Procédure de configurations des différents clients (Windows/Linux)

SOMMAIRE PROCEDURE

Prérequis

Pour démarrer la configuration des clients il faut au préalable savoir que :

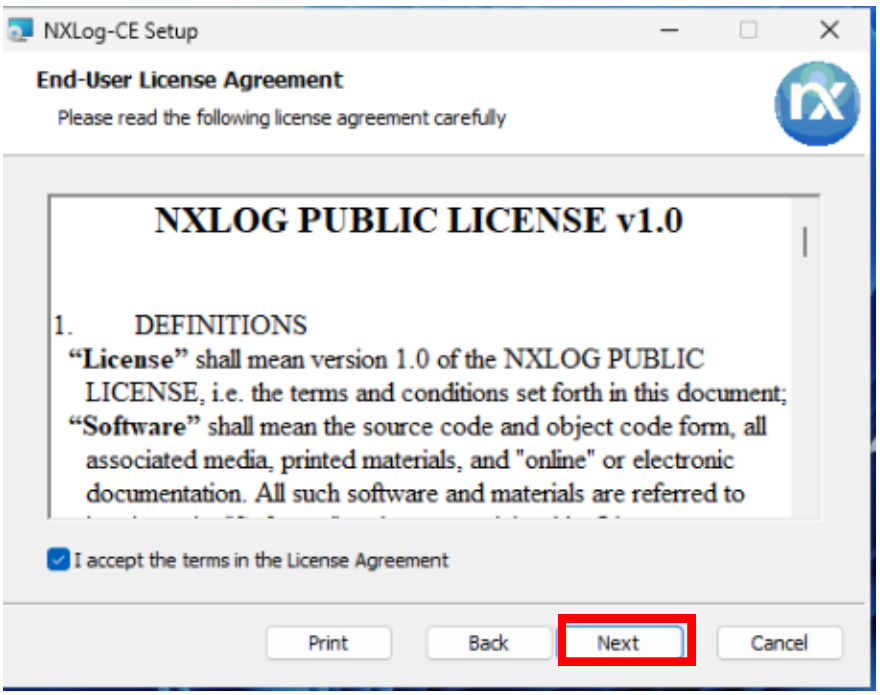
- Le remontée de logs sur Windows se fera via NXLOG, à télécharger et installer sur le poste.
- Pour Linux, il faut installer Rsyslog.
- Les équipements Cisco disposent nativement de fonctionnalités de journalisation configurables via leur interface d'administration.

I. Configuration de NXLOG sur Windows

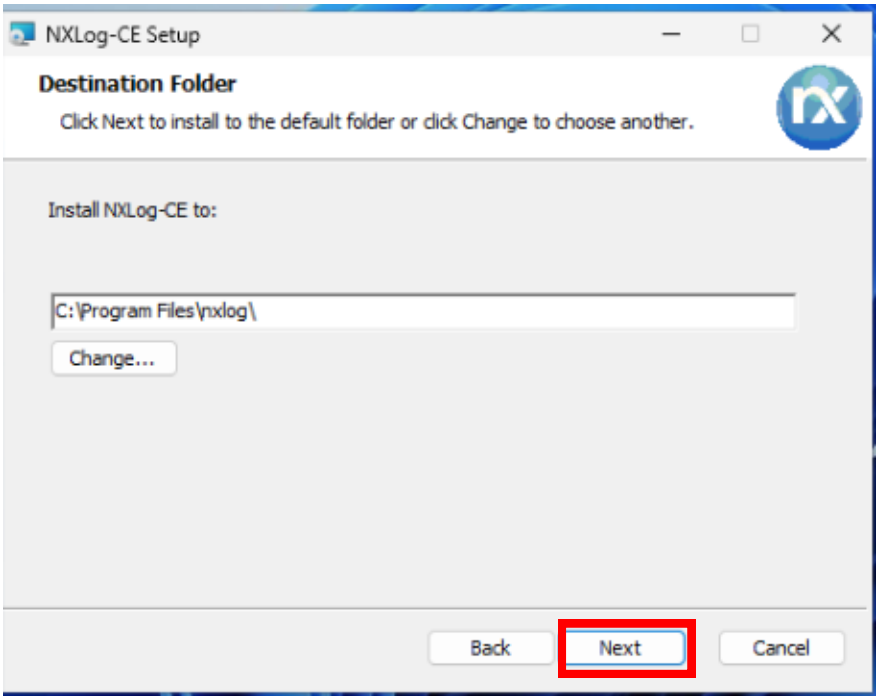
Sur Windows, se connecter en administrateur puis ouvrir une page web et aller sur le site https://nxlog.co/products/nxlog-community-edition, télécharger la version “Windows x86-64 nxlog-ce-3.2.2329.msi”

