

Mise en place de dispositifs de journalisation

Société menuimetal

Présenté par :

BAYERE Abdoul Fatahou

GUIHARD Mathieu

Sommaire

I. Introduction.....	1
II. Mise en place du Gantt.....	1
III. Mise à jour du schéma réseau.....	2
IV. Gestion des journaux (logs) : Concepts clés et outils.....	2
A. L'importance et la gestion des journaux (logs).....	2
B. Les différents outils de gestion des logs.....	3
1. Systemd ou syslog.....	3
2. Serveur Apache2 et SSH - "Srv-Debian-GLPI".....	5
a) Identification du système de gestion des journaux (systemd ou syslog).....	5
b) Consultation des journaux de chaque service.....	5
c) Consultation des logs les plus récents.....	6
d) Affichage des 20 dernières lignes de logs.....	7
e) Recherche d'erreurs dans les logs.....	8
f) Analyse des connexions distantes pour SSH.....	9
g) Vérification de l'espace disque occupé par les journaux.....	10
3. Serveur MariaDB et SSH - "MariaDB".....	11
a) Identification du système de gestion des journaux (systemd ou syslog).....	11
b) Consultation des journaux de chaque service.....	11
c) Consultation des logs les plus récents.....	12
d) Affichage des 20 dernières lignes de logs.....	12
e) Recherche d'erreurs dans les logs.....	13
f) Analyse des connexions distantes pour SSH.....	13
g) Vérification de l'espace disque occupé par les journaux.....	14
4. Administration des Serveurs Windows.....	14
a) Serveur Windows Server 2022 avec Active Directory - "SrvWin2022-Menuimetal".....	14
b) Serveur Windows Server 2022 avec DHCP - "Second-SrvWin2022-Menuimetal".....	16
V. Les outils de centralisation.....	17
A. Graylog.....	17
1. Création et configu de la vm.....	17
2. Référencement DNS du serveur, intégration avec Nagios et GLPI.....	19
3. Installation et configuration de graylog.....	22
4. Installation et configuration de graylog sur debian 9.....	24
5. Envoi de logs depuis Nagios vers Graylog.....	42
6. Création d'un premier log.....	45
B. Rsyslog et script.....	46

Liens vers les ressources partagées :

Gestion VMs et VLANS :

+ (GUIHARD_BAYERE) Gestion VLAN et VMs du contexte "Menui...

Gantt :

+ AP9 - Diagramme de Gantt

I. Introduction

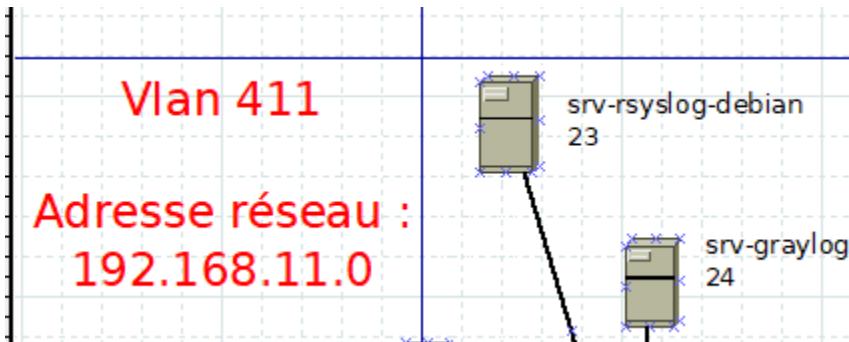
En 1980, Jean Morin crée Menuimetal.SA à Lens, une entreprise spécialisée dans la conception et la fabrication de structures en métal et en verre. Tout en se concentrant sur la production de huisseries et d'éléments de façade, Menuimetal délègue la pose à des partenaires externes. Avec un bureau d'étude capable de répondre aux besoins spécifiques de ses clients, l'entreprise propose des solutions sur mesure et poursuit sa croissance en cherchant à optimiser ses services informatiques.

II. Mise en place du Gantt

Tâches ou WBS					
Lettre	Titre	Jour et heure de début	Antécédent(s)	Durée en heure	Affectée à
A	Questions	12/11/2024 14:00:00		0,5	Mathieu
B	Questions	12/11/2024 14:00:00	A	0,5	Abdoul
C	Test de commande de log sur des services Apache2	12/11/2024 15:30:00	B	0,5	Mathieu
D	Test de commande de log sur des services MariaDB	12/11/2024 15:30:00	C	0,5	Abdoul
E	Analyse des logs Windows via l'observateur d'événements (DHCP)	14/11/2024 08:30:00	D	0,5	Abdoul
F	Analyse des logs Windows via l'observateur d'événements (ADDS)	14/11/2024 08:30:00	E	0,5	Mathieu
G	Référencement DNS, GLPI, Nagios	14/11/2024 09:30:00	F	1	Mathieu et Abdoul
H	Installation et configuration de MongoDB pour Graylog	14/11/2024 10:35:00	G	3	Abdoul
I	Installation et configuration de rsyslog	14/11/2024 11:35:00	H	0,5	Mathieu
J	Serveur de Temps (Switch HP + Machine Linux + Serveur Windows)	14/11/2024 13:35:00	I	1	Mathieu
K	Mise en place de l'analyse des logs via script bash (SSH)	14/11/2024 14:35:00	J	1	Mathieu
L	Mise en place de la sauvegarde des logs sur le serveur OMV	14/11/2024 15:35:00	K	1	Mathieu
M	Gestion des logs pour un équipement réseau	14/11/2024 16:35:00	L	1	Mathieu
N	Installation et configuration d'une Debian 9	15/11/2024 13:30:00	M	1	Abdoul
O	Installation et configuration de MongoDB pour Graylog	15/11/2024 14:30:00	N	1	Abdoul
P	Installation et configuration de Elasticsearch pour Graylog	15/11/2024 15:30:00	O	1	Abdoul
Q	Installation et configuration de Graylog	15/11/2024 16:30:00	P	1	Abdoul
R	Envoyer des logs de nagios vers graylog	15/11/2024 16:50:00	Q	1	Abdoul
S			R		
T			S		

Visualisation du Gantt

III. Mise à jour du schéma réseau



Visualisation du schéma réseau mis à jour

IV. Gestion des journaux (logs) : Concepts clés et outils

A. L'importance et la gestion des journaux (logs)

Questions :

- **Tous les systèmes (équipements, applicatifs) produisent-ils des logs systématiquement ?**
Oui, tous les systèmes produisent des logs, plus ou moins détaillés, afin d'assurer une traçabilité des actions effectuées et/ou du fonctionnement du système.
- **Est-il judicieux de produire un grand volume de logs ? Justifiez votre réponse.**
Il n'est pas judicieux de produire un volume excessif de logs. Cela pourrait engendrer un stockage inutile et compliquer l'analyse des informations essentielles. Il est préférable de se concentrer sur les logs système ou ceux des applications critiques.
- **Pourquoi est-il intéressant de centraliser les logs ? Est-il judicieux de tout centraliser ?**
Centraliser les logs permet de les conserver de manière sécurisée,

notamment en cas d'attaque, sur un serveur distant. Toutefois, il n'est pas nécessaire de tout centraliser. Il est préférable de se focaliser sur les logs importants (système et applications sensibles) afin d'éviter une surcharge inutile.

- **Quels avantages offre la gestion des logs en cas de piratage ?**
En cas de piratage, la gestion des logs fournit des informations cruciales : identification des failles potentielles, compréhension des méthodes utilisées par les attaquants, et éventuelle identification de leur origine (adresse IP, machine utilisée, etc.).
- **L'horodatage des logs est-il important ?**
Oui, l'horodatage des logs est essentiel pour déterminer la chronologie exacte des événements, notamment pour localiser la date et l'heure précises d'un incident.

B. Les différents outils de gestion des logs

1. Systemd ou syslog

Questions :

- **Quelles sont les différences entre *systemd* et *syslog* ?**

La différence principale entre *systemd* et *syslog* est liée à leur fonctionnement et leur manière de gérer les journaux.

- **Syslog** est un protocole traditionnel utilisé depuis longtemps pour gérer les journaux système, stockant les messages sous forme de fichiers texte et permettant une gestion simple des logs. Il est couramment utilisé dans des environnements hétérogènes, notamment sur les équipements réseaux (comme les routeurs et commutateurs), car il est compatible avec de nombreux systèmes et outils.
- **Systemd** est un système d'initialisation moderne, incluant un gestionnaire de logs appelé *journald*. Celui-ci stocke les logs dans

un format binaire, ce qui permet une gestion plus efficace et une consultation rapide grâce à des outils comme journalctl. Contrairement à syslog, journald offre des fonctionnalités avancées, comme la possibilité de filtrer facilement les logs par service, priorité ou date, et est principalement utilisé dans les distributions Linux modernes. En résumé, syslog reste préféré dans des environnements réseaux ou multi-systèmes, tandis que systemd/journald est plus adapté aux systèmes Linux modernes avec systemd comme gestionnaire de services.

Syslog est souvent utilisé sur les équipements réseau parce qu'il est compatible avec beaucoup de systèmes. Systemd/journald est plutôt utilisé sur les systèmes Linux récents, car il est conçu pour ces environnements.

- **Quel système de journalisation (systemd ou syslog) est utilisé sur les équipements réseau ?**

Les équipements réseau utilisent généralement **syslog** pour la gestion des journaux, plutôt que systemd.

Syslog est un protocole standardisé et largement compatible qui permet de collecter, stocker et transférer des messages de log entre les différents dispositifs d'un réseau. Il est utilisé dans des environnements hétérogènes, notamment pour les équipements tels que les routeurs, commutateurs, et pare-feu, où la compatibilité avec de multiples systèmes et plateformes est essentielle. Tandis que **systemd** et son gestionnaire de logs journald sont couramment utilisés sur les systèmes Linux modernes pour centraliser les logs du noyau et des services système dans un format binaire, syslog reste préféré pour les équipements réseau en raison de sa simplicité et de sa flexibilité dans des environnements multi-systèmes.

2. Serveur Apache2 et SSH - "Srv-Debian-GLPI"

- a) Identification du système de gestion des journaux
(systemd ou syslog)

Cette commande permet de savoir si systemd ou syslog est utilisé :

-p 1 -o comm=ps

```
sio@srv-glpi:~$ ps -p 1 -o comm=systemd
```

Sur notre distribution Debian 12.7 (`cat/etc/debian_version`), le système de gestion des journaux est donc **systemd**.

- b) Consultation des journaux de chaque service

- Affichage des logs complets pour Apache2

```
journalctl -u apache2
```

- Affichage des logs complets pour SSH

journalctl -u ssh

```
root@srv-gplpi-1:~# journalctl -u ssh
sep 03 17:22:15 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
sep 03 17:22:16 debian sshd[431]: Server listening on 0.0.0.0 port 22.
sep 03 17:22:16 debian sshd[431]: Server listening on :: port 22.
sep 03 17:22:16 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
sep 03 17:24:56 debian sshd[431]: Disconnected from authentication user sio 172.17.219.31 port 39882 [preauth]
sep 03 17:24:57 debian sshd[440]: Accepted password for sio from 172.17.219.31 port 60804 ssh2
sep 03 17:24:57 debian sshd[440]: pam_unix(sshd:session): session opened for user sio(uid=1000) by (uid=0)
sep 03 17:24:57 debian sshd[440]: pam envsshd(session): deprecated reading of user environment enabled
sep 03 17:32:01 debian sshd[431]: Received signal 15; terminating.
sep 03 17:32:01 debian sshd[430]: Stopping ssh.service - OpenBSD Secure Shell server...
sep 03 17:32:08 debian systemd[1]: Stopped ssh.service - OpenBSD Secure Shell server.
-- Boot 573f51603e74d4a96653b07720d326 --
sep 03 17:33:10 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
sep 03 17:33:16 debian sshd[430]: Server listening on 0.0.0.0 port 22.
sep 03 17:33:16 debian sshd[430]: Server listening on :: port 22.
sep 03 17:33:16 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
-- Boot 074942a1e2405ea590c1ec350922d --
sep 05 13:32:38 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
sep 05 13:32:39 debian sshd[430]: Server listening on 0.0.0.0 port 22.
sep 05 13:32:39 debian sshd[430]: Server listening on :: port 22.
sep 06 15:54:45 debian sshd[430]: Received signal 15; terminating.
sep 06 15:54:45 debian sshd[430]: Stopping ssh.service - OpenBSD Secure Shell server...
sep 06 15:54:45 debian systemd[1]: ssh.service: Deactivated successfully.
sep 06 15:54:45 debian systemd[1]: Stopped sshd.service - OpenBSD Secure Shell server.
-- Boot 7a51cd1c024f14a57562126a7a8b --
sep 06 15:55:36 debian sshd[437]: Stopping sshd.service - OpenBSD Secure Shell server...
sep 06 15:55:36 debian sshd[437]: Server listening on 0.0.0.0 port 22.
sep 06 15:55:36 debian sshd[437]: Server listening on :: port 22.
sep 06 15:55:36 debian systemd[1]: Started sshd.service - OpenBSD Secure Shell server.
sep 10 15:50:31 debian sshd[3098]: Received disconnect from 192.168.11.250 port 55694[1]: Bye Bye [preauth]
sep 10 15:50:31 debian sshd[3098]: Disconnected from authentication user sio 192.168.11.250 port 55694 [preauth]
sep 10 15:50:31 debian sshd[3100]: Accepted password for sio from 192.168.11.250 port 55698 ssh2
sep 10 15:50:31 debian sshd[3100]: pam_unix(sshd:session): session opened for user sio(uid=1000) by (uid=0)
sep 10 15:50:32 debian sshd[3100]: pam envsshd(session): deprecated reading of user environment enabled
sep 24 14:05:10 debian systemd[1]: Stopping ssh.service - OpenBSD Secure Shell server...
sep 24 14:05:11 debian sshd[437]: Received signal 15; terminating.
sep 24 14:05:11 debian sshd[437]: Stopping sshd.service - OpenBSD Secure Shell server...
sep 24 14:05:11 debian sshd[437]: Server listening on 0.0.0.0 port 22.
sep 24 14:05:11 debian sshd[437]: Server listening on :: port 22.
-- Boot 0f288e02f141549ed Sad9r91112 --
sep 24 14:10:21 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
sep 24 14:10:21 debian sshd[430]: Server listening on 0.0.0.0 port 22.
sep 24 14:10:21 debian sshd[430]: Server listening on :: port 22.
sep 24 14:10:21 debian systemd[1]: Started sshd.service - OpenBSD Secure Shell server.
```

journalctl -u permet d'afficher les journaux (logs) d'un service spécifique

c) Consultation des logs les plus récents

- Affichage des logs complets pour Apache2 :

```
journalctl -u apache2 -f
```

```
[root@srv-gpli ~]# journalctl -u apache2 -f
Nov 09 00:00:03 srv-gpli systemd[1]: Reloading apache2.service - The Apache HTTP Server.
Nov 10 00:00:03 srv-gpli systemd[1]: Reloading apache2.service - The Apache HTTP Server...
Nov 10 00:00:03 srv-gpli apachectl[1:5336]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Nov 10 00:00:03 srv-gpli systemd[1]: Reloading apache2.service - The Apache HTTP Server.
Nov 11 00:00:02 srv-gpli systemd[1]: Reloading apache2.service - The Apache HTTP Server...
Nov 11 00:00:03 srv-gpli apachectl[1:8585]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Nov 11 00:00:03 srv-gpli systemd[1]: Reloading apache2.service - The Apache HTTP Server.
Nov 12 00:00:02 srv-gpli systemd[1]: Reloading apache2.service - The Apache HTTP Server...
Nov 12 00:00:03 srv-gpli apachectl[21772]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Nov 12 00:00:03 srv-gpli systemd[1]: Reloading apache2.service - The Apache HTTP Server.
```

- Affichage des logs complets pour SSH :

journalctl -u ssh -f

```
root@srv-glpi:~# journalctl -u ssh -f
nov. 12 14:41:20 srv-glpi systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
nov. 12 14:41:20 srv-glpi sshd[23957]: Server listening on 0.0.0.0 port 22.
nov. 12 14:41:20 srv-glpi sshd[23957]: Server listening on :: port 22.
nov. 12 14:41:20 srv-glpi systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
nov. 12 14:41:24 srv-glpi sshd[23958]: Invalid user mathieu from 192.168.13.250 port 37480
nov. 12 14:41:29 srv-glpi sshd[23958]: Received disconnect from 192.168.13.250 port 37480:11: Bye Bye [preauth]
nov. 12 14:41:29 srv-glpi sshd[23958]: Disconnected from invalid user mathieu 192.168.13.250 port 37480 [preauth]
nov. 12 14:41:29 srv-glpi sshd[23960]: Accepted password for sio from 192.168.13.250 port 37484 ssh2
nov. 12 14:41:29 srv-glpi sshd[23960]: pam_unix(sshd:session): session opened for user sio(uid=1000) by (uid=0)
nov. 12 14:41:29 srv-glpi sshd[23960]: pam_env(sshd:session): deprecated reading of user environment enabled
```

journalctl -u ssh -f permet d'afficher en temps réel les journaux du service SSH

d) Affichage des 20 dernières lignes de logs

- Affichage des logs pour Apache2 :

journalctl -u apache2 -n 20

```
root@srv-glpi:~# journalctl -u apache2 -n 20
nov. 06 00:00:03 srv-glpi apachectl[2062]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive.
nov. 06 00:00:03 srv-glpi systemd[1]: Reloaded apache2.service - The Apache HTTP Server.
nov. 07 00:00:01 srv-glpi apachectl[5247]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive.
nov. 07 00:00:01 srv-glpi apachectl[5247]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive.
nov. 07 00:00:01 srv-glpi apachectl[5247]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive.
nov. 08 00:00:03 srv-glpi apachectl[8609]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive.
nov. 08 00:00:03 srv-glpi apachectl[8609]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive.
nov. 08 00:00:03 srv-glpi apachectl[8609]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive.
nov. 08 00:00:03 srv-glpi apachectl[8609]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive.
nov. 08 00:00:03 srv-glpi apachectl[8609]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive.
nov. 09 00:00:03 srv-glpi apachectl[12107]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive.
nov. 09 00:00:03 srv-glpi apachectl[12107]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive.
nov. 10 00:00:03 srv-glpi apachectl[15336]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive.
nov. 10 00:00:03 srv-glpi apachectl[15336]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive.
nov. 11 00:00:02 srv-glpi apachectl[18585]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive.
nov. 11 00:00:03 srv-glpi apachectl[18585]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive.
nov. 12 00:00:02 srv-glpi apachectl[1]: Reloading apache2.service - The Apache HTTP Server...
nov. 12 00:00:03 srv-glpi apachectl[21772]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive.
nov. 12 00:00:03 srv-glpi apachectl[21772]: Reloaded apache2.service - The Apache HTTP Server...
```

