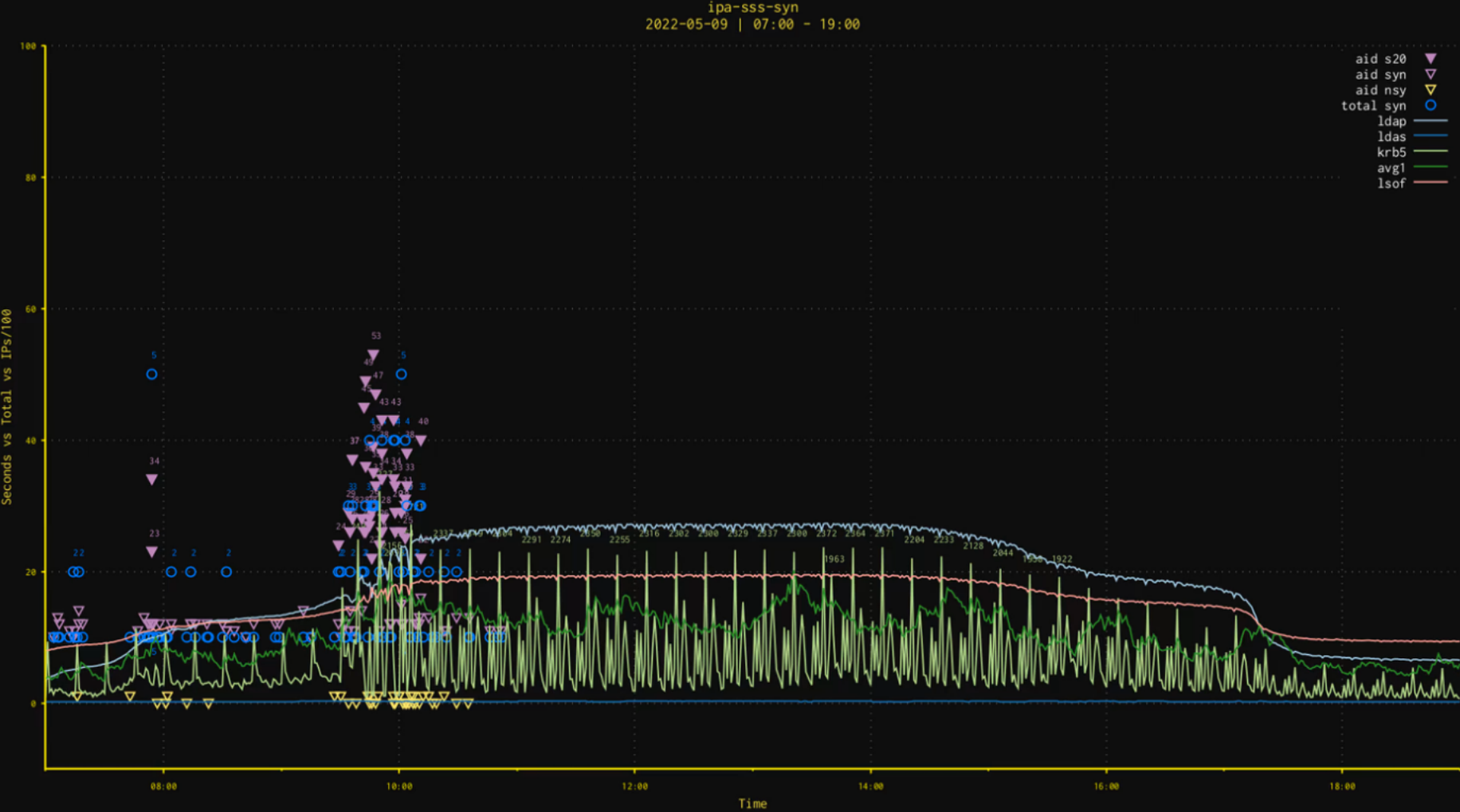
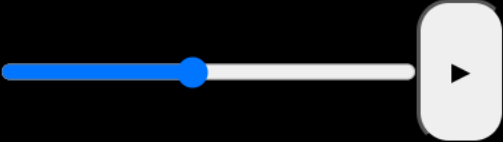




technology

ansible	2.9	centos	7
python	3.6	freeipa	4.6
awx	9.3	kernel	3.10
debian	10.9	ubuntu	18.04
pve	6.3	freeipa	4.7
kernel	5.4	kernel	4.15





