



# scriting

Astier Guillaume

09/01/2026



## Contents

<b>CIS services</b>	<b>2</b>
Services et binaires à activer et/ou supprimer . . . . .	2
function_Apply . . . . .	2
function_Check . . . . .	3
<b>CIS_Network</b>	<b>3</b>
Gestion du réseau . . . . .	3
<b>Cours : rsyslog syslog-ng journalctl</b>	<b>3</b>
Introduction . . . . .	3
Objectifs : . . . . .	3
Introduction à <b>rsyslog</b> . . . . .	4
Qu'est-ce que <b>rsyslog</b> ? . . . . .	4
Installation de <b>rsyslog</b> sur CentOS 7 . . . . .	4
Configuration de rsyslog . . . . .	4
Exemple de configuration simple . . . . .	4
Filtrage des messages . . . . .	5
Activer la rotation des logs avec logrotate : . . . . .	5
Démarrer et gérer rsyslog . . . . .	5
Introduction à syslog-ng . . . . .	5
Qu'est-ce que syslog-ng ? . . . . .	5
Installation de syslog-ng sur CentOS 7 . . . . .	6
Configuration de syslog-ng . . . . .	6
Comparaison entre <b>rsyslog</b> et <b>syslog-ng</b> . . . . .	7
Sécuriser les logs . . . . .	7
Sécurisation de l'envoi des logs . . . . .	7
Journalisation . . . . .	9
Fonctionnalités de <b>systemd-journald</b> : . . . . .	9
Le fichier de configuration : /etc/systemd/journald.conf . . . . .	9
Gestion des Journaux avec journalctl . . . . .	10
Commandes de base avec journalctl . . . . .	10
Filtrage avancé avec journalctl . . . . .	11
Utilisation de journalctl avec des options supplémentaires . . . . .	12
Gestion de la Taille des Journaux . . . . .	13
Paramètres de taille des journaux . . . . .	13
Sécurisation des Journaux . . . . .	13

---

Outils de dev . . . . .	14
un bon admin ? . . . . .	14
les protocoles . . . . .	15
ex de phpbb . . . . .	15
Programmation de base . . . . .	15
Steno . . . . .	15

## CIS services

Bien que l'application de mises à jour et de correctifs système permette de corriger les vulnérabilités connues, l'un des meilleurs moyens de protéger le système contre les vulnérabilités non encore signalées est de désactiver tous les services qui ne sont pas nécessaires au fonctionnement normal du système. Cela empêche l'exploitation des vulnérabilités découvertes ultérieurement. Si un service n'est pas activé, il ne peut pas être exploité. Les actions décrites dans cette section du document fournissent des conseils sur certains services qui peuvent être désactivés en toute sécurité et dans quelles circonstances, réduisant ainsi considérablement le nombre de menaces potentielles pour le système résultant. De plus, certains services qui doivent rester activés mais avec une configuration sécurisée sont couverts ainsi que les clients de services non sécurisés.

---

### Services et binaires à activer et/ou supprimer

- Vérifier que l'instance a le paquet chrony
  - Vérifier que le service chrony est lancé et que sa configuration est fonctionnelle
  - Vérifier que chrony n'est pas lancé en tant que root
  - Vérifier que les service autofs, samba, cups telnet et ftp ne sont pas activé
  - Vérifier que le server X n'est pas utilisé
  - Vérifier que les binaires ftp, ldap, nis et tftp ne sont pas présent sur le système
- 

### function\_Apply

- Créer une fonction permettant de lancer la désactivation de services
- Créer une fonction permettant la suppression de rpms

## **function\_Check**

- Créer une fonction permettant de vérifier la présence ou l'absence d'un service
- Créer une fonction permettant la présence ou l'absence de rpms

## **CIS\_Network**

Pour réduire la surface d'attaque d'un système, les périphériques inutilisés doivent être désactivés.

## **Gestion du réseau**

- Vérifier que le protocole IPV6 est désactivé
- Vérifier que les périphériques de type wifi sont désactivés
- Vérifier que les périphériques de type bluetooth sont désactivés
- Vérifier que l'ip forwarding est désactivé
- Vérifier que la redirection de paquet via l'icmp est désactivé
- Vérifier la présence d'un firewawll et de son activation

## **Cours : rsyslog syslog-ng journalctl**

### **Introduction**

Les systèmes Linux utilisent des outils de **journalisation** pour collecter et stocker des informations sur le fonctionnement du système, des applications, et des erreurs. Sur CentOS 7, deux des outils les plus courants sont **rsyslog** et **syslog-ng**. Ce cours va détailler leur installation, leur configuration et leurs différences.

