DOCUMENTATION D'EXPLOITATION

Centralisation des logs SMTP

Postfix / Rsyslog → SRV-LOG-01

Collecte centralisée, séparation SMTP-01 / SMTP-02, transport TCP et validation des flux.

Collecteur	Transport	Version
SRV-LOG-01	Rsyslog TCP/514	1.0

Objectif — centraliser sur un seul serveur les journaux Postfix des deux nœuds SMTP tout en conservant une séparation claire par serveur. Le collecteur doit permettre l'analyse d'incidents, le suivi des files, les refus SMTP et les événements du listener PROXY protocol.

Centralisation des logs SMTP - Rsyslog + Postfix

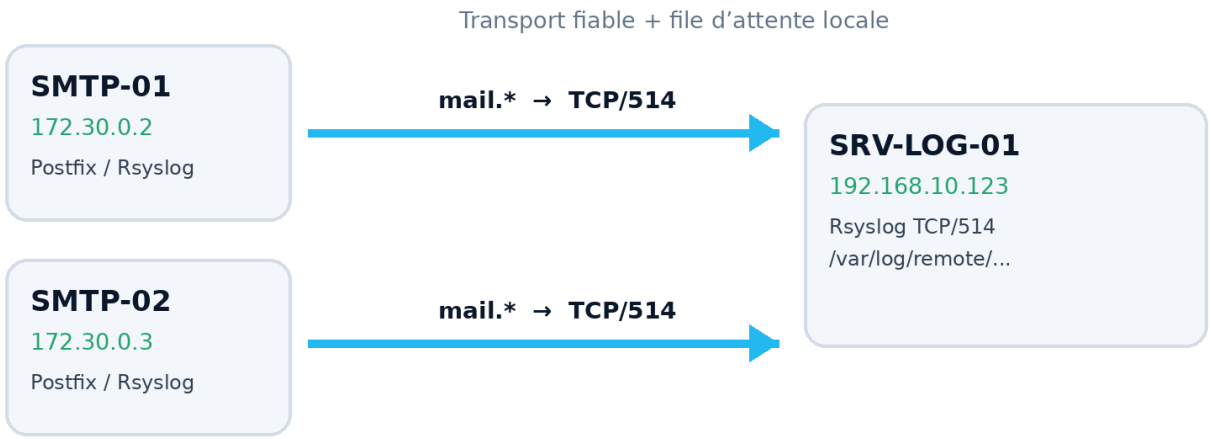

Figure 1 — Architecture de centralisation retenue.

1. Objectif et périmètre

Cette procédure met en place un flux Rsyslog depuis SMTP-01 et SMTP-02 vers SRV-LOG-01. Les événements de la facility mail sont transportés en TCP sur le port 514 puis écrits dans deux fichiers distincts sur le collecteur.

- SMTP-01 : 172.30.0.2 → /var/log/remote/smtp-01/mail.log
- SMTP-02 : 172.30.0.3 → /var/log/remote/smtp-02/mail.log
- Collecteur : SRV-LOG-01 — 192.168.10.123 — écoute Rsyslog TCP/UDP 514
- Flux centralisé : Postfix smtpd, proxy-smtpd, qmgr, smtp, cleanup, bounce et autres processus utilisant la facility mail.

Résultat obtenu — les deux fichiers distants reçoivent effectivement les événements Postfix. La capture de validation montre des événements distincts préfixés SMTP-01 et SMTP-02 sur SRV-LOG-01.

2. Pourquoi utiliser TCP et une file d'attente Rsyslog ?

Le transport TCP a été retenu plutôt qu'un envoi UDP simple afin de réduire le risque de perte de journaux lors d'une indisponibilité temporaire du collecteur. La configuration omfwd utilise en plus une file d'attente LinkedList et un nombre de tentatives illimité.

```
action.resumeRetryCount="-1"
queue.type="LinkedList"
queue.filename="smtp01-forward"
```

Point d'exploitation — si SRV-LOG-01 devient momentanément indisponible, Rsyslog peut mettre en attente les événements côté SMTP au lieu d'abandonner immédiatement le flux.