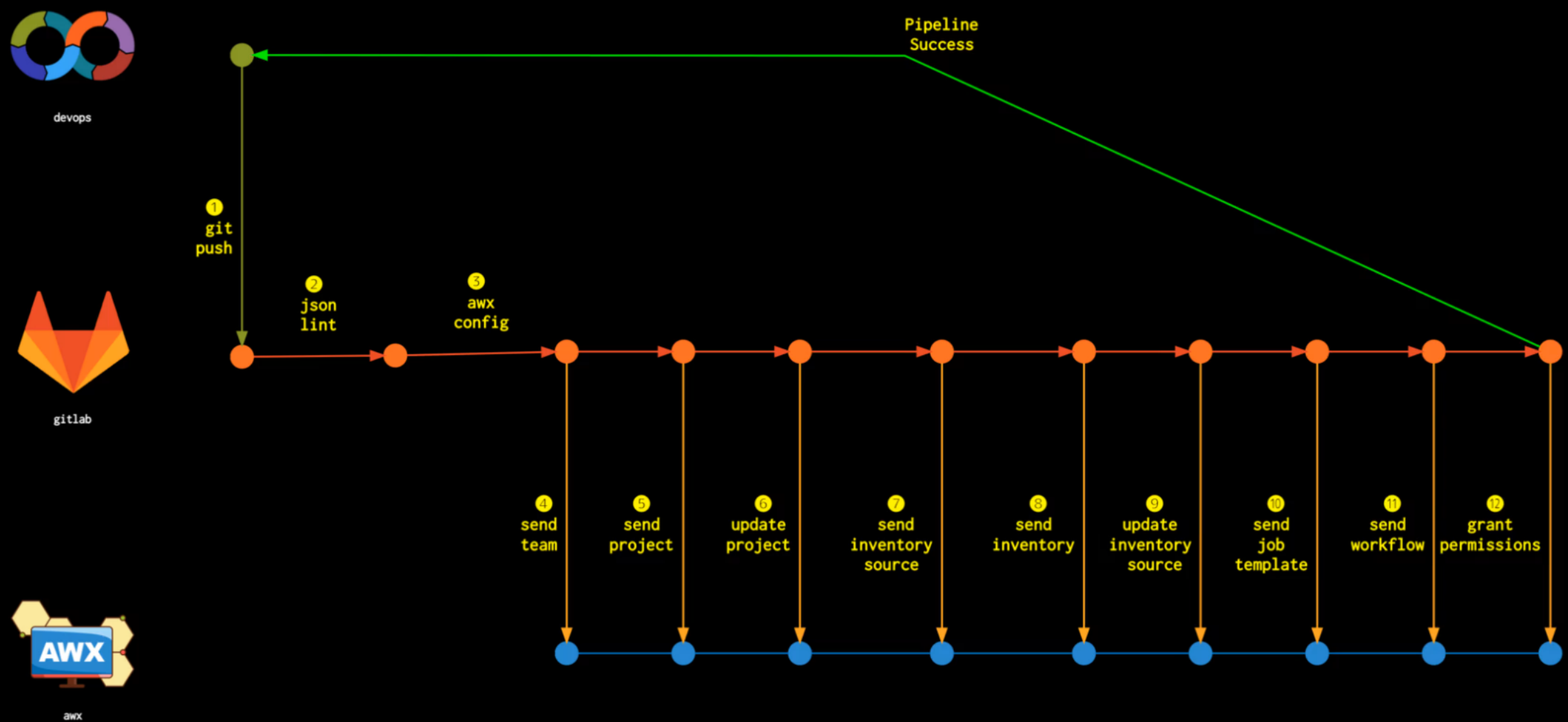
How to Provision, Install, Configure, and Keep Thousands of Debian and Debian-Based Systems Updated

