FICHE DE RÉVISION — SUPERVISION (MONITORING)

TSSR — SNMP, Centreon, collecteur centengine et agent SNMP Windows

1. Définitions essentielles

UN MOT DÉFINIT LA SUPERVISION : LA PROACTIVITÉ.

Notion	Définition
Supervision	Surveiller notre infrastructure afin d'**éviter les pannes** et les autres dysfonctionnements qui pourraient arriver. C'est superviser **l'état de nos serveurs et de nos services**.
SNMP	**Simple Network Management Protocol** : le protocole utilisé par les systèmes de supervision. Pour mettre ça en place, il faut un **serveur de supervision**, et tous utilisent SNMP.
Centreon	La solution de supervision utilisée ici — c'est **une parmi tant d'autres**.

2. Le code couleur de la supervision

En supervision, il y a **trois codes couleurs**, comme le feu tricolore :

Couleur	Signification
🟢 **Vert**	**Todo bueno** — tout va bien
🟠 **Orange**	il y a des **dysfonctionnements** et **on doit agir**
🔴 **Rouge**	c'est la merde

3. Installation de Centreon — débloquer l'accès root à MariaDB

Incident rencontré à l'installation, et sa résolution en quatre temps.

3.1 Diagnostic initial

```
SQLSTATE[HY000] [1698] Access denied for user 'root'@'localhost'
```

3.2 Diagnostic réel

La commande suivante révèle la vraie configuration du compte :

```
SHOW CREATE USER 'root'@'localhost';
```

Résultat :

```
CREATE USER `root`@`localhost` IDENTIFIED VIA mysql_native_password
USING 'invalid' OR unix_socket
```

> *Le compte root n'a pas de mot de passe exploitable (USING 'invalid') : il ne s'authentifie que par socket Unix. D'où le refus quand Centreon tente une connexion classique avec mot de passe.*

3.3 Correction appliquée

Dans la session ouverte avec `sudo mysql -u root` :

```
SET PASSWORD FOR 'root'@'localhost' = PASSWORD('root');
FLUSH PRIVILEGES;
```

3.4 Vérification

```
mysql -u root -p'root' -h localhost
```

Connexion réussie (`Welcome to the MariaDB monitor`, connection id 7) : le mot de passe `root` fonctionne maintenant.

4. Licence et communauté SNMP

Élément	À retenir
Licence Centreon	gratuite, permet de surveiller **jusqu'à 100 appareils**
Communauté SNMP	`public` — c'est le **mot de passe** qu'on va utiliser côté SNMP

5. Superviser les composants à l'intérieur de nos machines

5.1 Redémarrer un collecteur Centreon

Le service à cibler sur un collecteur est centengine (Centreon Engine), PAS un nom générique « centreon ».

```
systemctl status centengine
systemctl restart centengine
systemctl status centengine
systemctl restart cbd
```

6. TP — Changer l'IP du serveur Centreon

6.1 Vérifier la passerelle actuelle avant de toucher à quoi que ce soit

```
ip route show
```

6.2 Lancer l'outil

```
nmtui
```

6.3 Dans nmtui

- **Edit a connection** → sélectionner **eth0** → Entrée
- Descendre à **IPv4 CONFIGURATION**, passer de `<Automatic>` à **Manual**
- Renseigner : **Addresses** (l'IP fixe en `/24`), **Gateway**, **DNS servers**
- Descendre jusqu'à **<OK>** → Entrée

6.4 Appliquer le changement

Retour au menu principal → **Back**, puis :

```
systemctl restart NetworkManager
```

Sans ce redémarrage de NetworkManager, RIEN n'est appliqué.

7. TP — Configurer l'agent SNMP sous Windows

7.1 Installer la fonctionnalité

```
Install-WindowsFeature -Name SNMP-Service -IncludeManagementTools
```

7.2 Configuration via services.msc

`services.msc` → **Service SNMP** → **Propriétés** :

Onglet	Ce qu'on y fait
Agent	**Contact** et **Emplacement** — purement **informatif**, remonté via les OID `sysContact` / `sysLocation`, **aucun impact** sur le fonctionnement ou la sécurité
Sécurité	**Communautés acceptées** → Ajouter → nom de communauté → droits **LECTURE SEULE**. Puis **Accepter les paquets SNMP de ces hôtes** → ajouter l'@IP du collecteur Centreon (**préférable** à « n'importe quel hôte » pour la sécurité)

7.3 Ouvrir le pare-feu Windows — UDP 161 en entrant

Le sens de la règle est INBOUND (entrant) : la requête SNMP part du collecteur Centreon vers le serveur Windows, donc pour ce serveur c'est du trafic qui ARRIVE.

En PowerShell :

```
New-NetFirewallRule -DisplayName "SNMP-In" -Direction Inbound `
                    -Protocol UDP -LocalPort 161 -Action Allow
```

Ou en interface graphique :

- Taper `wf.msc` dans le CMD
- Cliquer sur **Règles de trafic entrant**
- Cliquer sur **Nouvelle règle…**
- Type de règle → sélectionner **Port** → Suivant
- Sélectionner **UDP**, puis **Ports locaux spécifiques** → taper **161**
- Sélectionner **Autoriser la connexion** → Suivant
- Cocher les profils concernés (Domaine / Privé / Public selon le réseau) → Suivant
- Nommer la règle (ex. `SNMP-In`) → Terminer

7.4 Redémarrer le service pour appliquer

```
Restart-Service SNMP
Get-Service SNMP
```

8. Pièges et points à retenir pour l'ECF

Le mot-clé de la supervision, c'est la PROACTIVITÉ : on surveille pour ÉVITER la panne, pas pour la constater.

- Le protocole de la supervision, c'est **SNMP**.
- Le service du collecteur s'appelle `centengine`, pas « centreon ». Le broker, c'est `cbd`.
- Licence gratuite Centreon = **100 appareils** maximum.
- La **communauté SNMP** (`public` par défaut) joue le rôle de **mot de passe** — donc on la change en prod.
- Communauté toujours en **LECTURE SEULE**, et on restreint aux **hôtes autorisés** (l'@IP du collecteur), pas « n'importe quel hôte ».
- **SNMP = UDP 161**, règle **entrante** sur le serveur supervisé.

- Onglet **Agent** (Contact / Emplacement) = purement informatif, remonté par les OID `sysContact` / `sysLocation`.
- Avant de changer une IP sous Linux : `ip route show` **d'abord**, pour connaître la passerelle actuelle.
- Après `nmtui`, il faut `systemctl restart NetworkManager` — sinon rien n'est appliqué.