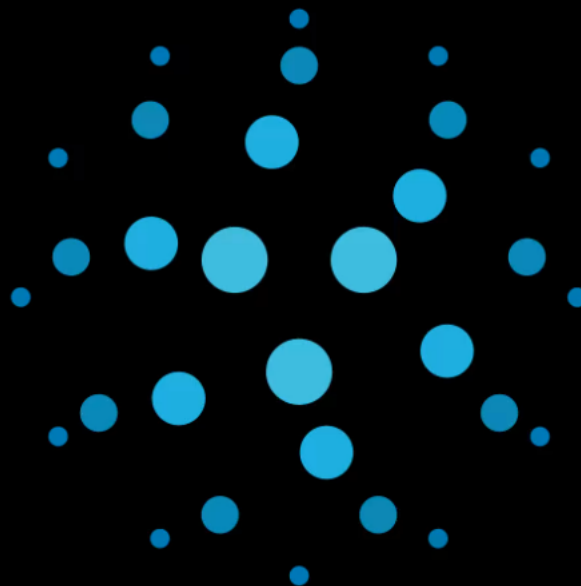




ANSIBLE



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



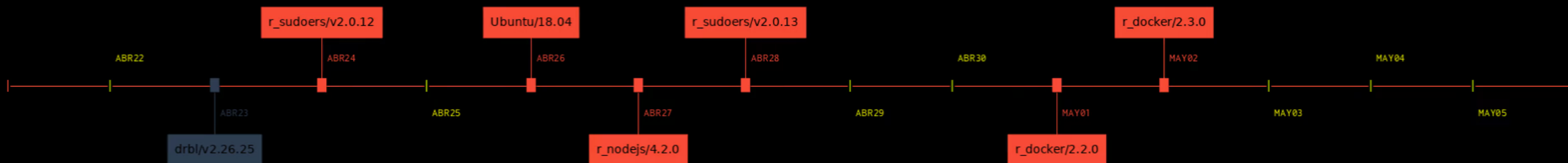
Ansible



git



AWX



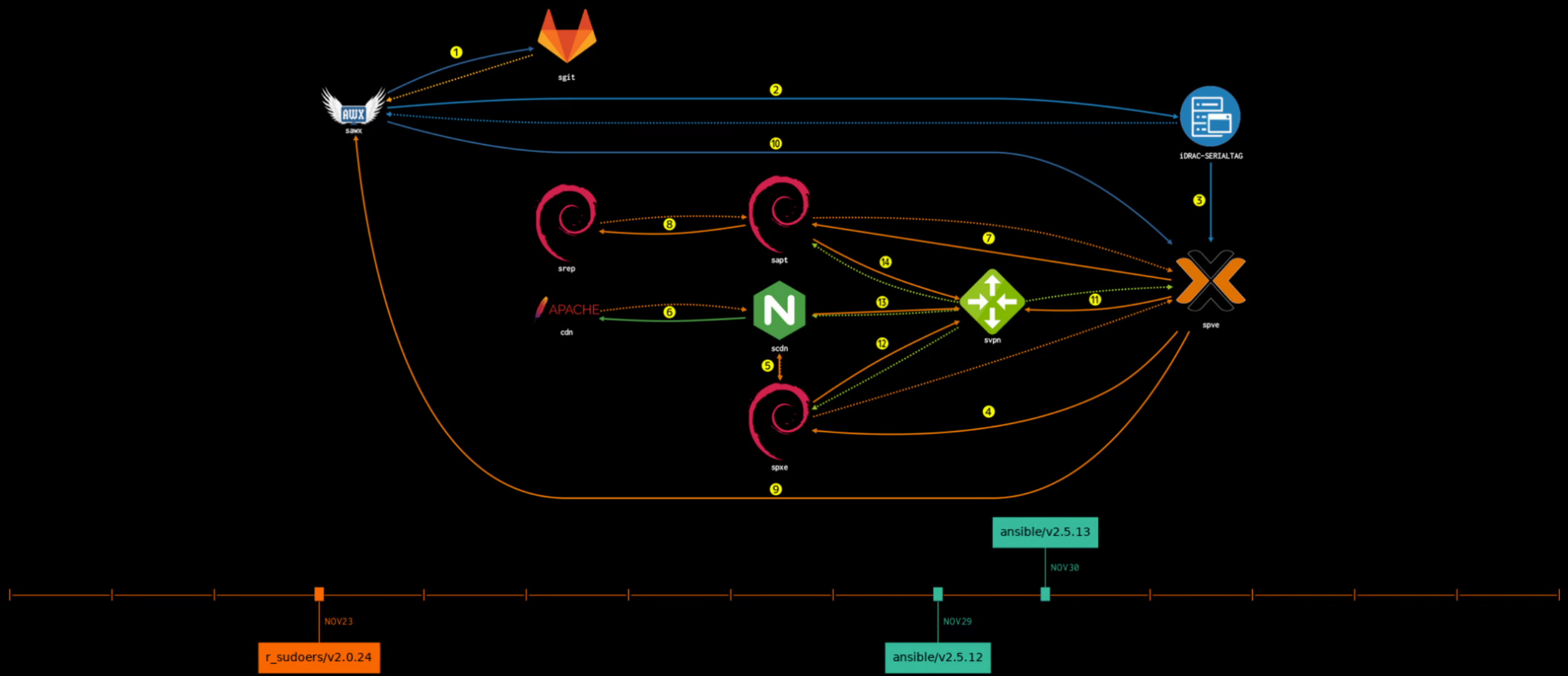
DebConf '26
SANTA FE | ARGENTINA

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



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

© 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: bash*
```

```
Ctrl + <g> LOCK <p> PANE <t> TAB <n> RESIZE <h> MOVE <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*
```

```
*PVE: NIC enp1s0f3
PVE: NIC enp3s0f1
PVE: NIC eno1
PVE: NIC eno2
```

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.