DebConf '26
SANTA FE | ARGENTINA

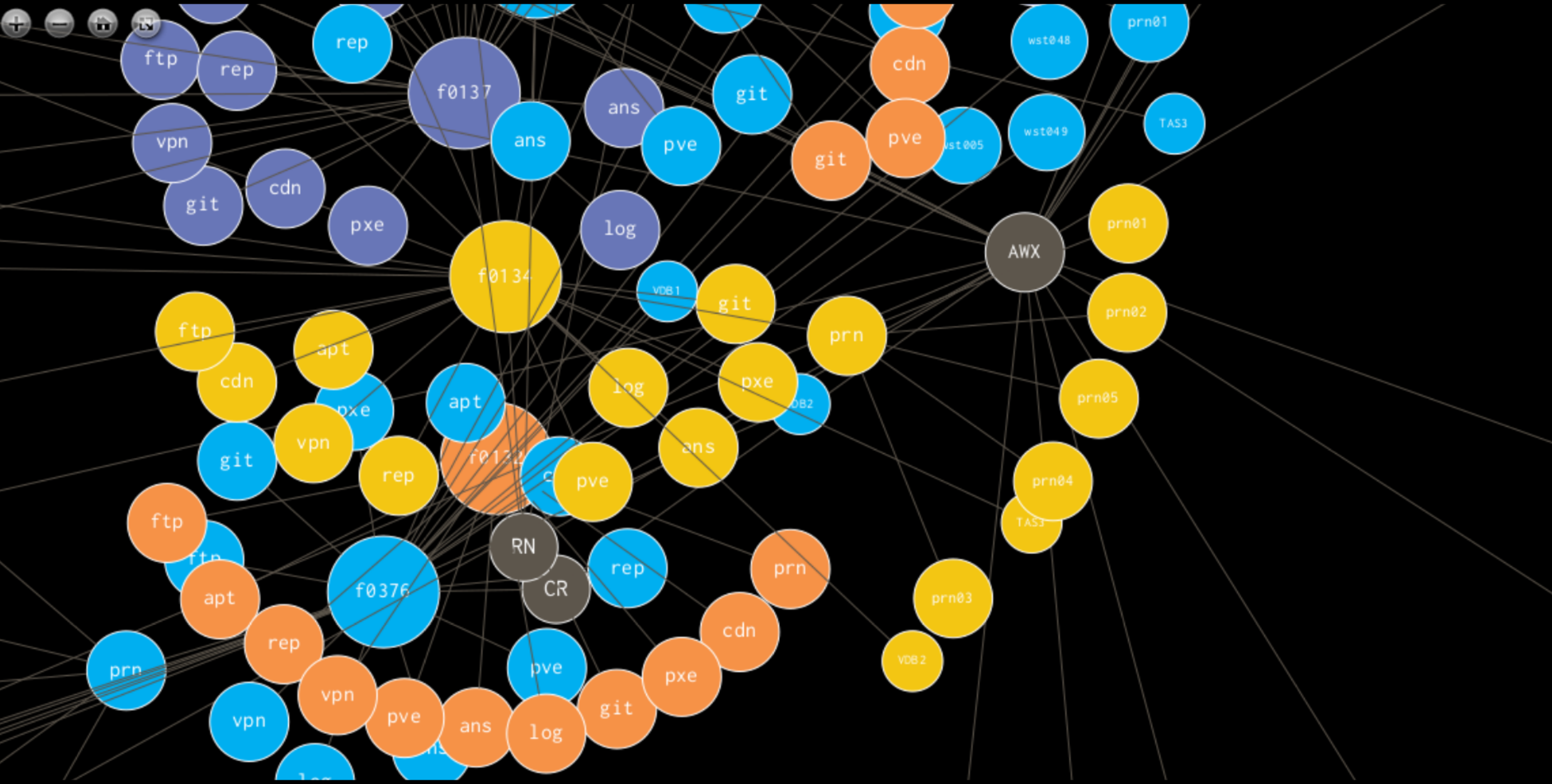
<https://filiales-gnu-linux.g.coop.ar/>

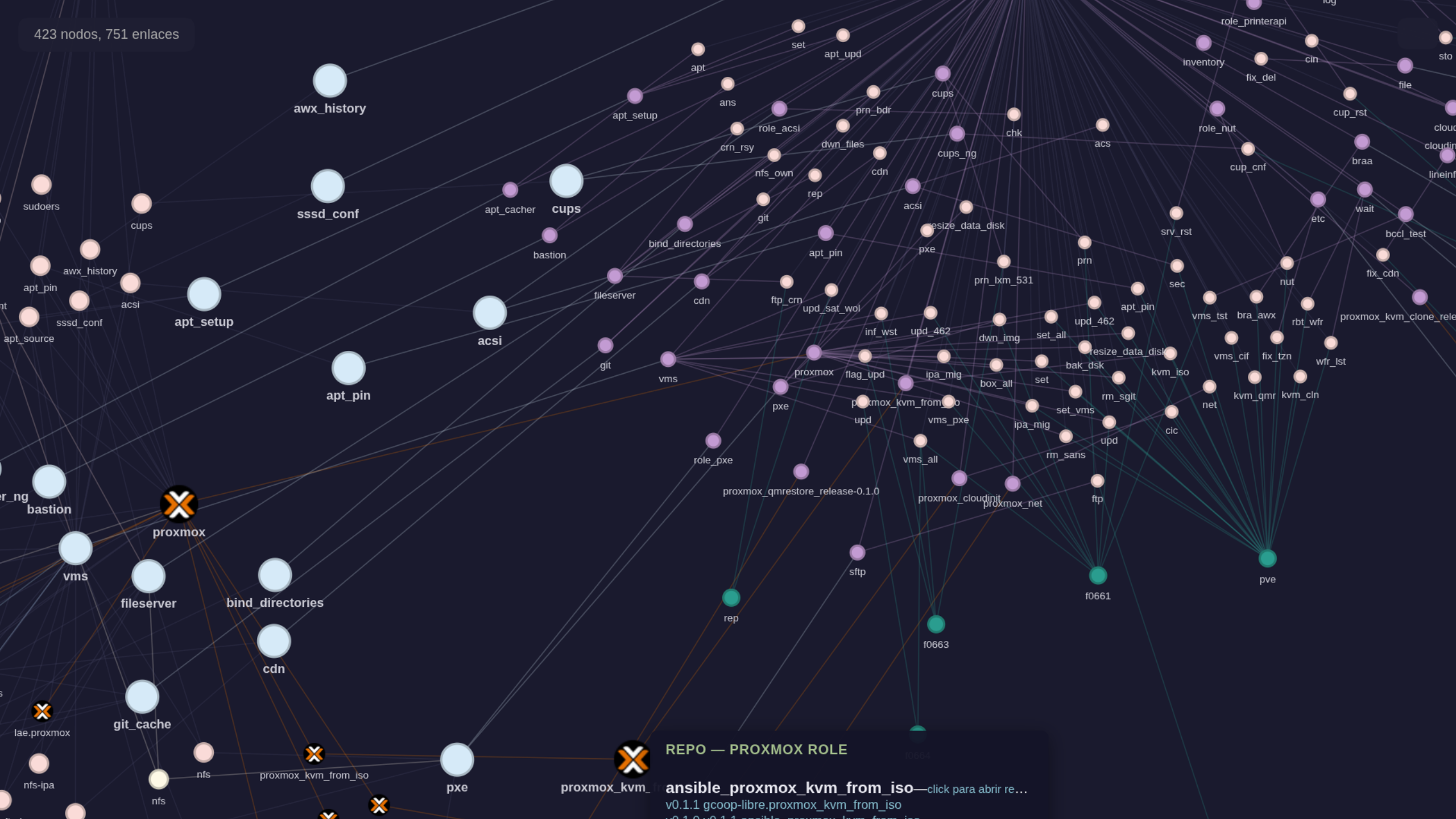
osiris@g.coop.ar

osix











Migration of 6,300+ Hosts to GNU/Linux

How to Provision, Install, Configure, and Keep Thousands of Debian and Debian-Based Systems Updated

DevOps Milestones & Automation Achievements

Based on gcoop & Banco Credicoop Infrastructure Project (2018–2022)



Project Scope & DevOps Objective

- **Scale:** 300 bank branches ~6,300+ workstations & servers
- **Goal:** Zero-downtime migration from legacy *W2K* to *GNU/Linux*
- **DevOps Approach:** Infrastructure as Code (*IaC*), Centralized Orchestration, *CI/CD* Pipelines, Automated Inventory & Compliance