3. Architecture retenue

Composant	Rôle	Adresse	Port / protocole
SMTP-01	Émetteur Postfix/Rsyslog	172.30.0.2	TCP/514
SMTP-02	Émetteur Postfix/Rsyslog	172.30.0.3	TCP/514
SRV-LOG-01	Collecte + routage + stockage	192.168.10.123	Rsyslog TCP/514

4. Configuration Rsyslog sur SMTP-01

Créer un fichier dédié afin de ne transférer que la facility mail. Cette approche évite d'envoyer inutilement tous les journaux système du serveur.

```
# /etc/rsyslog.d/60-forward-smtp.conf
mail.* action(
   type="omfwd"
   target="192.168.10.123"
   port="514"
   protocol="tcp"
   action.resumeRetryCount="-1"
   queue.type="LinkedList"
   queue.filename="smtp01-forward"
)
```

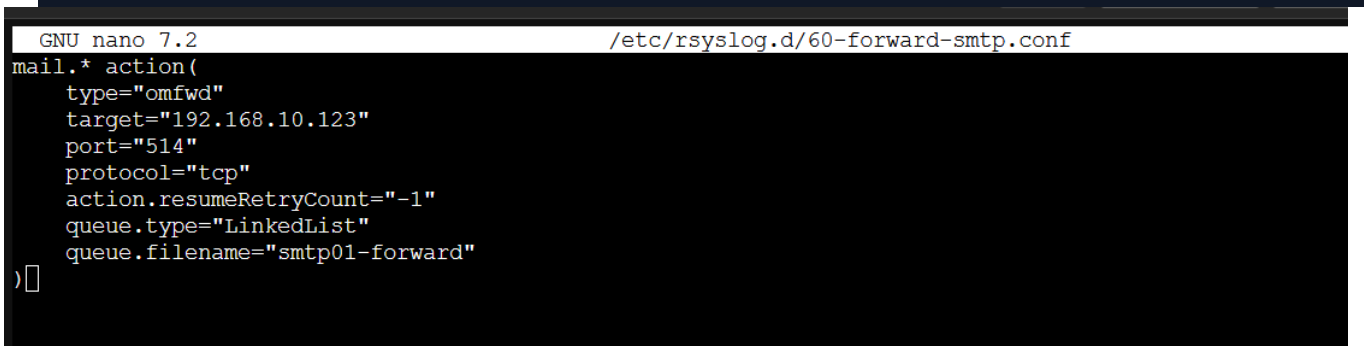

Figure 2 — Configuration réelle de transfert sur SMTP-01.

5. Configuration Rsyslog sur SMTP-02

La configuration est identique ; seul le nom de la file disque/logique est différencié afin de faciliter le diagnostic local.

```
# /etc/rsyslog.d/60-forward-smtp.conf
mail.* action(
   type="omfwd"
   target="192.168.10.123"
   port="514"
   protocol="tcp"
   action.resumeRetryCount="-1"
   queue.type="LinkedList"
   queue.filename="smtp02-forward"
)
```