-22

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

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

```
— filiales — zellii [1 01:32 ]
```



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

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

x

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

Summary

Console

Hardware

Cloud-Init

Options

Task History

Monitor

Backup

Replication

Snapshots

Firewall

Permissions

Virtual Machine 661 (wst) on node 'spve01f0218'

Start

Shutdown

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

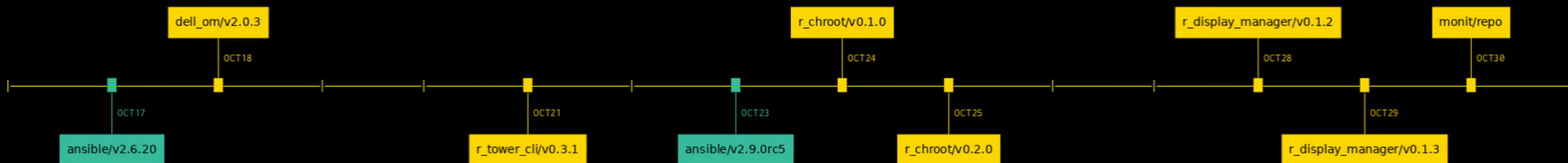
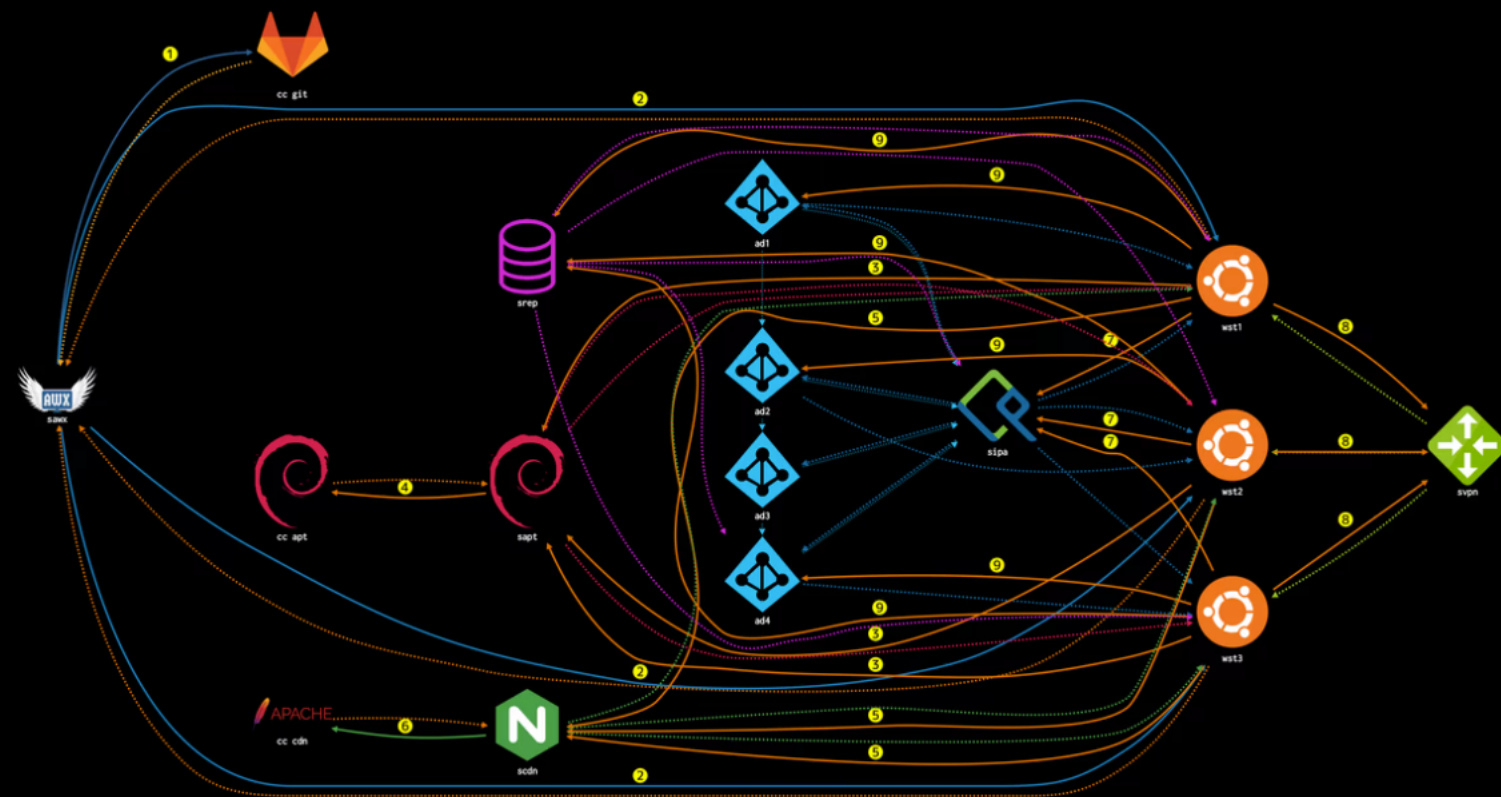
How to Provision, Install, Configure, and Keep Thousands of Debian and Debian-Based Systems Updated

DebConf '26
SANTA FE | ARGENTINA

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

osiris@g.coop.ar

OSIUX



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



<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

python 3.6

awx 9.3

centos 7

freeipa 4.6

kernel 3.10

debian 10.9

pve 6.3

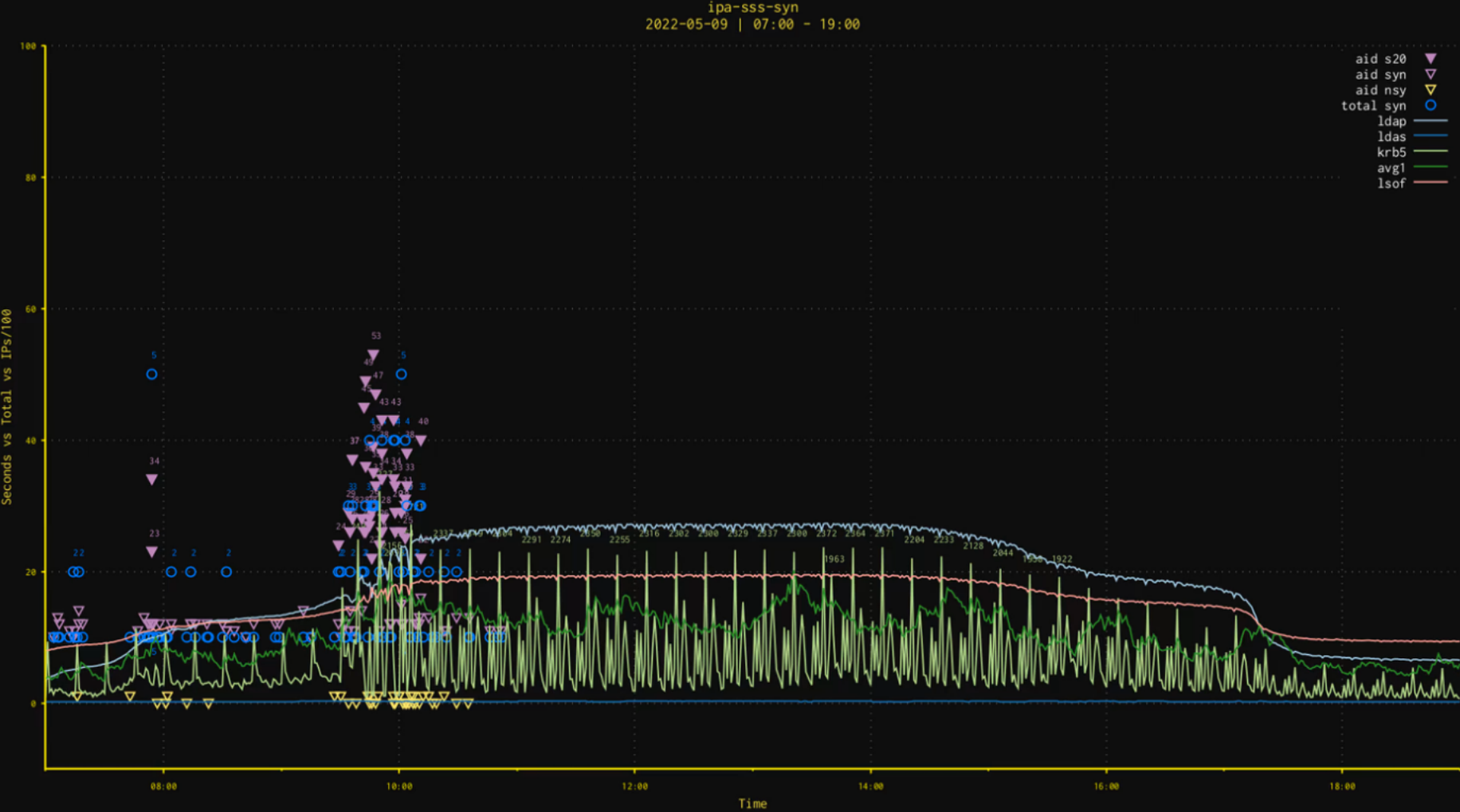
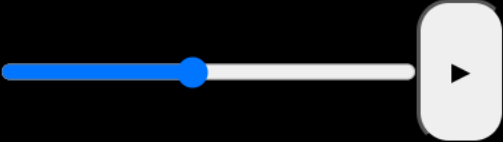
kernel 5.4

ubuntu 18.04

freeipa 4.7

kernel 4.15





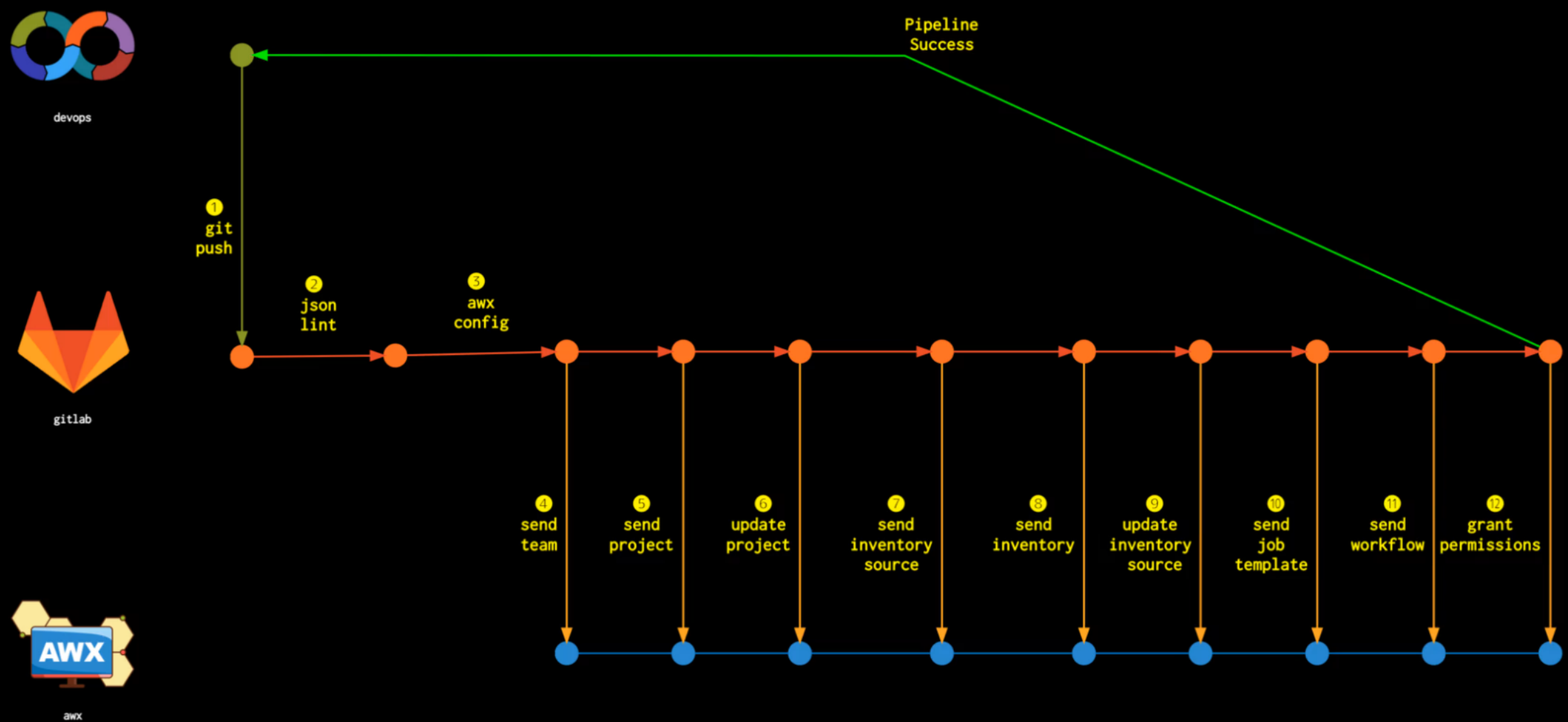
How to Provision, Install, Configure, and Keep Thousands of Debian and Debian-Based Systems Updated

DebConf '26
SANTA FE | ARGENTINA

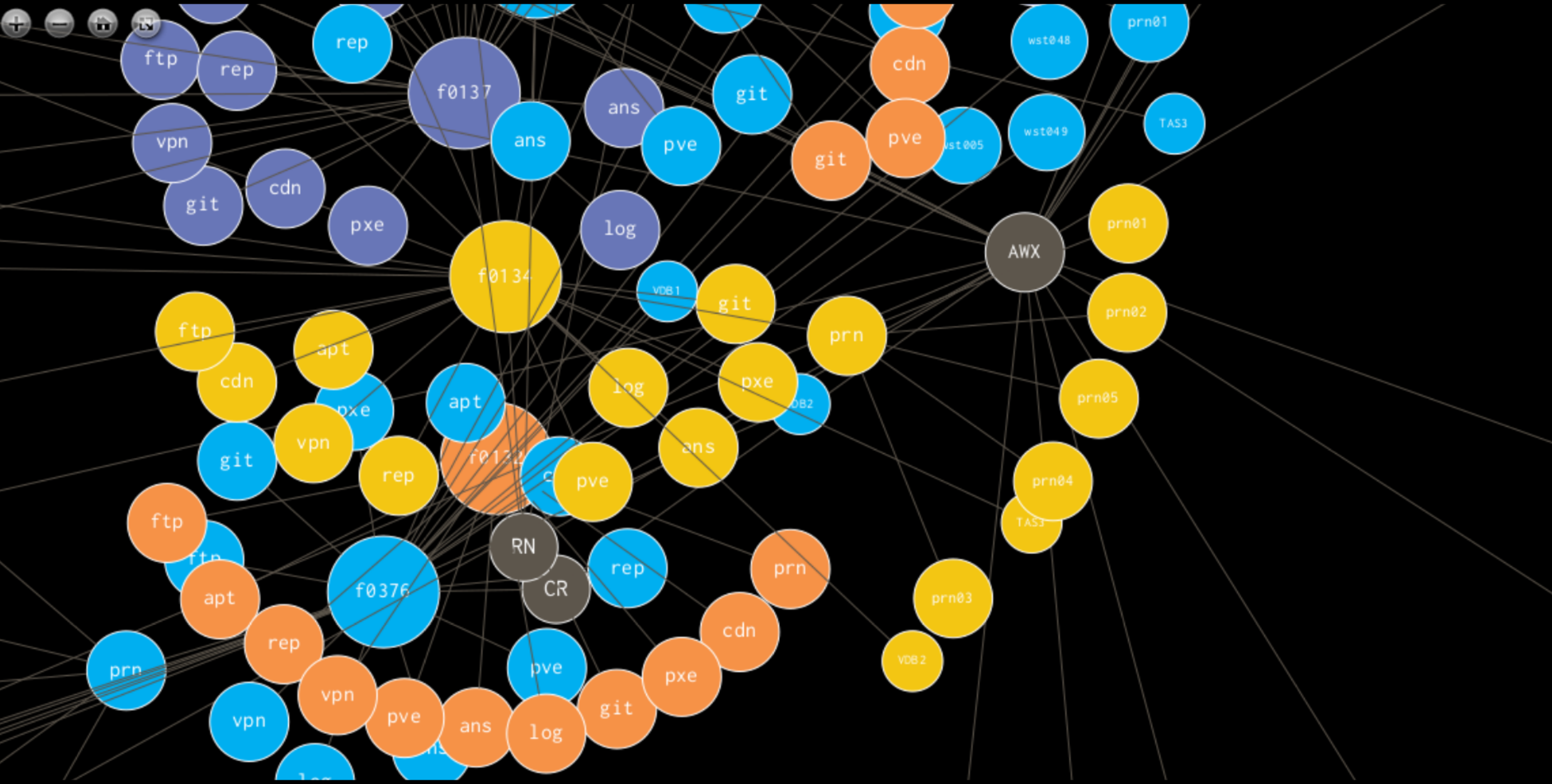
<https://filiales-gnu-linux.g.coop.ar/>

osiris@g.coop.ar

osix









Migración de 6,300+ Hosts a GNU/Linux

Cómo Aprovisionar, Instalar, Configurar y Mantener Actualizados Miles de Sistemas Debian y basados en Debian

Hitos de DevOps & Logros de Automatización

Basado en el Proyecto de Infraestructura gcoop & Banco Credicoop (2018-2022)



Alcance del Proyecto & Objetivo DevOps

- **Escala:** 300 sucursales bancarias ~6,300+ workstations & servers
- **Objetivo:** Migración Zero-downtime desde *W2K* legacy a *GNU/Linux*
- **Enfoque DevOps:** Infrastructure as Code (*IaC*), Centralized Orchestration, Pipelines *CI/CD*, Automated Inventory & Compliance



Fase 1: Lab & Proof of Concept (6 meses)

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



Fase 2: Development & IaC (1 año)

- Built `>200` repositorios *Git* (*playbooks, roles, configs* de *AWX*)
- Automated server lifecycle: control de *iDRAC* → *PXE* boot → *Proxmox* → provisioning de *VMs*
- Workstation strategy: Factory base image + *AWX*-driven config sync & enrollment
- Centralized inventory & job templates managed entirely via code (sin GUI drift)



Fase 3: Staging & Validation (87 días)

- Full production simulation en una single branch con hardware/traffic real