- Affichage des logs pour SSH :

journalctl -u ssh -n 20

```
root@srv-glpi:~# journalctl -u ssh -n 20
nov. 12 14:41:16 srv-glpi systemd[1]: Stopped ssh.service - OpenBSD Secure Shell server.
nov. 12 14:41:16 srv-glpi systemd[1]: ssh.service: Consumed 1.578s CPU time.
nov. 12 14:41:16 srv-glpi systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
nov. 12 14:41:16 srv-glpi sshd[23952]: Server listening on 0.0.0.0 port 22.
nov. 12 14:41:16 srv-glpi sshd[23952]: Server listening on :: port 22.
nov. 12 14:41:16 srv-glpi systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
nov. 12 14:41:20 srv-glpi sshd[23952]: Received signal 15; terminating.
nov. 12 14:41:20 srv-glpi systemd[1]: Stopping ssh.service - OpenBSD Secure Shell server...
nov. 12 14:41:20 srv-glpi systemd[1]: ssh.service: Deactivated successfully.
nov. 12 14:41:20 srv-glpi systemd[1]: Stopped ssh.service - OpenBSD Secure Shell server.
nov. 12 14:41:20 srv-glpi systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
nov. 12 14:41:20 srv-glpi sshd[23957]: Server listening on 0.0.0.0 port 22.
nov. 12 14:41:20 srv-glpi sshd[23957]: Server listening on :: port 22.
nov. 12 14:41:20 srv-glpi systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
nov. 12 14:41:24 srv-glpi sshd[23958]: Invalid user mathieu from 192.168.13.250 port 37480
nov. 12 14:41:29 srv-glpi sshd[23958]: Received disconnect from 192.168.13.250 port 37480:11: Bye Bye [preauth]
nov. 12 14:41:29 srv-glpi sshd[23958]: Disconnected from invalid user mathieu 192.168.13.250 port 37480 [preauth]
nov. 12 14:41:29 srv-glpi sshd[23960]: Accepted password for sio from 192.168.13.250 port 37484 ssh2
nov. 12 14:41:29 srv-glpi sshd[23960]: pam_unix(sshd:session): session opened for user sio(uid=1000) by (uid=0)
nov. 12 14:41:29 srv-glpi sshd[23960]: pam_env(sshd:session): deprecated reading of user environment enabled
```

e) Recherche d'erreurs dans les logs

- Affichage des logs pour Apache 2 :

journalctl -u apache2 -p err

```
root@srv-glpi:~# journalctl -u apache2 -p err
-- No entries --
```

- Affichage des logs pour SSH :

journalctl -u ssh -p err

```
root@srv-glpi:~# journalctl -u ssh -p err
-- No entries --
```

f) Analyse des connexions distantes pour SSH

• Connexions depuis la reprise des vacances

○ Affichage des logs pour SSH :

```
journalctl -u ssh --since "2024-11-04"
```

```
root@raspberrypi:~# journalctl -u ssh -s --since "2024-11-04"
... No entries ...
```

Nov 05 14:33:21 raspberrypi systemd[1]: Starting ssh.service - OpenSSH Secure Shell server...
Nov 05 14:33:28 raspberrypi sshd[4941]: Server listening on 0.0.0.0 port 22.
Nov 05 14:33:28 raspberrypi sshd[4941]: Server listening on :: port 22.
Nov 05 15:24:22 raspberrypi sshd[777]: Unable to negotiate with 127.0.0.1 port 49078: no matching host key type found. Their offer: sk-ecdsa-sha2-nistp256@openssh.com [preauth]
Nov 05 15:24:23 raspberrypi sshd[774]: Connection closed by 127.0.0.1 port 49946 [preauth]
Nov 05 15:24:23 raspberrypi sshd[774]: Unable to negotiate with 127.0.0.1 port 49078: no matching host key type found. Their offer: sk-ecdsa-sha2-nistp256@openssh.com [preauth]
Nov 05 15:24:23 raspberrypi sshd[774]: Connection closed by 127.0.0.1 port 49946 [preauth]
Nov 05 15:24:23 raspberrypi sshd[774]: Connection closed by 127.0.0.1 port 49946 [preauth]
Nov 05 15:24:23 raspberrypi sshd[774]: Connection closed by 127.0.0.1 port 49946 [preauth]
Nov 05 15:28:58 raspberrypi sshd[4102]: Unable to negotiate with 127.0.0.1 port 38136: no matching host key type found. Their offer: sk-ecdsa-sha2-nistp256@openssh.com [preauth]
Nov 05 15:28:58 raspberrypi sshd[4102]: Connection closed by 127.0.0.1 port 38136 [preauth]
Nov 05 15:28:58 raspberrypi sshd[4100]: Unable to negotiate with 127.0.0.1 port 38108: no matching host key type found. Their offer: sk-ecdsa-sha2-nistp256@openssh.com [preauth]
Nov 05 15:28:58 raspberrypi sshd[4100]: Connection closed by 127.0.0.1 port 38108 [preauth]
Nov 05 15:28:58 raspberrypi sshd[4101]: Unable to negotiate with 127.0.0.1 port 38116: no matching host key type found. Their offer: sk-ssh-ed25519@openssh.com [preauth]
Nov 05 15:28:58 raspberrypi sshd[4101]: Connection closed by 127.0.0.1 port 38116 [preauth]
Nov 07 13:49:01 raspberrypi sshd[7343]: Unable to negotiate with 127.0.0.1 port 38136: no matching host key type found. Their offer: sk-ecdsa-sha2-nistp256@openssh.com [preauth]
Nov 07 13:49:01 raspberrypi sshd[7343]: Connection closed by 127.0.0.1 port 38136 [preauth]
Nov 07 13:49:01 raspberrypi sshd[7343]: Connection closed by 127.0.0.1 port 38453 [preauth]
Nov 07 13:49:01 raspberrypi sshd[7340]: Connection closed by 127.0.0.1 port 34542 [preauth]
Nov 07 13:49:01 raspberrypi sshd[7340]: Connection closed by 127.0.0.1 port 34542 [preauth]
Nov 07 13:49:02 raspberrypi sshd[7342]: Unable to negotiate with 127.0.0.1 port 34550: no matching host key type found. Their offer: sk-ecdsa-sha2-nistp256@openssh.com [preauth]
Nov 07 13:49:02 raspberrypi sshd[7342]: Connection closed by 127.0.0.1 port 34550 [preauth]
Nov 08 14:03:49 raspberrypi sshd[10519]: Connection closed by 127.0.0.1 port 43714 [preauth]
Nov 08 14:03:49 raspberrypi sshd[10517]: Connection closed by 127.0.0.1 port 43704 [preauth]
Nov 08 14:03:49 raspberrypi sshd[10519]: Connection closed by 127.0.0.1 port 43704 [preauth]
Nov 08 14:03:49 raspberrypi sshd[10520]: Unable to negotiate with 127.0.0.1 port 43726: no matching host key type found. Their offer: sk-ecdsa-sha2-nistp256@openssh.com [preauth]
Nov 08 14:03:49 raspberrypi sshd[10521]: Unable to negotiate with 127.0.0.1 port 43728: no matching host key type found. Their offer: sk-ssh-ed25519@openssh.com [preauth]
Nov 08 16:24:49 raspberrypi sshd[10991]: Disconnected from authenticating user sio 192.168.1.201 port 45480 [preauth]
Nov 09 13:39:13 raspberrypi sshd[13948]: Connection closed by 127.0.0.1 port 36612 [preauth]
Nov 09 13:39:13 raspberrypi sshd[13947]: Connection closed by 127.0.0.1 port 36596 [preauth]
Nov 09 13:39:13 raspberrypi sshd[13946]: Connection closed by 127.0.0.1 port 36596 [preauth]
Nov 09 13:39:13 raspberrypi sshd[13950]: Unable to negotiate with 127.0.0.1 port 36640: no matching host key type found. Their offer: sk-ecdsa-sha2-nistp256@openssh.com [preauth]
Nov 09 13:39:13 raspberrypi sshd[13951]: Unable to negotiate with 127.0.0.1 port 36652: no matching host key type found. Their offer: sk-ssh-ed25519@openssh.com [preauth]
Nov 10 13:31:10 raspberrypi sshd[17143]: Connection closed by 127.0.0.1 port 51888 [preauth]
Nov 10 13:31:10 raspberrypi sshd[17144]: Connection closed by 127.0.0.1 port 51888 [preauth]
Nov 10 13:31:10 raspberrypi sshd[17145]: Connection closed by 127.0.0.1 port 51870 [preauth]
Nov 11 12:25:15 raspberrypi sshd[20316]: Connection closed by 127.0.0.1 port 57664 [preauth]
Nov 11 12:25:15 raspberrypi sshd[20314]: Connection closed by 127.0.0.1 port 57664 [preauth]
Nov 11 12:25:15 raspberrypi sshd[20313]: Connection closed by 127.0.0.1 port 57664 [preauth]
Nov 11 12:25:15 raspberrypi sshd[20318]: Unable to negotiate with 127.0.0.1 port 57676: no matching host key type found. Their offer: sk-ecdsa-sha2-nistp256@openssh.com [preauth]
Nov 12 12:05:18 raspberrypi sshd[23480]: Unable to negotiate with 127.0.0.1 port 48792: no matching host key type found. Their offer: sk-ssh-ed25519@openssh.com [preauth]
Nov 12 12:05:18 raspberrypi sshd[23471]: Connection Closed by 127.0.0.1 port 48792 [preauth]
Nov 12 12:05:18 raspberrypi sshd[23471]: Connection Closed by 127.0.0.1 port 48792 [preauth]
Nov 12 12:05:19 raspberrypi sshd[23428]: Connection closed by 127.0.0.1 port 48760 [preauth]
Nov 12 12:05:19 raspberrypi sshd[23428]: Connection closed by 127.0.0.1 port 48760 [preauth]
Nov 12 12:05:19 raspberrypi sshd[23428]: Connection closed by 127.0.0.1 port 48767: no matching host key type found. Their offer: sk-ecdsa-sha2-nistp256@openssh.com [preauth]

• Connexions depuis le dernier démarrage

○ Affichage des logs pour SSH :

```
journalctl -u ssh -b
```

```
[root@svr-gpl1 ~]# journalctl -u ssh -b
Nov 05 14:33:26 svr-gpl1 [systemd]: Starting ssh.service OpenBSD Secure Shell server...
Nov 05 14:33:26 svr-gpl1 sshd[4941]: listening on port 22
Nov 05 14:33:28 svr-gpl1 [systemd]: Started ssh.service OpenBSD Secure Shell server
Nov 05 15:24:23 svr-gpl1 sshd[774]: Connection closed by 127.0.0.1 port 49846 [preauth]
Nov 05 15:24:23 svr-gpl1 sshd[775]: Connection closed by 127.0.0.1 port 49858 [preauth]
Nov 05 15:24:23 svr-gpl1 sshd[776]: Connection closed by 127.0.0.1 port 49860 [preauth]
Nov 05 15:24:23 svr-gpl1 sshd[777]: Unable to negotiate with 127.0.0.1 port 49888; no matching host key type found. Their offer: sk-ecdsa-sha2-nistp256@openssh.com [preauth]
Nov 05 15:26:58 svr-gpl1 sshd[4102]: Unable to negotiate with 127.0.0.1 port 38139; no matching host key type found. Their offer: sk-ssh-ed25519@openssh.com [preauth]
Nov 05 15:26:58 svr-gpl1 sshd[4103]: Connection closed by 127.0.0.1 port 38138 [preauth]
Nov 05 15:26:58 svr-gpl1 sshd[4104]: Connection closed by 127.0.0.1 port 38136 [preauth]
Nov 07 14:59:01 svr-gpl1 sshd[7343]: Received negotiate from 127.0.0.1 port 45466; no matching host key type found. Their offer: sk-ssh-ed25519@openssh.com [preauth]
Nov 07 14:59:01 svr-gpl1 sshd[7343]: Unable to negotiate with 127.0.0.1 port 45466; no matching host key type found. Their offer: sk-ssh-ed25519@openssh.com [preauth]
Nov 07 14:59:01 svr-gpl1 sshd[7344]: Connection closed by 127.0.0.1 port 45438 [preauth]
Nov 07 14:59:02 svr-gpl1 sshd[7345]: Connection closed by 127.0.0.1 port 45458 [preauth]
Nov 07 14:59:02 svr-gpl1 sshd[7346]: Connection closed by 127.0.0.1 port 45458 [preauth]
Nov 07 14:59:02 svr-gpl1 sshd[7347]: Unable to negotiate with 127.0.0.1 port 45558; no matching host key type found. Their offer: sk-ecdsa-sha2-nistp256@openssh.com [preauth]
Nov 08 14:03:49 svr-gpl1 sshd[10517]: Connection closed by 127.0.0.1 port 49364 [preauth]
Nov 08 14:03:49 svr-gpl1 sshd[10518]: Connection closed by 127.0.0.1 port 49370 [preauth]
Nov 08 14:03:49 svr-gpl1 sshd[10519]: Received negotiate from 127.0.0.1 port 49371; no matching host key type found. Their offer: sk-ecdsa-sha2-nistp256@openssh.com [preauth]
Nov 08 14:03:49 svr-gpl1 sshd[10521]: Unable to negotiate with 127.0.0.1 port 49378; no matching host key type found. Their offer: sk-ssh-ed25519@openssh.com [preauth]
Nov 08 16:24:49 svr-gpl1 sshd[10999]: Received disconnect from 192.168.1.251 port 49426[1]; Bye [preauth]
Nov 09 13:39:13 svr-gpl1 sshd[13941]: Connection closed by 127.0.0.1 port 49421 [preauth]
Nov 09 13:39:13 svr-gpl1 sshd[13941]: Connection closed by 127.0.0.1 port 49421 [preauth]
Nov 09 13:39:13 svr-gpl1 sshd[13941]: Connection closed by 127.0.0.1 port 49422 [preauth]
Nov 09 13:39:13 svr-gpl1 sshd[13950]: Unable to negotiate with 127.0.0.1 port 36649; no matching host key type found. Their offer: sk-ecdsa-sha2-nistp256@openssh.com [preauth]
Nov 09 13:39:13 svr-gpl1 sshd[13951]: Unable to negotiate with 127.0.0.1 port 36652; no matching host key type found. Their offer: sk-ssh-ed25519@openssh.com [preauth]
Nov 10 13:31:10 svr-gpl1 sshd[17143]: Connection closed by 127.0.0.1 port 51858 [preauth]
Nov 10 13:31:10 svr-gpl1 sshd[17144]: Connection closed by 127.0.0.1 port 51864 [preauth]
Nov 10 13:31:10 svr-gpl1 sshd[17145]: Connection closed by 127.0.0.1 port 51866 [preauth]
Nov 10 13:31:10 svr-gpl1 sshd[17147]: Unable to negotiate with 127.0.0.1 port 51886; no matching host key type found. Their offer: sk-ssh-ed25519@openssh.com [preauth]
Nov 11 12:51:15 svr-gpl1 sshd[20316]: Connection closed by 127.0.0.1 port 57664 [preauth]
Nov 11 12:51:15 svr-gpl1 sshd[20317]: Connection closed by 127.0.0.1 port 57665 [preauth]
Nov 11 12:51:15 svr-gpl1 sshd[20315]: Connection closed by 127.0.0.1 port 57648 [preauth]
Nov 11 12:51:15 svr-gpl1 sshd[20317]: Unable to negotiate with 127.0.0.1 port 57672; no matching host key type found. Their offer: sk-ecdsa-sha2-nistp256@openssh.com [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23480]: Connection closed by 127.0.0.1 port 49792; no matching host key type found. Their offer: sk-ssh-ed25519@openssh.com [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23482]: Connection closed by 127.0.0.1 port 49793 [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23481]: Connection closed by 127.0.0.1 port 49796 [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23483]: Connection closed by 127.0.0.1 port 49797 [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23484]: Connection closed by 127.0.0.1 port 49798 [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23485]: Connection closed by 127.0.0.1 port 49799 [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23486]: Connection closed by 127.0.0.1 port 49800 [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23487]: Connection closed by 127.0.0.1 port 49801 [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23488]: Connection closed by 127.0.0.1 port 49802 [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23489]: Connection closed by 127.0.0.1 port 49803 [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23490]: Connection closed by 127.0.0.1 port 49804 [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23491]: Connection closed by 127.0.0.1 port 49805 [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23492]: Connection closed by 127.0.0.1 port 49806 [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23493]: Connection closed by 127.0.0.1 port 49807 [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23494]: Connection closed by 127.0.0.1 port 49808 [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23495]: Connection closed by 127.0.0.1 port 49809 [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23496]: Connection closed by 127.0.0.1 port 49810 [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23497]: Connection closed by 127.0.0.1 port 49811 [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23498]: Connection closed by 127.0.0.1 port 49812 [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23499]: Connection closed by 127.0.0.1 port 49813 [preauth]
Nov 12 02:05:18 svr-gpl1 sshd[23500]: Connection closed by 127.0.0.1 port 49814 [preauth]
```

- g) Vérification de l'espace disque occupé par les journaux

- **Affichage des logs pour SSH :**

journalctl --disk-usage

```
root@srv-glpi:~# journalctl --disk-usage
Archived and active journals take up 45.5M in the file system.
```

3. Serveur MariaDB et SSH - "MariaDB"

- a) Identification du système de gestion des journaux (systemd ou syslog)

Cette commande permet de savoir si systemd ou syslog est utilisé :

ps -p 1 -o comm=

```
root@mariadb:~# ps -p 1 -o comm=
systemd
root@mariadb:~#
```

