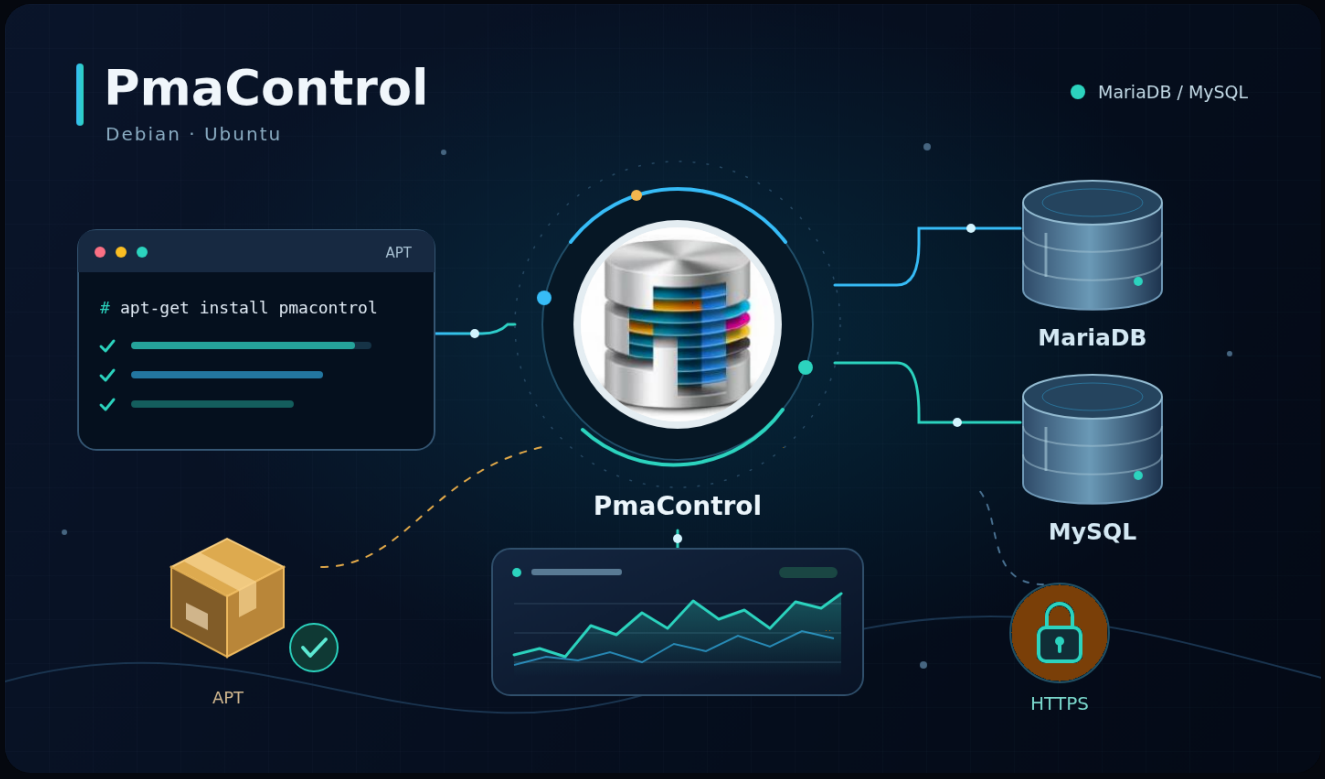
Installer PmaControl sur Debian et Ubuntu : guide complet et état de Docker

Aurélien LEQUOY · 26 septembre 2026

PMACONTROL INSTALLATION DEBIAN UBUNTU DOCKER MARIADB FRANKENPHP HTTPS



Ce guide explique comment déployer PmaControl pour superviser des serveurs **MariaDB / MySQL**, puis vérifier que l'interface, la base locale et la collecte fonctionnent.

La voie d'installation actuelle est le paquet `pmacontrol`, distribué par le dépôt APT signé du projet. Il installe MariaDB, le plugin RocksDB, PHP CLI, FrankenPHP et les dépendances applicatives. Il initialise aussi la base, les comptes, les tâches planifiées et la configuration web. Une machine dédiée ou une VM évite les conflits avec des services existants.

Installation en une commande

Sur une machine dédiée Debian 12/13 ou Ubuntu 24.04/26.04 en **amd64**, lancez cette commande dans un terminal. Le script vérifie le système et la clé du dépôt signé, puis installe le paquet PmaControl et ses dépendances. Il demande les droits administrateur via `sudo`.

```
curl -fsSL https://pmacontrol.com/install.sh | sudo bash
```

Si vous êtes déjà root, remplacez `sudo bash` par `bash`. Consulter le script. Après l'installation, poursuivez avec les contrôles, HTTPS et la première connexion décrits ci-dessous.

1. Choisir son système

Système	Suite APT	Architecture	Méthode
Debian 12	`bookworm`	`amd64`	Paquet APT
Debian 13	`trixie`	`amd64`	Paquet APT
Ubuntu 24.04 LTS	`noble`	`amd64`	Paquet APT
Ubuntu 26.04 LTS	`resolute`	`amd64`	Paquet APT
Docker	—	—	Voir la section Docker

Au **26 septembre 2026**, les quatre suites proposent le paquet **5.4.36-1**. `apt-cache policy pmacontrol` reste la référence pour la version disponible au moment de votre installation. La branche de développement peut être plus récente que le paquet publié. Les paquets ARM64 et les anciennes versions Ubuntu ne font pas partie de cette procédure.

2. Préparer la machine et le réseau

Prévoyez un accès administrateur, un DNS fonctionnel, une horloge synchronisée et un stockage persistant. Pour démarrer sur une petite infrastructure, **2 à 4 vCPU, 4 à 8 Gio de RAM et 40 Gio de SSD** constituent une base de dimensionnement indicative, pas un minimum garanti. La volumétrie dépend du nombre de serveurs, des métriques, de la rétention et des sauvegardes. Séparez le stockage des sauvegardes si vous activez cette fonction.

Autorisez les accès entrants TCP **443** depuis les utilisateurs autorisés et TCP **80** pour la redirection et, si nécessaire, ACME. UDP **443** sert à HTTP/3 et reste optionnel pour les clients. Prévoyez les sorties HTTPS vers les dépôts, DNS/NTP vers vos services, SQL vers les serveurs surveillés sur leurs ports réels et SSH **22** seulement pour les fonctions qui l'utilisent. La base locale n'a pas besoin d'être exposée à Internet.

Exécutez ces contrôles avant l'installation. Si `/var/lib/mysql` n'existe pas encore, contrôlez l'espace du système de fichiers qui l'hébergera. Les ports web doivent être libres : le paquet refuse un listener étranger et ne désactive pas automatiquement Apache, Nginx ou Caddy.

```
cat /etc/os-release
dpkg --print-architecture
df -h / /var/lib/mysql
free -h
timedatectl status
ss -ltnp '( sport = :80 or sport = :443 )'
ss -lunp 'sport = :443'
```

3. Installer sur Debian 12 ou Debian 13

Sur une machine Debian dédiée, utilisez le bloc suivant. Il sélectionne automatiquement `bookworm` ou `trixie`, vérifie `amd64`, ajoute uniquement la clé de ce dépôt avec `signed-by`, affiche la version candidate et simule l'installation avant de l'exécuter. À l'étape de simulation, vérifiez les paquets ajoutés et les éventuels changements. Les commandes suivantes s'exécutent dans le shell root ouvert par `sudo -i`.