- Validación de peripheral compatibility (*scanners*, ticket printers, dispositivos *POS*)
- Detección de login concurrency bottleneck → implementación de cache sync + *API* gateway
- Establecimiento de deployment limits por branch para prevenir *network/API* saturation



Fase 4: Production Rollout (347 días)

- Migración de 300 branches overnight (ventana de mantenimiento 06:00–09:00)
- Zero manual provisioning; fully automated desde *AWX* → target nodes
- Implementación de pipeline *GitLab CI/CD: Dev* → *Staging* → *Production* (sync de templates *JSON*)
- Validación de Firewall/rule integrada vía requests en *JIRA* + compliance checks con *Ansible*



Challenges Clave & Soluciones de *DevOps*

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



Tech Stack & Automation Pipeline

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



Impacto & Estado Actual

- Migración 99% automatizada; 1% de intervención manual post-rollout
- Infraestructura consistente, auditable y reproducible en todas las branches
- Open-sourced de >30 roles & herramientas de Ansible vía gcoop (*GitHub/GitLab*)
- En progreso: despliegue de *FreeIPA* cluster, *CI/CD* hardening, continuous improvement



Plataforma de Automatización AWX

Hitos de DevOps y Evolución del Proyecto

Automatización de infraestructura distribuida en más de 285 ubicaciones

2022-10-22 → 2026-07-07



Descripción General de la Plataforma

Métrica	Valor
Releases desde 2022-10-22	198
Job Templates	155
Projects	201
Inventories	13



Fundación y Automatización Central

45 *releases*

- Primeros workflows en *Proxmox* + compatibilidad con servidores *Dell R350*
- Automatización inicial de workstations (`wst_upd v1.7 / wst_ipa`)
- Scaffold del project en *AWX* + permisos para equipos centrales (`awx-test/gcoop/impl/mant/trans`)
- *hardening* de `sysctl` — bloqueo de source route y redirecciones *ICMP*



Ecosistema de Workstations

47 *releases*

- Automatización de tools *FreeIPA* y *SSSD* — inicio automático de servicios `krb5kdc/httpd`
- `boot` con *PXE* y *Clonezilla* — recuperación/clone remoto de *WST* por red
- Despliegue en batch de *Wake-On-Lan* con verificación de conectividad para *SSH*
- Migración de *Firefox*: `v68` → `v120` (`ffox120`) con perfiles aislados



Expansión de Servicios

16 *releases*

- Provisioning de cámaras *CCTV* — inventory dedicado + job templates
- Automatización del servicio de impresoras — `ppd` desde *CDN*, configuración de `cups_ng`
- Detección de *HP Linux Tools* mediante Admin Password en *BIOS* + workflow de *WakeOnLAN*
- Despliegue de reglas *ACSI* con conversión automática a modo de archivo octal



Seguridad y Cumplimiento