### **Objectifs :**

- Comprendre le rôle de rsyslog et syslog-ng
  - Installer et configurer ces outils sur CentOS 7
  - Configurer la collecte des journaux et leur redirection
  - Gérer les fichiers de logs sur un serveur Linux
-

## Introduction à rsyslog

### Qu'est-ce que rsyslog ?

**rsyslog** est un démon de journalisation utilisé pour collecter et transmettre des messages de journalisation (logs) générés par le système et les applications. Il est très populaire sous Linux, car il est flexible et performant.

Il permet : - La collecte locale des logs - L'envoi des logs à un serveur distant - La gestion des fichiers de logs - Le filtrage et l'archivage des logs

---

### Installation de rsyslog sur CentOS 7

**rsyslog** est installé par défaut sur CentOS 7. Pour vérifier si rsyslog est installé, utilisez la commande suivante :

```
1 rpm -q rsyslog
```

Si rsyslog n'est pas installé, vous pouvez l'installer avec :

```
1 sudo yum install rsyslog
```

---

### Configuration de rsyslog

Le fichier principal de configuration de rsyslog se trouve dans /etc/rsyslog.conf. Vous pouvez y définir des règles pour la collecte et la redirection des logs.

### Exemple de configuration simple

Activer l'envoi de logs à un serveur distant :

```
1 *.* @logserver.example.com:514
```

---

## Filtrage des messages

```
1 authpriv.*    /var/log/secure
2 *.info        /var/log/messages
```

## Activer la rotation des logs avec logrotate :

Editez le fichier /etc/logrotate.conf pour configurer la fréquence de rotation et la conservation des logs.

---

## Démarrer et gérer rsyslog

Pour démarrer ou redémarrer le service rsyslog :

```
1 sudo systemctl start rsyslog
2 sudo systemctl enable rsyslog
```

---

Pour vérifier son statut :

```
1 sudo systemctl status rsyslog
```

---

## Introduction à syslog-ng

### Qu'est-ce que syslog-ng ?

syslog-ng est un autre démon de journalisation similaire à rsyslog, mais il offre plus de fonctionnalités avancées telles que le traitement des logs en temps réel, des filtrages plus poussés et une meilleure gestion des formats de logs.

---

## Installation de syslog-ng sur CentOS 7

Pour installer syslog-ng sur CentOS 7, vous devez d'abord activer le dépôt EPEL :

```
1 sudo yum install epel-release
2 sudo yum install syslog-ng
```

---

## Configuration de syslog-ng

Le fichier principal de configuration se trouve dans /etc/syslog-ng/syslog-ng.conf

### Exemple de configuration de base

**Définir une source :**

```
1 source s_local {
2     system();
3     internal();
4 };
```

**Définir une destination :**

```
1 destination d_file {
2     file("/var/log/messages");
3 };
```

**Définir une règle de filtrage :**

```
1 log { source(s_local); destination(d_file); };
```

**Envoi des logs à un serveur distant :**

```
1 destination d_remote {
2     tcp("logserver.example.com" port(514));
3 };
4 log { source(s_local); destination(d_remote); };
```

**Démarrer et gérer syslog-ng** Pour démarrer et activer le service syslog-ng :

```
1 sudo systemctl start syslog-ng
2 sudo systemctl enable syslog-ng
```

Vérifiez le statut avec :

```
1 sudo systemctl status syslog-ng
```

## Comparaison entre rsyslog et syslog-ng

Critère	rsyslog	syslog-ng
<b>Installation</b>	Par défaut sur CentOS 7	Nécessite l'installation via EPEL
<b>Facilité de configuration</b>	Configuration simple via <code>/etc/rsyslog.conf</code>	Configuration plus complexe mais plus flexible
<b>Protocole</b>	Utilise principalement UDP/TCP pour l'envoi à distance	Supporte plus de protocoles et formats
<b>Performances</b>	Très performant pour des logs classiques	Très performant avec une meilleure gestion des logs en temps réel
<b>Filtrage avancé</b>	Filtrage de base via <code>/etc/rsyslog.conf</code>	Filtrage avancé et personnalisation complète
<b>Soutien communautaire</b>	Large communauté, bien documenté	Moins répandu mais puissant pour des cas complexes

## Sécuriser les logs

### Sécurisation de l'envoi des logs

Lorsque vous envoyez des logs à un serveur distant, il est crucial de sécuriser la transmission pour éviter les interceptions. Vous pouvez utiliser TLS (Transport Layer Security) pour chiffrer les messages envoyés.