L'empreinte de la clé vérifiée le 26 septembre 2026 est **`CAFD ABF8 7717 CC60 291E 68E4 D56A 0ADA AB5F 97E2`**. Si elle change, confirmez la rotation auprès du projet avant de continuer. N'utilisez pas `trusted=yes` pour contourner une erreur de signature.

```
sudo -i
set -eu
. /etc/os-release
case "$ID:$VERSION_CODENAME" in
  debian:bookworm|debian:trixie|ubuntu:noble|ubuntu:resolute) ;;
  *) echo "Unsupported distribution: $ID:$VERSION_CODENAME" >&2; exit 1 ;;
esac
test "$(dpkg --print-architecture)" = amd64
apt-get update
apt-get install -y ca-certificates curl gnupg
install -d -m 0755 /etc/apt/keyrings
curl -fsSL --retry 3   https://repo.pmacontrol.com/debian/pmacontrol-archive-keyring.gpg   -
o /etc/apt/keyrings/pmacontrol-archive-keyring.gpg
chmod 0644 /etc/apt/keyrings/pmacontrol-archive-keyring.gpg
```

```
gpg --show-keys --with-fingerprint   /etc/apt/keyrings/pmacontrol-archive-keyring.gpg
printf 'deb [arch=amd64 signed-by=/etc/apt/keyrings/pmacontrol-archive-keyring.gpg]
https://repo.pmacontrol.com/debian %s main\n'   "$VERSION_CODENAME" >
/etc/apt/sources.list.d/pmacontrol.list
apt-get update
apt-cache policy pmacontrol
apt-get -s install pmacontrol
apt-get install pmacontrol
```

4. Installer sur Ubuntu 24.04 ou Ubuntu 26.04

Sur Ubuntu, exécutez **le même bloc APT de la section précédente** : il choisit `noble` pour 24.04 et `resolute` pour 26.04. Conservez les dépôts officiels Ubuntu déjà configurés et leur suite correcte. Le dépôt PmaControl fournit le paquet et les dépendances nécessaires ; ne remplacez pas `noble` par `trixie` sur une machine Ubuntu.

Après `apt-get install pmacontrol`, ne relancez pas `install.sh`, ne créez pas manuellement la base et ne rajoutez pas une seconde pile Apache/PHP-FPM. Le post-install du paquet effectue déjà l'initialisation. Le PHP de la ligne de commande et le PHP intégré à FrankenPHP sont deux runtimes distincts : un `php -v` seul ne valide pas le runtime web.

5. Vérifier l'installation et récupérer les accès

Le paquet doit être dans l'état `install ok installed`, `dpkg --audit` ne doit pas signaler de configuration incomplète, et MariaDB, FrankenPHP et cron doivent être actifs. Le marqueur du runtime doit afficher `frankenphp`. Vérifiez aussi que RocksDB est chargé. La requête HTTP doit rediriger vers HTTPS ; la route HTTPS de connexion doit répondre sans erreur serveur.

Le `-k` de ce contrôle local sert uniquement à tester le certificat interne initial. Pour l'accès normal des utilisateurs, configurez le certificat de la section suivante et vérifiez sans `-k`.

```
dpkg-query -W -f='${Status} ${Version}\n' pmacontrol
dpkg --audit
systemctl is-active mariadb frankenphp cron
systemctl is-enabled mariadb frankenphp cron
cat /etc/pmacontrol/active-runtime
mariadb -N -e "SELECT VERSION(); SELECT 1;"
mariadb -e "SHOW PLUGINS;" | awk 'NR == 1 || /ROCKSDB/'
```

```
curl -q --noproxy '*' -I http://127.0.0.1/
curl -q --noproxy '*' -k -I https://localhost/fr/user/connection/
```

Les identifiants générés sont conservés dans **`/root/pmacontrol-install.env`**, accessible uniquement à root, normalement en mode **0600**. Consultez-le dans un terminal privé : `PMACTRL_ADMIN_LOGIN` et `PMACTRL_ADMIN_PASSWORD` donnent l'accès administrateur ; les variables webservice concernent l'API. N'envoyez pas ce fichier dans un ticket, un dépôt ou une capture.

Ouvrez `https://VOTRE-HOTE/fr/user/connection/`, connectez-vous puis définissez un mot de passe personnel depuis votre profil. Conservez le fichier de récupération dans une sauvegarde chiffrée et adaptez-le si vous faites une rotation des accès qu'il contient. Après une initialisation réussie, le fichier temporaire `/root/pmacontrol-install.json` doit avoir disparu. Sa présence peut indiquer un bootstrap inachevé : cherchez l'erreur avant de le supprimer.

```
sudo stat -c '%a %U %G %n' /root/pmacontrol-install.env
sudo less /root/pmacontrol-install.env
sudo test ! -e /root/pmacontrol-install.json
```

6. Configurer un vrai nom DNS et HTTPS

Par défaut, FrankenPHP utilise un certificat interne pour `localhost`. Un accès par IP ou un nom non configuré peut donc produire une alerte de confiance ou de nom. Pour un nom public, créez un enregistrement DNS qui pointe vers l'instance et remplacez **chaque occurrence** de `pmacontrol.example.com` ci-dessous par votre nom.

Le bloc importe le snippet fourni par PmaControl. Caddy peut obtenir automatiquement un certificat public si le nom et les challenges ACME sont joignables. Pour un réseau privé, utilisez une autorité approuvée par vos clients ou vos propres fichiers `tls /chemin/fullchain.pem /chemin/private.key`. Assurez la lecture de la clé par le service sans la rendre publique. Les fichiers placés dans `/etc/pmacontrol/frankenphp.d/` sont conservés lors des mises à jour ; les fichiers Caddy générés par le paquet peuvent être régénérés.

```
sudo install -d -m 0755 /etc/pmacontrol/frankenphp.d
sudo tee /etc/pmacontrol/frankenphp.d/pmacontrol.example.com.caddyfile >/dev/null <<'CADDY'
pmacontrol.example.com {
    import pmacontrol_app
}
```

```
CADDY
(
  set -eu
  validation_dir="$(mktemp -d /tmp/pmacontrol-validation.XXXXXX)"
  trap 'sudo rm -rf -- "$validation_dir"' EXIT
  sudo env HOME="$validation_dir" frankenphp validate     --adapter caddyfile --config
/etc/frankenphp/Caddyfile
)
sudo systemctl reload frankenphp
curl -I https://pmacontrol.example.com/fr/user/connection/
```

7. Utiliser un reverse proxy

Privilégiez une liaison **HTTPS avec validation du certificat** entre le proxy et FrankenPHP. Conservez le `Host` public original et remplacez la valeur reçue de `X-Forwarded-Proto` par la valeur calculée par le proxy.

Si votre architecture exige un upstream HTTP, déclarez uniquement l'IP du proxy immédiatement connecté dans `/etc/pmacontrol/trusted-proxies`. Remplacez `192.0.2.10` dans l'exemple ; n'autorisez pas tout Internet. Le paquet n'accepte l'application sur HTTP que pour un pair autorisé avec `X-Forwarded-Proto: https` exact. Les autres requêtes sont redirigées. Reconfigurez le paquet pour appliquer cette politique.

```
sudo tee /etc/pmacontrol/trusted-proxies >/dev/null <<'PROXY'
192.0.2.10
PROXY
sudo chown root:root /etc/pmacontrol/trusted-proxies
sudo chmod 0644 /etc/pmacontrol/trusted-proxies
sudo apt-get install --reinstall pmacontrol
```

8. Ajouter les premiers serveurs MariaDB / MySQL

Depuis l'interface, ajoutez l'adresse, le port et les identifiants SQL du serveur à superviser, puis testez la connexion. La base MariaDB locale de PmaControl est distincte des serveurs surveillés : vous n'avez pas à déplacer vos bases applicatives.

Créez un compte de supervision dédié, limité à l'adresse de PmaControl, et accordez les droits nécessaires aux fonctions choisies. Les droits de lecture des métriques, de réplication, d'analyse,