18 releases

- job template `sec_chk` — generación automatizada de reportes de cumplimiento *ACSI*
- Refactor del role de *ACSI* + gestión de sudoers para usuarios `xcontrol`
- Rollout de *WST* `v1.8.1` / *Firefox* `120` / imagen de *WST* `v1.9.0`
- Rotación de access token de *Git* para credenciales de *VM* en `sgit`



Modernización de Infraestructura

16 releases

- Refactor de workflow en *PVE* → *playbook* — deployments idempotentes
- Actualización de *Debian Installer* `v11` (build `20210731-deb11u10`)
- Recopilación de facts para *CMDB*: detección de hardware, disco y red en *WST*
- *Ansible_vms* `v0.7.0` — generación completa de *VMs* sobre *Proxmox*



Escala y Confiabilidad

40 *releases*

- Serie incremental de `wst_upd` `1.8.x` con soporte para flag de rollback de *SREP*
- Corrección de errores en reglas *ACSI* — resolución automática de modo octal de archivos
- Automatización de reemplazo de drivers de impresora *Lexmark* `531→610`
- `wst_upd` `v1.8.11` / `wst_ffx` `v0.5.0` — inventory `v0.48.0`



Estado Actual

16 releases

- Nombres de project versionados (`ansible_wst_v1.8.13` + `wst_upd_v1.8.13`)
- Actualizaciones en *ACSI* `v0.4.16` + role `auditd` `v0.1.0-filiales`
- *Inventory* `v0.52.0` — grants multi-equipos para 6 equipos
- Plantillas de migración de servers en *FreeIPA* (ramas *PVE* + *VMS* + *WST*)



Impacto en Números

Categoría	Alcance	Releases
Automatización de Workstations	<code>wst_upd 1.7 → 1.8.x</code>	16
Integración de <i>FreeIPA</i>	<i>SSSD</i> + <i>DNS</i> + migración	37
Despliegues de <i>CCTV</i>	Gestión completa del ciclo de vida	14
Cumplimiento <i>ACSI</i>	<code>sec_chk</code> + generación automatizada de reportes	15



Línea de Tiempo Resumida

Período	Rango de Versiones	Enfoque
2022-23	v0.10-v0.67	Fundación de Workstation + <i>FreeIPA</i>
2024	v0.68-v0.89	Seguridad, <i>ACSI</i> , <i>Firefox</i> 120 , refactor en <i>PVE</i>
2025	v0.90-v0.97	Escala, confiabilidad, serie wst_upd 1.8.x
2026	v0.98-v0.106	<i>ACSI</i> v0.4 , automatización de inventory, migración de <i>IPA</i>



Plataforma de Virtualización *PVE Proxmox*

Hitos de DevOps en la Infraestructura Virtual de Sucursales

Automatización del clúster VE de Proxmox impulsada por Ansible en más de 285 ubicaciones de sucursal

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



Vista General de la Plataforma

Métrica	Valor
Lanzamientos totales (desde 2022-10-22)	17
Playbooks	box-all / box-pve / box-vms / pve-update / vms-*
Hipervisor Objetivo	Proxmox VE (Debian-based)
Roles Clave	Proxmox / ACSI / auditd / nut / cloud-init



Automatización de Migración del Servidor *FreeIPA*

