Superviser la disponibilité de l'infrastructure et en présenter les résultats

Table des matières

Module 1 : Introduction à la supervision de l'infrastructure 2
1.1. Définition et importance de la supervision 2
1.2. Types de supervision 2
1.3. Objectifs de la supervision 3
1.4. Processus de supervision 4
1.5. Outils de supervision 4
Module 2 : La mise à niveau – Superviser la disponibilité de l'infrastructure 5
2.1. Outils de supervision pour la disponibilité 5
2.2. Architecture d'une solution de supervision 5
2.3. Définir les éléments de l'infrastructure à superviser 6
2.4. Définir des seuils d'alerte 7
2.5. Suivi et gestion des alertes 7
Module 3 : La mise à niveau – Superviser la disponibilité de l'infrastructure : Centreon 7
3.1. Introduction à Centreon 8
3.2. Installation de Centreon 8
3.3. Configuration de Centreon pour surveiller la disponibilité 9
3.4. Définir des seuils d'alerte 9
3.5. Gestion des alertes et notifications 10
3.6. Visualisation des données avec Centreon 10
Module 4 : La mise en œuvre et l'exploitation d'une solution de supervision 11
4.1. Introduction à la mise en œuvre d'une solution de supervision 11
4.2. Planification de la mise en œuvre de la supervision 11
4.3. Installation et configuration de la solution de supervision 12
4.4. Exploitation et gestion de la solution de supervision 13
4.5. Reporting et analyse des performances 13
Module 5 : La mise en œuvre d'une solution de centralisation des journaux d'événements 14
5.1. Introduction à la centralisation des journaux d'événements 14
5.2. Choisir une solution de centralisation des journaux d'événements 15
5.3. Mise en œuvre de la centralisation des journaux d'événements 15
5.4. Analyse des journaux d'événements centralisés 16
5.5. Gestion des alertes et notifications 16
Module 6 : L'analyse des journaux d'événements 17
6.1. Introduction à l'analyse des journaux d'événements 17
6.2. Outils et techniques d'analyse des journaux d'événements 18
6.3. Processus d'analyse des journaux d'événements 18
6.4. Utilisation des résultats de l'analyse des journaux d'événements 20

Module 1 : Introduction à la supervision de l'infrastructure

Objectif du module :
Ce module vise à introduire les concepts fondamentaux de la supervision de l'infrastructure informatique. Il est essentiel pour comprendre les enjeux et les mécanismes de la surveillance des systèmes informatiques, en particulier pour assurer leur disponibilité, leur sécurité, et leur performance.

1.1. Définition et importance de la supervision

1.1.1. Qu'est-ce que la supervision de l'infrastructure ?

La supervision de l'infrastructure consiste à surveiller et à gérer les composants de l'infrastructure informatique (serveurs, réseaux, applications, bases de données, etc.) afin de garantir leur bon fonctionnement et leur disponibilité. Cela inclut la détection des pannes, la gestion des performances, ainsi que la prévention et la résolution des incidents.

Elle s'étend à la surveillance de :

- **Serveurs physiques et virtuels** : CPU, mémoire, disque, et services qui s'exécutent sur ces serveurs.
- **Réseaux** : Connectivité des équipements (switches, routeurs, pare-feu, etc.).
- **Applications** : Fonctionnement des logiciels, de leurs bases de données et de leurs services.
- **Services Web** : Vérification de l'accessibilité des pages, des bases de données, etc.

1.1.2. Pourquoi la supervision est-elle importante ?

Une infrastructure non supervisée peut entraîner des pannes imprévues, des baisses de performance, ou même des violations de sécurité. Voici les principaux enjeux de la supervision :

- **Disponibilité** : Assurer que les services sont toujours accessibles et fonctionnels.
- **Performance** : Optimiser les ressources en identifiant les goulets d'étranglement ou les problèmes de capacité.
- **Sécurité** : Détecter des comportements anormaux ou des tentatives d'intrusion.
- **Prévention des pannes** : Anticiper et résoudre les problèmes avant qu'ils ne causent des interruptions de service.
- **Conformité** : Certaines entreprises doivent se conformer à des normes (ex : RGPD) et garder une trace des incidents.

1.2. Types de supervision

La supervision se divise en plusieurs catégories selon l'objectif de surveillance. Voici les principales :

1.2.1. Supervision de la disponibilité

Cela consiste à s'assurer que tous les composants essentiels de l'infrastructure sont accessibles et fonctionnent correctement. Par exemple, on surveille :

- **Les serveurs** pour vérifier s'ils sont allumés et répondent.
- **Les services** pour s'assurer qu'ils ne sont pas en panne (ex : base de données, serveur web, etc.).
- **Les équipements réseau** pour confirmer qu'ils ne sont pas déconnectés ou en surcharge.