Etape 1. Installation du logiciel sur le poste

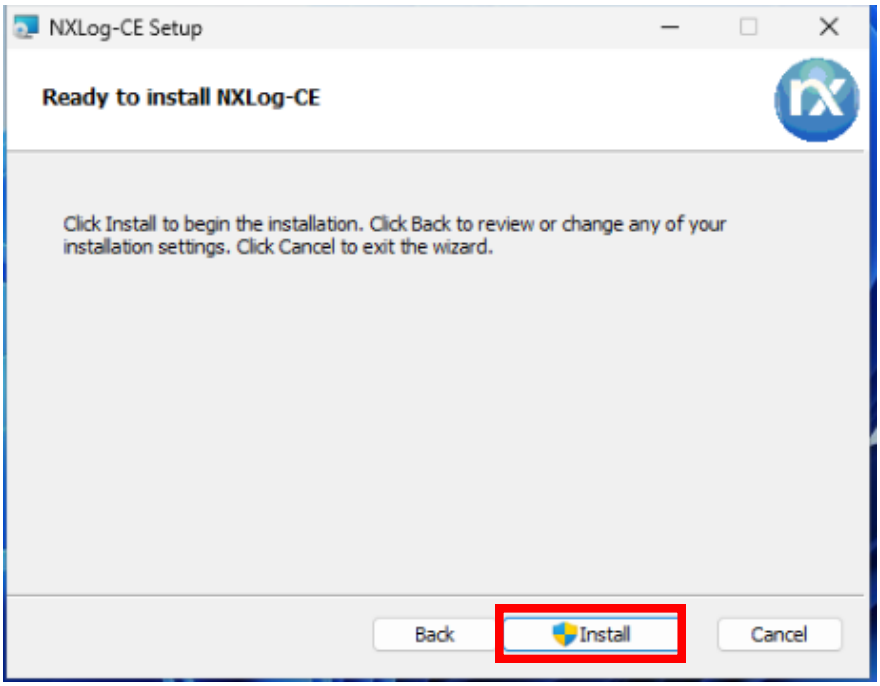
Lancer l’installation et acceptez le contrat de licence puis cliquer sur suivant.



Laisser le chemin par défaut C:\Program Files\nxlog\ puis cliquer sur suivant.