- b) Consultation des journaux de chaque service

- Affichage des logs complets pour MariaDB

journalctl -u mariadb

```
root@mariadb:~# journalctl -u mariadb
-- Journal begins at Tue 2021-09-28 10:25:57 CEST, ends at Tue >
Sep 28 10:25:59 mariadb systemd[1]: Starting MariaDB 10.3.17 da>
Sep 28 10:26:00 mariadb mysqld[417]: 2021-09-28 10:26:00 0 [Not>
Sep 28 10:26:01 mariadb /etc/mysql/debian-start[531]: Upgrading>
Sep 28 10:26:01 mariadb systemd[1]: Started MariaDB 10.3.17 dat>
Sep 28 10:26:02 mariadb /etc/mysql/debian-start[535]: /usr/bin/>
```

c) Consultation des logs les plus récents

- Affichage des logs pour MariaDB

journalctl -xe

```
root@mariadb:~# journalctl -xe
Nov 12 14:54:36 mariadb systemd[6452]: Reached target Timers.
-- Subject: A start job for unit UNIT has finished successfully
-- Defined-By: systemd
-- Support: https://www.debian.org/support
--
-- A start job for unit UNIT has finished successfully.
--
```

d) Affichage des 20 dernières lignes de logs

- Affichage des logs pour MariaDB

journalctl -u mariadb -n 20

```
root@mariadb:~# journalctl -u mariadb -n 20
-- Journal begins at Tue 2024-11-28 10:25:57 CET, ends at Tue 2024-11-12 14:54:40 CET, -- 
Sep 12 17:04:25 mariadb systemd[1]: Starting MariaDB 10.3.29 database server...
Sep 12 17:04:25 mariadb systemd[1]: mariadb.service: Succeeded!
Sep 12 17:04:25 mariadb systemd[1]: Stopped MariaDB 10.3.29 database server.
Sep 12 17:04:25 mariadb systemd[1]: mariadb.service: Consumed 28.399s CPU time.
Sep 12 17:04:25 mariadb systemd[1]: Starting MariaDB 10.3.29 database server...
Sep 12 17:04:25 mariadb mysqld[1416]: 2024-09-12 17:04:25 0 [Note] /usr/sbin/mysqld (mysqld 10.3.29-MariaDB-0+deb10u1) starting as process 1416 ...
Sep 12 17:04:25 mariadb systemd[1]: Started MariaDB 10.3.29 database server.
Sep 12 17:04:25 mariadb /etc/mysql/debian-start[1454]: /usr/bin/mysql_upgrade: the '--basedir' option is always ignored
Sep 12 17:04:25 mariadb /etc/mysql/debian-start[1454]: Looking for 'mysql' as: /usr/bin/mysql
Sep 12 17:04:25 mariadb /etc/mysql/debian-start[1454]: Looking for 'mysqlcheck' as: /usr/bin/mysqlcheck
Sep 12 17:04:25 mariadb /etc/mysql/debian-start[1454]: This installation of MySQL is already upgraded to 10.3.29-MariaDB, use --force if you still need to run mysql_upgrade
Sep 12 17:04:25 mariadb debian-start[1468]: WARNING: tempfile is deprecated; consider using mktemp instead.
Oct 22 18:09:34 mariadb systemd[1]: Starting MariaDB 10.3.29 database server...
Oct 22 18:09:34 mariadb systemd[1]: mariadb.service: Succeeded!
Oct 22 18:09:34 mariadb systemd[1]: Stopped MariaDB 10.3.29 database server.
Oct 22 18:09:34 mariadb systemd[1]: mariadb.service: Consumed 1h 7min 49.057s CPU time.
-- Boot 47cd145cf68e494991d02f1edcea5ad9 --
Nov 05 14:34:00 mariadb systemd[1]: Starting MariaDB 10.3.29 database server...
Nov 05 14:34:21 mariadb mysqld[489]: 2024-11-05 14:34:21 0 [Note] /usr/sbin/mysqld (mysqld 10.3.29-MariaDB-0+deb10u1) starting as process 489 ...
Nov 05 14:34:57 mariadb systemd[1]: Started MariaDB 10.3.29 database server.
Nov 05 14:35:08 mariadb debian-start[556]: WARNING: tempfile is deprecated; consider using mktemp instead.
root@mariadb:~#
```

e) Recherche d'erreurs dans les logs

- Affichage des logs pour MariaDB

journalctl -p err -u mariadb

```
root@mariadb:~# journalctl -p err -u mariadb
-- Journal begins at Tue 2021-09-28 10:25:57 CEST, ends at Tue 2024-11-12 14:54:40 CET. --
-- No entries --
root@mariadb:~#
```

f) Analyse des connexions distantes pour SSH

- Connexions depuis la reprise des vacances
 - Affichage des logs pour MariaDB

journalctl -u ssh --since "2024-11-01"

```
root@mariadb:~# journalctl -u ssh --since "2024-11-01"
```

```
Nov 05 15:12:59 mariadb sshd[762]: Connection closed by 127.0.0.1 port 40048 [preauth]
Nov 05 15:12:59 mariadb sshd[761]: Connection closed by 127.0.0.1 port 40032 [preauth]
Nov 05 15:13:00 mariadb sshd[763]: Connection closed by 127.0.0.1 port 40056 [preauth]
Nov 05 15:13:00 mariadb sshd[764]: Accepted connection from 127.0.0.1 port 40058...
```

- Connexions depuis le dernier démarrage
 - Affichage des logs pour MariaDB

journalctl -u ssh -b

```
root@mariadb:~# journalctl -u ssh -b
root@mariadb:~# journalctl -u ssh -b
-- Journal begins at Tue 2021-09-28 10:25:57 CEST, ends at Tue 2024-11-12 14:54:40 CET. --
Nov 05 14:34:01 mariadb systemd[1]: Starting OpenBSD Secure Shell server...
Nov 05 14:34:15 mariadb sshd[497]: Server listening on 0.0.0.0 port 22.
Nov 05 14:34:15 mariadb sshd[497]: Server listening on :: port 22.
Nov 05 14:34:15 mariadb systemd[1]: Started OpenBSD Secure Shell server.
```

g) Vérification de l'espace disque occupé par les journaux

- Affichage des logs pour MariaDB

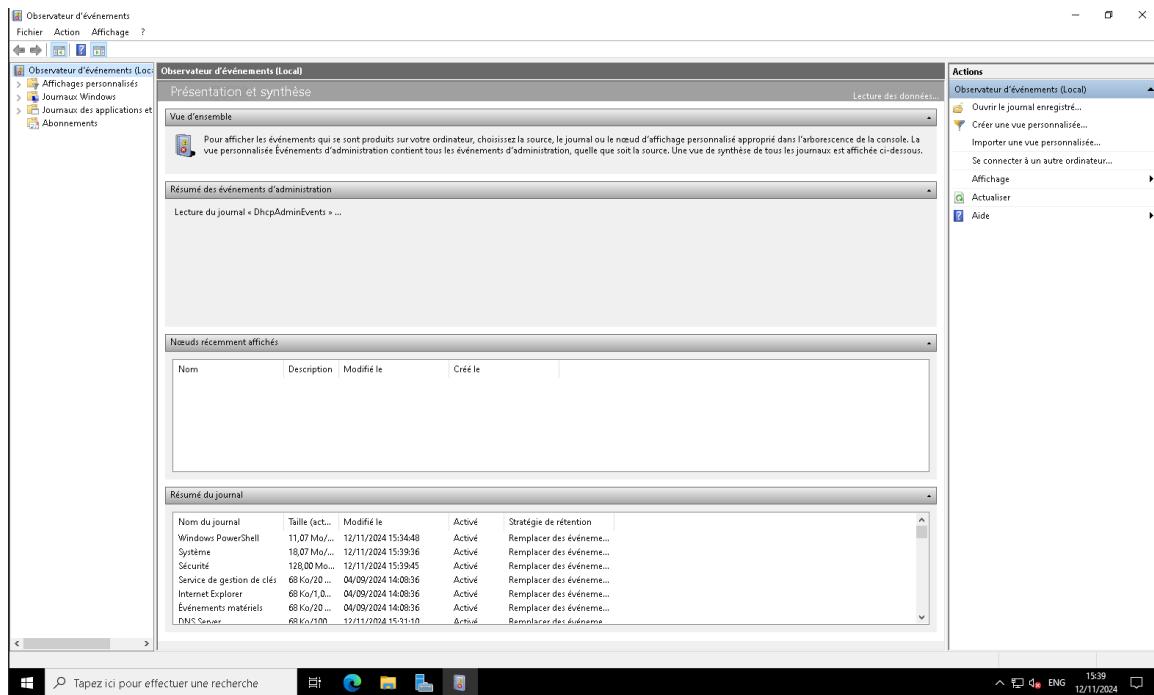
journalctl --disk-usage

```
root@mariadb:~# journalctl --disk-usage
Archived and active journals take up 80.0M in the file system.
root@mariadb:~#
```

4. Administration des Serveurs Windows

a) Serveur Windows Server 2022 avec Active Directory - "SrvWin2022-Menuimetal"

- Démarrage de l'observateur d'événements



- Recherche des événements liés au service

Observateur d'événements

Fichier Action Affichage ?

Back Forward Home Help

Journaux des applications et des services

Nom	Type	Nombre d'événement	Taille
Directory Service	Administration	816	1,00 Mo
DNS Server	Administration	124	68 Ko
Internet Explorer	Administration	0	68 Ko
Microsoft			
OpenSSH	Dossier		
Réplication DFS	Administration	207	1,07 Mo
Service de gestion de clés	Administration	0	68 Ko
Services Web Active Directory	Administration	122	68 Ko
Windows PowerShell	Administration	8 056	11,07 Mo
Événement Microsoft			
Événement réseau Microsoft			
Événements matériels	Administration	0	68 Ko
Abonnements			

Observateur d'événements

Fichier Action Affichage ?

Back Forward Home Help

Directory Service Nombre d'événements : 816

Niveau	Date et heure	Source	ID de l'événement	Catégorie de la tâche
Avertissement	12/11/2024 15:37:08	ActiveDirectory_DomainSer...	2092	Réplication
Information	12/11/2024 15:36:15	ActiveDirectory_DomainSer...	3027	Nettoyage de la mémoire
Information	12/11/2024 15:36:15	ActiveDirectory_DomainSer...	3033	Nettoyage de la mémoire
Information	12/11/2024 15:36:09	ActiveDirectory_DomainSer...	1869	Catalogue global
Avertissement	12/11/2024 15:26:09	ActiveDirectory_DomainSer...	1308	Vérificateur de cohérence d...
Avertissement	12/11/2024 15:22:09	ActiveDirectory_DomainSer...	2092	Réplication
Information	12/11/2024 15:21:38	ActiveDirectory_DomainSer...	1394	Contrôle du service
Information	12/11/2024 15:21:07	ActiveDirectory_DomainSer...	1000	Contrôle du service
Avertissement	12/11/2024 15:21:07	ActiveDirectory_DomainSer...	3041	Interface LDAP
Avertissement	12/11/2024 15:21:07	ActiveDirectory_DomainSer...	2886	Interface LDAP
Information	12/11/2024 15:20:57	ActiveDirectory_DomainSer...	2405	Configuration interne
Information	12/11/2024 15:20:57	ActiveDirectory_DomainSer...	2405	Configuration interne
Information	12/11/2024 15:20:57	ActiveDirectory_DomainSer...	2120	Configuration interne
Information	12/11/2024 15:20:57	ActiveDirectory_DomainSer...	2172	Configuration interne
Information	12/11/2024 15:20:57	ActiveDirectory_DomainSer...	2168	Configuration interne
Information	12/11/2024 15:20:57	ActiveDirectory_DomainSer...	2406	Configuration interne
Information	12/11/2024 15:20:57	ActiveDirectory_DomainSer...	2121	Configuration interne
Avertissement	12/11/2024 15:20:56	ActiveDirectory_DomainSer...	3054	Sécurité
Avertissement	12/11/2024 15:20:56	ActiveDirectory_DomainSer...	3051	Sécurité
Avertissement	07/11/2024 01:54:22	ActiveDirectory_DomainSer...	2092	Réplication
Information	07/11/2024 01:53:25	ActiveDirectory_DomainSer...	3027	Nettoyage de la mémoire
Information	07/11/2024 01:53:25	ActiveDirectory_DomainSer...	3033	Nettoyage de la mémoire

Événement 2092, ActiveDirectory_DomainService

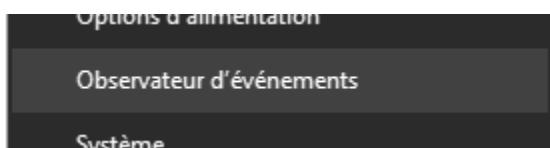
Général Détails

Le serveur est le propriétaire du rôle FSMO suivant, mais ne le considère pas comme étant valide. Pour la partition qui contient FSMO, ce serveur n'a effectué de réplication.

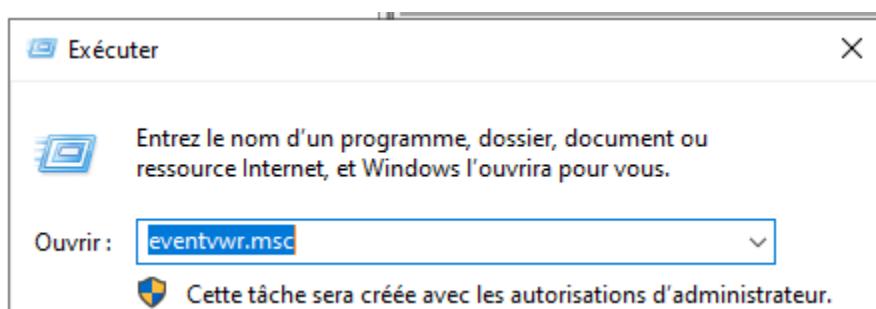
Journal: Directory Service
 Source: ActiveDirectory_DomainService Connecté: 12/11/2024 15:37:08
 Événement: 2092 Catégorie: Réplication
 Niveau: Avertissement Mots-clés: Classique
 Utilisateur: ANONYMOUSLOGON Ordinateur: SvWIn2022-Menuimetal.win.menuimetal.fr
 Opcode: Informations
 Informations: [Aide sur le Journal](#)

b) Serveur Windows Server 2022 avec DHCP -
"Second-SrvWin2022-Menuimetal"

- Démarrage de l'observateur d'événements



OU



- Recherche des événements liés au service

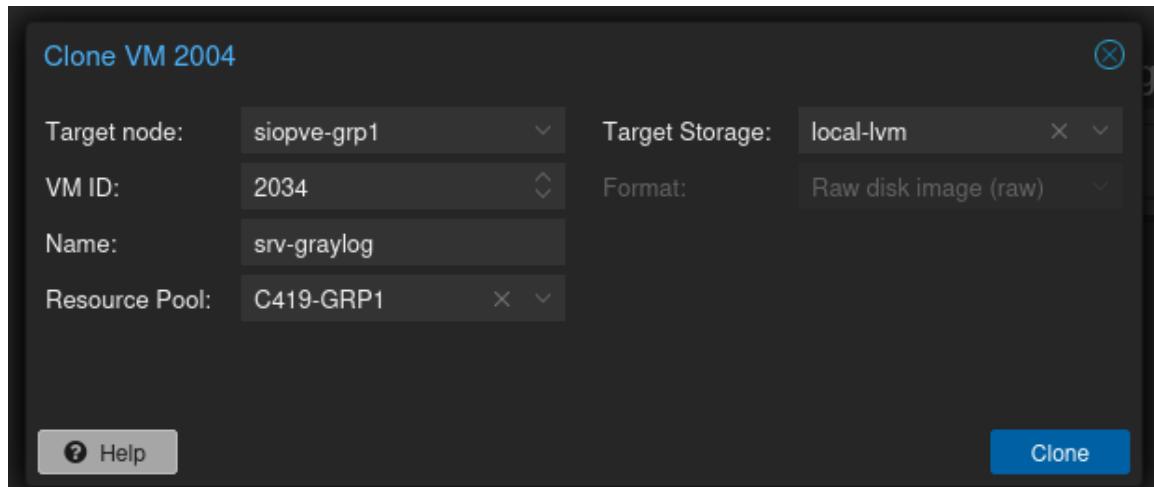
A screenshot of the Windows Event Viewer. The left pane shows a tree view of logs: "Observateur d'événements (Local)", "Affichages personnalisés", "Rôles de serveurs" (with "Serveur DHCP" expanded), "Événements d'administration", "Journaux Windows", "Journaux des applications et services", and "Abonnements". The right pane displays a list of events for the "Serveur DHCP" log. The list is titled "Nombre d'événements : 8". The events are listed in descending order of date, with the most recent at the top. The first event is selected:

Niveau	Date et heure
Information	12/11/2024 14:36:52
Avertissement	12/11/2024 14:36:52
Information	08/10/2024 13:57:52
Avertissement	08/10/2024 13:57:52
Information	03/10/2024 16:58:00
Erreur	03/10/2024 16:22:57
Avertissement	03/10/2024 16:22:57
Avertissement	03/10/2024 16:22:53

V. Les outils de centralisation

A. Graylog

1. Création et configu de la vm



Changement de nom :

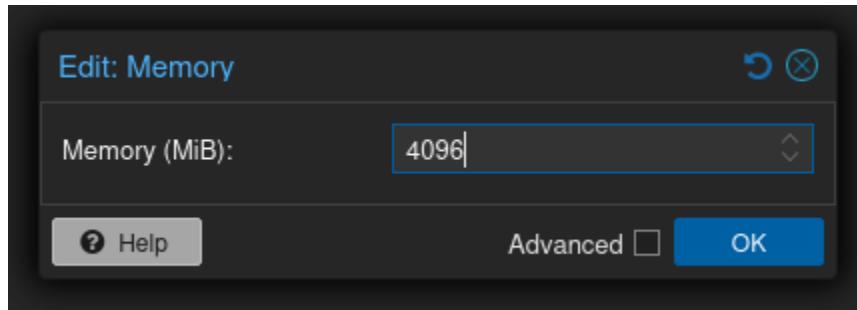
```
root@srv-debian-base:~# vim /etc/hostname
0srv-graylog
```

Configuration Ip :

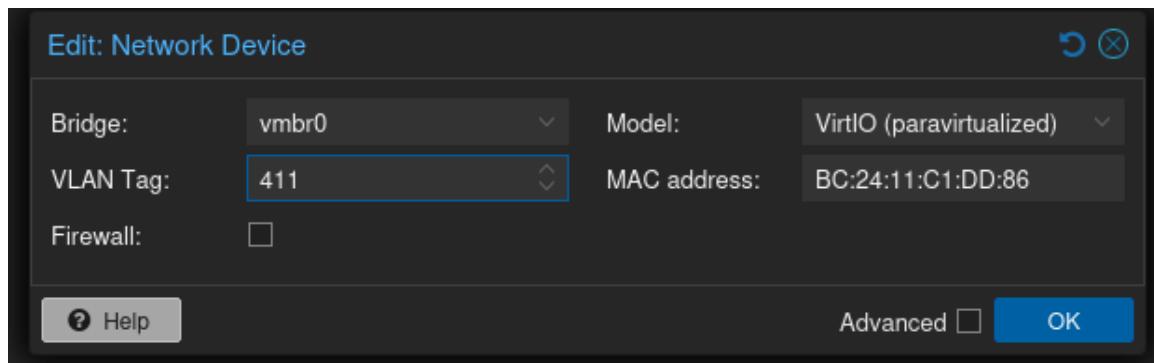
```
GL# The loopback network interface
auto lo
iface lo inet loopback
vi
()# The primary network interface
allow-hotplug ens18
iface ens18 inet static
    address 192.168.11.24
    netmask 255.255.255.0
    broadcast 192.168.11.255
    gateway 192.168.11.254
```