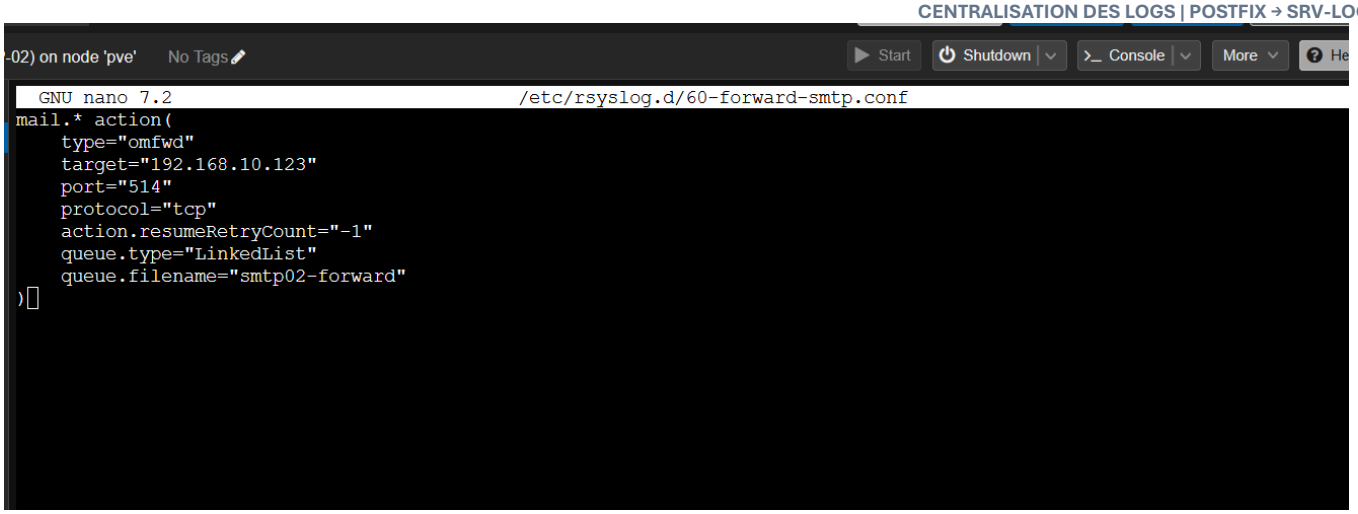

Figure 3 — Configuration réelle de transfert sur SMTP-02.

6. Validation des deux émetteurs

```
rsyslogd -N1
systemctl restart rsyslog
```

La commande rsyslogd -N1 doit terminer sans erreur. Après validation, le service Rsyslog est redémarré sur chacun des deux serveurs SMTP.

Vigilance — si le collecteur n'est pas joignable, vérifier d'abord la route réseau et le port TCP/514 avant de modifier la configuration Rsyslog.

7. Préparation du collecteur SRV-LOG-01

Le collecteur doit écouter sur le port 514. Dans l'environnement existant, l'écoute TCP et UDP est déjà activée dans /etc/rsyslog.conf.

```
module(load="imudp")
input(type="imudp" port="514")

module(load="imtcp")
input(type="imtcp" port="514")

rsyslogd -N1
systemctl restart rsyslog
ss -lntup | grep ':514'
```

8. Création des répertoires de stockage

```
mkdir -p /var/log/remote/smtp-01
mkdir -p /var/log/remote/smtp-02
```

Les fichiers mail.log n'ont pas besoin d'être créés manuellement : l'action omfile peut les créer lors de la première réception, sous réserve que le répertoire parent existe et soit accessible à Rsyslog.

9. Routage des événements par serveur

Le filtrage est réalisé avec $fromhost-ip et $syslogfacility-text. Les IP sources permettent de séparer clairement SMTP-01 et SMTP-02 même si les deux utilisent les mêmes programmes Postfix.

```
# /etc/rsyslog.d/40-smtp.conf
if ($fromhost-ip == "172.30.0.2" and $syslogfacility-text == "mail") then {
    action(
        type="omfile"
        file="/var/log/remote/smtp-01/mail.log"
    )
    stop
}

if ($fromhost-ip == "172.30.0.3" and $syslogfacility-text == "mail") then {
    action(
        type="omfile"
        file="/var/log/remote/smtp-02/mail.log"
    )
    stop
}
```

```
  GNU nano 8.4                                                  /etc/rsyslog.d/40-smtp.conf
if ($fromhost-ip == "172.30.0.2" and $syslogfacility-text == "mail") then {
    action(
        type="omfile"
        file="/var/log/remote/smtp-01/mail.log"
    )
    stop
}

if ($fromhost-ip == "172.30.0.3" and $syslogfacility-text == "mail") then {
    action(
        type="omfile"
        file="/var/log/remote/smtp-02/mail.log"
    )
    stop
}
```

Figure 4 — Règles de routage réelles sur SRV-LOG-01.