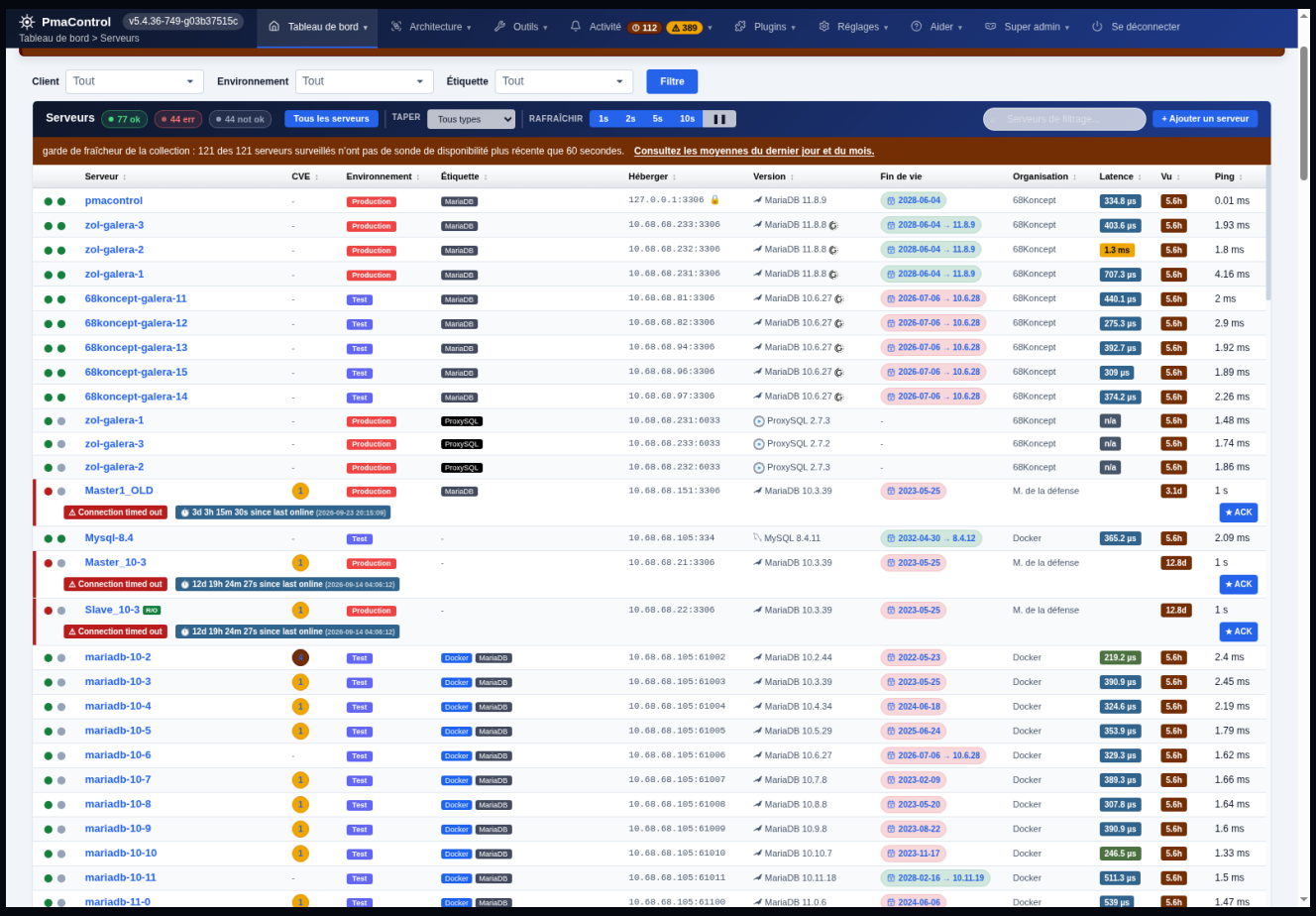
de sauvegarde ou d’administration diffèrent selon MariaDB, MySQL et leur version ; ne remplacez pas ce travail par un compte root distant universel. Activez Performance Schema sur les cibles si les vues choisies l’exigent. SSH est optionnel et concerne les fonctions de collecte système, de logs ou de sauvegarde qui en ont besoin.

Après quelques cycles de collecte, vérifiez la date du dernier échantillon, les graphiques et la topologie. Une page de connexion disponible ne prouve pas que les métriques sont fraîches. Contrôlez aussi les erreurs et les tâches actives dans l’interface ; n’activez pas tous les daemons sans tenir compte des fonctions volontairement désactivées.

PmaControl en images

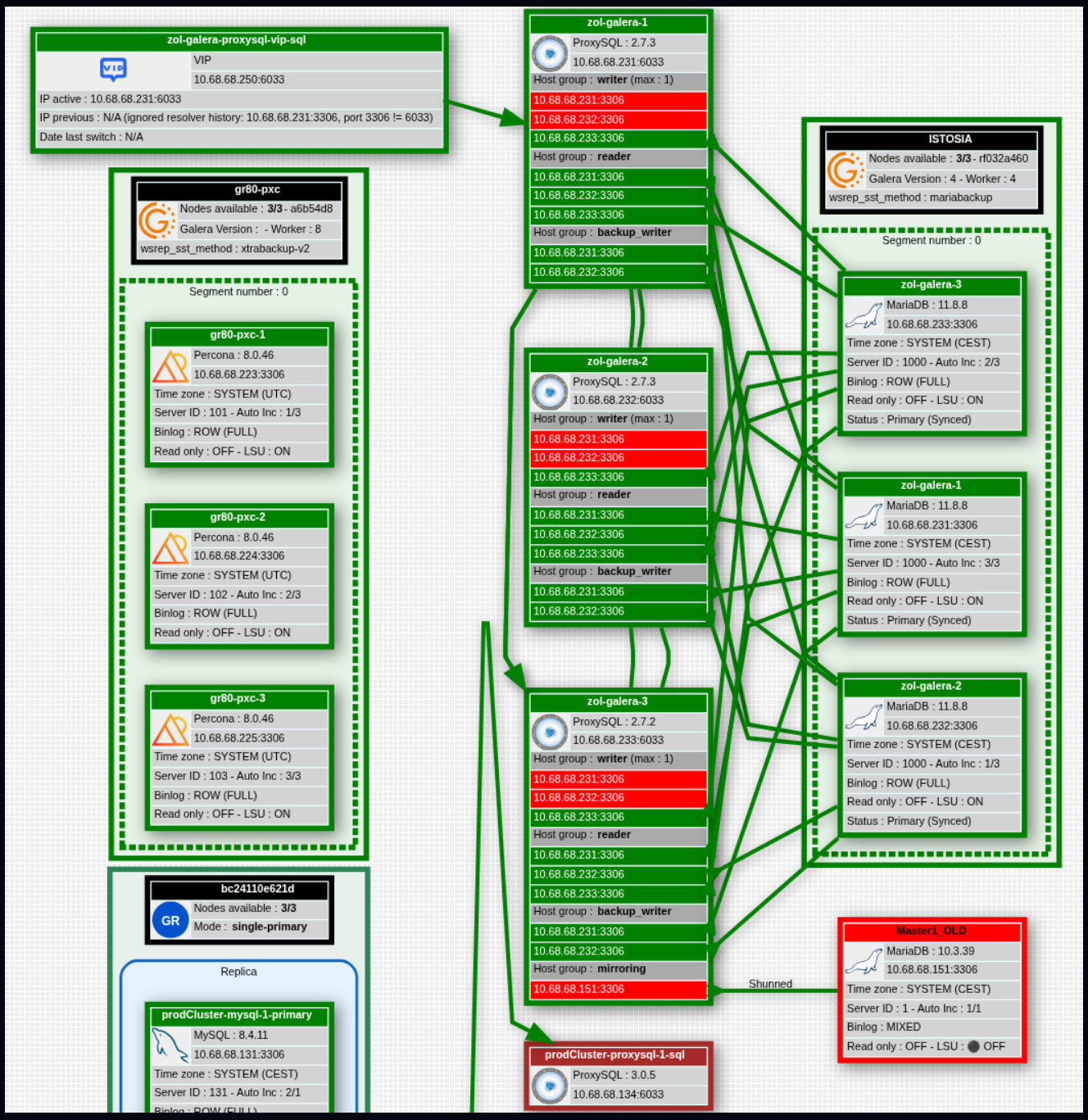
Dix vues pour découvrir la supervision, les topologies et les outils de PmaControl. Cliquez sur une capture pour l’ouvrir en taille originale. Captures réalisées le 26 septembre 2026.