Attribution de ressources

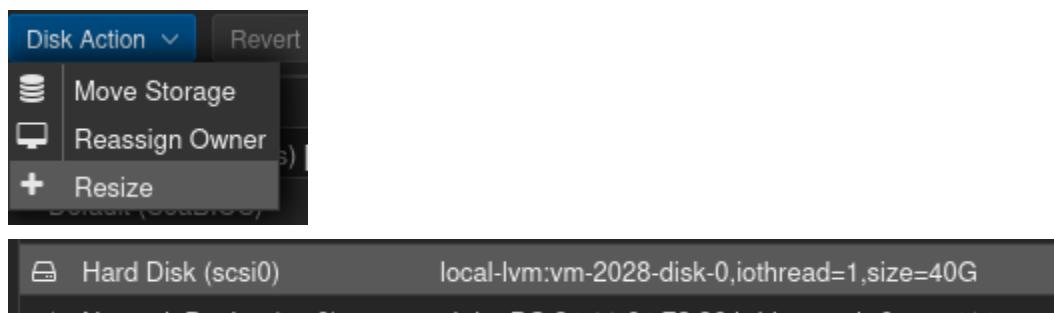
- 4 Go de mémoire vive



- Attribution du Vlan



- 40 Go de disque dur



2. Référencement DNS du serveur, intégration avec Nagios et GLPI

- Référencement DNS

```
srv-1 syslog-debian IN H 192.168.11
srv-graylog IN A 192.168.11.24
~
root@dns:~# systemctl restart named.service
root@dns:~# -
```

- Référencement DNS sur le serveur

```
nameserver 192.168.12.1
~
```

- Test de connectivité avec nslookup

```
root@dns:~# nslookup
> srv-graylog
Server:      192.168.12.1
Address:     192.168.12.1#53

Name:   srv-graylog.menuimetal.fr
Address: 192.168.11.24
> -
```

- Référencement sur le serveur Nagios

```
root@srv-nagios:~# vim /usr/local/nagios/etc/servers/graylog.cfg
root@srv-nagios:~# -
```

```

# Nagios Host configuration file template
define host {
    use                      linux-server
    host_name                srv-graylog
    alias                     Ubuntu Host
    address                  192.168.11.24
    register                 1
}

define service {
host_name                srv-graylog
service_description        PING
check_command              check_ping!100.0,20%!500.0,60%
max_check_attempts         2
}

```

Remarque : En plus, nous utiliserons le plugin **check_log** pour surveiller les fichiers journaux et détecter les événements ou erreurs spécifiques sur le serveur.

```

define service {
    host_name                mtr-ubuntu
    service_description        Check Log
    check_command              check_log!path/to/logfile!"error"
    max_check_attempts         2
    check_interval             2
    retry_interval             2
    check_period               24x7
    check_freshness            1
    contact_groups             admins
    notification_interval      2
    notification_period        24x7
    notifications_enabled       1
    register                   1
}

```

- Configuration de la commande **check_log**

```

root@srv-nagios:~# vim /usr/local/nagios/etc/objects/commands.cfg

define command {
    command_name    check_log
    command_line    /usr/local/nagios/libexec/check_log -F $ARG1$ -O /tmp/check_log_$HOSTNAME$_$SERV
ICEDESC$.state -q $ARG2$
}

```

Le plugin **check_log** permet de surveiller les fichiers journaux et d'envoyer des alertes en cas de détection de motifs spécifiques, facilitant ainsi la gestion des erreurs système ou applicatives.

- Du côté du serveur Graylog

```
root@srv-graylog:~# apt install nagios-nrpe-server nagios-plugins
```

```
root@srv-graylog:~# vim /etc/nagios/nrpe.cfg
```

```
allowed_hosts=127.0.0.1,192.168.13.2
```

- Résultat sur l'interface web de Nagios

srv-graylog		UP	11-14-2024 16:07:32	0d 0h 3m 23s	PING OK - Paquets perdus = 0%, RTA = 1.18 ms
srv-graylog	Check Log	UNKNOWN	11-14-2024 16:07:32	0d 0h 1m 11s	1/2 Unknown argument: Log.state
	Check SSH	OK	11-14-2024 16:08:16	0d 0h 1m 54s+	SSH OK - OpenSSH_9.2p1 Debian-2+deb12u3 (protocol 2.0)
	Check Users	OK	11-14-2024 16:06:53	0d 0h 1m 54s+	UTILISATEURS OK - 2 utilisateurs actuellement connectés sur
	Local Disk	PENDING	N/A	0d 0h 1m 54s+	Service check scheduled for Thu Nov 14 16:08:45 CET 2024
	PING	OK	11-14-2024 16:08:03	0d 0h 1m 54s+	PING OK - Paquets perdus = 0%, RTA = 1.06 ms
	Total Process	OK	11-14-2024 16:08:06	0d 0h 1m 54s+	PROCS OK: 0 processus avec ETAT = RSZDT

- Référencement sur glpi
 - Du côté du serveur Graylog :

```
root@srv-graylog:~# wget https://github.com/glpi-project/glpi-agent/releases/download/1.7.1/glpi-agent-1.7.1-linux-installer.pl
```

```
root@srv-graylog:~# apt install perl
```

```
perl glpi-agent-1.7.1-linux-installer.pl -s http://192.168.13.1/ --runnow --install
```

- Résultat sur l'interface web de GLPI



3. Installation et configuration de graylog

- ### • Installation de MongoDB

```
root@srv-graylog:~# apt-get install gnupg curl
```

```
root@srv-graylog:~# curl -fsSL --proxy "http://172.16.0.51:8080" https://www.mongodb.org/static/pgp/server-7.0.asc | gpg -o /usr/share/keyrings/mongodb-server-7.0.gpg --dearmor
```

- Vérification de l'ajout de la clé

```
root@srv-graylog:~# ls -l /usr/share/keyrings/mongodb-server-7.0.gpg
-rw-r--r-- 1 root root 1162 14 nov. 08:51 /usr/share/keyrings/mongodb-server-7.0.gpg
```

```
root@srv-graylog:~# cat /usr/share/keyrings/mongodb-server-7.0.gpg
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.2.20 (Debian)
Comment: https://www.mongodb.com/developer/nodejs

iQEcUfQnR0Q[NED[M vjH0mJSr 00\0r000m0U00~0-Rylw,200s$0309000*RE.00.00\$07Bn>m
0060`w0|000000M:006$ha-000:00U:TN00Byv 0`00h{0}00
6E4C0|00806<00c000!
-----END PGP SIGNATURE-----
```

```
root@srv-graylog:~# vim /etc/apt/sources.list.d/mongodb-org-7.0.list  
root@srv-graylog:~#
```

```
root@srv-graylog:~# echo "deb [ signed-by=/usr/share/keyrings/mongodb-server-7.0.gpg ] http://repo.mongodb.org/apt/debian bookworm/mongodb-org/7.0 main" | tee /etc/apt/sources.list.d/mongodb-org-7.0.list
deb [ signed-by=/usr/share/keyrings/mongodb-server-7.0.gpg ] http://repo.mongodb.org/apt/debian bookworm/mongodb-org/7.0 main
root@srv-graylog:~#
```

```
root@srv-graylog:~# apt-get update
Réception de :1 http://deb.debian.org/debian bookworm InRelease [151 kB]
Récupération des listes de packages... Fait
```

```
root@srv-graylog:~# apt-get install -y mongodb-org
Lecture des listes de paquets... Fait
```

```
root@srv-graylog:~# systemctl daemon-reload
```

```
root@srv-graylog:~# systemctl enable mongod.service
Created symlink /etc/systemd/system/multi-user.target.wants/mongod.service → /lib/systemd/system/mongod.service.
```

```
root@srv-debian-base:~# systemctl status mongod.service
● mongod.service - MongoDB Database Server
   Loaded: loaded (/lib/systemd/system/mongod.service; disabled; preset: enabled)
   Active: failed (Result: signal) since Thu 2024-11-14 08:22:43 CET; 28h ago
     Duration: 28ms
       Docs: https://docs.mongodb.org/manual
      Process: 2782 ExecStart=/usr/bin/mongod --config /etc/mongod.conf (code=killed, signal=ILL)
        Main PID: 2782 (code=killed, signal=ILL)
          CPU: 21ms

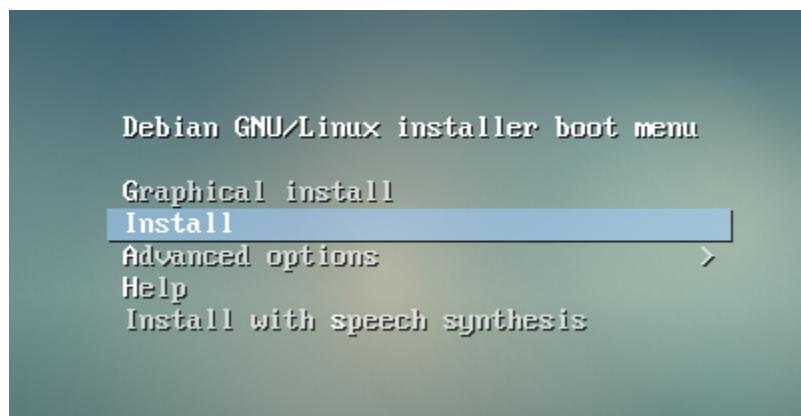
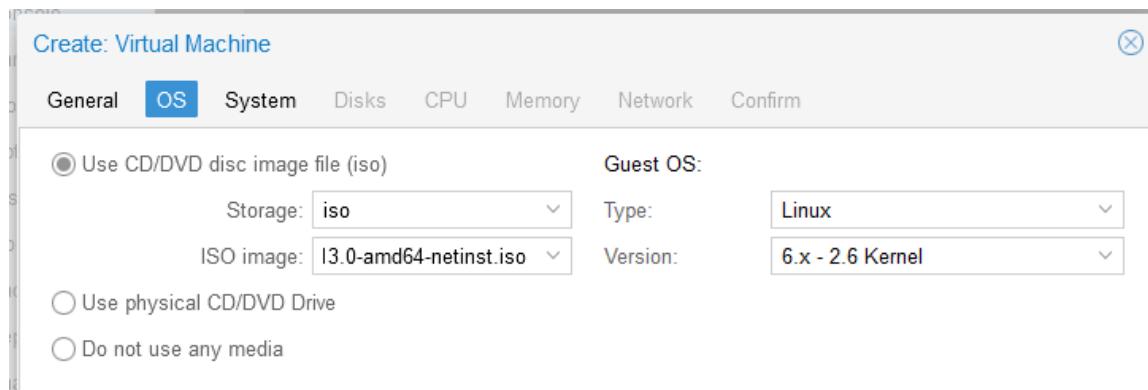
nov. 14 08:22:43 srv-debian-base systemd[1]: Started mongod.service - MongoDB Database Server.
nov. 14 08:22:43 srv-debian-base systemd[1]: mongod.service: Main process exited, code=killed, status=4/ILL
nov. 14 08:22:43 srv-debian-base systemd[1]: mongod.service: Failed with result 'signal'.
root@srv-debian-base:~# _
```

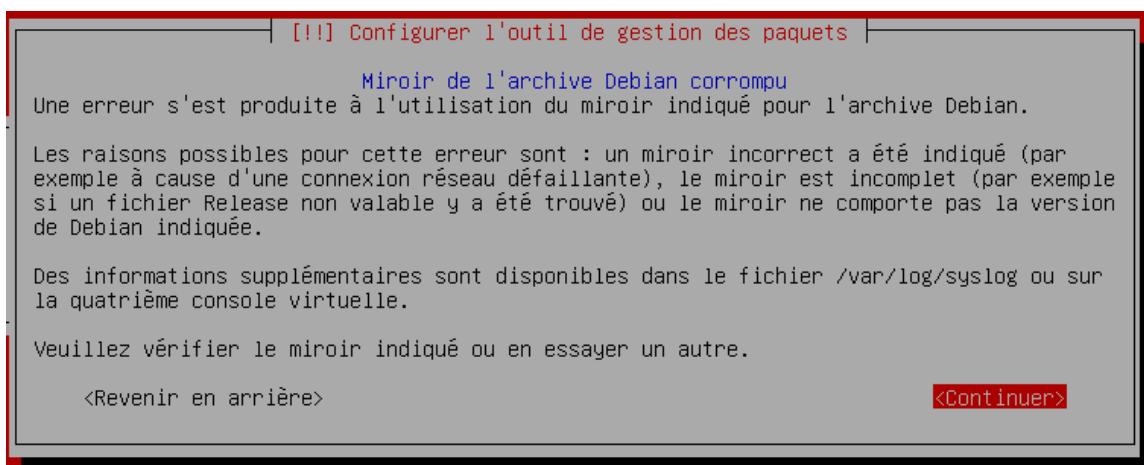
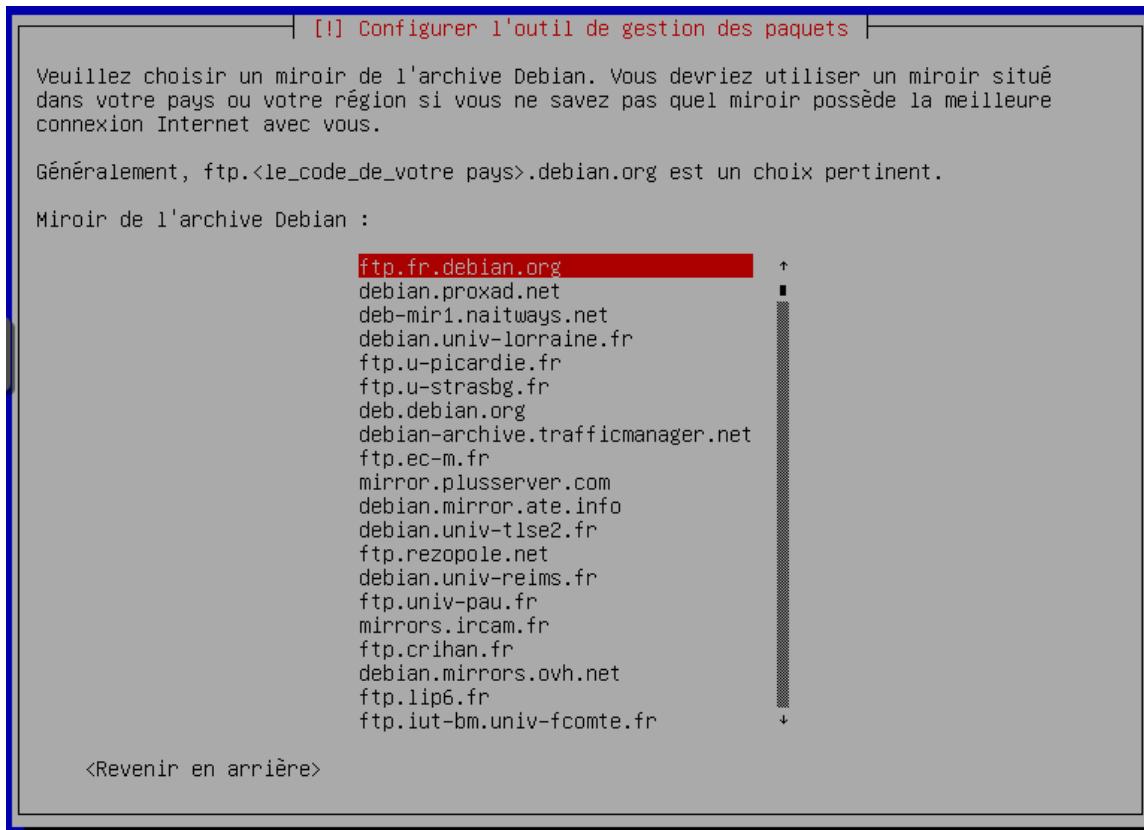
Commentaire : Il semble y avoir un problème de compatibilité entre Proxmox et MongoDB. Bien que MongoDB fonctionne correctement sur VirtualBox, il rencontre des difficultés pour démarrer sur Proxmox. Cela pourrait être lié à des différences dans la gestion de la virtualisation (KVM dans Proxmox contre VirtualBox) ou à des configurations spécifiques requises par MongoDB pour fonctionner correctement dans un environnement virtualisé sur Proxmox.

Suite à cette erreur, nous avons tenté de changer le processeur virtuel sur Proxmox, mais cela n'a pas résolu le problème. En fin de compte, nous

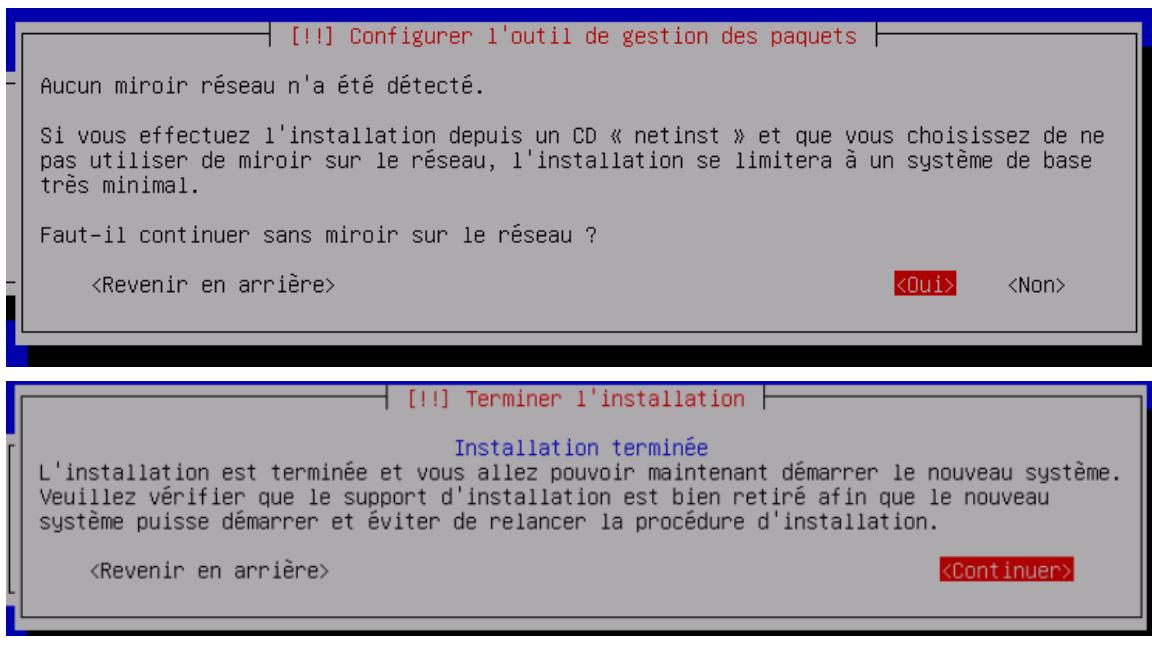
avons opté pour l'installation de MongoDB sur une version antérieure de Debian, à savoir Debian 9.