Pourquoi stop ? — après l'écriture dans le fichier cible, stop interrompt le traitement de l'événement par les règles suivantes. Cela limite les duplications dans d'autres journaux généraux du collecteur.

10. Validation de bout en bout

Sur SRV-LOG-01, suivre chaque fichier dans un terminal distinct :

```
tail -f /var/log/remote/smtp-01/mail.log

tail -f /var/log/remote/smtp-02/mail.log
```

Pour générer un événement de test explicite depuis chaque serveur SMTP :

```
# sur SMTP-01
logger -p mail.info "TEST CENTRALISATION SMTP-01"

# sur SMTP-02
logger -p mail.info "TEST CENTRALISATION SMTP-02"
```

Dans la validation réelle, les deux fichiers ont reçu des événements Postfix du listener proxy-smtpd. La capture ci-dessous constitue la preuve de réception simultanée des deux nœuds.

```
root@SRV-LOG-01:~# mkdir -p /var/log/remote/smtp-01
mkdir -p /var/log/remote/smtp-02
root@SRV-LOG-01:~# tail -f /var/log/remote/smtp-01/mail.log
2026-08-25T14:11:21+02:00 SMTP-01 postfix/proxy-smtpd/smtpd[170858 disconnect from unknown[172.30.0.1] commands=0/0
2026-08-25T14:11:23+02:00 SMTP-01 postfix/proxy-smtpd/smtpd[170858 connect from unknown[172.30.0.1]
2026-08-25T14:11:23+02:00 SMTP-01 postfix/proxy-smtpd/smtpd[170858 lost connection after CONNECT from unknown[172.30.0.1]
2026-08-25T14:11:23+02:00 SMTP-01 postfix/proxy-smtpd/smtpd[170858 disconnect from unknown[172.30.0.1] commands=0/0
2026-08-25T14:11:25+02:00 SMTP-01 postfix/proxy-smtpd/smtpd[170858 connect from unknown[172.30.0.1]
2026-08-25T14:11:25+02:00 SMTP-01 postfix/proxy-smtpd/smtpd[170858 lost connection after CONNECT from unknown[172.30.0.1]
2026-08-25T14:11:25+02:00 SMTP-01 postfix/proxy-smtpd/smtpd[170858 disconnect from unknown[172.30.0.1] commands=0/0
2026-08-25T14:11:27+02:00 SMTP-01 postfix/proxy-smtpd/smtpd[170858 connect from unknown[172.30.0.1]
2026-08-25T14:11:27+02:00 SMTP-01 postfix/proxy-smtpd/smtpd[170858 lost connection after CONNECT from unknown[172.30.0.1]
2026-08-25T14:11:27+02:00 SMTP-01 postfix/proxy-smtpd/smtpd[170858 disconnect from unknown[172.30.0.1] commands=0/0
2026-08-25T14:11:29+02:00 SMTP-01 postfix/proxy-smtpd/smtpd[170858 connect from unknown[172.30.0.1]
2026-08-25T14:11:29+02:00 SMTP-01 postfix/proxy-smtpd/smtpd[170858 lost connection after CONNECT from unknown[172.30.0.1]