1. Liste des serveurs



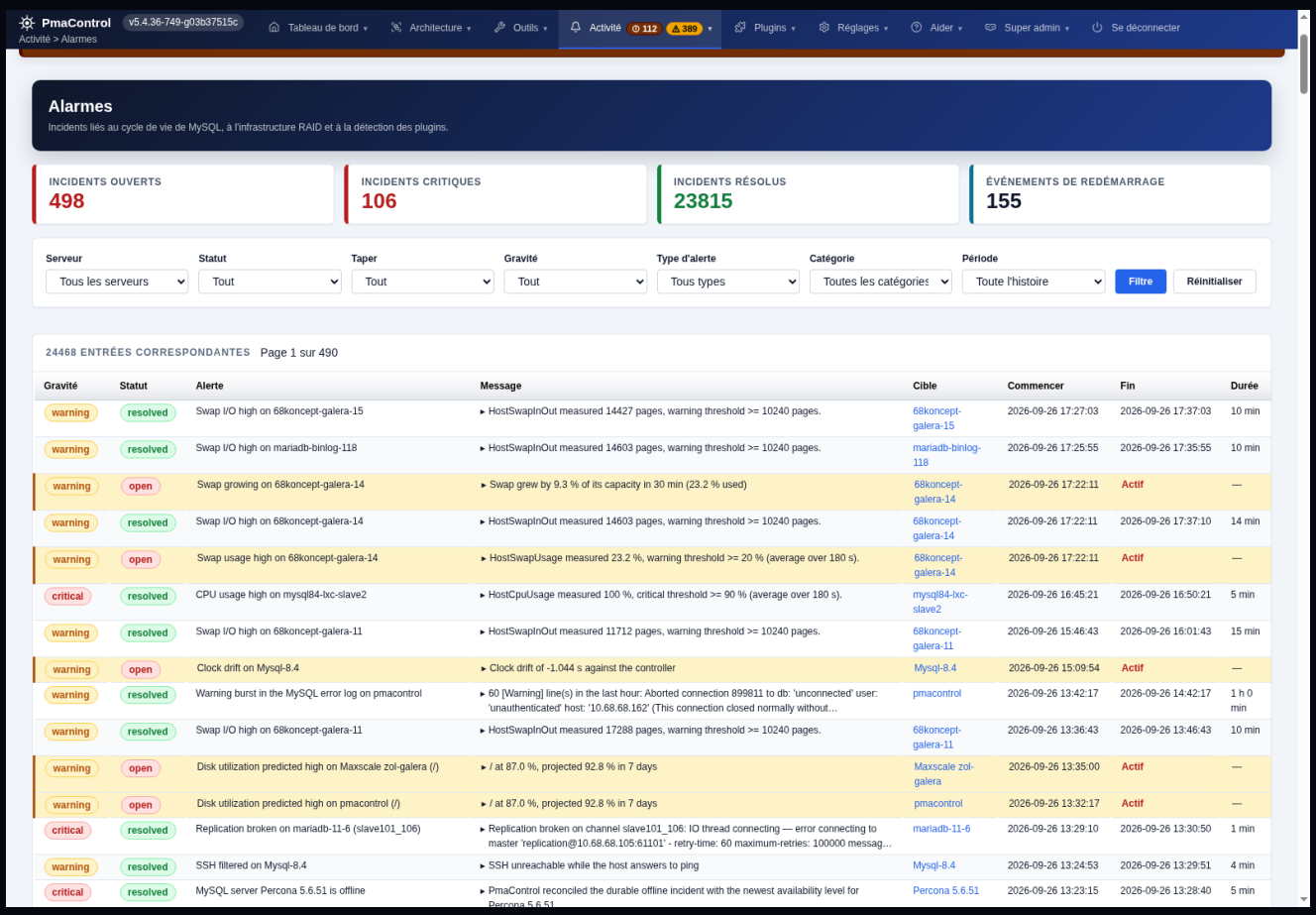
Inventaire des serveurs, disponibilité, versions et date de la dernière collecte.

2. Architecture Galera + ProxySQL



Visualisation des VIP, des groupes ProxySQL et des membres des clusters Galera.

3. Alarmes et incidents

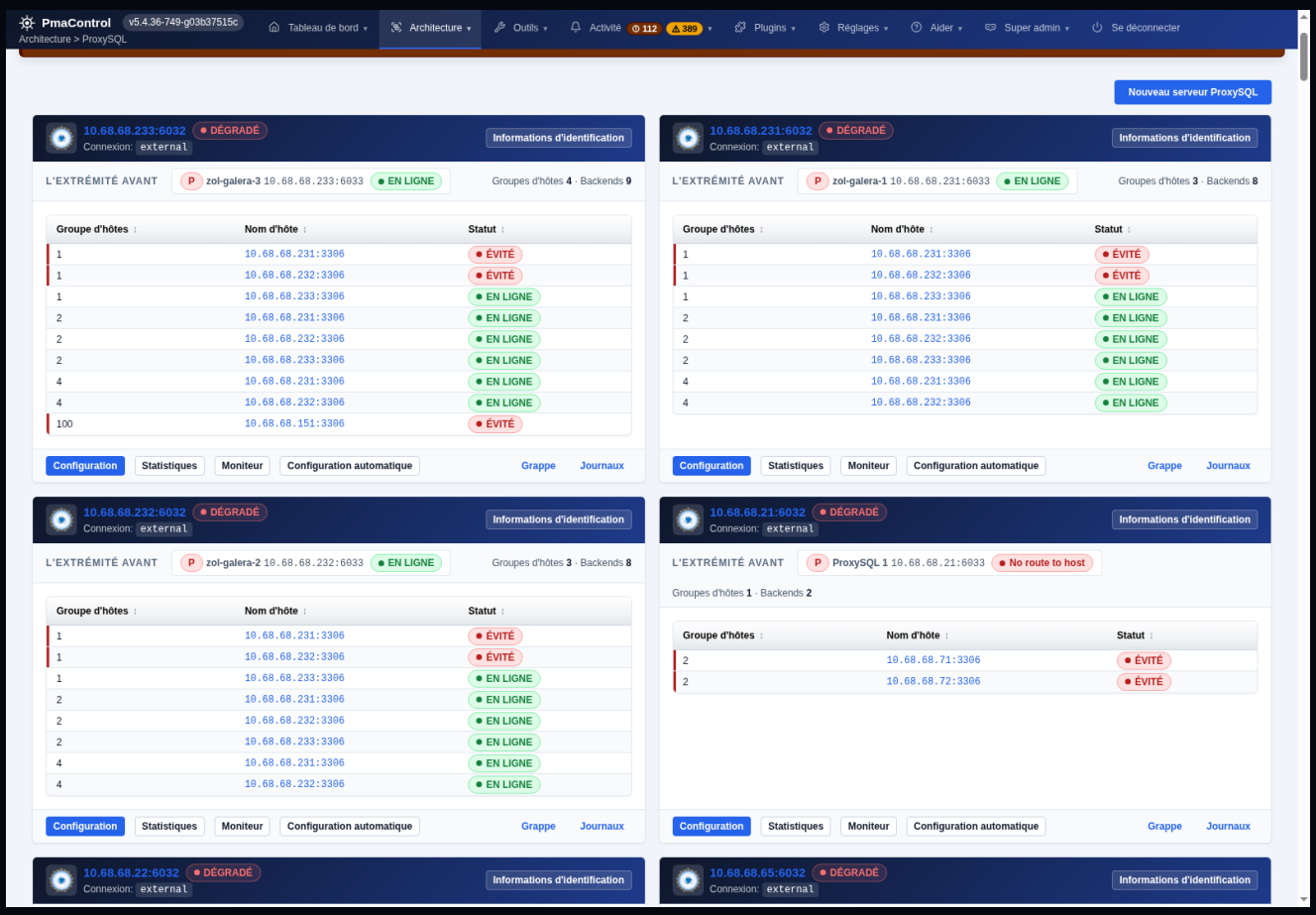


Incidents ouverts et résolus, niveaux de gravité et filtres par serveur.

