scriting

Astier Guillaume

09/01/2026

CIS services

CIS_Network

Cours : **rsyslog syslog-ng journalctl**

CIS services

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

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 fonctionelle

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 fonctionelle
- Vérifier que chrony n'est pas lancé en tant que root

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 fonctionelle
- 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

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 fonctionelle
- 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

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 fonctionelle
- 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

function_Check

function_Apply

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

function_Check

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

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

CIS_Network

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

Gestion du réseau

- Vérifier que le protocole IPV6 est désactivé
- Vérifier que les périphérique de type wifi sont désactivé

Gestion du réseau

- Vérifier que le protocole IPV6 est désactivé
- Vérifier que les périphérique de type wifi sont désactivé
- Vérifier que les périphérique de type bluetooth sont désactivé

Gestion du réseau

- Vérifier que le protocole IPV6 est désactivé
- Vérifier que les périphérique de type wifi sont désactivé
- Vérifier que les périphérique de type bluetooth sont désactivé
- Vérifier que l'ip forwarding est désactivé

Gestion du réseau

- Vérifier que le protocole IPV6 est désactivé
- Vérifier que les périphérique de type wifi sont désactivé
- Vérifier que les périphérique de type bluetooth sont désactivé
- Vérifier que l'ip forwarding est désactivé
- Vérifier que la redirection de paquet via l'icmp est désactivé

Gestion du réseau

- Vérifier que le protocole IPV6 est désactivé
- Vérifier que les périphérique de type wifi sont désactivé
- Vérifier que les périphérique de type bluetooth sont désactivé
- 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 avtivation

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

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

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

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 :

```
rpm -q rsyslog
```

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

```
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 :

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

Filtrage des messages

```
authpriv.*      /var/log/secure
*.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 :

```
sudo systemctl start rsyslog
sudo systemctl enable rsyslog
```

Pour vérifier son statut :

```
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 :

```
sudo yum install epel-release
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 :

```
source s_local {
    system();
    internal();
};
```

Définir une destination :

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

Définir une règle de filtrage :

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

Envoi des logs à un serveur distant :

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

Démarrer et gérer syslog-ng

Pour démarrer et activer le service syslog-ng :

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

Vérifiez le statut avec :

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

Comparaison entre **rsyslog** et **syslog-ng**

Critère	**rsyslog**	**syslog-ng**
Installation	Par défaut sur CentOS 7	Nécessite l'installation via EPEL
Facilité de configuration	Configuration simple via `/etc/rsyslog.conf`	Configuration plus complexe mais plus flexible
Protocole	Utilise principalement UDP/TCP pour l'envoi à distance	Supporte plus de protocoles et formats
Performances	Très performant pour des logs classiques	Très performant avec une meilleure gestion des logs en temps réel
Filtrage avancé	Filtrage de base via `/etc/rsyslog.conf`	Filtrage avancé et personnalisation complète
Soutien communautaire	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 :

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

Modifier /etc/rsyslog.conf pour activer TLS

```
module(load="imtcp")  # Charge le module TCP
input(type="imtcp" port="514")

$DefaultNetstreamDriver gtls
$DefaultNetstreamDriverCAFile /etc/rsyslog.d/ca.crt
$DefaultNetstreamDriverCertFile /etc/rsyslog.d/cert.crt
$DefaultNetstreamDriverKeyFile /etc/rsyslog.d/cert.key
*.* @@logserver.example.com:514
```

Exemple de configuration avec TLS dans syslog-ng :

Générer un certificat :

```
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 :

```
destination d_tls {
    tcp("logserver.example.com" port(514)
        tls(cert_file("/etc/syslog-ng/cert.crt") key_file("/etc/syslog-ng/cert.key
            ") ca_file("/etc/syslog-ng/ca.crt")));
};
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.

Fonctionnalités de **systemd-journald** :

- Journalisation des messages des services **systemd** et des applications.
- Collecte des journaux du noyau (kernel logs).

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).

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.

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 :

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).

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).

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`.

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` :

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

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

```
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 :

```
journalctl
```

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

```
journalctl -u sshd
```

Afficher les journaux du noyau :

```
journalctl -k
```

Afficher les journaux depuis un moment spécifique :

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

Afficher les dernières entrées du journal :

```
journalctl -n 50
```

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

```
journalctl -f
```

Afficher les logs d'un certain niveau de priorité :

```
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 :

```
journalctl -n 100
```

Afficher les journaux d'un service depuis le démarrage :

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

Filtrage avancé avec journalctl

Vous pouvez filtrer les journaux selon différents critères :

Afficher les logs d'un utilisateur spécifique :

```
journalctl _UID=1001
```

Afficher les logs avec une priorité spécifique :

```
journalctl -p warning
```

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

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

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

```
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 :

```
journalctl -b
```

Afficher les logs des 5 derniers démarrages :

```
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 :

```
journalctl > logs.txt
```

limiter le logs

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

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

Afficher les journaux jusqu'à une date précise :

```
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).

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.

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` :

```
[Journal]
SystemMaxUse=500M
SystemKeepFree=1G
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 :

```
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

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 utilisé afin de modifer le contenue 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'énigme 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'énigme 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 ...

Connaisez 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