4. Installation et configuration de graylog sur debian 9





Nous avons contourné cette étape car elle génère une erreur d'installation, mais nous ajouterons les dépôts plus tard.



```
root@graylog:~# cat /etc/debian_version
9.13
```

Une fois la machine installée, nous ajouterons les dépôts archivés dans le fichier `/etc/apt/sources.list`.

- **deb http://archive.debian.org/debian stretch main contrib non-free**
- **deb http://archive.debian.org/debian-security stretch/updates main contrib non-free**

```
# deb cdrom:[Debian GNU/Linux 9.13.0 _Stretch_ - Official amd64 NETINST 20200718-11:07]/ stretch main
#deb cdrom:[Debian GNU/Linux 9.13.0 _Stretch_ - Official amd64 NETINST 20200718-11:07]/ stretch main
deb http://archive.debian.org/debian stretch main contrib non-free
deb http://archive.debian.org/debian-security stretch/updates main contrib non-free
```

- Ajout du proxy dans le fichier vi /etc/apt/apt.conf.

```
Acquire::http::Proxy "http://172.16.0.51:8080";
```

- Désactivation de la vérification SSL pour les anciens dépôts

Étant donné que les dépôts Debian archivés ne sont plus signés avec des clés valides, nous devons désactiver cette vérification pour éviter les erreurs.

Création d'un fichier de configuration pour désactiver la vérification de la validité des certificats des dépôts :

vim /etc/apt/apt.conf.d/99ignore-releases

```
Acquire::Check-Valid-Until "false";
```

Mis à jour des paquets pour que le système Debian 9 soit à jour avec les derniers paquets des dépôts archivés :

apt update

apt upgrade

- **Installation des outils nécessaires :**
 - **Installer gnupg (si ce n'est pas déjà fait)**
 - **Installer apt-transport-https pour les dépôts HTTPS**
 - **apt update**
- **Ajouter des dépôts MongoDB 4.0**

Maintenant, on va ajouter le dépôt officiel de MongoDB pour Debian 9

- Téléchargez et ajoutez la clé GPG pour MongoDB :

- wget -qO - https://pgp.mongodb.com/server-4.0.asc | sudo apt-key add -

```
root@srv-graylog:~# wget -qO - https://pgp.mongodb.com/server-4.0.asc | apt-key add -
OK
root@srv-graylog:~#
```

- **Ajout d'un dépôt MongoDB**

- echo "deb [trusted=yes] https://repo.mongodb.org/apt/debian stretch/mongodb-org/4.0 main" | tee /etc/apt/sources.list.d/mongodb-org-4.0.list

```
root@srv-graylog:~# echo "deb [trusted=yes] https://repo.mongodb.org/apt/debian stretch/mongodb-org/4.0 main" | tee /etc/apt/sources.list.d/mongodb-org-4.0.list
deb [trusted=yes] https://repo.mongodb.org/apt/debian stretch/mongodb-org/4.0 main
```

L'option **[trusted=yes]** permet de contourner les problèmes de signature GPG en cas de clés expirées.

- **Mis à jour des informations des paquets**

Une fois les dépôts ajoutés, mettez à jour les informations des paquets pour inclure le dépôt MongoDB :

apt update --allow-unauthenticated

```
root@srv-graylog:~# apt update --allow-unauthenticated
Ign:1 http://archive.debian.org/debian stretch InRelease
Ign:2 https://repo.mongodb.org/apt/debian stretch/mongodb-org/4.0 InRelease
```

Pour être sûr qu'il n'y aura pas d'erreurs liées à la vérification des signatures des paquets, nous utiliserons également la commande **apt update --allow-unauthenticated**.

- **Installation MongoDB**

apt install mongodb-org

```
root@srv-graylog:~# apt install mongodb-org
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
```

- Vérification de l'installation de MongoDB

mongo --version

systemctl start mongod

systemctl enable mongod

```
root@srv-graylog:~# systemctl start mongod
root@srv-graylog:~# systemctl enable mongod
Created symlink /etc/systemd/system/multi-user.target.wants/mongod.service → /lib/systemd/system/mongod.service.
root@srv-graylog:~# systemctl status mongod
```

systemctl status mongod

```
root@srv-graylog:~# systemctl status mongod
● mongod.service - MongoDB Database Server
  Loaded: loaded (/lib/systemd/system/mongod.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2024-11-15 13:40:40 CET; 3min 19s ago
    Docs: https://docs.mongodb.org/manual/
   Main PID: 1284 (mongod)
      Tasks: 28
     CGroup: /system.slice/mongod.service
             └─1284 /usr/bin/mongod --config /etc/mongod.conf

nov. 15 13:40:40 srv-graylog systemd[1]: Started MongoDB Database Server.
root@srv-graylog:~# █
```

Graylog Version	Minimum MongoDB Version	Maximum MongoDB Version	Minimum OpenSearch Version	Maximum OpenSearch Version
4.0.x	3.6	4.2	Not Supported	Not Supported
4.1.x	3.6	4.4	Not Supported	Not Supported
4.2.x	3.6	4.4	Not Supported	Not Supported

OpenSearch n'est pas une version compatible avec la version de Graylog que nous déployons ici, à savoir la version 4.0, sur le serveur Debian 9. Cette version a été choisie pour garantir la compatibilité avec MongoDB. D'après les images et la documentation officielle de Graylog, la version d'OpenSearch que nous avons essayée n'est pas supportée. Par

conséquent, nous allons opter pour une alternative basée sur Elasticsearch, qui est compatible avec Graylog 4.0.

- **Étapes d'installation d'Elasticsearch sur Debian 9**

Installation de **OpenJDK 8**, car Elasticsearch nécessite Java pour fonctionner :

apt install openjdk-8-jdk

```
root@srv-graylog:~# apt install openjdk-8-jdk
```

Vérification de l'installation de Java avec la commande suivante :

java -version

```
root@srv-graylog:~# java -version
openjdk version "1.8.0_252"
OpenJDK Runtime Environment (build 1.8.0_252-8u252-b09-1~deb9u1-b09)
OpenJDK 64-Bit Server VM (build 25.252-b09, mixed mode)
root@srv-graylog:~# □
```

- **Ajout du dépôt d'Elasticsearch**

Ajout de la clé GPG pour le dépôt d'Elasticsearch :

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -

```
root@srv-graylog:~# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -
OK
root@srv-graylog:~#
```

Ajout du dépôt d'Elasticsearch pour installer la version 7.x :

echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/sources.list.d/elastic-7.x.list

```
root@srv-graylog:~# echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/
sources.list.d/elastic-7.x.list
root@srv-graylog:~#
```

- Installation d' Elasticsearch :

```
apt update
```

```
apt install elasticsearch
```

```
root@srv-graylog:~# apt install elasticsearch
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
```

- Activation et démarrage d'Elasticsearch :

```
systemctl enable elasticsearch.service
```

```
root@srv-graylog:~# systemctl enable elasticsearch.service
Synchronizing state of elasticsearch.service with SysV service script with /lib/systemd/systemd-sysv-
-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /usr/lib/systemd
/system/elasticsearch.service.
root@srv-graylog:~#
```

```
systemctl start elasticsearch.service
```

```
root@srv-graylog:~# systemctl start elasticsearch.service
root@srv-graylog:~#
```

- Modification de la configuration d'Elasticsearch :

```
vim /etc/elasticsearch/elasticsearch.yml
```

Activer le mode single-node et sécommenter http.port: 9200 :

```
"discovery.type: single-node"
#
http.port: 9200
```

```
systemctl restart elasticsearch
```

```
systemctl status elasticsearch
```

```
root@srv-graylog:~# systemctl restart elasticsearch
root@srv-graylog:~# systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
  Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2024-11-15 14:02:09 CET; 57s ago
    Docs: https://www.elastic.co
   Main PID: 6210 (java)
      Tasks: 50 (limit: 4915)
```

• Installation de graylog

Téléchargement du paquet du dépôt officiel :

```
wget
```

```
https://packages.graylog2.org/repo/packages/graylog-4.0-repository\_latest.deb
```

```
root@srv-graylog:~# wget https://packages.graylog2.org/repo/packages/graylog-4.0-repository_latest.deb
--2024-11-15 14:04:11--  https://packages.graylog2.org/repo/packages/graylog-4.0-repository_latest.deb
Connexion à 172.16.0.51:8080... connecté.
requête Proxy transmise, en attente de la réponse... 302 Found
Emplacement : https://graylog-package-repository.s3.eu-west-1.amazonaws.com/packages/graylog-4.0-repository_latest.deb?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20241115T130412Z&X-Amz-SignedHeaders=host&X-Amz-Expires=600&X-Amz-Credential=AKIAIJSI6MCSPXFVDPIA%2F20241115%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Signature=18dde373c782bbe4935c93b22a0edb53dc4cf6b8caf23c4ed624e1d288a4b3ef [suivant]
--2024-11-15 14:04:12--  https://graylog-package-repository.s3.eu-west-1.amazonaws.com/packages/graylog-4.0-repository_latest.deb?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20241115T130412Z&X-Amz-SignedHeaders=host&X-Amz-Expires=600&X-Amz-Credential=AKIAIJSI6MCSPXFVDPIA%2F20241115%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Signature=18dde373c782bbe4935c93b22a0edb53dc4cf6b8caf23c4ed624e1d288a4b3ef
Connexion à 172.16.0.51:8080... connecté.
requête Proxy transmise, en attente de la réponse... 200 OK
Taille : 2078 (2,0K) [application/x-debian-package]
Sauvegarde en : « graylog-4.0-repository_latest.deb »

graylog-4.0-repository_l 100%[=====] 2,03K ---KB/s in 0s
2024-11-15 14:04:13 (26,5 MB/s) - « graylog-4.0-repository_latest.deb » sauvegardé [2078/2078]
```

```
dpkg -i graylog-4.0-repository_latest.deb
```

```
root@srv-graylog:~# dpkg -i graylog-4.0-repository_latest.deb
Sélection du paquet graylog-4.0-repository précédemment désélectionné.
(Lecture de la base de données... 38959 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de graylog-4.0-repository_latest.deb ...
Dépaquetage de graylog-4.0-repository (1-2) ...
Paramétrage de graylog-4.0-repository (1-2) ...
root@srv-graylog:~#
```

Mettre à jour des dépôts :

apt update

apt install -y graylog-server

```
root@srv-graylog:~# apt install -y graylog-server
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
```

```
Paramétrage de graylog-server (4.0.17-1) ...
#####
Graylog does NOT start automatically!
Please run the following commands if you want to start Graylog automatically on system boot:
    sudo systemctl enable graylog-server.service
    sudo systemctl start graylog-server.service
#####
#
```

- **Génération d'un mot de passe secret pour Graylog**

```
root@srv-graylog:~# apt install pwgen
```

```
root@srv-graylog:~# pwgen -N 1 -s 96
QPNspHOagMVYXIFPjWKa0jitzbtQaXsAlXTtVUw10lkBUEKvP1gzj7BTQeFPErGrj68svf98txYw1HaPZU4eD9r5V18AJZBL
root@srv-graylog:~#
```

sortie :

QPNspHOagMVYXIFPjWKa0jitzbtQaXsAlXTtVUw10lkBUEKvP1gzj7BTQe
FPErGrj68svf98txYw1HaPZU4eD9r5V18AJZBL

- **Configuration de Graylog**

vim /etc/graylog/server/server.conf

Ajout du password secret dans le fichier de configuration :

```
password_secret =
QPNspHOagMVYXIFPjWKa0jitzbtQaXsAlXTtVUw10lkBUEKvP1gzj7BTQe
FPErGrj68svf98txYw1HaPZU4eD9r5V18AJZBL
```

```
password_secret =QPNspH0agMVYXIFPjWKa0jitzbtQaXsAlXTtVUw10lkBUeKvPlgzj7BTQeFPErGrj68svf98txYw1HaPZU4  
eD9r5V18AJZBL
```

Définition du mot de passe root pour Graylog :

```
echo -n "votre_mot_de_passe" | sha256sum
```

```
root@srv-graylog:~# echo -n "root" | sha256sum  
4813494d137e1631bba301d5acab6e7bb7aa74ce1185d456565ef51d737677b2  
root@srv-graylog:~#
```

sortie :

```
4813494d137e1631bba301d5acab6e7bb7aa74ce1185d456565ef51d7376  
77b2
```

Edition du fichier server.conf :

```
vim /etc/graylog/server/server.conf
```

Ajoutez le hash du mot de passe de l'utilisateur admin :

```
root_password_sha2  
=4813494d137e1631bba301d5acab6e7bb7aa74ce1185d456565ef51d737  
677b2
```

```
root_password_sha2 =4813494d137e1631bba301d5acab6e7bb7aa74ce1185d456565ef51d737677b2
```

- Configurer l'interface web de Graylog

Configuration de l'adresse IP et du port de l'interface web de Graylog dans le fichier server.conf :

```
vim /etc/graylog/server/server.conf
```

http_bind_address = 192.168.0.10:9000

```
http_bind_address = 192.168.11.50:9000  
#http_bind_address = [2001:db8::11:9000]
```

Si on accède à Graylog via une adresse IP publique, on configure aussi l'URI externe :

http_external_uri = https://ip_serveur:9000/

```
http_publish_uri = http://192.168.11.50:9000/
```

- Démarrage de Graylog

systemctl start graylog-server

- Activation de Graylog au démarrage

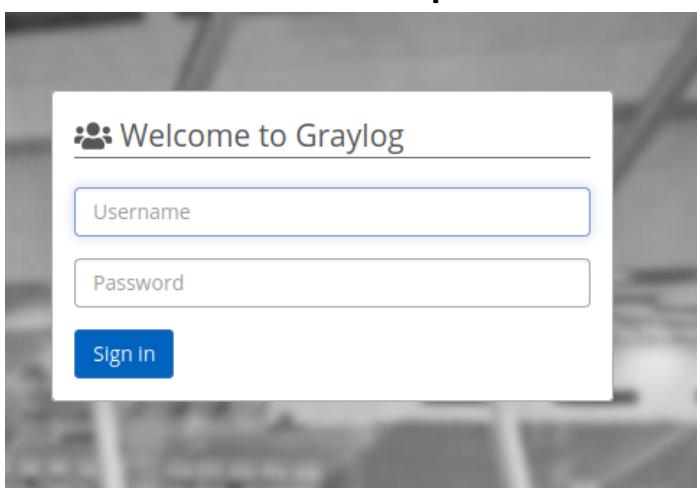
systemctl enable graylog-server

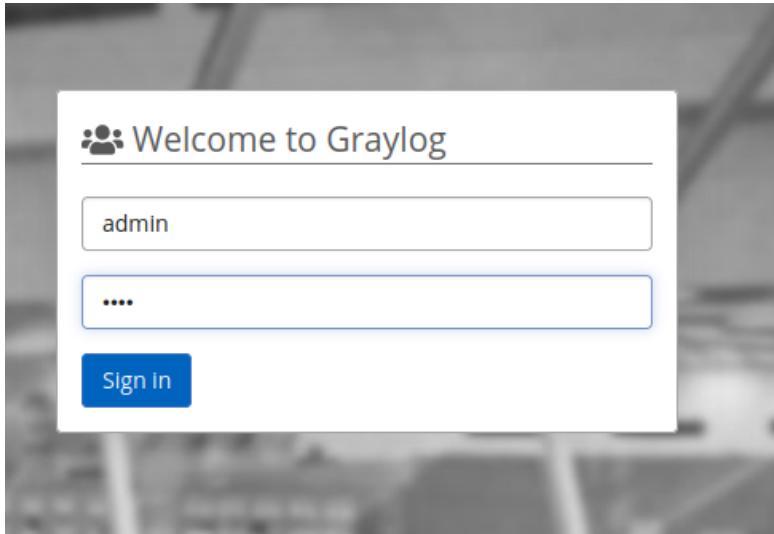
- Vérification du bon fonctionnement

systemctl status graylog-server

```
root@srv-graylog:~# systemctl status graylog-server
● graylog-server.service - Graylog server
   Loaded: loaded (/usr/lib/systemd/system/graylog-server.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2024-11-15 14:18:45 CET; 16s ago
     Docs: http://docs.graylog.org/
Main PID: 7073 (graylog-server)
```

Accès à l'interface web depuis l'adresse suivante : **192.168.11.50:9000**

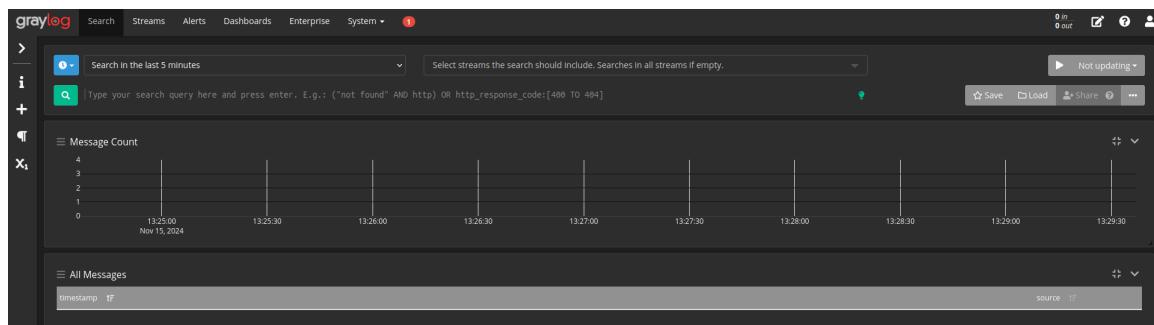




Login :

admin

root



Configuration de elasticsearch :

```
root@srv-graylog:~# vim /etc/elasticsearch/elasticsearch.yml  
root@srv-graylog:~# vim /etc/elasticsearch/elasticsearch.yml
```

```
#  
network.host: 0.0.0.0  
#
```

Liaison de elasticsearch avec graylog :

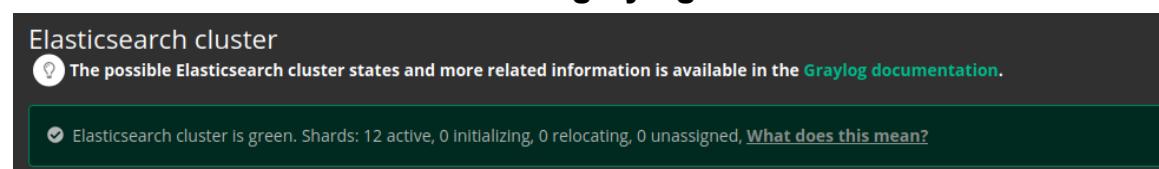
```
root@srv-graylog:~# vim /etc/graylog/server/server.conf
```

```
[...]  
elasticsearch_hosts = http://127.0.0.1:9200  
# If you have more than one Elasticsearch host, add them here.  
[...]
```

vérification de la connectivité avec la commande ci dessous : curl -X GET "localhost:9200/"

```
root@srv-graylog:~# curl -X GET "localhost:9200/"  
{  
    "name" : "srv-graylog",  
    "cluster_name" : "elasticsearch",  
    "cluster_uuid" : "a6mIi8FFRoW6PFFv8A6i0w",  
    "version" : {  
        "number" : "7.17.25",  
        "build_flavor" : "default",  
        "build_type" : "deb",  
        "build_hash" : "f9b6b57d1d0f76e2d14291c04fb50abeb642cfbf",  
        "build_date" : "2024-10-16T22:06:36.904732810Z",  
        "build_snapshot" : false,  
        "lucene_version" : "8.11.3",  
        "minimum_wire_compatibility_version" : "6.8.0",  
        "minimum_index_compatibility_version" : "6.0.0-beta1"  
    },  
    "tagline" : "You Know, for Search"  
}  
root@srv-graylog:~#
```

Vérification sur l'interface web de graylog :



Elasticsearch cluster
💡 The possible Elasticsearch cluster states and more related information is available in the [Graylog documentation](#).
✔ Elasticsearch cluster is green. Shards: 12 active, 0 initializing, 0 relocating, 0 unassigned, [What does this mean?](#)

Configuration d'input afin de recevoir un message test :

The screenshot shows the 'Inputs' section of the Graylog web interface. It includes a header with 'Inputs' and a sub-header 'Graylog nodes accept data via inputs. Launch or terminate as many inputs as you want here.' Below this are buttons for 'Select Input', 'Launch new input', and 'Find more inputs'. There are also 'Filter by title', 'Filter', and 'Reset' buttons. The 'Global inputs' section shows '0 configured' and a message 'There are no global inputs.' The 'Local inputs' section shows '0 configured' and a message 'There are no local inputs.'