4. État des nœuds Galera

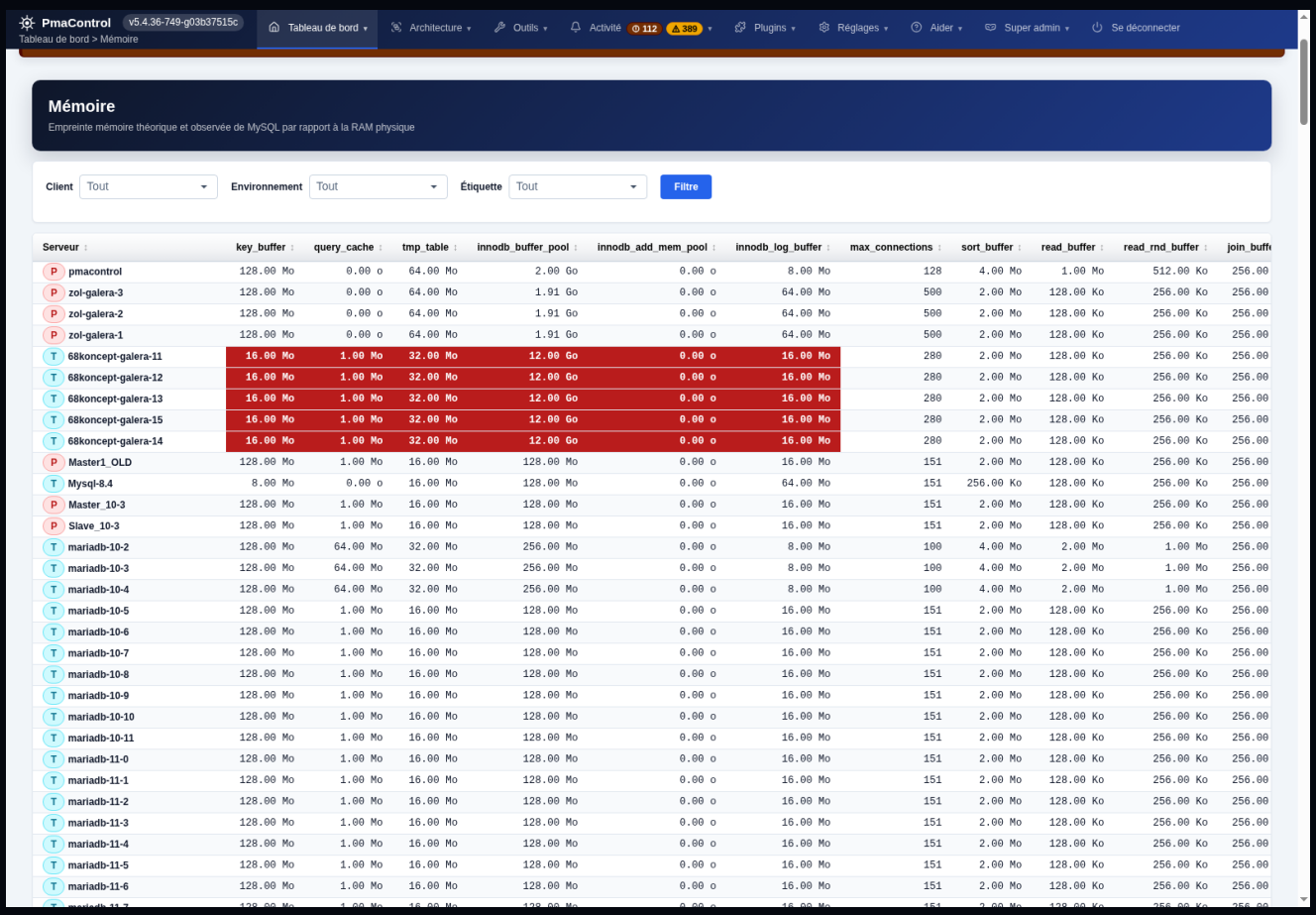
Membres des clusters, état de synchronisation, segments et versions.

5. Hostgroups et routage ProxySQL



Groupes writer et reader, backends et état des connexions.