Exemple :
Une alerte sera déclenchée si un serveur tombe en panne ou si une application devient inaccessible.

1.2.2. Supervision des performances

Elle vise à mesurer et analyser l'utilisation des ressources telles que :

- **Le CPU** : Utilisation excessive peut entraîner une lenteur des systèmes.
- **La mémoire RAM** : Vérifier qu'elle n'est pas saturée.
- **L'espace disque** : S'assurer que les serveurs ne manquent pas d'espace pour éviter des arrêts de services.
- **Le réseau** : Mesurer la bande passante et vérifier l'absence de congestion.

Exemple :
L'outil de supervision peut générer une alerte si la mémoire disponible sur un serveur tombe sous un seuil critique.

1.2.3. Supervision des événements (logs)

Les journaux d'événements (logs) sont des traces générées par les systèmes, applications et équipements réseau. La supervision des logs permet de :

- **Détecter les anomalies** (erreurs d'application, tentatives d'accès suspectes, etc.),
- **Analyser les incidents** après qu'ils se soient produits,
- **Mettre en place une action corrective** en fonction des anomalies détectées.

Exemple :
La surveillance des logs permet de repérer une tentative de connexion échouée répétée, signalant une tentative d'intrusion.

1.3. Objectifs de la supervision

Les objectifs principaux de la supervision sont les suivants :

1.3.1. Détection précoce des problèmes

La supervision permet d'identifier rapidement tout dysfonctionnement (panne, erreur, perte de performance) avant qu'il n'affecte les utilisateurs ou qu'il ne cause des interruptions majeures.

1.3.2. Optimisation de l'utilisation des ressources

La supervision des ressources (CPU, mémoire, stockage) permet d'identifier les composants sous-utilisés ou surchargés et de prendre des décisions d'optimisation.

1.3.3. Réduction des coûts opérationnels

En intervenant rapidement sur les problèmes de performance, les administrateurs peuvent éviter des réparations coûteuses ou des pertes de revenus dues à des pannes prolongées.

1.3.4. Gestion proactive de la capacité

En surveillant en temps réel la consommation des ressources, il est possible de prévoir les besoins futurs en termes de stockage, de puissance CPU ou de bande passante, et ainsi de mieux planifier les mises à niveau de l'infrastructure.

1.3.5. Prévention des incidents de sécurité

Les solutions de supervision permettent également de détecter des comportements anormaux, tels que des tentatives de connexion infructueuses ou des activités malveillantes, et d'alerter les administrateurs avant que des violations de sécurité ne surviennent.

1.4. Processus de supervision

La supervision de l'infrastructure suit généralement un processus en plusieurs étapes :

1. **Collecte des données** :
    - Des agents sont installés sur les serveurs pour collecter des métriques (utilisation CPU, mémoire, stockage, etc.).
    - Des outils de surveillance réseau collectent des informations sur l'état des équipements réseaux (commutateurs, routeurs).
2. **Analyse des données** :
    - Les données collectées sont analysées en temps réel pour détecter des anomalies ou des comportements inhabituels.
    - Ces outils comparent les données avec des seuils prédéfinis pour déterminer s'il y a une alerte à générer.
3. **Envoi des alertes** :
    - Lorsqu'une anomalie est détectée, des alertes sont envoyées par email, SMS, ou via des systèmes de notification.
    - Les alertes peuvent être classées en fonction de leur gravité (avertissement, critique, etc.).
4. **Réaction et résolution** :
    - Une fois qu'une alerte est reçue, les administrateurs analysent les logs, les métriques et prennent des mesures correctives (redémarrage d'un service, augmentation de la capacité, etc.).
5. **Rapports et documentation** :
    - Des rapports sont générés pour analyser les tendances de performance et la disponibilité sur une période donnée. Cela permet une meilleure planification des ressources et de la capacité.

1.5. Outils de supervision

Les outils de supervision sont essentiels pour mettre en œuvre une surveillance efficace. Quelques-uns des outils les plus populaires sont :

1.5.1. Centreon

Centreon est un outil de supervision open-source qui permet de surveiller l'infrastructure IT en temps réel. Il fournit des tableaux de bord, des alertes et des rapports sur les performances et la disponibilité des systèmes.

1.5.2. Nagios

Nagios est un autre outil de surveillance populaire, permettant de suivre les serveurs, les réseaux, et les applications. Il offre une grande flexibilité avec des plugins pour surveiller une grande variété d'équipements.

1.5.3. Zabbix

Zabbix est une solution de surveillance d'infrastructure qui permet de suivre la disponibilité, les performances et les journaux d'événements. Il dispose également de puissantes capacités de visualisation et d'alerte.