The screenshot shows the 'Launch new Syslog UDP input' configuration dialog. At the top are buttons for 'Launch new input' and 'Find more inputs'. The form fields include:

- Global**: A checkbox labeled 'Should this input start on all nodes'.
- Node**: A dropdown menu set to 'adf824b0 / srv-graylog'.
- Title**: An input field containing 'test'.
- Bind address**: An input field containing '0.0.0.0'.
- Port**: An input field containing '5555'.
- Receive Buffer Size (optional)**: An input field containing '262144'.
- No. of worker threads (optional)**: An input field containing '1'.
- Override source (optional)**: An input field with a placeholder 'The source is a hostname derived from the received packet by default. Set this if you want to override it with a custom string.'
- Force rDNS?**: A checkbox labeled 'Force rDNS resolution of hostname? Use if hostname cannot be parsed. (Be careful if you are sending DNS logs into this input because it can cause a feedback loop.)'

The screenshot shows the Graylog configuration interface. At the top, there are buttons for 'Filter by title', 'Filter', and 'Reset'. Below this, under 'Global inputs', it says '0 configured' and 'There are no global inputs.' Under 'Local inputs', it says '1 configured' and lists a single input named 'test' which is a 'Syslog UDP' type and is 'RUNNING'. The configuration details for 'test' include:

- allow_override_date: true
- bind_address: 0.0.0.0
- expand_structured_data: false
- force_rdns: false
- number_worker_threads: 1
- override_source: <empty>
- port: 5555
- recv_buffer_size: 262144
- store_full_message: false

On the right side of the interface, there are buttons for 'Show received messages' and 'Manage extractions'. At the bottom right, there is a 'Throughput / Metrics' section showing network statistics.

Envoie du message depuis le serveur graylog pour tester la communication :

```
root@srv-graylog:~# echo "Hello Graylog from UDP" | nc -u -wl 127.0.0.1 5555
root@srv-graylog:~#
```

Résultat :

The screenshot shows the Graylog search interface. At the top, there is a search bar with a clock icon and the placeholder text 'Search in all messages'. Below the search bar, there is another search bar with a magnifying glass icon and the placeholder text 'Type your search query here and press enter. E.g.: ("not found" AND'. The main area displays a list of messages under the heading 'All Messages'.

timestamp	message
2024-11-15 15:19:23.163 +00:00	Hello Graylog from UDP
2024-11-15 15:15:48.949 +00:00	Hello Graylog from UDP

5. Envoi de logs depuis Nagios vers Graylog

- Du côté du serveur nagios :

apt-get update

apt-get install rsyslog

```
root@srv-nagios:~# apt install rsyslog
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
```

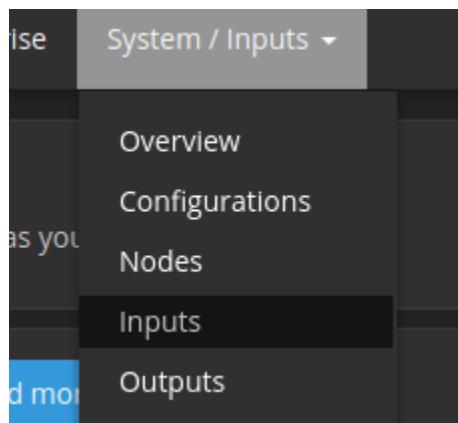
```
root@srv-nagios:~# vim /etc/rsyslog.conf
```

```
*.* @192.168.11.50:5555
# Remplacez l'IP et le po
```

systemctl restart rsyslog

- Configuration de l'input UDP dans Graylog :

Création de l'input dans System > Inputs :



Syslog UDP

Launch new input

Launch new *Syslog UDP* input

Global
Should this input start on all nodes

Node
adf824b0 / srv-graylog

On which node should this input start

Title
log_nagios

Select a name of your new input that describes it.

Bind address
0.0.0.0

Address to listen on. For example 0.0.0.0 or 127.0.0.1.

Port
5555

Port to listen on.

Receive Buffer Size (optional)
262144

The size in bytes of the recvBufferSize for network connections to this input.

No. of worker threads (optional)
1

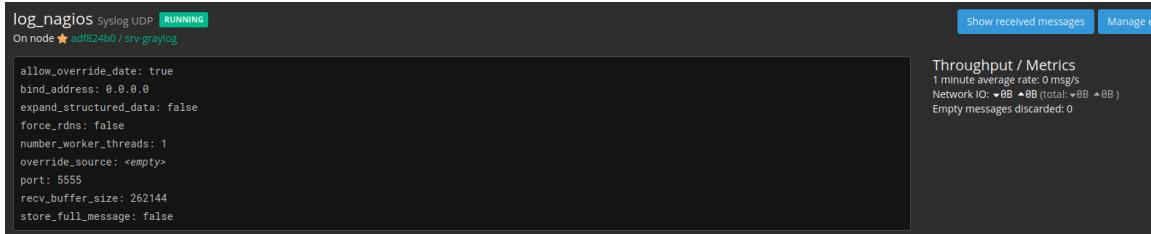
Number of worker threads processing network connections for this input.

Override source (optional)

The source is a hostname derived from the received packet by default. Set this if you want to override it with a custom string.

Force rDNS?
Force rDNS resolution of hostname? Use if hostname cannot be parsed. (Be careful if you are sending DNS logs into this input because it can cause a feedback)

- **Port : 5555 (Le port 5555 est utilisé pour le protocole UDP, qui permet une communication rapide et sans connexion)**
- **Bind address : 0.0.0.0 (pour écouter sur toutes les interfaces)**



- Vérification de l'envoi de logs
 - Test l'envoi de logs depuis Nagios

Une fois que rsyslog est configuré, on peut tester l'envoi de logs en déclenchant un événement de Nagios. Ici, forcez un échec dans Nagios pour voir si un message de log est généré.

```
root@srv-nagios:~# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
Nagios Core 4.5.5
Copyright (c) 2009-present Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 2024-09-17
License: GPL

Website: https://www.nagios.org
Reading configuration data...
  Read main config file okay...
Error: Unexpected token or statement in file '/usr/local/nagios/etc/servers/graylog.cfg' on line 1
Error: Invalid max_check_attempts value for host 'clt-debian-nagios'
Error: Could not register host (config file '/usr/local/nagios/etc/servers/debian-client.cfg', s
ing on line 2)
  Error processing object config files!

***> One or more problems was encountered while processing the config files...

Check your configuration file(s) to ensure that they contain valid
directives and data definitions. If you are upgrading from a previous
version of Nagios, you should be aware that some variables/definitions
may have been removed or modified in this version. Make sure to read
the HTML documentation regarding the config files, as well as the
'Whats New' section to find out what has changed.

root@srv-nagios:~#
```

● Vérification dans Graylog

All Messages	source
timestamp: 1f	
2024-11-15 15:33:54.000 +00:00	
srv-nagios nagios: SERVICE NOTIFICATION: nagiosadmin;client1;Virtual Memory Usage;CRITICAL;notify-service-by-email;(No output on stdout) stderr: Usage: check_ncpa.py [options]	srv-nagios
2024-11-15 15:33:54.000 +00:00	
srv-nagios nagios: wproc: host=client1; service=Virtual Memory Usage; contact=nagiosadmin	srv-nagios
2024-11-15 15:33:54.000 +00:00	
srv-nagios nagios: wproc: NOTIFY job 6927 from worker Core Worker 272363 is a non-check helper but exited with return code 127	srv-nagios
2024-11-15 15:33:54.000 +00:00	
srv-nagios nagios: wproc: early_timeout@; exited_ok@; wait_status=32512; error_code@;	srv-nagios
2024-11-15 15:33:54.000 +00:00	
srv-nagios nagios: wproc: stderr line 02: /usr/bin/printf: erreur d'écriture: Relais brisé (pipe)	srv-nagios
2024-11-15 15:33:54.000 +00:00	
srv-nagios nagios: wproc: stderr line 01: /bin/sh: 1: /bin/mail: not found	srv-nagios
2024-11-15 15:33:54.000 +00:00	
srv-nagios nagios: wproc: host=srv-rsyslog-debian; service=Check Log; contact=nagiosadmin	srv-nagios
2024-11-15 15:33:58.000 +00:00	
srv-nagios nagios: wproc: stderr line 01: /bin/sh: 1: /bin/mail: not found	srv-nagios
2024-11-15 15:33:58.000 +00:00	
srv-nagios nagios: SERVICE NOTIFICATION: nagiosadmin;srv-rsyslog_debian;Check Log;UNKNOWN;notify-service-by-email;Unknown argument: Log.state	srv-nagios

6. Création d'un premier log

Dans l'interface Web de Graylog, allez dans Streams :

Creating Stream

Title
srv-nagios

Description
What kind of messages are routed into this stream?

Index Set
Default index set

Messages that match this stream will be written to the configured index set.

Remove matches from 'All messages' stream
Remove messages that match this stream from the 'All messages' stream which is assigned to every message by default.

Cancel **Save**

- **Création d'un nouveau stream pour catégoriser les logs de Nagios.**

The first screenshot shows the 'Default index set' configuration with a single log source named 'log'. The second screenshot shows the 'nagios' stream configuration, which includes the same 'log' source and a 'filter' stage.

Dans Search, entrez nagios :

The search bar contains the term 'nagios', and the results pane is currently empty, indicating no results have been found yet.

Observation des logs concernant nagios :

The search results show several log entries from the 'nagios' index set:

```

2024-11-15 15:39:26.000 +00:00
srv-nagios nagios: wproc: host=svr-dhcp-debian; service=DHCP Status; contact=nagiosadmin
2024-11-15 15:39:26.000 +00:00
srv-nagios nagios: wproc: stderr Line 01: /bin/sh: 1: /bin/mail: not found
2024-11-15 15:39:26.000 +00:00
srv-nagios nagios: wproc: early_timeout=0; exited_ok=1; wait_status=32512; error_code=0;
2024-11-15 15:39:26.000 +00:00
srv-nagios nagios: SERVICE_NOTIFICATION: nagiosadmin;svr-dhcp-debian;DHCP Status:UNKNOWN;notify-service-by-email;Got unexpected non-option argument
2024-11-15 15:39:26.000 +00:00
srv-nagios nagios: wproc: NOTIFY job 6954 from worker Core Worker 272162 is a non-check helper but exited with return code 127
2024-11-15 15:39:26.000 +00:00
srv-nagios nagios: wproc: stderr line 02: /usr/bin/printf: erreur d'écriture: Relais brisé (pipe)
2024-11-15 15:39:01.000 +00:00
srv-nagios CRON[325443]: (root) CMD [ -x /usr/lib/php/sessionclean ] && if [ ! -d /run/systemd/system ]; then /usr/lib/php/sessionclean; fi

```

B. Rsyslog et script

Installation de Rsyslog :

Configuration côté serveur :

apt install rsyslog

Paramétrage du serveur pour qu'il accepte les logs venant de l'extérieur :

vim **/etc/rsyslog.conf** (on décommente les deux lignes suivantes) :

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

service rsyslog restart

On vérifie que notre serveur est bien à l'écoute :

netstat -npl

```
root@srv-rsyslog-debian:~# netstat -npl
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale          Adresse distante      Etat        PID/Program name
udp        0      0 0.0.0.0:111              0.0.0.0:*            0/0
udp        0      0 0.0.0.0:514              0.0.0.0:*            0/0
udp6       0      0 ::1:111                :::*                  0/0
udp6       0      0 ::::514                :::*                  0/0
```

Port 514 ouvert en UDP sur notre serveur Rsyslog

Récupérer les logs d'une machine de type Linux :

Récupérez les logs de votre serveur Mariadb :

```
root@mariadb:~# apt install rsyslog
```

Paramétrage du client pour rediriger tous les logs sur le serveur :

vim **/etc/rsyslog.conf** (on ajoute cette ligne à la fin du fichier) :

Clonage de la VM, changement du nom, de l'IP et du VLAN :

```
sio@srv-rsyslog-debian:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:53:2d:18 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.11.23/24 brd 192.168.11.255 scope global ens18
        valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe53:2d18/64 scope link
        valid_lft forever preferred_lft forever
```

```
⇒ Network Device (net0)      virtio=BC:24:11:53:2D:18,bridge=vmbr0,tag=411
```

Supervision avec Nagios :

Création du fichier de configuration (côté serveur) définissant la machine et les services à surveiller :

vim **/usr/local/nagios/etc/servers/srv_rsyslog_debian.cfg**

```

Nagios Host configuration file template
define host {
    use                      linux-server
    host_name                srv-rsyslog-debian
    alias                     Ubuntu Host
    address                  192.168.11.23
    register                 1
}

    define service {
host_name                srv-rsyslog-debian
service_description        PING
check_command              check_ping!100.0,20%!500.0,60%
max_check_attempts         2
check_interval             2
retry_interval             2
check_period               24x7
check_freshness            1
contact_groups             admins
notification_interval      2
notification_period         24x7
notifications_enabled       1
register                   1
}

define service {
host_name                srv-rsyslog-debian
service_description        Check Users
check_command              check_local_users!20!50
max_check_attempts         2
check_interval             2
retry_interval             2
check_period               24x7
check_freshness            1
contact_groups             admins
notification_interval      2
notification_period         24x7
notifications_enabled       1
register                   1
}

define service {
host_name                srv-rsyslog-debian
service_description        Local Disk
check_command              check_local_disk!20%!10%!
max_check_attempts         2
check_interval             2
retry_interval             2
check_period               24x7
check_freshness            1
}

define service {
host_name                mtr-ubuntu
service_description        Check Log
check_command              check_log!path/to/logfile!"error"
max_check_attempts         2
check_interval             2
retry_interval             2
check_period               24x7
check_freshness            1
contact_groups             admins
notification_interval      2
notification_period         24x7
notifications_enabled       1
register                   1
}

```

Configuration côté client :

apt install nagios-nrpe-server nagios-plugins

vim /etc/nagios/nrpe.cfg

```
allowed_hosts=127.0.0.1,192.168.13.2
```

systemctl restart nagios-nrpe-server

Configuration côté serveur :

/usr/local/nagios/libexec/check_nrpe -H 192.168.11.23

```
root@srv-nagios:~# /usr/local/nagios/libexec/check_nrpe -H 192.168.11.23
NRPE v4.1.0
```

```
root@srv-nagios:~# service nagios restart
root@srv-nagios:~# service apache2 restart
```

Le serveur rsyslog est bien supervisé dans le Nagios

srv-rsyslog-debian		Check Log	UNKNOWN	11-14-2024 16:07:37	0d 0h 1m 6s	1/2	PING OK - Paquets perdus = 0%, RTA = 1.14 ms
srv-rsyslog-debian	Check SSH	OK	OK	11-14-2024 16:08:29	1d 23h 36m 24s	1/2	SSH OK - OpenSSH_9.2p1 Debian-2+deb12u3 (protocol 2.0)
	Check Users	OK	OK	11-14-2024 16:07:42	1d 23h 37m 18s	1/2	UTILISATEURS OK - 2 utilisateurs actuellement connectés sur
	Local Disk	OK	OK	11-14-2024 16:08:28	1d 23h 36m 29s	1/2	DISK OK - free space: / 26988MIB (91% inode=97%):
	PING	OK	OK	11-14-2024 16:08:04	1d 23h 37m 0s	1/2	PING OK - Paquets perdus = 0%, RTA = 1.4 ms
	Total Process	OK	OK	11-14-2024 16:07:25	1d 23h 37m 42s	1/2	PROCS OK: 0 processus avec ETAT = RSZDT
							Page Tour

