



1. Installer Node Exporter sur les machines Linux et Windows Exporter sur Windows.
2. SRV-Prometheus :

Ajouter les IP des serveurs dans le fichier de configuration (*par rapport à mon environnement virtuel*)

```
user@srv-Prometheus:~$ sudo nano /etc/prometheus/prometheus.yml
```

```
- job_name: "node_exporter"

# metrics_path defaults to '/metrics'
# scheme defaults to 'http'.

static_configs:
  - targets: ["localhost:9100"]
    labels:
      instance: 'SRV-Prometheus'

  - targets: ["192.168.17.5:9100"]
    labels:
      instance: 'SRV-Snort'

  - targets: ["192.168.17.15:9100"]
    labels:
      instance: 'SRV-Nessus'

  - targets: ["192.168.17.20:9100"]
    labels:
      instance: 'SRV-Fail2Ban'

  - targets: ["192.168.17.25:9100"]
    labels:
      instance: 'SRV-LAMP-GLPI-BackupManager'
```

```
user@srv-Prometheus:~$ sudo systemctl restart Prometheus
```

3. Accéder à l'interface graphique de Prometheus : <http://192.168.17.10:9090>

Status > Targets

Endpoint	State	Labels	Last Scrape	Scrape Duration	Error
http://localhost:9100/metrics	UP	instance="localhost:9100" job="node_exporter"	10.428s ago	26.649ms	
http://192.168.17.5:9100/metrics	UP	instance="192.168.17.5:9100" job="node_exporter"	8.714s ago	13.363ms	
http://192.168.17.10:9100/metrics	UP	instance="192.168.17.10:9100" job="node_exporter"	271.000ms ago	27.530ms	
http://192.168.17.15:9100/metrics	DOWN	instance="192.168.17.15:9100" job="node_exporter"	23.266s ago	10.0s	Get "http://192.168.17.15:9100/metrics": context deadline exceeded
http://192.168.17.20:9100/metrics	DOWN	instance="192.168.17.20:9100" job="node_exporter"	24.170s ago	10.0s	Get "http://192.168.17.20:9100/metrics": context deadline exceeded
http://192.168.17.25:9100/metrics	UP	instance="192.168.17.25:9100" job="node_exporter"	5.366s ago	12.332ms	

Endpoint	State	Labels	Last Scrape	Scrape Duration	Error
http://localhost:9090/metrics	UP	instance="localhost:9090" job="prometheus"	4.815s ago	3.323ms	

Remarque :

Si certaines machine sont en DOWN, activer le port 9100 :



user@srv-Prometheus:~\$ sudo ufw allow 9100

Endpoint	State	Labels	Last Scrape	Scrape Duration	Error
http://192.168.17.10:9100/metrics	UP	instance="192.168.17.10:9100" job="node_exporter"	3.297s ago	15.131ms	
http://192.168.17.15:9100/metrics	UP	instance="192.168.17.15:9100" job="node_exporter"	11.293s ago	16.286ms	
http://192.168.17.20:9100/metrics	UP	instance="192.168.17.20:9100" job="node_exporter"	12.198s ago	14.508ms	
http://192.168.17.25:9100/metrics	UP	instance="192.168.17.25:9100" job="node_exporter"	8.393s ago	12.730ms	
http://localhost:9100/metrics	UP	instance="localhost:9100" job="node_exporter"	13.455s ago	15.204ms	
http://192.168.17.5:9100/metrics	UP	instance="192.168.17.5:9100" job="node_exporter"	11.742s ago	20.433ms	

Endpoint	State	Labels	Last Scrape	Scrape Duration	Error
http://localhost:9090/metrics	UP	instance="localhost:9090" job="prometheus"	7.844s ago	3.203ms	

4. SRV-Fail2Ban

Cette machine là à 15Go de stockage. On va installer des fichiers de 1Go pour utiliser un maximum d'espace disque et voir si l'alerte est bien déclenché.