2026-08-25T14:11:29+02:00 SMTP-01 postfix/proxy-smtpd/smtpd[170858 disconnect from unknown[172.30.0.1] commands=0/0
2026-08-25T14:11:31+02:00 SMTP-01 postfix/proxy-smtpd/smtpd[170858 connect from unknown[172.30.0.1]
2026-08-25T14:11:31+02:00 SMTP-01 postfix/proxy-smtpd/smtpd[170858 lost connection after CONNECT from unknown[172.30.0.1]
2026-08-25T14:11:31+02:00 SMTP-01 postfix/proxy-smtpd/smtpd[170858 disconnect from unknown[172.30.0.1] commands=0/0
^C
root@SRV-LOG-01:~# tail -f /var/log/remote/smtp-02/mail.log
2026-08-25T14:11:29+02:00 SMTP-02 postfix/proxy-smtpd/smtpd[208205 disconnect from unknown[172.30.0.1] commands=0/0
2026-08-25T14:11:31+02:00 SMTP-02 postfix/proxy-smtpd/smtpd[208205 connect from unknown[172.30.0.1]
2026-08-25T14:11:31+02:00 SMTP-02 postfix/proxy-smtpd/smtpd[208205 lost connection after CONNECT from unknown[172.30.0.1]
2026-08-25T14:11:31+02:00 SMTP-02 postfix/proxy-smtpd/smtpd[208205 disconnect from unknown[172.30.0.1] commands=0/0
2026-08-25T14:11:33+02:00 SMTP-02 postfix/proxy-smtpd/smtpd[208205 connect from unknown[172.30.0.1]
2026-08-25T14:11:33+02:00 SMTP-02 postfix/proxy-smtpd/smtpd[208205 lost connection after CONNECT from unknown[172.30.0.1]
2026-08-25T14:11:33+02:00 SMTP-02 postfix/proxy-smtpd/smtpd[208205 disconnect from unknown[172.30.0.1] commands=0/0
2026-08-25T14:11:35+02:00 SMTP-02 postfix/proxy-smtpd/smtpd[208205 connect from unknown[172.30.0.1]
2026-08-25T14:11:35+02:00 SMTP-02 postfix/proxy-smtpd/smtpd[208205 lost connection after CONNECT from unknown[172.30.0.1]
2026-08-25T14:11:35+02:00 SMTP-02 postfix/proxy-smtpd/smtpd[208205 disconnect from unknown[172.30.0.1] commands=0/0
2026-08-25T14:11:37+02:00 SMTP-02 postfix/proxy-smtpd/smtpd[208205 connect from unknown[172.30.0.1]
2026-08-25T14:11:37+02:00 SMTP-02 postfix/proxy-smtpd/smtpd[208205 lost connection after CONNECT from unknown[172.30.0.1]
2026-08-25T14:11:37+02:00 SMTP-02 postfix/proxy-smtpd/smtpd[208205 disconnect from unknown[172.30.0.1] commands=0/0
2026-08-25T14:11:39+02:00 SMTP-02 postfix/proxy-smtpd/smtpd[208205 connect from unknown[172.30.0.1]
2026-08-25T14:11:39+02:00 SMTP-02 postfix/proxy-smtpd/smtpd[208205 lost connection after CONNECT from unknown[172.30.0.1]
2026-08-25T14:11:39+02:00 SMTP-02 postfix/proxy-smtpd/smtpd[208205 disconnect from unknown[172.30.0.1] commands=0/0
^C
root@SRV-LOG-01:~#
```