## Exemple de configuration avec TLS dans rsyslog :

### Installer les paquets nécessaires :

```
1 sudo yum install rsyslog-gnutls
```

### Modifier /etc/rsyslog.conf pour activer TLS

```
1 module(load="imtcp") # Charge le module TCP
2 input(type="imtcp" port="514")
3
4 $DefaultNetstreamDriver gtls
5 $DefaultNetstreamDriverCAFile /etc/rsyslog.d/ca.crt
6 $DefaultNetstreamDriverCertFile /etc/rsyslog.d/cert.crt
7 $DefaultNetstreamDriverKeyFile /etc/rsyslog.d/cert.key
8 *.* @logserver.example.com:514
```

## Exemple de configuration avec TLS dans syslog-ng :

### Générer un certificat :

```
1 openssl req -new -x509 -days 365 -keyout /etc/syslog-ng/cert.key -out /etc/syslog-ng/cert.crt
```

### Modifier /etc/syslog-ng/syslog-ng.conf pour activer TLS :

```
1 destination d_tls {
2     tcp("logserver.example.com" port(514)
3         tls(cert_file("/etc/syslog-ng/cert.crt") key_file("/etc/syslog-
4             ng/cert.key") ca_file("/etc/syslog-ng/ca.crt")));
5     };
6 log { source(s_local); destination(d_tls); };
```

## Journalisation

**systemd-journald** est un service de journalisation intégré à **systemd**, qui est devenu l'outil par défaut de gestion des processus et des services sous CentOS 7. **journald** est responsable de la collecte, de la gestion et du stockage des journaux système, des logs d'applications et des messages du noyau dans un format binaire.

Contrairement aux systèmes traditionnels comme **syslog**, qui utilisent des fichiers texte, **journald** stocke les journaux dans un format binaire qui permet une gestion plus efficace et un accès plus rapide aux données.

---

### Fonctionnalités de **systemd-journald** :

- Journalisation des messages des services **systemd** et des applications.
  - Collecte des journaux du noyau (kernel logs).
  - Support de la journalisation persistante (les logs peuvent être stockés sur disque dur).
  - Gestion automatique de la taille des journaux et des fichiers.
  - Indexation des journaux pour une consultation rapide avec **journalctl**.
- 

### Le fichier de configuration : `/etc/systemd/journald.conf`

Le fichier `/etc/systemd/journald.conf` permet de configurer le comportement de **journald**. Ce fichier contient plusieurs paramètres importants, notamment la gestion du stockage des journaux et leur rétention.

Voici quelques paramètres importants à connaître :

- **Storage** : Détermine où les journaux sont stockés. Les options sont :
  - **persistent** : Les journaux sont stockés sur disque dans `/var/log/journal/` (journalisation persistante).
  - **volatile** : Les journaux sont stockés en mémoire (les logs seront perdus au redémarrage).
  - **auto** : Choisit **persistent** si le répertoire `/var/log/journal/` existe, sinon utilise **volatile**.

- **MaxRetentionSec** : Définit la durée maximale pendant laquelle les journaux sont conservés. Par exemple, `MaxRetentionSec=1month` conservera les logs pendant 1 mois.

- **MaxFileSec** : Définit la durée de rétention des fichiers journaux individuels.

#### **Exemple de fichier `/etc/systemd/journald.conf`:**

```
1 [Journal]
2 Storage=persistent
3 MaxRetentionSec=1month
4 MaxFileSec=1week
```

Après avoir modifié ce fichier, vous devez redémarrer `systemd-journald` pour que les changements prennent effet :

```
1 sudo systemctl restart systemd-journald
```

## **Gestion des Journaux avec `journalctl`**

`journalctl` est l'outil principal pour interroger et afficher les journaux collectés par `journald`. Il permet d'accéder aux logs du système, des services, et des applications de manière centralisée et efficace.

### **Commandes de base avec `journalctl`**

Voici quelques commandes de base pour utiliser `journalctl` :

#### **Afficher tous les journaux :**

```
1 journalctl
```

#### **Afficher les journaux d'un service spécifique (par exemple, pour `sshd`) :**

```
1 journalctl -u sshd
```

**Afficher les journaux du noyau :**

```
1 journalctl -k
```

**Afficher les journaux depuis un moment spécifique :**

```
1 journalctl --since "2025-02-01" --until "2025-02-10"
```

**Afficher les dernières entrées du journal :**

```
1 journalctl -n 50
```

**Suivre les logs en temps réel (similaire à tail -f) :**

```
1 journalctl -f
```

**Afficher les logs d'un certain niveau de priorité :**

```
1 journalctl -p err
```

Cette commande affiche uniquement les logs de niveau err (erreur) et supérieur (critique).