Automatización de la migración de hosts srep entre dominios *FreeIPA* con zero downtime:

- `v0.9.1` (`2026-06`): Playbook completo para migrar un host srep de old -> new *FreeIPA* server
- `v0.9.0` (`2026-05`): Configuración de `cloud-init` para domain bootstrap del nuevo dominio *FreeIPA*
- Corrección de vulnerabilidades detectadas en los compliance scans **"Copy Fail"** y **"Dirty Tags"**
- Actualizaciones automatizadas de DNS records durante el IPA migration lifecycle



Cumplimiento de *ACSI* y Auditoría de Seguridad

Automatización continua de security compliance para hosts *Proxmox*:

- `v0.8.2` (`2026-04`): Rol de *ACSI* actualizado + integración de auditd para security auditing
- `v0.8.1` (`2025-07`): Bumped del rol *ACSI* a v0.4.14 -- latest compliance ruleset
- `v0.6.1` (`2025-05`): Deployment del rol de *ACSI* v0.4.9 en el clúster de *PVE*
- `v0.5.5/4` : Corrección del nombre del rol de auditd en requirements.yml para *ACSI*
`v0.4.2`
- Generación automática de audit rules y pipeline de compliance reports



Gestión del Kernel y Boot Stack

Actualizaciones automatizadas del kernel con safe initramfs regeneration:

- **initramfs regeneration:** Tarea añadida para safe initramfs rebuild tras kernel updates
- Corrección de lint errors en regenerate-initramfs -- asegura execution idempotente
- Control flow añadido para skip regenerate en fallos de lint -- previene broken boot images
- Ruta segura de upgrade para el kernel de *PVE* sin manual intervention por host



Infraestructura de Box Image y Repositorios de *PVE*

Construcción y mantenimiento de standardized *PVE* base images con correct repositories:

- **box-pve playbook:** Crea estandarized *PVE* box images para deployment de *VMs*
- **box-all / box-vms:** Generación unificada de imágenes en todos los nodos del clúster de *PVE*
- **tower-cli fix (v0.5.4):** Corrected *Proxmox* repository source en la configuración de box-pve
- **box wfw playbook (v0.5.3):** Implementación del workflow para automated box creation pipeline
- Repository pinning asegura consistent *PVE* package versions across deployments



Playbooks de Ciclo de Vida de VMs y Gestión del Clúster

Automatización integral de virtual machine management:

- **vms-delete-sans** (v0.7.0/v0.8.0): Automated VM cleanup -- elimina sans VMs sin git tracking
- **vms-delete-sgit**: Eliminación de VMs compatible con git con automated resource reclamation
- **vms-backup-disk**: Orquestación de cross-node VM backup disk
- **vms-startup-order**: Secuencia de inicio configurable de VMs para cluster boot ordering
- **pve-kvm-state**: Monitoreo y reporting en real-time del KVM VM state
- **pve-update**: Main playbook -- PVE host updates con integración de NUT (UPS)