Figure 5 — Preuve de réception des logs SMTP-01 et SMTP-02 sur SRV-LOG-01.

Interprétation — les événements affichés connect/disconnect et lost connection after CONNECT sont des connexions sur le listener Postfix proxy-smtpd. Les connexions très régulières depuis 172.30.0.1 peuvent correspondre aux health checks HAProxy ; un vrai échange SMTP client doit être vérifié séparément pour confirmer l'adresse client transmise par PROXY protocol.

11. Journaux Postfix utiles à rechercher

- postfix/proxy-smtpd ou postfix/smtpd : connexions entrantes, EHLO, restrictions et refus.
- postfix/qmgr : entrée/sortie de messages dans la queue.
- postfix/smtp : livraison vers les serveurs distants et codes SMTP reçus.
- postfix/cleanup : préparation des messages et identifiants de queue.
- postfix/bounce : génération des notifications d'échec.
- status=deferred : messages temporairement non livrés.
- Relay access denied / reject_unauth_destination : tentatives de relay refusées.

12. Commandes de diagnostic rapides

```
# Vérifier la syntaxe Rsyslog
rsyslogd -N1

# Vérifier l'écoute du collecteur
ss -lntup | grep ':514'

# Vérifier la connectivité depuis un SMTP
nc -vz 192.168.10.123 514

# Suivre les deux fichiers centralisés
tail -f /var/log/remote/smtp-01/mail.log
tail -f /var/log/remote/smtp-02/mail.log

# Chercher les erreurs de livraison
grep -E 'status=(deferred|bounced)|Relay access denied' /var/log/remote/smtp-01/mail.log

# Chercher une queue ID précise
grep 'QUEUE_ID' /var/log/remote/smtp-01/mail.log
```

13. Sécurité du collecteur

Le port 514 ne doit pas être exposé plus largement que nécessaire. Dans ce scénario, seuls SMTP-01 et SMTP-02 ont besoin d'atteindre SRV-LOG-01 en TCP/514.

```
iptables -A INPUT -p tcp -s 172.30.0.2 --dport 514 -j ACCEPT
iptables -A INPUT -p tcp -s 172.30.0.3 --dport 514 -j ACCEPT
# règle de refus générale ensuite, selon la politique du pare-feu
```

Point de vigilance — si SRV-LOG-01 collecte aussi d'autres équipements sur 514, ne pas ajouter un DROP global qui casserait leurs flux. Adapter les sources autorisées à l'ensemble des producteurs légitimes.

14. Rotation et rétention

Les mail.log centralisés peuvent croître rapidement, notamment en cas de spam, de boucle de retry ou de forte activité SMTP. Une rotation doit être prévue.

```
# Exemple /etc/logrotate.d/remote-smtp
/var/log/remote/smtp-01/mail.log
/var/log/remote/smtp-02/mail.log {
    daily
    rotate 14
    compress
    delaycompress
    missingok
    notifempty
    create 0640 syslog adm
}
```

À adapter — la durée de rétention doit correspondre aux besoins d'exploitation, de sécurité et de conformité. Vérifier aussi l'utilisateur effectif utilisé par Rsyslog avant de figer les droits create.

15. Dépannage

Symptôme	Contrôles prioritaires
Aucun fichier créé	Vérifier mkdir du répertoire parent, rsyslogd -N1, droits et arrivée d'un premier événement.
Aucun log reçu	Tester nc -vz 192.168.10.123 514 depuis le SMTP ; vérifier firewall/routage.
Tous les logs vont dans le même fichier	Contrôler $fromhost-ip et les IP réellement vues par SRV-LOG-01.
Logs dupliqués ailleurs	Vérifier la présence de stop après chaque action omfile.
Beaucoup de connect/disconnect 172.30.0.1	Peut correspondre aux health checks HAProxy ; vérifier avec un vrai test SMTP externe.
Le collecteur est indisponible	Vérifier que la queue omfwd est active et surveiller l'espace disque côté SMTP.

16. Checklist de remise en service

☐ SRV-LOG-01 écoute bien sur TCP/514.

☐ Les répertoires /var/log/remote/smtp-01 et smtp-02 existent.

☐ Le fichier 40-smtp.conf passe rsyslogd -N1.

☐ SMTP-01 et SMTP-02 passent rsyslogd -N1.

☐ Les deux SMTP atteignent 192.168.10.123:514.

☐ Un logger -p mail.info apparaît dans le bon fichier central.

☐ Les vrais événements Postfix arrivent après un test SMTP.

☐ La rotation des fichiers est en place et l'espace disque est surveillé.

17. Conclusion

La centralisation Postfix est fonctionnelle : SMTP-01 et SMTP-02 transfèrent leur facility mail en TCP vers SRV-LOG-01, qui sépare ensuite les événements dans deux fichiers dédiés. Cette architecture fournit un point d'analyse unique pour les incidents SMTP et prépare la mise en place d'alertes, de corrélations et d'une supervision plus avancée.

État du déploiement — fonctionnel et validé par la réception simultanée d'événements Postfix provenant des deux serveurs SMTP sur SRV-LOG-01.