LES DIFFERENTS TYPES DE TESTS

1. Tests fonctionnels

Ces tests, c’est pour vérifier que tout marche , selon ce qu’on a prévu.

- **Gestion des alertes et notifications** : On regarde si les alertes se déclenchent bien quand il faut, par exemple si un seuil est dépassé ou si quelque chose cloche, comme une surcharge dans le réseau.
- **Analyse des performances réseau** : On s’assure que les tableaux de bord affichent les bonnes infos sur les performances – latence, débit, tout ça – sans raconter n’importe quoi.
- **Surveillance en temps réel** : Là, on vérifie que les données qu’on voit à l’écran sont bien à jour, sans aucun décalage.
- **Stockage et analyse des logs** : On teste si les logs sont bien enregistrés quelque part et si leur analyse permet de repérer les anomalies sans problème.
- **Génération de rapports** : On regarde si les rapports qu’on sort sont justes et utiles, avec les bonnes données dedans.
- **Gestion centralisée des configurations** : On s’assure que quand on change une config, ça se répercute bien sur tous les appareils concernés.
- **Authentification avancée** : On teste les systèmes d’authentification (comme OAuth2 ou LDAP) pour voir s’ils tiennent la route.
- **Gestion des accès** : On vérifie que seuls ceux qui ont le droit peuvent accéder à certaines fonctions – par exemple, un simple utilisateur réseau ne peut pas aller trifouiller les configs.

2. Tests de performance

Comme le système doit surveiller en temps réel et analyser les performances, on veut être sûrs qu’il tient le coup même quand ça chauffe.

- On simule plein d’appareils connectés pour voir si la surveillance en temps réel suit sans ramer.
- On teste la génération de rapports avec un gros tas de données, pour vérifier que ça reste fluide.
- On mesure combien de temps il faut pour afficher les tableaux de bord ou détecter une anomalie.

3. Tests de sécurité

Ici, on se concentre sur la catégorie "Sécurité et authentification" pour protéger les accès et repérer les trucs louches.

- **Test d’authentification** : On essaie de se connecter avec de mauvais identifiants pour voir si le système dit bien "non".
- **Test de gestion des rôles** : On s’assure qu’un utilisateur avec peu de droits (genre un utilisateur réseau) ne peut pas jouer les admins.
- **Test d’injection** : On simule des attaques, comme des injections SQL ou XSS, pour vérifier que le système est blindé.

- **Surveillance des comportements suspects** : On fait semblant de faire des trucs bizarres (genre plein de tentatives de connexion ou un trafic chelou) pour voir si le système capte et nous alerte.

4. Tests d'intégration

Le système travaille avec plein de trucs différents (logs, configs, authentification), donc on teste si tout s'emboîte bien.

- On vérifie que les changements de config se synchronisent correctement avec tous les appareils du réseau.
- On teste l'intégration avec des systèmes d'authentification externes, comme OAuth2 ou LDAP.
- On s'assure que les logs arrivent bien des appareils au stockage et à l'analyse sans se perdre en route.

5. Tests de charge et de stress

On pousse le système dans ses retranchements pour voir s'il tient le choc.

- On simule une grosse surcharge réseau (un pic de trafic, par exemple) pour vérifier qu'il reste stable.
- On teste ce qui se passe si un composant plante, comme un serveur de logs qui tombe en rade.

6. Tests d'interface utilisateur (UI)

On regarde si l'interface est agréable à utiliser et si tout s'affiche bien.

- On vérifie que les tableaux de bord sont clairs, intuitifs et montrent les bonnes données.
- On teste la navigation entre les sections (supervision, rapports, configs) pour voir si c'est fluide.
- On s'assure que les messages d'erreur ou les alertes sont compréhensibles pour l'utilisateur.

7. Tests de compatibilité

On veut être sûrs que le système marche partout.

- On le teste sur différents navigateurs ou interfaces (si c'est une appli web) pour voir s'il fonctionne bien.
- On vérifie qu'il est compatible avec tout type d'appareils réseau : routeurs, commutateurs, etc.

8. Tests de régression

Après chaque mise à jour ou changement, on refait des tests pour être sûrs qu'on n'a rien cassé.

- On relance les tests sur des trucs comme la génération de rapports ou la surveillance en temps réel pour voir si tout fonctionne toujours nickel.

9. Tests d’acceptation utilisateur (UAT)

Là, on met les vrais utilisateurs dans le coup – admins réseau, ingénieurs, utilisateurs classiques – pour tester en conditions réelles.

- On vérifie si le système répond à leurs attentes : est-ce qu’il est facile de sortir un rapport ? Est-ce que les alertes sont pertinentes ?