DOCUMENTATION D'EXPLOITATION

Centralisation des logs Nginx

Catelsys → SRV-LOG-01

Réception Syslog, redirection NAT, séparation des access/error logs et validation du flux.

Serveur de collecte	Date de validation	Version
SRV-LOG-01	**22 juin 2026**	**1.0**

Objectif du volet — centraliser les logs Nginx d'un serveur web Catelsys sur SRV-LOG-01, puis préparer la séparation des journaux d'accès et d'erreurs dans des fichiers distincts.

1. Objectif et périmètre

Cette procédure décrit la mise en place d'un flux Syslog entre le serveur Nginx de Catelsys et le serveur central de logs SRV-LOG-01. Le flux permet de conserver les logs Nginx à distance, de simplifier l'analyse des erreurs et de disposer d'un point de collecte unique.

Résultat obtenu — les logs Nginx ont commencé à être reçus par SRV-LOG-01. La séparation finale est configurée grâce à deux tags dédiés : www_catelsys_access et www_catelsys_error ; elle sera confirmée à la première écriture dans chaque fichier cible.

2. Architecture retenue

Composant	Rôle	Adresse / FQDN	Port / protocole
Serveur Nginx	Émetteur des logs web	Catelsys / srv-nginx	UDP Syslog 514
Point d'entrée public	FQDN utilisé par Nginx	domont.sadek.ovh	514
Pare-feu	Redirection NAT	WAN → SRV-LOG-01	TCP/UDP 514
Collecteur	Réception et écriture des logs	192.168.10.123	Rsyslog 514

Le serveur Nginx envoie les événements vers le FQDN domont.sadek.ovh sur le port 514. Le pare-feu reçoit ce trafic côté WAN et le redirige vers SRV-LOG-01 (192.168.10.123), où Rsyslog écoute les flux Syslog.

3. Redirection NAT sur le pare-feu

Une règle de redirection est active sur l'interface WAN. Elle accepte le trafic TCP/UDP reçu sur le port 514 par le pare-feu et le transfère vers SRV-LOG-01 sur le même port.

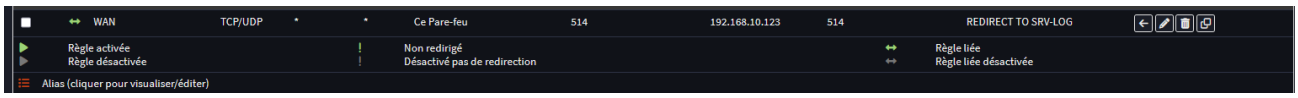

Figure 1 — Règle NAT « REDIRECT TO SRV-LOG » : WAN, TCP/UDP 514 → 192.168.10.123:514.

Point de vigilance sécurité — le port Syslog 514 est exposé via la redirection WAN. Dès que les adresses sources sont stabilisées, il est recommandé de limiter la règle NAT/firewall à l'IP publique du ou des serveurs autorisés à envoyer des logs.

4. Préparation de SRV-LOG-01 : réception Rsyslog

La configuration principale de Rsyslog a été ajustée dans /etc/rsyslog.conf pour écouter les messages Syslog reçus en UDP et TCP sur le port 514.

```
# /etc/rsyslog.conf

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")
```

Même si la configuration Nginx observée émet les messages via Syslog UDP, l'écoute TCP a également été activée afin de permettre la réception d'autres équipements ou services utilisant ce protocole.

5. Validation de l'écoute Rsyslog

Après modification de la configuration, la syntaxe a été validée puis le service redémarré. La commande ss confirme l'écoute active sur IPv4 et IPv6, en UDP comme en TCP.

```
root@SRV-LOG-01:~# rsyslogd -N1
rsyslogd: version 8.2504.0, config validation run (level 1), master config /etc/rsyslog.conf
rsyslogd: End of config validation run. Bye.

root@SRV-LOG-01:~# systemctl restart rsyslog

root@SRV-LOG-01:~# ss -lntup | grep ':514'
udp   UNCONN 0 0 0.0.0.0:514 0.0.0.0:* users:(("rsyslogd",pid=14451,fd=6))
udp   UNCONN 0 0 [::]:514 [::]:* users:(("rsyslogd",pid=14451,fd=7))
tcp   LISTEN 0 25 0.0.0.0:514 0.0.0.0:* users:(("rsyslogd",pid=14451,fd=8))
tcp   LISTEN 0 25 [::]:514 [::]:* users:(("rsyslogd",pid=14451,fd=9))
```

Validation — la vérification rsyslogd -N1 ne retourne aucune erreur et les quatre écouteurs nécessaires sont visibles sur le port 514.

6. Configuration Nginx sur Catelsys

La configuration Nginx a été modifiée afin d'envoyer les access logs et les error logs vers SRV-LOG-01. Deux tags distincts sont utilisés pour permettre le routage vers deux fichiers séparés côté collecteur.

```
include snippets/block-dangerous-php.conf;

access_log syslog:server=domont.sadek.ovh:514,facility=local7,tag=www_catelsys_access,severity=info
combined;

error_log syslog:server=domont.sadek.ovh:514,facility=local7,tag=www_catelsys_error warn;
```

La directive include conserve le mécanisme de blocage des fichiers PHP dangereux. Les deux directives de logs utilisent la facility local7 afin d'isoler ce flux applicatif des autres journaux système.

Élément	Rôle
server=domont.sadek.ovh:514	Point d'entrée public utilisé pour joindre le serveur de collecte via la redirection NAT.
facility=local7	Facility dédiée aux journaux Nginx de Catelsys afin de faciliter le filtrage.
www_catelsys_access	Tag réservé aux access logs Nginx.
www_catelsys_error	Tag réservé aux error logs Nginx.
severity=info	Niveau Syslog attribué aux access logs.
warn	Niveau minimal utilisé pour les messages error_log. Il se place à la fin de la directive, sans severity=.
combined	Format d'accès Nginx classique contenant notamment IP client, requête, code HTTP et user-agent.