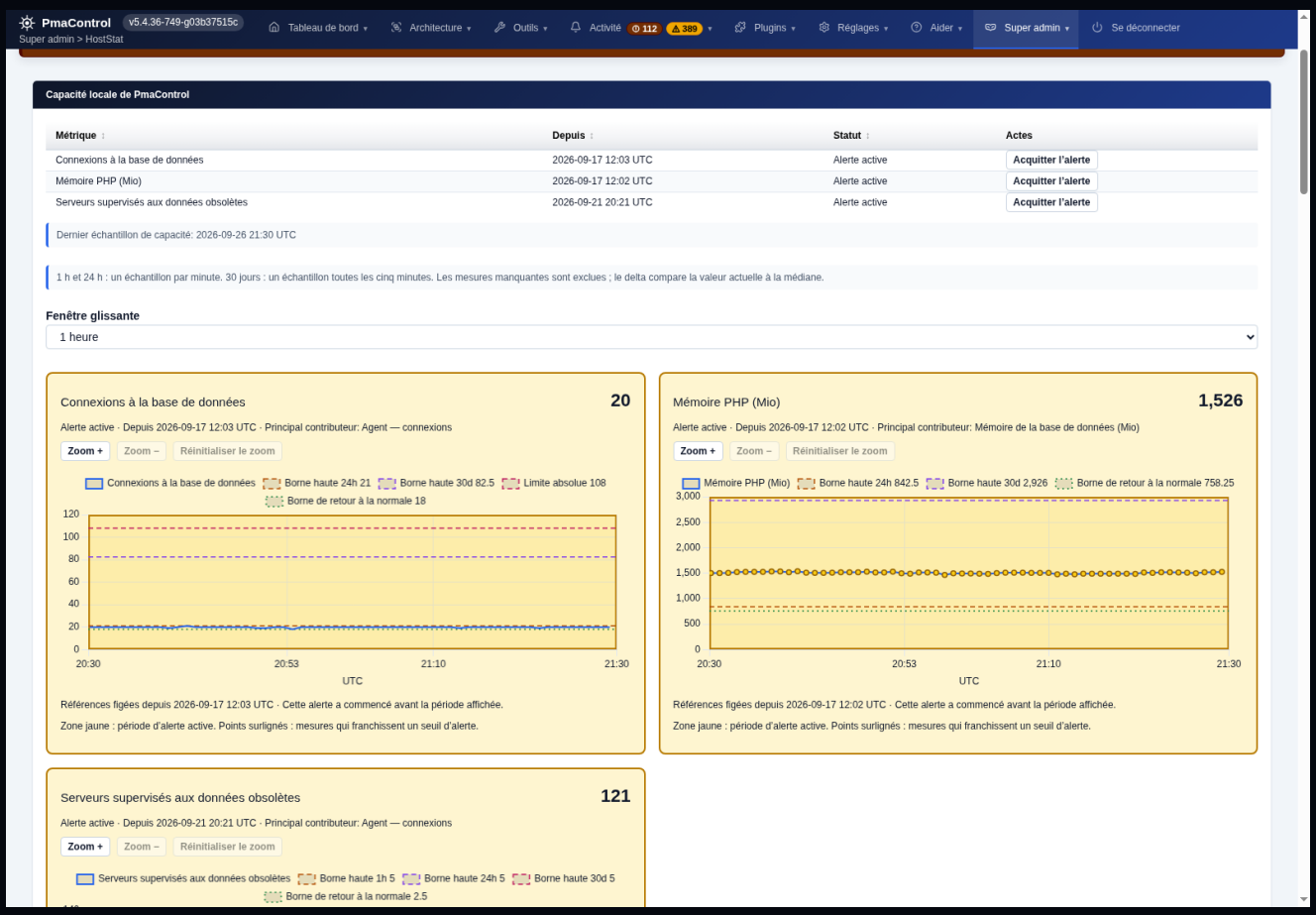
6. Mémoire des bases de données



Serveur	key_buffer	query_cache	tmp_table	innodb_buffer_pool	innodb_add_mem_pool	innodb_log_buffer	max_connections	sort_buffer	read_buffer	read_rnd_buffer	join_buffe
P pmacontrol	128.00 Mo	0.00 o	64.00 Mo	2.00 Go	0.00 o	8.00 Mo	128	4.00 Mo	1.00 Mo	512.00 Ko	256.00
P zol-galera-3	128.00 Mo	0.00 o	64.00 Mo	1.91 Go	0.00 o	64.00 Mo	500	2.00 Mo	128.00 Ko	256.00 Ko	256.00
P zol-galera-2	128.00 Mo	0.00 o	64.00 Mo	1.91 Go	0.00 o	64.00 Mo	500	2.00 Mo	128.00 Ko	256.00 Ko	256.00
P zol-galera-1	128.00 Mo	0.00 o	64.00 Mo	1.91 Go	0.00 o	64.00 Mo	500	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T 68koncept-galera-11	16.00 Mo	1.00 Mo	32.00 Mo	12.00 Go	0.00 o	16.00 Mo	280	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T 68koncept-galera-12	16.00 Mo	1.00 Mo	32.00 Mo	12.00 Go	0.00 o	16.00 Mo	280	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T 68koncept-galera-13	16.00 Mo	1.00 Mo	32.00 Mo	12.00 Go	0.00 o	16.00 Mo	280	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T 68koncept-galera-15	16.00 Mo	1.00 Mo	32.00 Mo	12.00 Go	0.00 o	16.00 Mo	280	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T 68koncept-galera-14	16.00 Mo	1.00 Mo	32.00 Mo	12.00 Go	0.00 o	16.00 Mo	280	2.00 Mo	128.00 Ko	256.00 Ko	256.00
P Master1_OLD	128.00 Mo	1.00 Mo	16.00 Mo	128.00 Mo	0.00 o	16.00 Mo	151	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T Mysql-8.4	8.00 Mo	0.00 o	16.00 Mo	128.00 Mo	0.00 o	64.00 Mo	151	256.00 Ko	128.00 Ko	256.00 Ko	256.00
P Master_10-3	128.00 Mo	1.00 Mo	16.00 Mo	128.00 Mo	0.00 o	16.00 Mo	151	2.00 Mo	128.00 Ko	256.00 Ko	256.00
P Slave_10-3	128.00 Mo	1.00 Mo	16.00 Mo	128.00 Mo	0.00 o	16.00 Mo	151	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T mariadb-10-2	128.00 Mo	64.00 Mo	32.00 Mo	256.00 Mo	0.00 o	8.00 Mo	100	4.00 Mo	2.00 Mo	1.00 Mo	256.00
T mariadb-10-3	128.00 Mo	64.00 Mo	32.00 Mo	256.00 Mo	0.00 o	8.00 Mo	100	4.00 Mo	2.00 Mo	1.00 Mo	256.00
T mariadb-10-4	128.00 Mo	64.00 Mo	32.00 Mo	256.00 Mo	0.00 o	8.00 Mo	100	4.00 Mo	2.00 Mo	1.00 Mo	256.00
T mariadb-10-5	128.00 Mo	1.00 Mo	16.00 Mo	128.00 Mo	0.00 o	16.00 Mo	151	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T mariadb-10-6	128.00 Mo	1.00 Mo	16.00 Mo	128.00 Mo	0.00 o	16.00 Mo	151	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T mariadb-10-7	128.00 Mo	1.00 Mo	16.00 Mo	128.00 Mo	0.00 o	16.00 Mo	151	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T mariadb-10-8	128.00 Mo	1.00 Mo	16.00 Mo	128.00 Mo	0.00 o	16.00 Mo	151	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T mariadb-10-9	128.00 Mo	1.00 Mo	16.00 Mo	128.00 Mo	0.00 o	16.00 Mo	151	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T mariadb-10-10	128.00 Mo	1.00 Mo	16.00 Mo	128.00 Mo	0.00 o	16.00 Mo	151	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T mariadb-10-11	128.00 Mo	1.00 Mo	16.00 Mo	128.00 Mo	0.00 o	16.00 Mo	151	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T mariadb-11-0	128.00 Mo	1.00 Mo	16.00 Mo	128.00 Mo	0.00 o	16.00 Mo	151	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T mariadb-11-1	128.00 Mo	1.00 Mo	16.00 Mo	128.00 Mo	0.00 o	16.00 Mo	151	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T mariadb-11-2	128.00 Mo	1.00 Mo	16.00 Mo	128.00 Mo	0.00 o	16.00 Mo	151	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T mariadb-11-3	128.00 Mo	1.00 Mo	16.00 Mo	128.00 Mo	0.00 o	16.00 Mo	151	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T mariadb-11-4	128.00 Mo	1.00 Mo	16.00 Mo	128.00 Mo	0.00 o	16.00 Mo	151	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T mariadb-11-5	128.00 Mo	1.00 Mo	16.00 Mo	128.00 Mo	0.00 o	16.00 Mo	151	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T mariadb-11-6	128.00 Mo	1.00 Mo	16.00 Mo	128.00 Mo	0.00 o	16.00 Mo	151	2.00 Mo	128.00 Ko	256.00 Ko	256.00
T mariadb-11-7	128.00 Mo	1.00 Mo	16.00 Mo	128.00 Mo	0.00 o	16.00 Mo	151	2.00 Mo	128.00 Ko	256.00 Ko	256.00

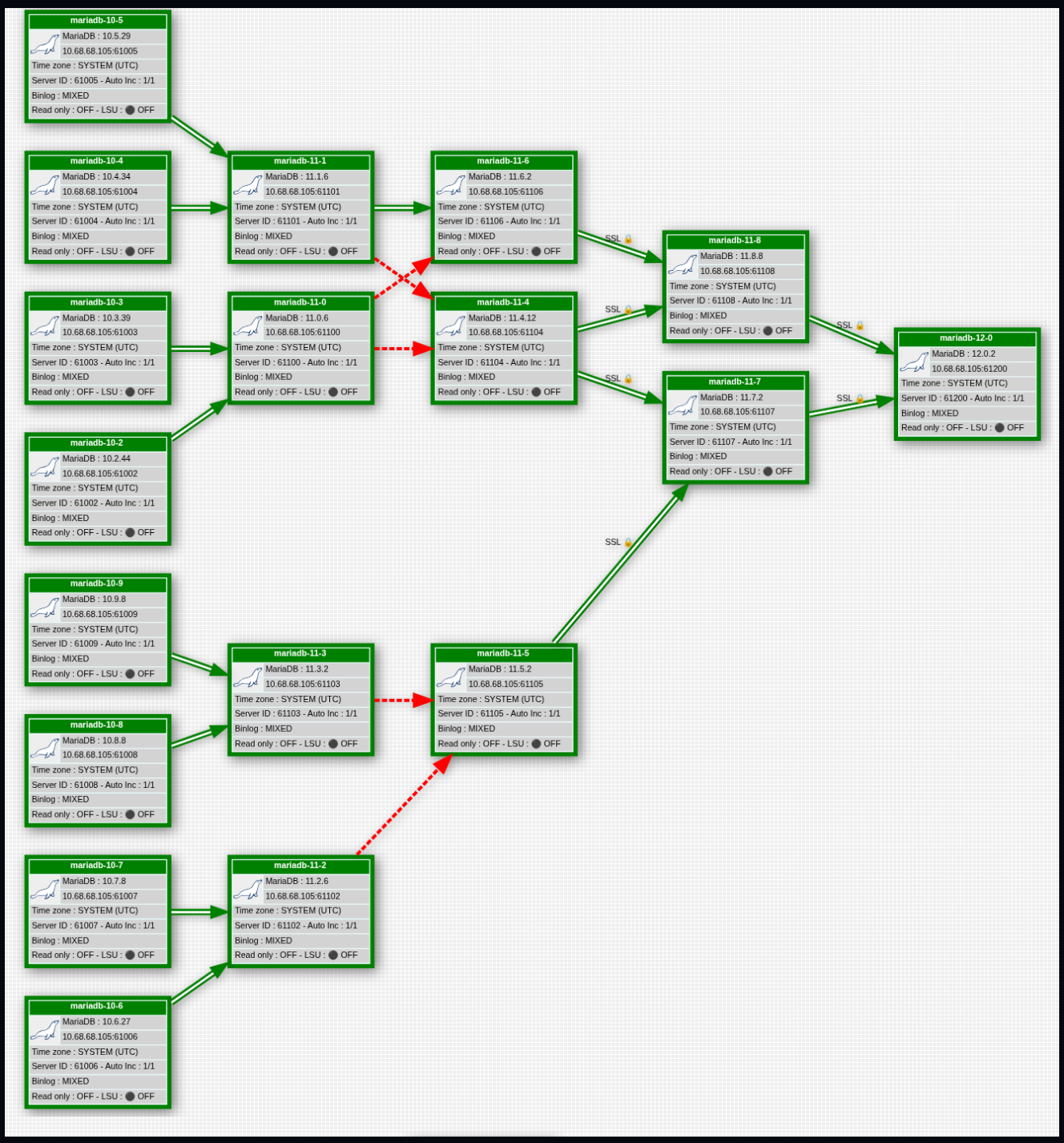
Comparaison des buffers et des paramètres mémoire par serveur.