Référencer la VM dans GLPI :

```
root@srv-rsyslog-debian:~# wget https://github.com/glpi-project/glpi-agent/releases/download/1.7.1/glpi-agent-1.7.1-linux-installer.pl
```

```
root@srv-rsyslog-debian:~# perl glpi-agent-1.7.1-linux-installer.pl -s http://192.168.13.1/ --runnow --install
```

```
root@srv-rsyslog-debian:~# systemctl status glpi-agent.service
● glpi-agent.service - GLPI agent
  Loaded: loaded (/lib/systemd/system/glpi-agent.service; enabled; preset: enabled)
  Active: active (running) since Tue 2024-11-12 15:55:32 CET; 44min ago
    Docs: man:glpi-agent(8)
   Process: 5561 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCESS)
 Main PID: 425 (glpi-agent: wai)
   Tasks: 1 (limit: 2306)
     Memory: 94.7M
        CPU: 3.935s
      CGroup: /system.slice/glpi-agent.service
              └─425 "glpi-agent: waiting"

nov. 12 16:37:42 srv-rsyslog-debian systemd[1]: Reloaded glpi-agent.service - GLPI agent.
nov. 12 16:37:43 srv-rsyslog-debian systemd[1]: glpi-agent.service: Sent signal SIGUSR1 to main process 425 (glpi-agent: wai) on client request.
nov. 12 16:37:43 srv-rsyslog-debian glpi-agent[425]: [info] GLPI Agent requested to run all targets now
nov. 12 16:37:43 srv-rsyslog-debian glpi-agent[425]: [info] target server0: server http://192.168.13.1/
nov. 12 16:37:43 srv-rsyslog-debian glpi-agent[425]: [info] sending configuration to server0
nov. 12 16:37:44 srv-rsyslog-debian glpi-agent[5567]: [info] running task Inventory
nov. 12 16:37:44 srv-rsyslog-debian glpi-agent[5567]: [info] New inventory from debian-2024-09-26-13-38-54 for server0
nov. 12 16:37:47 srv-rsyslog-debian glpi-agent[5567]: Use of uninitialized value $hostname in substitution ($///) at /usr/share/glpi-agent/lib/GLPI/Agent/Tools/Hostname.pm
nov. 12 16:37:47 srv-rsyslog-debian glpi-agent[5567]: Use of uninitialized value $hostname in index at /usr/share/glpi-agent/lib/GLPI/Agent/Task/Inventory/Generic/Domains.pm
nov. 12 16:38:13 srv-rsyslog-debian glpi-agent[425]: [info] target server0: next run: Wed Nov 13 16:31:15 2024 - http://192.168.13.1/
```



Notre serveur rsyslog est bien référencé dans le GLPI ; on l'ajoute à l'entité “Etage-2 (Salle serveur)”

Ajouter le serveur rsyslog dans le DNS :

Côté serveur :

```
root@dns:~# vim /var/cache/bind/db.menuimetal.fr
```

```
2419200          ; Expire
604800 )        ; Negative Cache TTL
;
@      IN      NS      dns
@      IN      MX 10  Srv-mail.menuimetal.fr.
        IN      A      192.168.12.1
dns    IN      A      192.168.12.1
mysql  IN      A      192.168.11.1
web    IN      A      192.168.12.2
routeur IN      A      192.168.12.254
WebWordpress IN A 192.168.11.8
WebDokuWiki IN A 192.168.11.9
srv-glpi IN      A      192.168.13.1
Srv-mail IN      A      192.168.12.3
smtp   IN      CNAME  Srv-mail
imap   IN      CNAME  Srv-mail
srv-nagios IN     A      192.168.13.2
srv-rancid IN     A      192.168.13.3
srv-OMV  IN     A      192.168.11.18
srv-radius-debian IN     A      192.168.13.4
srv-dhcp-debian IN     A      192.168.11.22
srv-rsyslog-debian IN A 192.168.11.23
```

Côté client :

```
root@srv-rsyslog-debian:~# vim /etc/resolv.conf
```

```
nameserver 192.168.12.1
```

Vérification côté serveur DNS:

```
nslookup srv-rsyslog-debian
```

```
root@dns:~# nslookup srv-rsyslog-debian
Server:      192.168.12.1
Address:      192.168.12.1#53

Name:  srv-rsyslog-debian.menuimetal.fr
Address: 192.168.11.23
```

L'accès en SSH est déjà permis (ex : connexion Via Reminna) :

Pour permettre la connexion faudra configurer l'accès par authentification :

```

Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO
#mininfo

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication no

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no

```

```

192.168.13.1 192.168.11.10 192.168.13.2 192.168.12.1 192.168.11.23

nov. 12 16:37:43 srv-rsyslog-debian glpi-agent[425]: [info] target server0: server http://192.168.13.1/
nov. 12 16:37:43 srv-rsyslog-debian glpi-agent[425]: [info] sending contact request to server0
nov. 12 16:37:44 srv-rsyslog-debian glpi-agent[5567]: [info] running task Inventory
nov. 12 16:37:44 srv-rsyslog-debian glpi-agent[5567]: [info] New inventory from debian-2024-09-26-13-38-54 for
server0
nov. 12 16:37:47 srv-rsyslog-debian glpi-agent[5567]: Use of uninitialized value $hostname in substitution ($/
//) at /usr/share/glpi-agent/lib/GLPI/Agent/Tools/Hostname.pm
nov. 12 16:37:47 srv-rsyslog-debian glpi-agent[5567]: Use of uninitialized value $hostname in index at /usr/sh
are/glpi-agent/lib/GLPI/Agent/Task/Inventory/Generic/Domains
nov. 12 16:38:13 srv-rsyslog-debian glpi-agent[425]: [info] target server0: next run: Wed Nov 13 16:31:15 2024
- http://192.168.13.1/
root@srv-rsyslog-debian:~# vim /etc/resolv.conf
root@srv-rsyslog-debian:~# vim /etc/resolv.conf ^C
root@srv-rsyslog-debian:~# nslookup
> root@srv-rsyslog-debian:~#
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:53:2d:18 brd ff:ff:ff:ff:ff:ff
    alname enp0s18
    inet 192.168.11.23/24 brd 192.168.11.255 scope global ens18
        valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe53:2d18/64 scope link
        valid_lft forever preferred_lft forever
root@srv-rsyslog-debian:~#

```

Récupérer les logs d'une machine de type Linux :

Serveur mariadb "MariaDB" :

```
root@mariadb:~# apt install rsyslog
```

```
root@mariadb:~# vim /etc/rsyslog.conf
```

On ajoute cette ligne à la fin du fichier ci-dessus pour dire à notre serveur "MariaDB" d'envoyer ses logs sur notre serveur rsyslog :

```
*.* @192.168.11.23:514
```

```
root@mariadb:~# service rsyslog restart
```

On redémarre le service "mariadb" :

```
root@mariadb:~# service mariadb restart
```

On vérifie dans le fichier **/var/log/syslog** ; les logs de notre serveur mariadb sont bien présents :

```
2024-11-14T08:57:59+01:00 mariadb rsyslogd: imuxsock: Acquired UNIX socket '/run/syslogd/imuxsock' (fd 3) from systemd. [v8.230.0]
2024-11-14T08:57:59+01:00 mariadb rsyslogd: [info] "Software='rsyslogd' swVersion='0.2102.0'" pid="7843" x-info="https://www.rsyslog.com/l/start"
2024-11-14T08:57:59+01:00 mariadb systemd[1]: Started System Logging Service.
2024-11-14T08:58:07+01:00 mariadb qemu-ga: info: guest-ping called
2024-11-14T08:58:19+01:00 mariadb qemu-ga: info: guest-ping called
2024-11-14T08:59:17.821536+01:00 srv-rrsyslog-debian qemu-ga: info: guest-ping calle
d
2024-11-14T08:59:28.345584+01:00 srv-rrsyslog-debian qemu-ga: info: guest-ping calle
d
2024-11-14T08:59:32.147130+01:00 srv-rrsyslog-debian systemd[1]: Started session-50.
scope: Session 50 of User sio.
2024-11-14T08:59:38.771244+01:00 srv-rrsyslog-debian qemu-ga: info: guest-ping calle
d
2024-11-14T08:59:55+01:00 mariadb systemd[1]: Stopping MariaDB 10.3.29 database ser
ver...
2024-11-14T08:59:59+01:00 mariadb systemd[1]: mariadb.service: Succeeded.
2024-11-14T08:59:59+01:00 mariadb systemd[1]: Stopped MariaDB 10.3.29 database serv
er.
2024-11-14T08:59:59+01:00 mariadb systemd[1]: mariadb.service: Consumed 17min 29.42
9s CPU time.
2024-11-14T08:59:59+01:00 mariadb systemd[1]: Starting MariaDB 10.3.29 database ser
ver...
2024-11-14T09:00:08+01:00 mariadb mysqld[7916]: 2024-11-14 9:00:00 0 [Note] /usr/s
bin/mysql [mysqld 10.3.29-MariaDB-0+deb10u1] starting as process 7916 ...
2024-11-14T09:00:08+01:00 mariadb systemd[1]: Started MariaDB 10.3.29 database serv
er.
2024-11-14T09:00:08+01:00 mariadb /etc/mysql/debian-start[7951]: Upgrading MySQL ta
bles if necessary.
2024-11-14T09:00:08+01:00 mariadb /etc/mysql/debian-start[7956]: /usr/bin/mysql_up
grade: the '--basedir' option is always ignored.
2024-11-14T09:00:08+01:00 mariadb /etc/mysql/debian-start[7956]: Looking for 'mysql'
as: /usr/bin/mysql.
2024-11-14T09:00:08+01:00 mariadb /etc/mysql/debian-start[7956]: Looking for 'mysql
check': /usr/bin/mysql-check.
2024-11-14T09:00:08+01:00 mariadb /etc/mysql/debian-start[7956]: This installation
of MySQL is already upgraded to 10.3.29-MariaDB, use --force if you still need to r
un mysql_upgrade.
2024-11-14T09:00:08+01:00 mariadb /etc/mysql/debian-start[7964]: Checking for insed
ure root accounts.
2024-11-14T09:00:08+01:00 mariadb /etc/mysql/debian-start[7964]: Triggering myisam-
recover for all MyISAM tables and aria-recover for all Aria tables.
2024-11-14T09:00:08+01:00 mariadb debian-start[7970]: WARNING: tempfile is deprecat
ed; consider using tmpfile instead.
```

Récupérer les logs du serveur Wordpress “SrvWebWordpress” :

Serveur Wordpress :

Modification du VirtualHost (fichier **/etc/apache2/sites-available/000-default.conf**) pour choisir quels logs envoyer (logs d'erreur et d'accès) :

```
root@srv-web-wp:~# vim /etc/apache2/sites-available/000-default.conf
```

```
ErrorLog "|/usr/bin/logger -t apachewordpress -p local6.info"
CustomLog "|/usr/bin/logger -t apachewordpress -p local6.info" combined
```

Modification du fichier **/etc/rsyslog.conf** pour envoyer les logs sur le serveur de logs :

On ajoute cette ligne à la fin du fichier et on redémarre le service :

```
local6.* @192.168.11.23
```

```
root@srv-web-wp:~# systemctl restart apache2
root@srv-web-wp:~# systemctl restart rsyslog
```

Serveur Rsyslog :

Modification du fichier **/etc/rsyslog.conf** pour recevoir les logs web sur le serveur Rsyslog dans le fichier **/var/log/wordpress.log** :

```
local6.*                                     -/var/log/wordpress.log
                                                _IMPROFICIENCY
```

On vérifie avec la commande **tail -f /var/log/wordpress.log** pour afficher les derniers logs du serveur Wordpress :

```
root@srv-rsyslog-debian:~# tail -f /var/log/wordpress.log
2024-11-15T16:00:00+01:00 srv-web-up apachewordpress: 192.168.11.250 - - [15/Nov/2024:15:59:59 +0100] "POST /wp-login.php HTTP/1.1" 200 2485 "http://192.168.11.5/wp-login.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:129.0) Gecko/20100101 Firefox/129.0"
2024-11-15T16:00:04+01:00 srv-web-up apachewordpress: 192.168.11.250 - - [15/Nov/2024:16:00:04 +0100] "POST /wp-login.php HTTP/1.1" 200 2486 "http://192.168.11.5/wp-login.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:129.0) Gecko/20100101 Firefox/129.0"
```

Récupération des logs SSH du serveur **srv-radius-debian** :

Installation de rsyslog :

```
root@srv-radius-debian:~# apt install rsyslog
```

Ajout de cette ligne dans le fichier **/etc/rsyslog.conf** pour récupérer les logs d'un service spécifique (en l'occurrence SSH) et les envoyer vers notre serveur rsyslog :

```
auth,authpriv.* @192.168.11.23:514
```

```
root@srv-radius-debian:~# service rsyslog restart
```

On vérifie dans le fichier **/var/log/auth.log** sur notre serveur rsyslog :

```
2024-11-14T10:18:23.974038+01:00 srv-rsyslog-debian sshd[10078]: Connection closed by 192.168.13.2 port 59080 [preauth]
2024-11-14T10:20:23.997878+01:00 srv-rsyslog-debian sshd[10082]: Connection closed by 192.168.13.2 port 39912 [preauth]
2024-11-14T10:22:23.020940+01:00 srv-rsyslog-debian sshd[10085]: Connection closed by 192.168.13.2 port 33682 [preauth]
2024-11-14T10:24:23.043888+01:00 srv-rsyslog-debian sshd[10087]: Connection closed by 192.168.13.2 port 58396 [preauth]
2024-11-14T10:25:30+01:00 srv-radius-debian sshd[15485]: Received signal 15; terminating.
2024-11-14T10:25:30+01:00 srv-radius-debian sshd[15548]: Server listening on 0.0.0.0 port 22.
2024-11-14T10:25:30+01:00 srv-radius-debian sshd[15548]: Server listening on :: port 22.
2024-11-14T10:25:54+01:00 srv-radius-debian sshd[15549]: Connection closed by 192.168.13.2 port 45002 [preauth]
2024-11-14T10:26:23.066393+01:00 srv-rsyslog-debian sshd[10103]: Connection closed by 192.168.13.2 port 53688 [preauth]
2024-11-14T10:26:10+01:00 srv-radius-debian sshd[15548]: Received signal 15; terminating.
2024-11-14T10:26:10+01:00 srv-radius-debian sshd[15557]: Server listening on 0.0.0.0 port 22.
2024-11-14T10:26:10+01:00 srv-radius-debian sshd[15557]: Server listening on :: port 22.
2024-11-14T10:26:48+01:00 srv-radius-debian sshd[15037]: Received disconnect from 192.168.13.250 port 51422:11: Bye Bye
```

Mise en place d'analyse de logs :

Script bash :

```
#!/bin/bash

# Vérification de l'existence d'un seul argument (nom d'utilisateur)
if [ $# -eq 0 -o $# -gt 1 ]; then
    echo "Erreur : problème d'argument"
    echo "Usage : $0 nom_utilisateur"
    exit 1
fi

# Nom de l'utilisateur passé en argument
login="$1"

# Vérification de l'existence du fichier de log
log_file="/var/log/auth.log"
if [ ! -e "$log_file" ]; then
    echo "Le fichier de log $log_file n'existe pas"
    exit 1
fi

# Calcul du nombre de connexions échouées pour l'utilisateur donné
nbr_errors=$(grep "Failed password for $login" "$log_file" | wc -l)

# Affichage du nombre de connexions échouées
if [ $nbr_errors -eq 0 ]; then
    echo "Aucune connexion échouée pour l'utilisateur $login."
else
    echo "Le nombre de connexions échouées pour l'utilisateur $login est de : $nbr_errors"

    # Affichage des adresses IP d'origine des connexions échouées
    echo "Adresses IP à l'origine des connexions échouées :"
    grep "Failed password for $login" "$log_file" | awk '{print $(NF-3)}' | sort | uniq -c | sort -nr
fi
```

Récupérer les logs du serveur Apache2 “SrvDokuwiki” :

```
root@srv-webdokuwiki:~# apt install rsyslog
```

3] Gestion des logs pour un équipement réseau

Examinez les logs de votre commutateur HP avec sa configuration actuelle (config radius fonctionnelle ou autre) :

```
|ProCurve Switch 2626(config)# show logging
|  Keys:  W=Warning   I=Information
|        M=Major     D=Debug
|---- Event Log listing: Events Since Boot ----
M 01/01/90 00:00:04 sys: 'System reboot due to Power Failure'
I 01/01/90 00:00:04 system: -----
I 01/01/90 00:00:04 system: System went down without saving crash information
I 01/01/90 00:00:14 lacp: Passive Dynamic LACP enabled on all ports
I 01/01/90 00:00:15 udpf: DHCP relay agent feature enabled
I 01/01/90 00:00:15 stack: Stack Protocol enabled
I 01/01/90 00:00:16 tftp: Enable succeeded
I 01/01/90 00:00:16 system: System Booted.
I 01/01/90 00:00:16 cdp: CDP enabled
I 01/01/90 00:00:16 lldp: LLDP - enabled
I 01/01/90 00:01:41 mgr: SME CONSOLE Session - MANAGER Mode
I 01/01/90 01:18:56 ports: port 5 is Blocked by LACP
I 01/01/90 01:18:58 ports: port 5 is now on-line
I 01/01/90 01:18:58 vlan: gestion virtual LAN enabled
I 01/01/90 01:18:59 ip: gestion: network enabled on 192.168.13.60
I 11/14/24 15:13:01 SNTP: updated time by 1100439642 seconds
|---- Bottom of Log : Events Listed = 16 ----
```

Configurez votre commutateur HP pour qu'il puisse envoyer ses logs à votre serveur Rsyslog :

On précise l'adresse IP du serveur Rsyslog dans la configuration du switch HP :

```
ProCurve Switch 2626(config)# logging facility local0
ProCurve Switch 2626(config)# logging 192.168.11.23
ProCurve Switch 2626(config)# show debug

  Debug Logging

  Destination:
    Logging --
      192.168.11.23
      Facility = local0

  Enabled debug types:
    event
```

Puis write-memory pour sauvegarder la configuration

On va ensuite dans le fichier **/etc/rsyslog.conf** puis on ajoute cette ligne pour recevoir les logs du switch HP :

```
local0.*          -/var/log/switch_hp.log
```

On vérifie ensuite dans le fichier généré à l'emplacement **/var/log/switch_hp.log** :

```
root@srv-rsyslog-debian:~# tail -f /var/log/switch_hp.log
2024-01-01T03:01:00+01:00 192.168.13.60 mgr: SME TELNET from 192.168.13.250 - MANAGER Mode
2024-01-01T03:09:11+01:00 192.168.13.60 mgr: SME TELNET from 192.168.13.250 - MANAGER Mode
2024-01-01T03:11:28+01:00 192.168.13.60 mgr: SME TELNET from 192.168.13.250 - MANAGER Mode
```

4] Serveur de temps

a) Pour le commutateur

Ajout de la passerelle :

```
ProCurve Switch 2626(config)# ip default-gateway 192.168.13.254
ProCurve Switch 2626(config)# write memory
```

```

ProCurve Switch 2626# show ip

Internet (IP) Service

IP Routing : Disabled

Default Gateway : 192.168.13.254
Default TTL    : 64
Arp Age        : 20

VLAN      | IP Config   IP Address     Subnet Mask
-----+-----+-----+-----+
DEFAULT_VLAN | DHCP/Bootp
VLAN50      | Disabled
VLAN99      | Disabled
gestion     | Manual       192.168.13.60  255.255.255.0
lan          | Disabled
dmz          | Disabled
internet    | Disabled
invites     | Disabled