Au départ :

Machine virtuelle 204 (SRV-Fail2ban) sur le noeud turgot-sio

Résumé

SRV-Fail2ban (Durée de fonctionnement: 01:56:28)

Statut	running
Etat de la haute disponibilité	aucun
Nosud	turgot-sio
Utilisation processeur	0.80 % de 4 Processeur(s)
Utilisation mémoire	86.81% (1.74 Gio sur 2.00 Gio)
Taille du disque d'amorçage	15.00 Gio
IPs	Agent invité non configuré

Utilisation processeur

9
8
7
6
5
4
3
2
1
0



```
root@SRV-Fail2ban:~# df -h
Sys. de fichiers Taille Utilisé Dispo Utile% Monté sur
udev          951M      0  951M  0% /dev
tmpfs         197M  1,2M  196M  1% /run
/dev/sda1     14G  7,5G  5,7G  57% /
tmpfs         984M      0  984M  0% /dev/shm
tmpfs         5,0M      0  5,0M  0% /run/lock
tmpfs         197M  108K  197M  1% /run/user/1000
root@SRV-Fail2ban:~# dd if=/dev/zero of=~/test_file1 bs=M count=2000
2000+0 enregistrements lus
2000+0 enregistrements écrits
2097152000 octets (2,1 GB, 2,0 GiB) copiés, 2,22593 s, 942 MB/s
```

5. Remplir l'espace disque (pour tester)
- Vérifier l'utilisation de l'espace disque

Tu peux vérifier l'espace disque pour voir si tu as bien réduit l'espace libre à moins de 20 % en utilisant la commande suivante :

```
user@srv-fail2ban:~$ df -h
```

- Créer un fichier de grande taille (2Go)

```
user@srv-fail2ban:~$ dd if=/dev/zero of=~/test_file1 bs=1M count=2000
```

Une fois avoir créer plusieurs fichiers :



```
root@SRV-Fail2ban:~# df -h
Sys. de fichiers Taille Utilisé Dispo Utile% Monté sur
udev          951M      0  951M  0% /dev
tmpfs        197M  1,2M 196M  1% /run
/dev/sda1     14G    12G  1,7G 87% /
tmpfs        984M      0  984M  0% /dev/shm
tmpfs        5,0M      0  5,0M  0% /run/lock
tmpfs        197M   112K 197M  1% /run/user/1000
root@SRV-Fail2ban:~#
```

6. Vérifier si l'alerte se déclenche dans Prometheus

Une fois l'espace disque réduit sous les 20 %, vérifie que l'alerte est bien déclenchée dans **Prometheus**. Consulter les alertes actives dans Prometheus avec la commande suivante :

- Accéder à l'interface web de Prometheus (<http://192.168.17.10:9090>).
- Aller dans l'onglet **Alerts** pour voir les alertes actives. Si l'alerte est bien configurée, tu devrais la voir apparaître une fois que l'espace disque tombe sous les 20 %.

The screenshot shows the Prometheus Alert Rules interface. The alert rule is named 'LowDiskSpace' and is described as follows:

```
name: LowDiskSpace
expr: (node_filesystem_avail_bytes{fstype=~"ext4|xfs"} / node_filesystem_size_bytes{fstype=~"ext4|xfs"}) < 0.2
for: 5m
labels:
  severity: critical
annotations:
  description: L'espace disque est inférieur à 20% sur {{ $labels.instance }}
  summary: Espace disque faible sur {{ $labels.instance }}
```

The alert table shows the following data:

Labels	State	Active Since	Value
alarmname=LowDiskSpace,device=/dev/sda1,fstype=ext4,instance=SRV-Fail2Ban (192.168.17.20),job=node_exporter,mountpoint=/,severity=critical	PENDING	2025-04-06T22:16:15.551272403Z	0.12337509263938719

📌 Résumé de la situation dans Prometheus

- **⚠️ Alerte détectée** : LowDiskSpace est en état **PENDING**.
- **⌚ Depuis** : le 6 avril 2025 à 22:05 UTC.
- **📉 Valeur actuelle** : 0.123 → soit **12.3 % d'espace libre**.
- **💻 Instance concernée** : SRV-Fail2Ban (192.168.17.20).
- **💾 Périphérique** : /dev/sda1, monté sur /.

🔍 Que signifie le statut PENDING ?

L'état PENDING dans Prometheus signifie que :

- La condition de l'alerte est **vraie** maintenant, mais elle doit rester vraie **pendant 5 minutes** (comme spécifié dans `for: 5m`) **avant de passer à l'état FIRING**, qui déclenche Alertmanager.



👉 Donc actuellement, **l'alerte attend** de voir si le disque reste sous 20 % de libre **pendant 5 minutes complètes** avant de t'envoyer une alerte via Alertmanager.

7. Notification par mail