Compatibilidad de Hardware e Infraestructura de Red

Expansión del supported hardware y automatización del network stack:

- Compatibilidad con *Dell* R350 (v0.2.3/v0.5.2): Soporte completo para servers *Dell PowerEdge* R350
- Integración del rol NUT (v0.5.1): Monitoreo de *UPS* y automated graceful shutdown
- Roles de cloud-init: Automated *VM* provisioning con cloud-init metadata injection
- Network stack hardening alongside *Proxmox* package updates



Configuración y Mantenimiento de APT Source

Garantía de reliable package management en todos los hosts de *PVE*:

- **Valid-Until fix** (v0.5.7): Manejo de apt indexes con atributos Valid-Until
- **Release info change** (v0.5.6): Corrección de apt update para permitir `--allow-releaseinfo-change`
- **Backports fix**: Corrected backports apt source en box-pve -- previene package pinning issues
- Asegura que los hosts de *PVE* se mantengan actualizados sin manual apt configuration intervention



Cronología Resumen

Período	Rango de Versiones	Logros Clave
Mitad 2023	v0.2.3-v0.5.1	Compatibilidad con <i>Dell</i> R350 , integración de <i>UPS</i> NUT, roles <code>cloud-init</code>
Inicio 2024	v0.5.2-v0.5.7	Pipeline de box images, Valid-Until fix en <code>apt</code> , corrección de <code>tower-cli</code>
Mitad 2025	v0.6.0-v0.8.1	ACSI compliance chain, backports fix, playbooks para eliminar <i>VMs</i>
2026	v0.8.2-v0.9.1	Gestión de <code>initramfs</code> , integración de <code>auditd</code> , automatización de <i>FreeIPA</i> migration



Módulos Principales de Playbooks (ansible_proxmox)

Playbook	Propósito
<code>box-pve</code>	Crear estandarized <i>PVE</i> base box image
<code>box-all</code>	Generar box images en todos los nodos del clúster
<code>box-vms</code>	<i>VM</i> template generation desde el <i>PVE</i> box
<code>pve-update</code>	Main playbook -- <i>PVE</i> host updates con <i>UPS</i> NUT integration
<code>vms-backup-disk</code>	Orquestación de cross-node <i>VM</i> backup disk
<code>vms-delete-sans</code>	Automated sans <i>VM</i> cleanup (sin git tracking)
<code>vms-delete-sgit</code>	Eliminación de <i>VMs</i> compatible con git con 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 y reporting



WST Workstation Automation

Hitos de DevOps en la Infraestructura de Escritorio de Sucursales

Gestión del ciclo de vida de estaciones de trabajo impulsada por Ansible en más de 285 ubicaciones de sucursal

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



Vista General de la Plataforma

Métrica	Valor
Total de releases (desde 2022-10-22)	21
Playbooks	Serie wst - * con 50+ módulos
Navegadores compatibles	Firefox v68 / Firefox v120 / Chrome