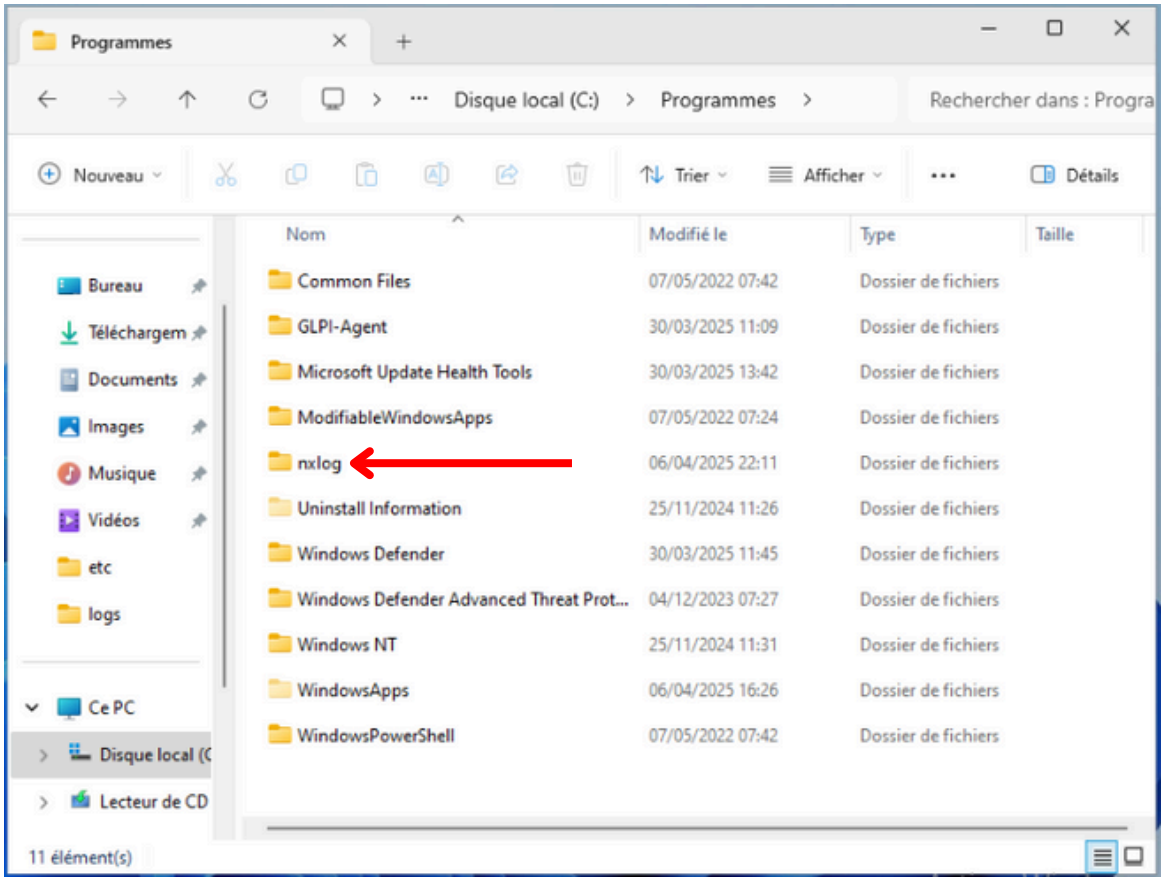


Cliquer sur Install pour finir l'installation.