**Limiter l'affichage à un certain nombre de lignes :**

```
1 journalctl -n 100
```

**Afficher les journaux d'un service depuis le démarrage :**

```
1 journalctl -u sshd -b
```

## Filtrage avancé avec journalctl

Vous pouvez filtrer les journaux selon différents critères :

**Afficher les logs d'un utilisateur spécifique :**

```
1 journalctl _UID=1001
```

**Afficher les logs avec une priorité spécifique :**

```
1 journalctl -p warning
```

**Afficher les logs d'une unité spécifique (par exemple, nginx.service) :**

```
1 journalctl -u nginx.service
```

**Afficher les logs d'un service en particulier avec un niveau de priorité spécifique :**

```
1 journalctl -u nginx.service -p err
```

**Utilisation de journalctl avec des options supplémentaires**

Limiter la sortie à un certain nombre de logs par unité de temps :

**Afficher les logs du dernier démarrage :**

```
1 journalctl -b
```

**Afficher les logs des 5 derniers démarrages :**

```
1 journalctl -b -5
```

**Exporter les logs dans un fichier** Exporter les logs dans un fichier : Vous pouvez rediriger la sortie de journalctl vers un fichier texte pour une consultation ultérieure ou pour des analyses plus approfondies :

```
1 journalctl > logs.txt
```

**limiter le logs** Limiter les logs affichés à une période spécifique : Afficher les journaux depuis une date précise :

```
1 journalctl --since "2025-02-01"
```

Afficher les journaux jusqu'à une date précise :

```
1 journalctl --until "2025-02-10"
```

## Gestion de la Taille des Journaux

**systemd-journald** est conçu pour gérer automatiquement la taille des journaux, mais vous pouvez personnaliser cette gestion en modifiant le fichier `/etc/systemd/journald.conf`.

### Paramètres de taille des journaux

- **SystemMaxUse** : Définit la taille maximale que les journaux peuvent occuper sur le disque (par exemple, `SystemMaxUse=500M` limite les logs à 500 Mo).
- **SystemKeepFree** : Assure qu'un certain pourcentage de l'espace disque reste libre pour d'autres usages.
- **SystemMaxFileSize** : Limite la taille des fichiers journaux individuels.

#### Exemple de configuration dans `/etc/systemd/journald.conf`:

```
1 [Journal]
2 SystemMaxUse=500M
3 SystemKeepFree=1G
4 SystemMaxFileSize=50M
```

## Sécurisation des Journaux

**systemd-journald** stocke les journaux dans un format binaire qui peut être consulté uniquement par les utilisateurs ayant les permissions appropriées. Voici quelques bonnes pratiques pour sécuriser les journaux :

- **Restreindre l'accès aux journaux** : Par défaut, seul l'utilisateur root et les membres du groupe `systemd-journal` peuvent accéder aux journaux binaires. Vous pouvez ajouter un utilisateur à ce groupe si nécessaire :

```
1 sudo usermod -aG systemd-journal <username>
```

Activer le chiffrement des journaux : Si vous devez protéger vos logs sensibles, vous pouvez utiliser un serveur distant pour stocker vos logs en utilisant TLS avec rsyslog ou journald. ## Préparation

---

Afin de réaliser ce TP nous allons utiliser un site d'apprentissage de hacking/cracking

Ce dernier se nomme root-me.org

Vous avez la possibilité de vous créer un compte ou d'utiliser celui de la session 2018 de MTN :

- user : mtn2018
  - pass : 2018mtn2018
- 

## Outils de dev

---

Les outils de développement des navigateur :

Tous les navigateurs modernes possèdent un ensemble d'outils destinés aux développeurs.

Ces outils permettent de réaliser différentes actions : inspecter le code HTML, CSS ou JavaScript chargé à la volée dans la page, montrer les fichiers téléchargés et le temps de chargement, etc.

Ces outils peuvent donc être utilisés afin de modifier le contenu d'un site pour changer son comportement en local et potentiellement modifier l'accès à certaines données du code source.

Après vous être loggué sur root-me tenté de résoudre l'éénigme ci-dessous :

<http://challenge01.root-me.org/web-client/ch25/>

## un bon admin ?

---

Certains admin doivent être brûlé !!!

Sans trop d'explication essayé de résoudre l'éénigme ci-dessous :

<http://challenge01.root-me.org/web-serveur/ch3/>

---

## les protocoles

---

Les trames Ftp ...

<http://challenge01.root-me.org/reseau/ch1/ch1.pcap>

---

## ex de phpbb

---

Quand on a fini d'installer quelque chose ...

Connaissez vos outils !!!!

<http://challenge01.root-me.org/web-serveur/ch6/>

---

## Programmation de base

---

Programmez du javascript c'est bien ... mais là ...

<http://challenge01.root-me.org/web-client/ch1/ch1.html>

---

## Steno

---

Trouver les outils qui analyse les fichiers binaires

<https://www.root-me.org/fr/Challenges/Steganographie/Pas-tres-carre>