SO base	Ubuntu Desktop (kernel v5.15+)



Integración con *FreeIPA* y Autenticación I

Habilitando identidad de estación de trabajo segura y vinculada a la red en todas las sucursales:

- `wst-ipa` *playbook* (`v1.7.0`): Creó el ciclo de vida de unión/desunión para la membresía en el dominio *FreeIPA*
- `wst-nip` *playbook*: Automatizó la configuración de interfaces de red junto con el registro en *IPA*
- `apt_pin` *role* (`v1.7.4`): Fijó paquetes críticos para prevenir deriva de versiones en el stack de *IPA*



Integración con *FreeIPA* y Autenticación II

Habilitando identidad de estación de trabajo segura y vinculada a la red en todas las sucursales:

- `wst-ipa-uninstall` (`v1.7.5` → `1.7.7`): Desregistro completo con limpieza automatizada de registros `A` de *DNS*
- `wst-sssd-service` : Garantiza el ordenamiento `After=network-online.target` + reinicio automático en caso de falla
- `fix_owner_fix` (`v1.7.16`): Omite la copia de seguridad cuando la carpeta del usuario en `srep` está vacía, previniendo fallas en cascada



Estrategia de Navegadores: *Firefox* + *Chrome*

Soportando ecosistemas paralelos de navegadores para diversas necesidades de sucursal:

- Integración del rol *Firefox*: (`v1.7.3`): Políticas, preferencias y gestión de extensiones
- Migración *Firefox* `v68` → `v120` : Soporte dual con perfiles aislados por usuario
- Despliegue de *Chrome*: Implementación paralela junto a *Firefox* para sucursales que requieran funciones basadas en Chromium
- `wst-ffox-policies` + `wst-ffox-prefs` : Aplicación centralizada de políticas de navegador mediante plantillas *ADMX*
- Configuración de *proxy* (`wst-ffox-check-proxy`): Detección dinámica de proxy y failover



Fiabilidad y Resiliencia del Despliegue

Construyendo una cadena de despliegue de estaciones de trabajo tolerante a fallas:

- **wst-wol-all**: Despliegue por lotes Wake-On-Lan delegado al `spve` de cada grupo, sin intervención manual
- **Integración WOL + Wait-for** (v1.7.19): Tareas nativas de suspensión/reinicio en `wst-update` con timeouts configurables
- **Actualización de kernel** (v1.8.0): La imagen base se movió al kernel v5.15 para soporte de hardware moderno
- **wst-reboot**: *playbook* de reinicio inteligente con modo opcional sin espera, soporta despliegues no supervisados
- **Correcciones de sftp-mount** (v1.7.11): Integración confiable del servidor de archivos para recursos compartidos de sucursal



Monitoreo de Salud de Seguridad e Identidad

Verificación continua de autenticación y gestión del ciclo de vida de credenciales:

- **wst-ipa-health-check** (v1.7.18): Cadena completa de pruebas de salud: WoL → espera SSH → `ipa-hlt-chk` en `greeter-script-setup` de lightdm