7. Règles de routage dans Rsyslog

Un fichier de règles dédié a été créé sur SRV-LOG-01 afin de diriger les deux tags Nginx vers des fichiers distincts.

```
# /etc/rsyslog.d/30-catelsys-nginx.conf

if ($programname == "www_catelsys_access") then {
    action(
        type="omfile"
        file="/var/log/remote/catelsys/nginx-access.log"
    )
    stop
}

if ($programname == "www_catelsys_error") then {
    action(
        type="omfile"
        file="/var/log/remote/catelsys/nginx-error.log"
    )
    stop
}
```

Le mot-clé stop met fin au traitement après l'écriture dans le fichier cible. Il évite qu'un même événement soit ensuite repris par des règles générales de Rsyslog et dupliqué dans des journaux système.

8. Création du répertoire cible et chargement des règles

```
root@SRV-LOG-01:~# mkdir -p /var/log/remote/catelsys

root@SRV-LOG-01:~# rsyslogd -N1
rsyslogd: version 8.2504.0, config validation run (level 1), master config /etc/rsyslog.conf
rsyslogd: End of config validation run. Bye.

root@SRV-LOG-01:~# systemctl restart rsyslog
```

Comportement attendu — seul le répertoire /var/log/remote/catelsys doit être créé à l'avance. Les fichiers nginx-access.log et nginx-error.log sont créés automatiquement par Rsyslog/omfile à la première réception du flux correspondant.

9. Validation côté Nginx

```
nginx -t
systemctl reload nginx
```

Après le rechargement, une requête vers le site déclenche l'envoi d'une ligne d'access log vers le collecteur. Les fichiers de destination peuvent être suivis en temps réel sur SRV-LOG-01.

```
tail -f /var/log/remote/catelsys/nginx-access.log

tail -f /var/log/remote/catelsys/nginx-error.log
```

10. Preuve de réception du flux

Le serveur de logs a reçu un message Nginx valide portant le tag www_catelsys. Cet exemple a été capturé avant l'adoption des tags finaux distincts et correspond à une requête HTTP enregistrée dans le format combined.

```
2026-06-22T22:35:13+02:00 srv-nginx www_catelsys: 66.249.65.70 - - [22/Jun/2026:22:35:13 +0200] "GET
/article/loosest-slots-at-hollywood-casino.html HTTP/1.1" 404 241 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X
Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/148.0.7778.96 Mobile Safari/537.36 (compatible;
Googlebot/2.1; +http://www.google.com/bot.html)"
```

Interprétation — le message prouve que le chemin Nginx → domont.sadek.ovh:514 → NAT → SRV-LOG-01 → Rsyslog est opérationnel. Le code HTTP 404 correspond à une ressource demandée mais absente ; ce comportement est attendu pour ce type de requête.

11. Observation : trafic parasite sur le port Syslog

Un message non interprétable a également été reçu sur le port 514 :

```
2026-06-22T22:34:11.637879+02:00 109.190.94.232 [illegible]#006[illegible]#006[illegible]#021#021#015
```

Ce type de contenu ne correspond pas à un access log Nginx classique. Il peut s'agir d'un paquet non conforme, d'un scan ou d'un trafic parasite envoyé vers le port exposé. Cette observation renforce la nécessité de limiter la règle de pare-feu aux sources Syslog autorisées lorsque cela est possible.

12. Exploitation et points de contrôle

- Vérifier régulièrement l'arrivée des access logs dans /var/log/remote/catelsys/nginx-access.log.
- Consulter nginx-error.log lors d'incidents Nginx, PHP-FPM, FastCGI, reverse proxy ou erreurs applicatives.
- Conserver des tags distincts par application ou serveur afin de rendre les recherches et les alertes plus simples.
- Surveiller la croissance des fichiers et mettre en place une rotation adaptée (logrotate ou politique Rsyslog).
- Limiter la règle WAN/514 aux IP sources connues pour réduire la réception de trafic parasite.
- Prévoir, à terme, un mécanisme de transport chiffré et authentifié si les journaux transitent par Internet ou contiennent des données sensibles.

13. Commandes de diagnostic rapides

```
# Vérifier que Rsyslog écoute sur le port attendu
ss -lntup | grep ':514'

# Vérifier la syntaxe des règles Rsyslog
rsyslogd -N1

# Vérifier la configuration Nginx
nginx -t

# Suivre les fichiers Nginx centralisés
tail -f /var/log/remote/catelsys/nginx-access.log
tail -f /var/log/remote/catelsys/nginx-error.log

# Vérifier la résolution du FQDN utilisé par Nginx
getent ahostsv4 domont.sadek.ovh
```

14. Conclusion

Le volet de centralisation des logs Nginx de Catelsys est fonctionnel pour la réception Syslog. SRV-LOG-01 écoute les flux sur le port 514 en UDP et TCP, le pare-feu redirige le trafic WAN vers 192.168.10.123, et Nginx est configuré avec deux tags dédiés. La réception d'un access log a été confirmée ; la création effective des deux fichiers finaux doit être vérifiée après génération d'un événement access et d'un événement error. Cette séparation améliore la lisibilité et prépare une future supervision ou corrélation des événements de sécurité.

État du déploiement — fonctionnel pour la réception Syslog, validé par réception d'un access log Nginx. La séparation par tags est configurée ; elle doit être confirmée par l'apparition des deux fichiers après génération d'un access log puis d'un error log. La prochaine amélioration recommandée est le durcissement de la règle WAN/514 et la mise en place de la rotation / supervision des fichiers centralisés.