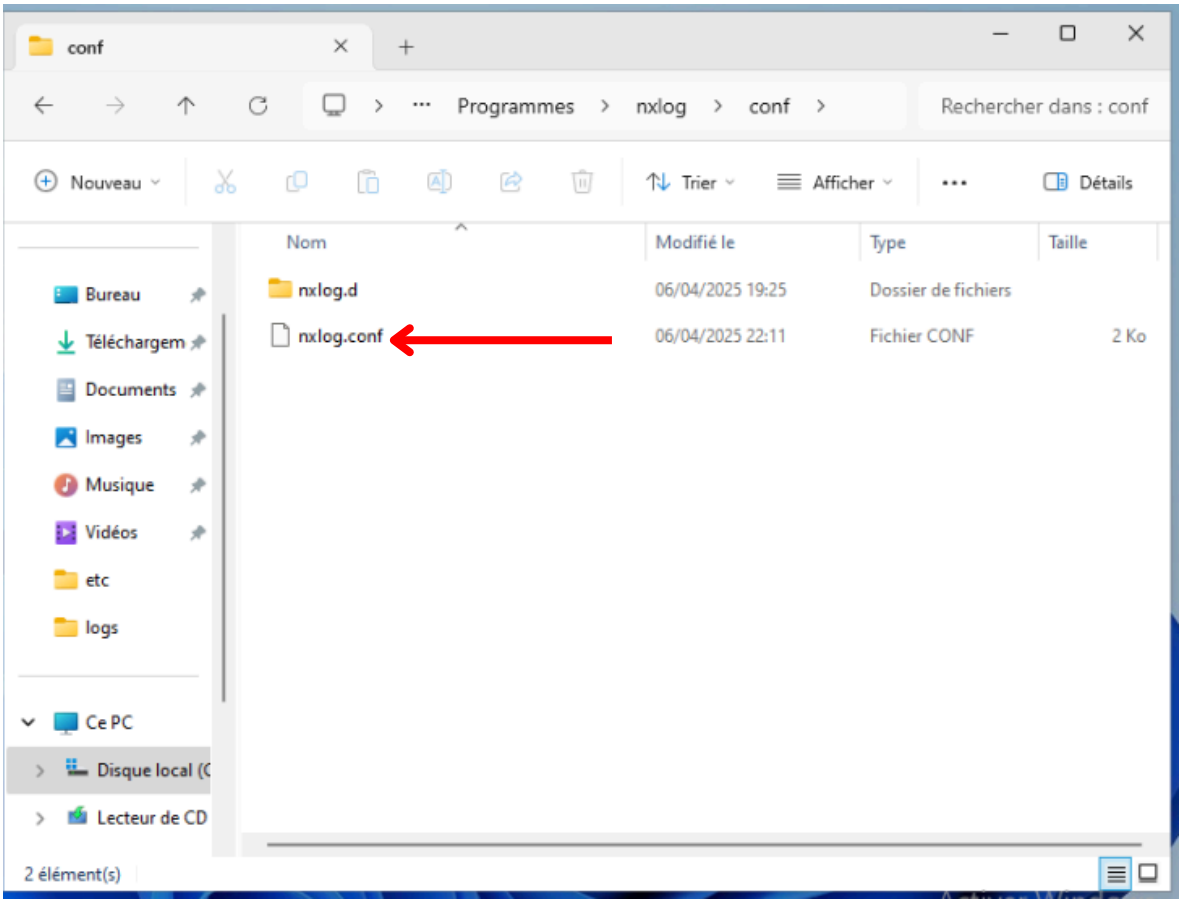


Etape 2 Configuration du fichier conf de NXLOG

Ouvrir à présent l'explorateur de fichiers et aller ouvrir le dossier nommé "nxlog"



Ensuite ouvrir le dossier “conf” et cliquer droit sur le fichier nxlog.conf et l’ouvrir avec un editeur de texte comme notepad, en administrateur.

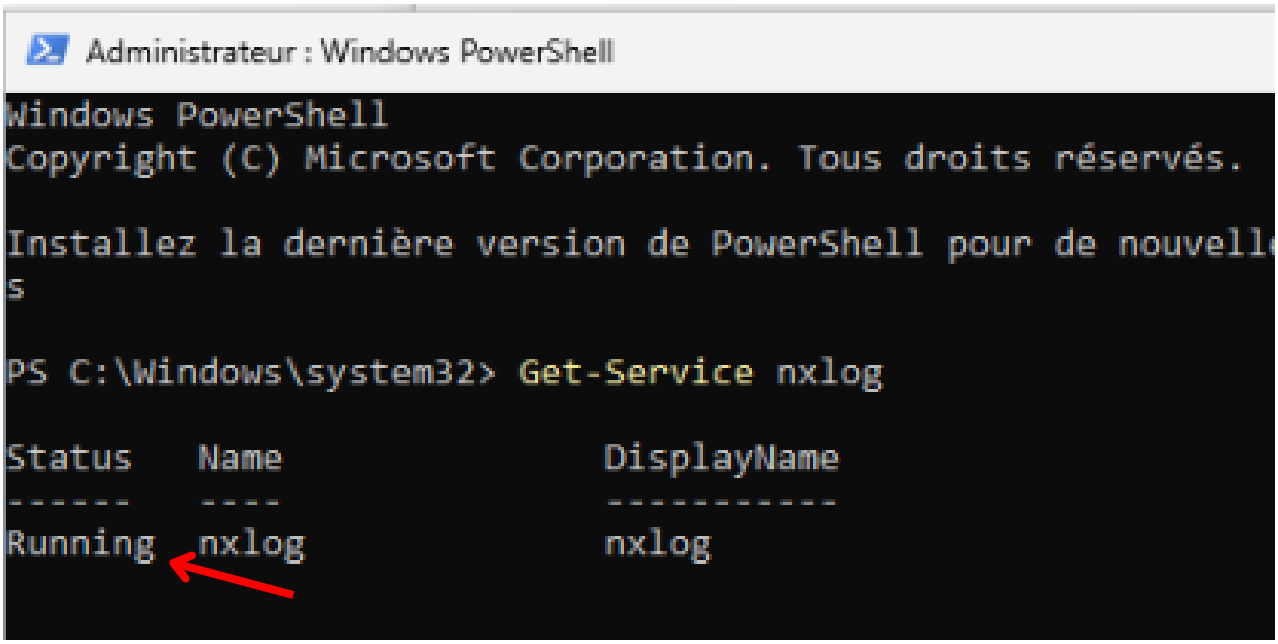


Supprimer le contenu présent et remplacer par celui sur la page suivante.
Ces modifications vont permettre de charger le module GELF, configurer l’input (entrée) pour pouvoir charger les logs Windows Event Logs.