- **wst-krb-chk** (v1.4.6): Validación de keytab de Kerberos para prevenir fallos de autenticación
- **Gestión de grupos/contraseñas wst-adminws**: Provisión centralizada de espacios de trabajo administrativos con vinculación de dirección MAC
- **Roles apparmor + dconf**: Control de acceso obligatorio y endurecimiento de configuración de escritorio
- **Role loginhelper** (v1.5.0): Notificación segura de inicio de sesión con hooks pre/post sesión



Integración SREP, Seguridad ante Rollback, Auditoría y Control

- **Playbook wst-full:** Reconstrucción completa de la imagen de la estación, ejecutando todos los roles en estrategia por lotes en serie
- **Port backport etc-keeper (v1.6.0):** Versionado de configuración `/etc` via `etckeeper` + modo `check-only`
- **Manejo de respaldos srep:** `fix_owner` omite carpetas `srep` vacías, evitando activadores de rollback falsos positivos
- **Despliegue por lotes en serie:** `wst-v1.5.0` introdujo `serial: 1` para rollout controlado a través de grupos
- **Base kernel v1.8.0** + actualizaciones de roles (admin, apparmor, cups_ng, etc.): Cadena unificada de actualizaciones



Línea de Tiempo de un Vistazo

Período	Rango de Versión	Hitos Clave
Oct 2022	v1.7.0–v1.6.0	Creación de playbooks wst-ipa + wst-nip, backport etc-keeper
Inicio 2023	v1.7.4–v1.7.11	Gestión de servicio SSSD, desregistro IPA, sftp-mount, apt_pin
Final 2023	v1.7.14–v1.8.0	Firefox/Chrome paralelo, kernel v5.15, health checks, WoL+Wait
2024+	v1.7.18–v1.7.19	WOL+WFL nativo en wst-update, endurecimiento de fiabilidad



Módulos Principales de Playbooks (serie `wst - *`)

Playbook	Propósito
<code>wst-update</code>	Cadena principal de despliegue de roles para estaciones
<code>wst-full</code>	Reconstrucción completa de la imagen (todos los roles en serie)
<code>wst-ipa</code>	Ciclo de vida de unión/desunión a FreeIPA
<code>wst-nip</code>	Configuración de interfaces de red
<code>wst-adminws</code>	Provisión de espacio de trabajo + escritorio para admins
<code>wst-desktop-launchers</code>	Gestión de accesos directos de escritorio



Módulos Principales de Playbooks (serie `wst - *`)

Playbook	Propósito
<code>wst-sssd-service</code>	Estado del servicio SSSD y ordenamiento de red
<code>wst-sftp-mount</code>	Integración de compartidos de servidor de archivos seguro
<code>wst-wol-all</code>	Despliegue por lotes Wake-On-Lan
<code>wst-ipa-health-check</code>	Cadena de pruebas de salud de autenticación
<code>wst-kernel-upg</code>	Actualizaciones de versión del kernel
<code>wst-krb-chk</code>	Validación de keytab de Kerberos



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>