7. Capacité de PmaControl



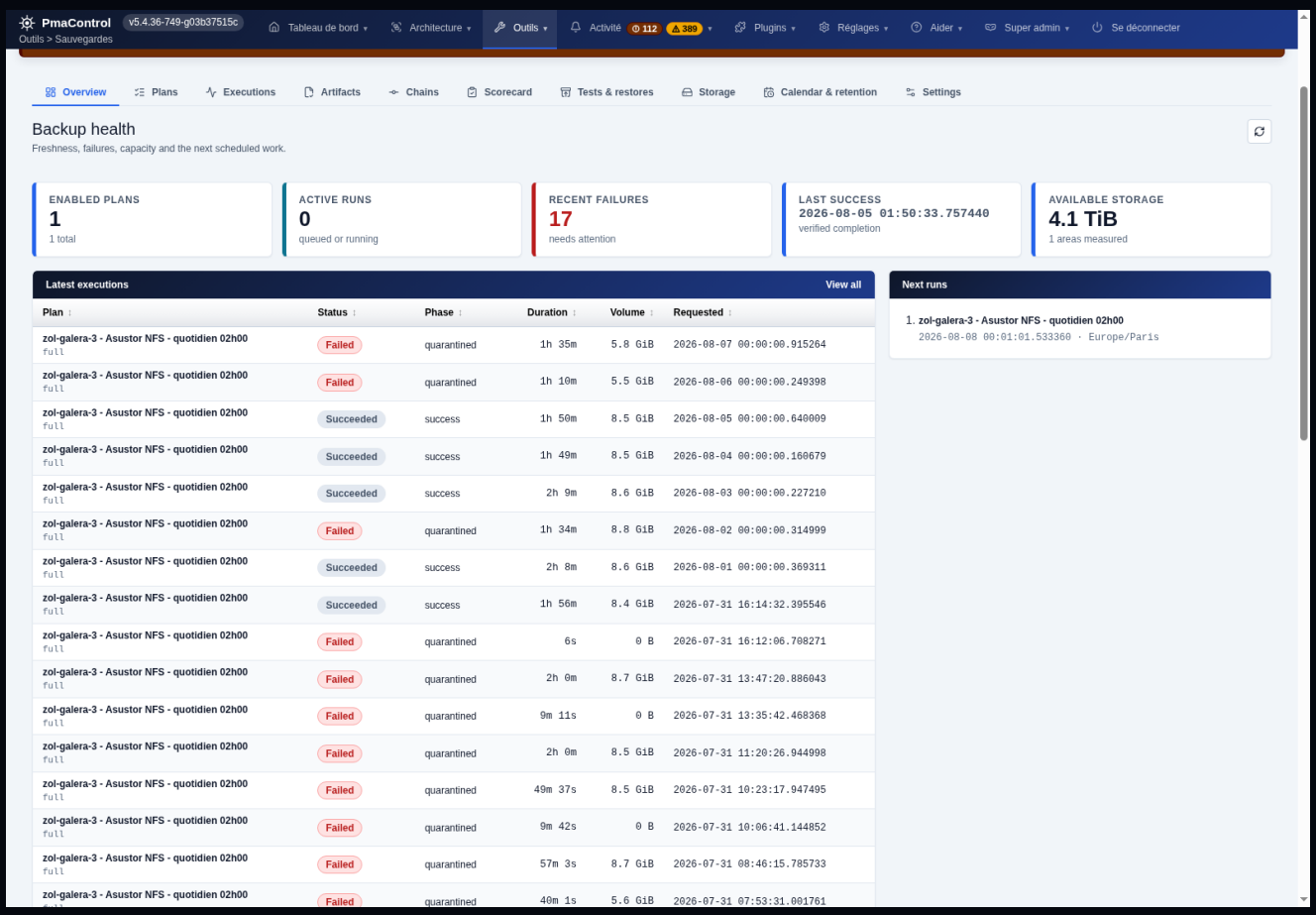
Graphiques des connexions, de la mémoire et des alertes de capacité.

8. Réplication MariaDB



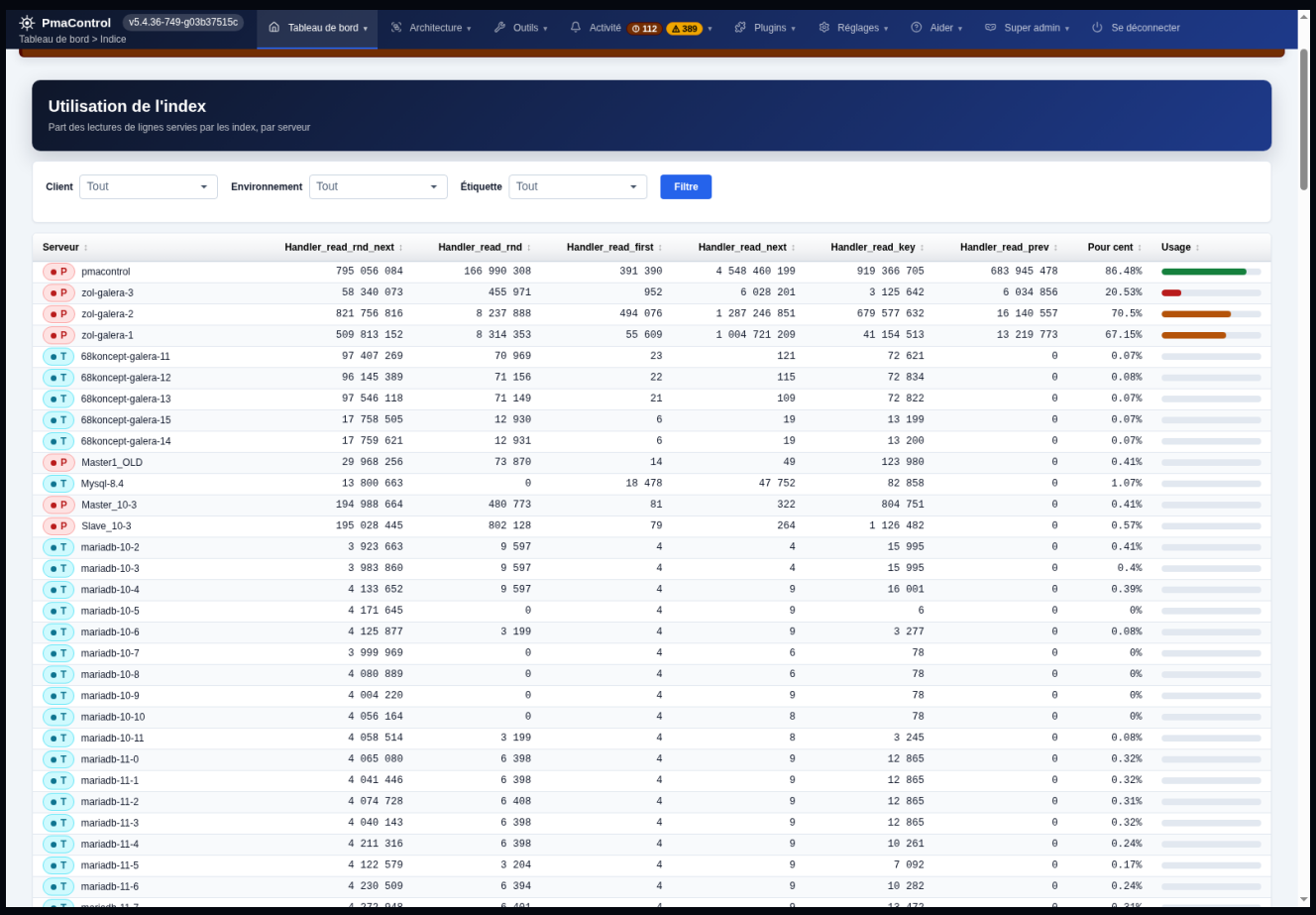
Sources, chaînes de réplication, versions et liens SSL.

9. Sauvegardes et planification



Historique des exécutions, espace de stockage et planification des sauvegardes.