La section “output” (sortie) va permettre d’envoyer les logs au format GELF via UDP à l’adresse IP et au port du serveur Graylog.
Enfin, la route connecte l’entrée à la sortie :

```
# Panic Soft
#NoFreeOnExit TRUE

define ROOT     C:\Program Files\nxlog
define CERTDIR  %ROOT%\cert
define CONFDIR  %ROOT%\conf\nxlog.d
define LOGDIR   %ROOT%\data

include %CONFDIR%\\*.conf
define LOGFILE  %LOGDIR%\nxlog.log
LogFile %LOGFILE%

Moduledir %ROOT%\modules
CacheDir  %ROOT%\data
Pidfile   %ROOT%\data\nxlog.pid
SpoolDir  %ROOT%\data

<Extension _syslog>
    Module      xm_syslog
</Extension>

<Extension _charconv>
    Module      xm_charconv
    AutodetectCharsets iso8859-2, utf-8, utf-16, utf-32
</Extension>

<Extension _exec>
    Module      xm_exec
</Extension>

<Extension _fileop>
    Module      xm_fileop

    # Check the size of our log file hourly, rotate if larger than 5MB
    <Schedule>
        Every   1 hour
        Exec    if (file_exists('%LOGFILE%') and \
                   (file_size('%LOGFILE%') >= 5M)) \
                    file_cycle('%LOGFILE%', 8);
    </Schedule>

    # Rotate our log file every week on Sunday at midnight
    <Schedule>
        When    @weekly
        Exec    if file_exists('%LOGFILE%') file_cycle('%LOGFILE%', 8);
    </Schedule>
</Extension>

<Extension _gelf>
    Module      xm_gelf
</Extension>

# Collecting event log
<Input in>
    Module      im_msvistalog
</Input>

# Converting events to GELF format and sending them out over UDP
<Output out>
    Module      om_udp
    Host        172.16.0.101
    Port        12201
    OutputType  GELF
</Output>

# Connect input 'in' to output 'out'
<Route 1>
    Path        in => out
</Route>
```

Ouvrir une fenêtre powershell en administrateur pour vérifier le statut de Nxlog, il doit être marqué en “running” :



II. Configuration de RSYSLOG sur Linux

Après avoir fait un apt update sur le systèmes Linux, installer simplement syslog.

```
root@Ubuntu-Cli:~# sudo apt install rsyslog -y
```

Une fois installé, regarder son statut pour s'assurer qu'il est bien en service :

```
root@Ubuntu-Cli:~# sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: >
     Active: active (running) since Wed 2025-04-23 08:01:21 CEST; 1h 42min ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 7212 (rsyslogd)
      Tasks: 4 (limit: 2273)
     Memory: 2.3M (peak: 5.2M)
        CPU: 98ms
     CGroup: /system.slice/rsyslog.service
             └─7212 /usr/sbin/rsyslogd -n -iNONE
```

Ensuite, créer le fichier de configuration pour envoyer les logs en UDP/TCP vers Graylog.

```
root@Ubuntu-Cli:~# sudo nano /etc/rsyslog.d/90-graylog.conf
```

Dans ce fichier, y inscrire les deux lignes suivantes, la première est pour l'UDP et la seconde pour le TCP (@ et @@), on y reseigner l'IP du sevreur, le port et le protocole Syslog.

```
  GNU nano 7.2                    /etc/rsyslog.d/90-graylog.conf
*.* @172.16.0.101:5140;RSYSLOG_SyslogProtocol23Format
*.* @@172.16.0.101:5140;RSYSLOG_SyslogProtocol23Format
```

Enfin, sauvegarder et quitter le fichier puis redémarrer le service.

```
root@Ubuntu-Cli:~# systemctl restart syslog
```