```

```

ProCurve Switch 2626# ping 192.168.13.254
192.168.13.254 is alive, time = 1 ms
ProCurve Switch 2626# ping 77.158.181.88
77.158.181.88 is alive, time = 25 ms

```

Ajout du serveur de temps :

```

mathieu@C419-11:~$ ping ntp.unice.fr
PING ntp.unice.fr (134.59.1.5) 56(84) bytes of data.
64 bytes from ntp.unice.fr (134.59.1.5): icmp_seq=1 ttl=46 time=18.8 ms
64 bytes from ntp.unice.fr (134.59.1.5): icmp_seq=2 ttl=46 time=18.8 ms
64 bytes from ntp.unice.fr (134.59.1.5): icmp_seq=3 ttl=46 time=18.6 ms
64 bytes from ntp.unice.fr (134.59.1.5): icmp_seq=4 ttl=46 time=18.4 ms

ProCurve Switch 2626(config)# timesync sntp
ProCurve Switch 2626(config)# sntp unicast
ProCurve Switch 2626(config)# sntp server 134.59.1.5
ProCurve Switch 2626(config)# time timezone +60
ProCurve Switch 2626(config)# show sntp

SNTP Configuration

Time Sync Mode: Sntp
SNTP Mode : Unicast
Poll Interval (sec) [720] : 720

IP Address      Protocol Version
-----+-----+
134.59.1.5      3

```

Puis write-memory pour sauvegarder la configuration

Vérification que l'heure est exacte :

```
ProCurve Switch 2626(config)# time  
Thu Nov 14 16:12:30 2024
```

b) Pour les machines Linux

Fichier **/etc/systemd/timesyncd.conf**

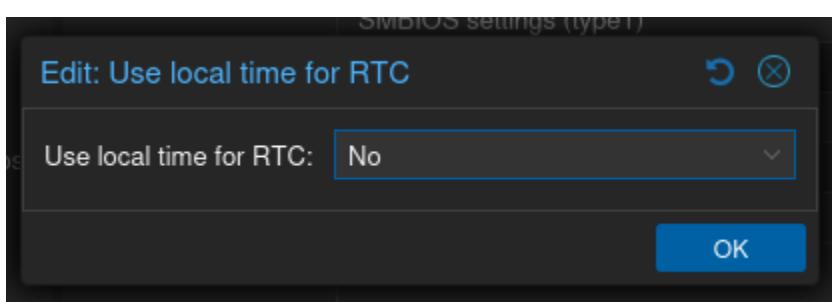
```
[Time]  
NTP=ntp.unice.fr
```

On vérifie que le serveur NTP est bien activé et que la date et l'heure sont corrects :

```
sio@srv-rsyslog-debian:~$ timedatectl status  
          Local time: jeu. 2024-11-14 15:17:45 CET  
              Universal time: jeu. 2024-11-14 14:17:45 UTC  
                  RTC time: jeu. 2024-11-14 14:17:45  
                 Time zone: Europe/Paris (CET, +0100)  
System clock synchronized: no  
          NTP service: active  
RTC in local TZ: no
```

c) Pour les machines Windows

On désactive la synchronisation automatique de la date sur Proxmox :



On tape les commandes nécessaires à la synchronisation du serveur Windows avec un serveur de temps :

```
PS C:\Users\Administrateur> w32tm /config /manualpeerlist:fr.pool.ntp.org /syncfromflags:manual
La commande s'est terminée correctement.
PS C:\Users\Administrateur> Restart-Service w32time
PS C:\Users\Administrateur>
```

On vérifie que la date est désormais synchronisée automatiquement :

Date et heure

*Certains de ces paramètres sont masqués ou gérés par votre organisation.

Date et heure du jour

16:07, jeudi 14 novembre 2024

Régler l'heure automatiquement



Définir le fuseau horaire automatiquement



Définir une date et une heure manuellement

[Modifier](#)

Synchroniser l'horloge

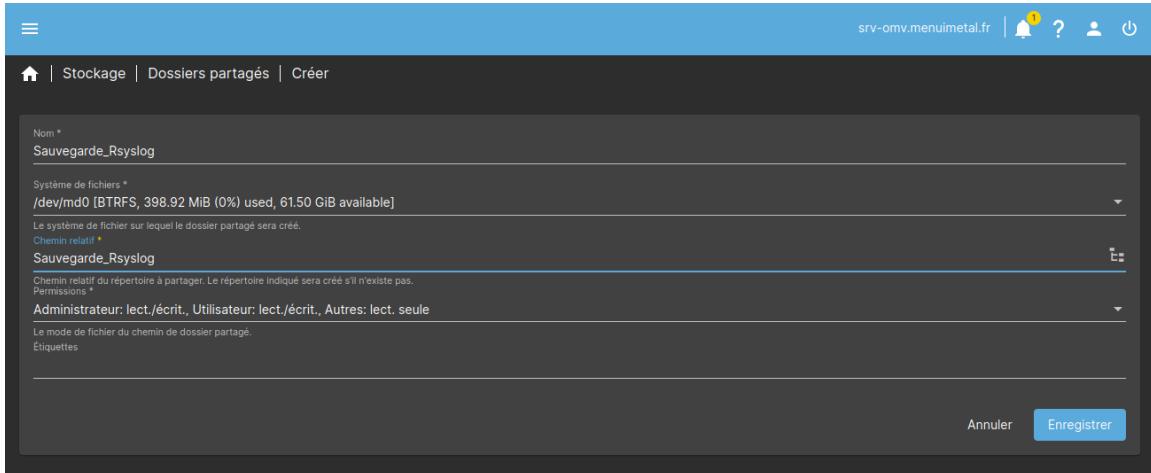
Dernière synchronisation de l'heure réussie : 14/11/2024 16:07:14

Serveur temporel : fr.pool.ntp.org

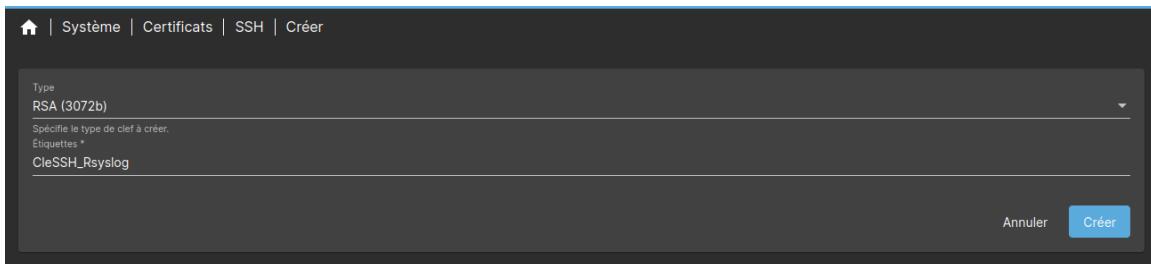
[Synchroniser maintenant](#)

5] Sauvegarde des logs

Création d'un dossier partagé sur OMV :



Création d'une clé SSH :



CleSSH_Rsyslog :

ssh-rsa

**AAAAB3NzaC1yc2EAAAQABAAQgQCkH9dg4hjMdqwjEes/lfBM
YYCi3JZ3bFu3QQWdHCeDi2Udz6+WKWiVltHEiO38w9Q5E0WrPXoOP
DP1AawV9ZpdKh1Lpgz85LzkieBozOqCqerpICcZaLGsSZjNXHkTtMus
qwZgEKSRe8pRc/hv+4E4CzEU+l+S8k9jxjTPQUUF74QrfL0NWf8+BlzT/
b8mNK82BIQZH8Bv6peC/hwuXit+AjU6L/Pyr5qDc9x+4XIFGBbExgLQk
KLiPSVwK+UxzzzJMP1Hv1vyHcohAMaT6jU/aw9jiILSmIwfaKgBLda3i9**

**WOIM057CUkl/fLb/gvggHchKiDjQ15SpI+5NdkLrEc6rk419QepOHjKtm
ma5RqKCR3IpNkcpAfKF0bzNVyxrmniyq3ypqNlp0tmwif3Pjq18Ulu+w
CYtCyxB5be43Si+epa/177h6NZ9cZxsLoVbMJImfo8geuXpItAuQ87UYV
wLY91fJbJ/TzgMIPZqm31xSqPH/z5nIX4WaqlHalgrU=
CleSSH_Rsyslog**

Notre clé est bien visible dans le répertoire **/etc/ssh** du serveur OMV :

```
263615 -rw----- 1 root root 2459 Nov 14 16:28 openmediavault-0a77c509-8afe-44da-ac20-7dbaaa2dd89e
263616 -rw-r--r--- 1 root root 568 Nov 14 16:28 openmediavault-0a77c509-8afe-44da-ac20-7dbaaa2dd89e.pub
```

```
root@srv-omv:/etc/ssh# cat openmediavault-0a77c509-8afe-44da-ac20-7dbaaa2dd89e.pub
ssh-rsa AAAAB3NzaC1yc2EAAAQAAgQCKHdg4hJMdqjEes/tfMYYYC1323bFu3QWdHceB12udz6+WKWivlTHE1038w905E0rrPxo0OPD1AawV9ZpdKh1Lpgz85LzkieBoz0qCqerpICcZaLGsSZjNXHKTtMsqwZg
EKSRspHC/hv+4E4czEU-I-Sek9jxjTPOUF740rlf0NWF8-B1ZT/b8mNK82BIOZ8Bv6pec/HwvXit+A)U6L/Pyr5qdC9x+4XFGB8ExglOkKL1PSWk+UxzzzJMP1Hv1yyHcohAMaT6jU/a9j1lSmIwfakgLda31woLM05
7CUkl/fLb/gvggHchKiDjQ15SpI+5NdkLrEc6rk419QepOHjKtmm5RqKCR3IpNkcpAfKf0bzNVyxrmniyq3ypqNlp0tmwif3Pjq18Ulu+wCYtCyxB5be43Si+epa/177h6NZ9cZxsLoVbMJImfo8geuXpItAuQ87UYVwLY91fJb
J/TzgMtpZqm31xSqPH/z5nIX4WaqlHalgrU= CleSSH Rsyslog
```

Configuration du service SSH de Rsyslog :

Installation de Rsync :

```
root@srv-rsyslog-debian:~# apt install rsync
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Paquets suggérés :
  python3-braceexpand
Les NOUVEAUX paquets suivants seront installés :
  rsync
0 mis à jour, 1 nouvellement installés, 0 à enlever et 39 non mis à jour.
Il est nécessaire de prendre 417 ko dans les archives.
Après cette opération, 795 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 rsync amd64 3.2.7-1 [417 kB]
417 ko réceptionnés en 0s (6 259 ko/s)
Sélection du paquet rsync précédemment désélectionné.
(Lecture de la base de données... 43663 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../rsync_3.2.7-1_amd64.deb ...
Dépaquetage de rsync (3.2.7-1) ...
Paramétrage de rsync (3.2.7-1) ...
rsync.service is a disabled or a static unit, not starting it.
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2) ...
root@srv-rsyslog-debian:~#
```

Fichier /etc/ssh/sshd_config

```
Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication no

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile    .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no
```

Redémarrage du service ssh :

```
root@srv-rsyslog-debian:~# systemctl restart sshd.service
root@srv-rsyslog-debian:~# systemctl restart ssh.service
```

Copie de la clé vers le serveur Rsyslog :

```
root@srv-omv:/etc/ssh# ssh-copy-id -i openmediavault-0a77c509-8afe-44da-ac20-7dbaaa2dd89e.pub root@192.168.11.23
```

```

/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "openmediavault-0a77c509-8afe-44da-ac20-7dbaaa2dd89e.pub"
The authenticity of host '192.168.11.23 (192.168.11.23)' can't be established.
ED25519 key fingerprint is SHA256:PpuM17hi1M6thT218VvcSwRGqf8v3JzL0jcJSEFl+XI.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
  ~/.ssh/known_hosts:4: [hashed name]
  ~/.ssh/known_hosts:10: [hashed name]
  ~/.ssh/known_hosts:11: [hashed name]
  ~/.ssh/known_hosts:12: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
root@192.168.11.23's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'root@192.168.11.23'"
and check to make sure that only the key(s) you wanted were added.

```

Vérification sur le serveur Rsyslog :

Fichier **/root/.ssh/authorized_keys**

```

root@srv-rsyslog-debian:~# cat /root/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQgQCkH9dg4hjMdqwjEes/lfBMYYCi3JZ3bFu3QQWdHCeDi2Udz6+WKKwiVltHEi038w9Q5E0WrPXo0PDP1AawV9ZpdKh1Lpgz85LzkieBoz0qCqerpICczaLgsSzjNXHKTtMusqwZgEKSRe8pRc/hv+4EczeU+i+S8k9jxjTPQUF740rfL0Nwf8+B1zT/b8mNK82BIQZH8Bv6peC/hwuXit+Aju6L/Pyr5qDc9x+4XIFGbbExglQKkLiPSVwK+UzzzzJMP1Hv1vyHcohAMaT6jU/aw9jiiLSmIwfaKgBLda3i9WolM057CUkl/fIb/gvvgHchKIdjQ15SpI+5NdklrEc6rk419Qep0HjKtmma5RqKCR3IpNkcpAfKf0bzNVyxrmmniyq3ypqNIp0tmwif3Pjq18UlU+wCYtCyxB5be43Si+epa/17h6NZ9cZxsLoVbMJImfo8geuxpltAuQ87UYVwLY91fJbJ/TzgMlpZqm3lxSqPH/z5nIX4WaqfHalgrU= CleSSH_Rsyslog

```

Changement de la configuration SSH du serveur Rsyslog pour permettre une connexion à distance avec une authentification par clé publique :

Fichier **/etc/ssh/sshd_config**

```
Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
```

Redémarrage du service ssh :

```
root@srv-rsyslog-debian:~# systemctl restart sshd.service
root@srv-rsyslog-debian:~# systemctl restart ssh.service
```

Création d'une nouvelle tâche de synchronisation :

Mode
Tirer

Serveur source
root@192.168.11.23:/var/log/

Serveur source distant (ex. [USER@]HOST:SRC, [USER@]HOST:SRC ou rsync://[USER@]HOST:PORT/SRC.
Destination shared folder
Sauvegarde_Rsyslog [on /dev/md0, Sauvegarde_Rsyslog/]

Authentification
Clé publique

SSH port
22

SSH certificate
CleSSH_Rsyslog

The SSH certificate used for authentication.

Date d'exécution
Toutes les 10 minutes

Minute *
10 Toutes les N minutes

Heure *
* Toutes les N heures

Jour du mois *
* Tous les N jours du mois

Mois *
*

Jour de semaine *
*

Envoi par mail de la sortie de la commande
Un mail contenant les traces de la commande (si disponible) est envoyé à l'administrateur.

Essai
Effectue un essai sans aucun changement

Supprime les messages de non-erreur

Mode archive

Traitement récursif dans les répertoires

Conserver les permissions
Définir les permissions de la destination à l'identique de celles de la source.

Conserver la date de modification
Transférer les heures de modification avec les fichiers et les mettre à jour sur le système distant.

Conserver le groupe
Définir le groupe pour le fichier de destination identique au fichier d'origine

Conserver le propriétaire
Définir le propriétaire pour le fichier de destination identique au fichier d'origine, mais seulement si la réception rsync est démarré en tant que super-utilisateur.

Compresser
Compresser les données des fichiers pendant le transfert.

Conserver les ACL
Mettre à jour les ACLs de la destination pour correspondre aux ACLs de la source.

Conserver les attributs étendus
Mettre à jour les attributs étendus de la destination pour correspondre aux attributs locaux.

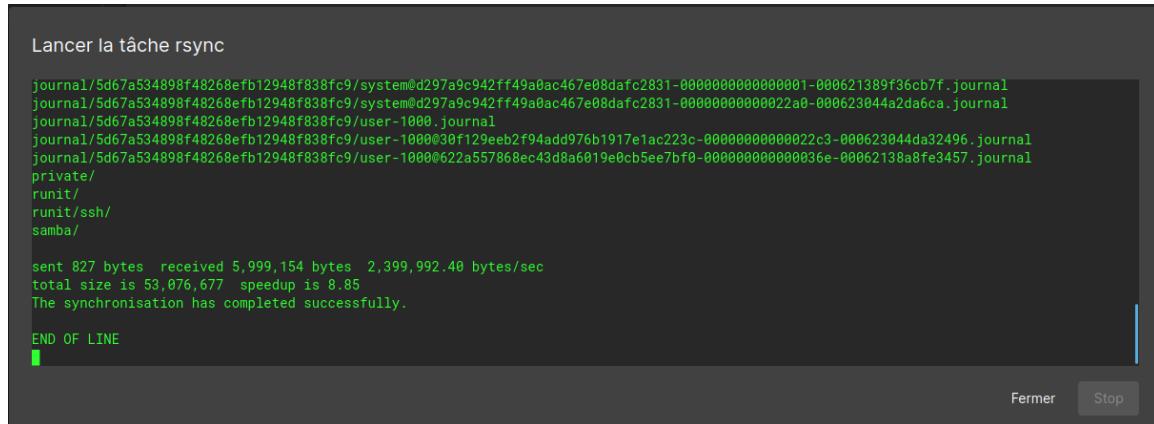
Conserve les fichiers partiellement transférés
Activer cette option pour conserver les fichiers partiellement transférés, sinon ils seront supprimés si le transfert est interrompu.

Supprimer
Supprimer sur la destination les fichiers qui n'existent pas sur la source.

Options supplémentaires

✓ Toutes les 10 minutes Remote root@192.168.11.23:/var/ log/ Sauvegarde_Rsyslog

On teste la tâche de sauvegarde :



Lancer la tâche rsync

```
journal/5d67a534898f48268efb12948f838fc9/system@d297a9c942ff49a0ac467e08dafc2831-0000000000000001-000621389f36cb7f.journal
journal/5d67a534898f48268efb12948f838fc9/system@d297a9c942ff49a0ac467e08dafc2831-00000000000022a0-000623044a2da6ca.journal
journal/5d67a534898f48268efb12948f838fc9/user-1000.journal
journal/5d67a534898f48268efb12948f838fc9/user-1000@30f129eeb2f94add976b1917e1ac223c-0000000000022c3-000623044da32496.journal
journal/5d67a534898f48268efb12948f838fc9/user-1000@622a557868ec43d8a6019e0cb5ee7bf0-00000000000036e-00062138a8fe3457.journal
private/
runit/
runit/ssh/
samba/

sent 827 bytes received 5,999,154 bytes 2,399,992.40 bytes/sec
total size is 53,076,677 speedup is 8.85
The synchronisation has completed successfully.

END OF LINE
```

Fermer Stop