10. Utilisation des index



Serveur	Handler_read_rnd_next	Handler_read_rnd	Handler_read_first	Handler_read_next	Handler_read_key	Handler_read_prev	Pour cent	Usage
P pmacontrol	795 056 084	166 990 308	391 390	4 548 460 199	919 366 705	683 945 478	86.48%	
P zol-galera-3	58 340 073	455 971	952	6 028 201	3 125 642	6 034 856	20.53%	
P zol-galera-2	821 756 816	8 237 888	494 076	1 287 246 851	679 577 632	16 140 557	70.5%	
P zol-galera-1	509 813 152	8 314 353	55 609	1 004 721 209	41 154 513	13 219 773	67.15%	
T 68koncept-galera-11	97 407 269	70 969	23	121	72 621	0	0.07%	
T 68koncept-galera-12	96 145 389	71 156	22	115	72 834	0	0.08%	
T 68koncept-galera-13	97 546 118	71 149	21	109	72 822	0	0.07%	
T 68koncept-galera-15	17 758 505	12 930	6	19	13 199	0	0.07%	
T 68koncept-galera-14	17 759 621	12 931	6	19	13 200	0	0.07%	
P Master1_OLD	29 968 256	73 870	14	49	123 980	0	0.41%	
T Mysql-8.4	13 800 663	0	18 478	47 752	82 858	0	1.07%	
P Master_10-3	194 988 664	480 773	81	322	804 751	0	0.41%	
P Slave_10-3	195 028 445	802 128	79	264	1 126 482	0	0.57%	
T mariadb-10-2	3 923 663	9 597	4	4	15 995	0	0.41%	
T mariadb-10-3	3 983 860	9 597	4	4	15 995	0	0.4%	
T mariadb-10-4	4 133 652	9 597	4	9	16 001	0	0.39%	
T mariadb-10-5	4 171 645	0	4	9	6	0	0%	
T mariadb-10-6	4 125 877	3 199	4	9	3 277	0	0.08%	
T mariadb-10-7	3 999 969	0	4	6	78	0	0%	
T mariadb-10-8	4 080 889	0	4	6	78	0	0%	
T mariadb-10-9	4 004 220	0	4	9	78	0	0%	
T mariadb-10-10	4 056 164	0	4	8	78	0	0%	
T mariadb-10-11	4 058 514	3 199	4	8	3 245	0	0.08%	
T mariadb-11-0	4 065 080	6 398	4	9	12 865	0	0.32%	
T mariadb-11-1	4 041 446	6 398	4	9	12 865	0	0.32%	
T mariadb-11-2	4 074 728	6 408	4	9	12 865	0	0.31%	
T mariadb-11-3	4 040 143	6 398	4	9	12 865	0	0.32%	
T mariadb-11-4	4 211 316	6 398	4	9	10 261	0	0.24%	
T mariadb-11-5	4 122 579	3 204	4	9	7 092	0	0.17%	
T mariadb-11-6	4 230 509	6 394	4	9	10 282	0	0.24%	

Compteurs de lecture et part des lectures servies par les index.

9. Fichiers, données et sauvegardes

Les chemins ci-dessous correspondent au déploiement par paquet. Sauvegardez la base locale, `/etc/pmacontrol/`, les données applicatives, vos certificats et les accès de récupération. La clé de chiffrement applicative fait partie de la configuration : une sauvegarde SQL seule ne suffit pas à restaurer les identifiants chiffrés.

Utilisez une sauvegarde MariaDB cohérente avec les moteurs de stockage présents. Un export `--single-transaction` seul ne garantit pas la cohérence de toutes les tables si plusieurs moteurs sont utilisés. Pour une copie de fichiers ou un snapshot, arrêtez la collecte et MariaDB dans une fenêtre prévue, ou employez un mécanisme de sauvegarde validé pour votre moteur et votre version. Testez la restauration sur une instance isolée avant de compter sur la sauvegarde.

```
/usr/share/pmacontrol/          application
/usr/bin/pmacontrol             CLI
/etc/pmacontrol/                configuration
```

```
/etc/pmacontrol/frankenphp.d/           operator TLS policy
/etc/pmacontrol/trusted-proxies         immediate trusted proxy peers
/var/lib/pmacontrol/                   persistent application data
/var/lib/mysql/                        local MariaDB data
/var/cache/pmacontrol/tmp/              application cache and logs
/etc/frankenphp/php.d/pmacontrol.ini    packaged PHP settings
/root/pmacontrol-install.env            bootstrap recovery credentials
```

10. Mettre à jour PmaControl

Avant toute mise à jour, préparez une sauvegarde restaurable des données et de la configuration et lisez les notes de la version candidate. Le post-install applique les migrations et remet les daemons dans leur état prévu ; les tâches volontairement arrêtées doivent le rester. La procédure normale est une mise à jour du paquet, pas un `git pull` dans `/usr/share/pmacontrol`.

Après la mise à jour, refaites les contrôles de la section 5, une connexion utilisateur et le contrôle de fraîcheur de collecte. Une régression peut exiger une restauration coordonnée du code **et** de la base : réinstaller un ancien paquet ne constitue pas un rollback de schéma.

```
sudo apt-get update
apt-cache policy pmacontrol
sudo apt-get -s install --only-upgrade pmacontrol
sudo apt-get install --only-upgrade pmacontrol
sudo dpkg --audit
systemctl is-active mariadb frankenphp cron
```

11. Docker : état actuel et choix de déploiement

État vérifié le 26 septembre 2026 : le dépôt actuel ne fournit pas de Dockerfile, de Compose ni de référence d'image PmaControl pour une installation complète supportée. Les fichiers Docker présents concernent des outils ou des bases de test. Il serait trompeur de proposer `docker pull pmacontrol/pmacontrol` sans image publiée et vérifiée.

Le paquet APT utilise systemd, MariaDB locale, cron, les droits de fichiers et des contrôles de listeners au démarrage. Le déposer dans une image PHP générique ne reproduit pas cette installation. Un portage Docker doit gérer l'initialisation et la réexécution, les volumes persistants, les secrets, les migrations, les daemons, les contrôles de santé et une restauration testée.

Vous pouvez dès maintenant installer PmaControl dans une VM Debian ou Ubuntu avec ce guide et superviser les serveurs MariaDB / MySQL qui tournent dans Docker, à condition que leurs adresses SQL soient accessibles. L'adresse `localhost` vue depuis un conteneur est celle du conteneur, pas celle de la VM PmaControl. Une procédure d'installation de PmaControl lui-même dans Docker sera ajoutée avec une image et des tests reproductibles ; elle ne doit pas être confondue avec la supervision de bases conteneurisées.

12. Diagnostiquer une installation incomplète

Commencez par les journaux et l'état des paquets. En cas d'erreur APT, vérifiez la suite, l'architecture, l'heure, la clé et l'accès réseau. En cas de conflit de ports, identifiez le service puis choisissez où héberger PmaControl ; le paquet ne doit pas interrompre un autre site. En cas d'erreur TLS, vérifiez DNS, challenges, certificat et permissions. Si le web fonctionne mais les graphiques restent anciens, contrôlez les connexions SQL/SSH, les daemons et les erreurs de collecte.

```
sudo journalctl -u frankenphp -u mariadb -u cron --since '-30 min' --no-pager
sudo tail -n 100 /var/cache/pmacontrol/tmp/log/error_php.log
sudo tail -n 100 /var/log/apt/term.log
sudo dpkg --audit
sudo ss -ltnp '( sport = :80 or sport = :443 )'
sudo ss -lunp 'sport = :443'
```

Après avoir corrigé **la cause signalée**, relancez la configuration avec les commandes suivantes. Une rotation de daemons échouée peut aussi nécessiter `sudo runuser -u www-data -- pmacontrol Daemon startAll`, mais uniquement pour reprendre l'état sauvegardé de cette opération et vérifier un unique résultat JSON `ok: true`. Ne supprimez pas la clé de chiffrement ou le fichier d'accès pour forcer un nouveau bootstrap.

```
sudo dpkg --configure -a
sudo apt-get -f install
```

13. Retirer le paquet

Commencez par sauvegarder et vérifier les données que vous voulez conserver. Simulez la suppression, puis retirez le paquet si c'est bien votre intention. `purge` est une opération

différente et ne remplace pas un plan de conservation. Les fichiers TLS opérateur peuvent rester sur disque ; contrôlez les services et les données conservées avant de réutiliser la machine.

```
sudo apt-get -s remove pmacontrol
sudo apt-get remove pmacontrol
```

14. Contrôle de mise en service

- Le paquet est configuré et les services nécessaires sont actifs.
- Le nom DNS et le certificat correspondent ; l'accès normal fonctionne sans `-k`.
- Les accès administrateur et webservice sont conservés de manière sûre.
- Un serveur MariaDB / MySQL répond au test de connexion.
- La collecte produit des échantillons récents et des graphiques cohérents.
- Les droits, la rétention et le stockage sont adaptés aux fonctions activées.
- Une sauvegarde complète peut être restaurée sur une instance isolée.

Sources et périmètre de vérification. Ce guide s'appuie sur les scripts d'installation et la documentation du dépôt officiel, ainsi que sur les index APT et le paquet 5.4.36-1 consultés le 26 septembre 2026. La signature de l'index a été vérifiée. Cette vérification documentaire ne constitue pas un nouveau test d'installation sur chacune des quatre distributions.

- PmaControl — Debian
- PmaControl — Ubuntu
- PmaControl — APT
- PmaControl — APT repository