Test de communication entre les serveurs avec la commande PING :

Ping depuis le serveur GRAYLOG vers le serveur Windows :

```
root@SRV-GRAYLOG:~# ping 172.16.0.105
PING 172.16.0.105 (172.16.0.105) 56(84) bytes of data.
64 bytes from 172.16.0.105: icmp_seq=1 ttl=64 time=0.345 ms
64 bytes from 172.16.0.105: icmp_seq=2 ttl=64 time=0.325 ms
64 bytes from 172.16.0.105: icmp_seq=3 ttl=64 time=0.354 ms
64 bytes from 172.16.0.105: icmp_seq=4 ttl=64 time=0.361 ms
^C
```

Ping depuis le serveur GRAYLOG vers le serveur Linux :

```
root@SRV-GRAYLOG:~# ping 172.16.0.104
PING 172.16.0.104 (172.16.0.104) 56(84) bytes of data.
64 bytes from 172.16.0.104: icmp_seq=1 ttl=128 time=0.381 ms
64 bytes from 172.16.0.104: icmp_seq=2 ttl=128 time=0.422 ms
64 bytes from 172.16.0.104: icmp_seq=3 ttl=128 time=0.372 ms
```

Ping depuis les 2 serveurs vers le serveur GRAYLOG :

```
Envoi d'une requête 'Ping'  172.16.0.101 avec 32 octets de données :
Réponse de 172.16.0.101 : octets=32 temps<1ms TTL=64
Réponse de 172.16.0.101 : octets=32 temps<1ms TTL=64
```

```
root@Ubuntu-Cli:~# ping 172.16.0.101
PING 172.16.0.101 (172.16.0.101) 56(84) bytes of data.
64 bytes from 172.16.0.101: icmp_seq=1 ttl=64 time=0.345 ms
64 bytes from 172.16.0.101: icmp_seq=2 ttl=64 time=0.215 ms
^C
```

Vérification de l'état des conteneurs du serveur GRAYLOG :

```
root@SRV-GRAYLOG:~# docker ps
CONTAINER ID   IMAGE                                                  COMMAND
    CREATED       STATUS                PORTS

                                                                                                  NAMES
cf7095154b64   graylog/graylog:4.3-jre11                              "tini -- /docker-ent…
"   5 days ago   Up 5 days (healthy)   0.0.0.0:5140->5140/tcp, :::5140->5140/tcp, 0.0.0.0:9
000->9000/tcp, 0.0.0.0:5140->5140/udp, :::9000->9000/tcp, :::5140->5140/udp, 0.0.0.0:12201-
>12201/tcp, 0.0.0.0:12201->12201/udp, :::12201->12201/tcp, :::12201->12201/udp   graylog-se
rver
e54653a729f7   mongo:4.4                                              "docker-entrypoint.s…
"   5 days ago   Up 5 days             27017/tcp

                                                                                                  graylog-mo
ngo
763e5c143d89   docker.elastic.co/elasticsearch/elasticsearch:7.10.2   "/tini -- /usr/local…
"   5 days ago   Up 5 days             9200/tcp, 9300/tcp

                                                                                                  graylog-el
asticsearch
root@SRV-GRAYLOG:~#
```

Vérification des statuts de NXLOG et RSYSLOG sur les 2 serveurs :

```
PS C:\Users\adminBA> Get-Service Nxlog

Status   Name               DisplayName
------   ----               -----------
Running  nxlog              Nxlog


PS C:\Users\adminBA>
```

```
root@Ubuntu-Cli:~# sudo systemctl status rsyslog
Warning: The unit file, source configuration file or drop-ins of rsyslog.service changed on dis
● rsyslog.service - System Logging Service
     Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-04-23 10:07:28 CEST; 2 days ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 24582 (rsyslogd)
      Tasks: 4 (limit: 2273)
     Memory: 2.4M (peak: 4.9M swap: 196.0K swap peak: 196.0K)
        CPU: 462ms
     CGroup: /system.slice/rsyslog.service
             └─24582 /usr/sbin/rsyslogd -n -iNONE

avril 23 10:07:28 Ubuntu-Cli systemd[1]: Starting rsyslog.service - System Logging Service...
avril 23 10:07:28 Ubuntu-Cli rsyslogd[24582]: imuxsock: Acquired UNIX socket '/run/systemd/jour
avril 23 10:07:28 Ubuntu-Cli rsyslogd[24582]: rsyslogd's groupid changed to 102
avril 23 10:07:28 Ubuntu-Cli systemd[1]: Started rsyslog.service - System Logging Service.
avril 23 10:07:28 Ubuntu-Cli rsyslogd[24582]: rsyslogd's userid changed to 102
avril 23 10:07:28 Ubuntu-Cli rsyslogd[24582]: [origin software="rsyslogd" swVersion="8.2312.0"
```

Test de remontée des logs depuis le serveur linux :

```
root@Ubuntu-Cli:~# logger "test log vers serveur graylog"
```

Remontée de logs du serveur Windows et Linux vers serveur GRAYLOG :

Exemple de log avec un utilisateur de l'AD sur le sevreur Windows :