Phase 1: Lab & Proof of Concept (6 months)

- Validated *FreeIPA* / *ActiveDirectory* integration for unified *SSO/auth*
- Proved *PXE netboot* → *Debian NetInstall* → *Proxmox* automation via *AWX*
- Defined target architecture: 1 bare-metal server + 10 KVM VMs per branch



Phase 2: Development & IaC (1 year)

- Built `>200` *Git* repositories (*playbooks, roles, AWX* configs)
- Automated server lifecycle: *iDRAC* control → *PXE* boot → *Proxmox* → *VM* provisioning
- Workstation strategy: Factory base image + *AWX*-driven config sync & enrollment
- Centralized inventory & job templates managed entirely via code (no GUI drift)



Phase 3: Staging & Validation (87 days)

- Full production simulation in a single branch with real hardware/traffic
- Validated peripheral compatibility (*scanners*, ticket printers, *POS* devices)
- Identified login concurrency bottleneck → implemented cache sync + *API* gateway
- Established deployment limits per branch to prevent *network/API* saturation



Phase 4: Production Rollout (347 days)

- Migrated 300 branches overnight (06:00–09:00 maintenance window)
- Zero manual provisioning; fully automated from *AWX* → target nodes
- Implemented *GitLab CI/CD* pipeline: *Dev* → *Staging* → *Production* (JSON template sync)
- Firewall/rule validation integrated via *JIRA* requests + *Ansible* compliance checks



Key Challenges & *DevOps* Solutions

Challenge	Solution
Dynamic <i>IP</i> /Network changes	<i>NetworkManager</i> Dispatcher + <i>SNMP</i> auto-updates <i>MAC/IP/host</i> in <i>AWX</i> inventory
Auth bottlenecks (2k+ simultaneous logins)	In-memory cache sync + <i>API gateway</i> → roadmap to <i>FreeIPA</i> cluster
Scale & parallelism	Dynamic job limits per branch; retry-on-failure with idempotent <i>playbooks</i>
Compliance & Auditability	100% <i>Git</i> versioning; <i>AWX</i> execution <i>logs</i> ; immutable infrastructure pattern



Tech Stack & Automation Pipeline

- **Provisioning:** *PXE, Debian NetInstall, Proxmox VE, KVM*
- **Orchestration:** *Ansible + AWX (Central HQ Hub)*
- **Identity:** *FreeIPA / ActiveDirectory sync (SSSD)*
- **CI/CD & IaC:** *GitLab CI, AWX REST API/CLI, JSON template export*
- **Inventory/Monitoring:** *SNMP traps, NetworkManager Dispatcher, Dynamic AWX inventory plugins*



Impact & Current State

- 99% automated migration; 1% manual intervention post-rollout
- Consistent, auditable, and reproducible infrastructure across all branches
- Open-sourced >30 Ansible roles & tools via gcoop (*GitHub/GitLab*)
- Ongoing: *FreeIPA* cluster deployment, *CI/CD* hardening, continuous improvement



AWX Automation Platform

DevOps Milestones & Project Evolution

Branch infrastructure automation across 285+ locations

2022-10-22 → 2026-07-07



Platform Overview

Metric	Value
Releases since 2022-10-22	198
Job Templates	155
Projects	201
Inventories	13



Foundation & Core Automation

45 *releases*

- First *Proxmox* workflows + *Dell* R350 server compatibility
- Initial workstation automation (`wst_upd` v1.7 / `wst_ipa`)
- *AWX* project scaffold + core team permissions (`awx-test/gcoop/impl/mant/trans`)
- `sysctl` *hardening* — source route & *ICMP* redirect blocking



Workstation Ecosystem

47 *releases*

- *FreeIPA SSSD* tools automation — auto-start `krb5kdc/httpd` services
- *PXE Clonezilla* `boot` — *WST* remote recovery/clone via network
- *Wake-On-Lan* batch deployment with *SSH* readiness check
- *Firefox* migration: `v68` → `v120` (`ffox120`) with isolated profiles



Service Expansion

16 *releases*

- CCTV camera provisioning — dedicated inventory + job templates
- Printer service automation — `ppd` from *CDN*, `cups_ng` configuration
- *HP Linux Tools* detection via *BIOS* Admin Password + *WakeOnLAN* workflow
- *ACSI* rules deployment with automatic octal file mode conversion



Security & Compliance

18 *releases*

- `sec_chk` job template — automated *ACSI* compliance reporting
- *ACSI* role refactor + `xcontrol` users sudoers management
- *WST* `v1.8.1` / *Firefox* `120` rollout / *WST* image `v1.9.0`
- *Git* access token rotation for `sgit` VM credentials



Infrastructure Modernization

16 *releases*

- *PVE* workflow → *playbook* refactor — idempotent deployments
- *Debian Installer* v11 update (build 20210731-deb11u10)
- *CMDB* facts collection: *WST* hardware, disk, network detection
- *Ansible_vms* v0.7.0 — full *VM* generation on *Proxmox*



Scale & Reliability

40 *releases*

- `wst_upd` `1.8.x` incremental series with *SREP* rollback flag support
- *ACSI* rules bugfixes — automatic file mode octal resolution
- *Lexmark* `531→610` printer driver replacement automation
- `wst_upd` `v1.8.11` / `wst_ffx` `v0.5.0` — inventory `v0.48.0`



Current State

16 *releases*

- Versioned project names (`ansible_wst_v1.8.13` + `wst_upd_v1.8.13`)
- *ACSI* `v0.4.16` + `auditd` `v0.1.0-filiales` role updates
- *Inventory* `v0.52.0` — multi-team grants across 6 teams
- *FreeIPA* server migration templates (*PVE* + *VMS* + *WST* branches)



Impact by the Numbers

Category	Scope	Releases
Workstation Automation	<code>wst_upd 1.7 → 1.8.x</code>	16
<i>FreeIPA</i> Integration	<i>SSSD</i> + <i>DNS</i> + migration	37
CCTV Deployments	Full lifecycle management	14
ACSI Compliance	<code>sec_chk</code> + automated reporting	15



Timeline at a Glance

Period	Version Range	Focus
2022-23	v0.10-v0.67	Workstation + <i>FreeIPA</i> foundation
2024	v0.68-v0.89	Security, <i>ACSI</i> , <i>Firefox</i> 120 , <i>PVE</i> refactor
2025	v0.90-v0.97	Scale, reliability, <i>wst_upd</i> 1.8.x series
2026	v0.98-v0.106	<i>ACSI</i> v0.4 , inventory automation, <i>IPA</i> migration



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	<i>Dell</i> R350 compat, <i>Nut UPS</i> integration, <code>cloud-init</code> roles
Early 2024	v0.5.2-v0.5.7	Box image pipeline, <code>apt</code> Valid-Until fix, <code>tower-cli</code> correction
Mid 2025	v0.6.0-v0.8.1	ACSI compliance chain, backports fix, VM delete playbooks
2026	v0.8.2-v0.9.1	<code>initramfs</code> mgmt, <code>auditd</code> integration, <i>FreeIPA</i> migration automation



Core Playbook Modules (ansible_proxmox)

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



WST Workstation Automation

DevOps Milestones in Branch Desktop Infrastructure

Ansible-driven workstation lifecycle management across 285+ branch locations

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



Platform Overview

Metric	Value
Total Releases (since 2022-10-22)	21
Playbooks	wst- * series 50+ modules
Supported Browsers	Firefox v68 / Firefox v120 / Chrome
Base OS	Ubuntu Desktop (kernel v5.15+)



FreeIPA & Authentication Integration I

Enabling secure, network-bound workstation identity across all branches:

- `wst-ipa` *playbook* (`v1.7.0`): Created join/unjoin lifecycle for *FreeIPA* domain membership
- `wst-nip` *playbook*: Automated network interface configuration alongside *IPA* enrollment
- `apt_pin` *role* (`v1.7.4`): Pinned critical packages to prevent version drift in *IPA* stack



FreeIPA & Authentication Integration II

Enabling secure, network-bound workstation identity across all branches:

- `wst-ipa-uninstall` (`v1.7.5` → `1.7.7`): Full unenrollment with *DNS* `A` record cleanup automation
- `wst-sssd-service` : Ensures `After=network-online.target` ordering + automatic restart on failure
- `fix_owner_fix` (`v1.7.16`): Skip backup when user folder in `srep` is empty prevents cascading failures



Browser Strategy: *Firefox* + *Chrome*

Supporting parallel browser ecosystems for diverse branch requirements:

- *Firefox* role integration: (`v1.7.3`): Policies, preferences, and extension management
- *Firefox* `v68` → `v120` migration: Dual-version support with isolated profiles per user
- *Chrome* rollout: Parallel deployment alongside *Firefox* for branches requiring Chromium-based features
- `wst-ffox-policies` + `wst-ffox-prefs` : Centralized browser policy enforcement via *ADMX* templates
- *Proxy* configuration (`wst-ffox-check-proxy`): Dynamic proxy detection and failover



Deployment Reliability & Resilience

Building fault-tolerant workstation deployment chain:

- **wst-wol-all**: Wake-On-Lan batch deployment delegated to spve of each group no manual intervention
- **WOL + Wait-for integration** (v1.7.19): Native sleep/reboot tasks in wst-update with configurable timeouts
- **Kernel upgrade** (v1.8.0): Base image moved to kernel v5.15 for modern hardware support
- **wst-reboot**: Smart reboot playbook with optional no-wait mode - supports unattended deployments
- **sftp-mount corrections** (v1.7.11): Reliable fileservers for branch shared resources



Security & Identity Health Monitoring

Continuous authentication verification and credential lifecycle management:

- **wst-ipa-health-check** (v1.7.18): Full health probe chain WoL → SSH wait → ipa-hlt-chk in lightdm greeter-script-setup
- **wst-krb-chk** (v1.4.6): Kerberos keytab validation to prevent auth failures
- **wst-adminws groups/password management**: Centralized admin workspace provisioning with mac address binding
- **apparmor + dconf roles**: Mandatory access control and desktop configuration hardening
- **loginhelper role** (v1.5.0): Secure login notification with pre/post session hooks
- **sudoers role**: Centralized privilege escalation policy enforcement



SREP Integration rollback safety and auditability & Control

- **wst-full playbook:** Complete workstation image rebuild all roles in serial batch strategy
- **etc-keeper backport (v1.6.0):** `/etc` configuration versioning via etckeeper + check-only mode
- **srep backup awareness:** `fix_owner` skips empty `srep` folders, preventing false-positive rollback triggers
- **Serial batch deployment:** `wst-v1.5.0` introduced `serial: 1` for controlled rollout across groups
- **v1.8.0 kernel base + role bumps** (admin, apparmor, cups_ng, etc.): Unified update chain



Timeline at a Glance

Period	Version Range	Key Achievements
Oct 2022	v1.7.0–v1.6.0	wst-ipa + wst-nip playbooks created, etc-keeper backport
Early 2023	v1.7.4–v1.7.11	SSSD service management, IPA uninstall, sftp-mount, apt_pin
Late 2023	v1.7.14–v1.8.0	Firefox/Chrome parallel, kernel v5.15, health checks, WoL+Wait
2024+	v1.7.18–v1.7.19	WOL+WFL native in wst-update, reliability hardening



Core Playbook Modules (wst-* series)

Playbook	Purpose
wst-update	Main workstation role deployment chain
wst-full	Complete image rebuild all roles serial batch
wst-ipa	FreeIPA domain join/unjoin lifecycle
wst-nip	Network interface configuration
wst-adminws	Admin workspace + desktop provisioning
wst-desktop-launchers	Desktop shortcut management



Core Playbook Modules (wst-* series)

Playbook	Purpose
<code>wst-sssd-service</code>	SSSD service state & networking ordering
<code>wst-sftp-mount</code>	Secure fileserv share integration
<code>wst-wol-all</code>	Wake-On-Lan batch deployment
<code>wst-ipa-health-check</code>	Authentication health probe chain
<code>wst-kernel-upg</code>	Kernel version updates
<code>wst-krb-chk</code>	Kerberos keytab validation



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>