1.5.4. Prometheus et Grafana

Prometheus est un système de monitoring open-source avec une forte capacité de collecte de métriques, souvent utilisé avec Grafana pour la visualisation de données.

1.5.5. ELK Stack (Elasticsearch, Logstash, Kibana)

L'ELK Stack est une suite d'outils pour collecter, analyser et visualiser les logs. C'est une solution puissante pour la supervision des journaux d'événements.

Module 2 : La mise à niveau – Superviser la disponibilité de l'infrastructure

Objectif du module :
Ce module est conçu pour permettre aux participants de comprendre et d'appliquer les concepts et les outils nécessaires pour superviser efficacement la disponibilité de l'infrastructure informatique. L'objectif principal est de garantir que tous les composants clés de l'infrastructure, y compris les serveurs, le réseau et les services, sont disponibles et fonctionnent de manière optimale.

2.1. Outils de supervision pour la disponibilité

2.1.1. Pourquoi utiliser des outils de supervision ?

Les outils de supervision permettent de collecter, d'analyser et de visualiser des données provenant des différentes parties de l'infrastructure informatique. La supervision de la disponibilité, en particulier, repose sur la surveillance en temps réel de la disponibilité des composants critiques du système (serveurs, réseaux, applications, etc.). Ces outils sont essentiels pour :

- **Détecter les pannes** : L'outil avertit immédiatement l'administrateur en cas de dysfonctionnement.
- **Garantir la continuité de service** : En détectant rapidement les problèmes, on peut prendre des mesures préventives avant qu'ils n'affectent les utilisateurs.
- **Optimiser la gestion des ressources** : En assurant un suivi constant de la disponibilité, les ressources peuvent être mieux allouées pour éviter les goulots d'étranglement.

2.1.2. Présentation des principaux outils de supervision

- **Centreon** : Un des outils de supervision les plus utilisés pour surveiller la disponibilité des composants IT. Centreon est une solution open-source qui permet de gérer efficacement les hôtes (serveurs, applications, équipements réseaux) et les services.
- **Nagios** : Outil de monitoring très populaire, il permet de surveiller la disponibilité, la performance et la sécurité des composants d'une infrastructure.
- **Zabbix** : Une autre solution open-source qui offre des fonctionnalités avancées pour la surveillance des serveurs et des applications. Zabbix permet également de superviser la disponibilité en temps réel.
- **Prometheus & Grafana** : Bien que Prometheus soit plus orienté vers la collecte de métriques, il peut être utilisé pour superviser la disponibilité via des règles d'alerte. Grafana permet une visualisation puissante des données collectées.

Ces outils permettent généralement de surveiller les composants via des **agents** installés sur les serveurs et des **protocoles standards** comme SNMP (Simple Network Management Protocol) ou ICMP (Internet Control Message Protocol) pour vérifier la disponibilité des hôtes.

2.2. Architecture d'une solution de supervision

Une solution de supervision de la disponibilité est constituée de plusieurs éléments. Voici les composants de base :

2.2.1. Composants d'une architecture de supervision

1. **Les agents de surveillance** :
    - Des petits programmes installés sur les serveurs ou les dispositifs réseau pour collecter des informations sur les performances et la disponibilité.
    - Ils envoient ces données vers le serveur de supervision central.
    - Ces agents peuvent utiliser des protocoles comme SNMP ou des agents dédiés comme ceux utilisés par Centreon et Zabbix.

2. **Le serveur de supervision central** :
    - Ce serveur reçoit les données collectées par les agents ou via des sondes réseau.
    - Il analyse et traite ces données en temps réel pour identifier les problèmes de disponibilité (pannes, déconnexions, etc.).
    - Il permet également de configurer des seuils de performance et d'alerte.
3. **La base de données** :
    - Utilisée pour stocker les historiques de disponibilité et les logs d'événements.
    - Ces données peuvent être utilisées pour analyser les tendances et prévoir les besoins en ressources.
4. **L'interface web** :
    - Elle permet aux administrateurs de consulter les données en temps réel, de visualiser les rapports et de gérer les alertes.
    - Les interfaces sont généralement interactives et offrent des tableaux de bord personnalisables.
5. **Les alertes et notifications** :
    - Des notifications peuvent être envoyées par email, SMS ou via des outils de messagerie pour informer les administrateurs d'une panne ou d'une anomalie.

2.2.2. Exemple d'architecture d'une solution de supervision

Imaginons un environnement d'entreprise avec plusieurs serveurs, des services critiques (comme une base de données), et des équipements réseau :

- **Serveurs de supervision** installent Centreon sur une machine dédiée.
- **Agents Centreon** sont déployés sur tous les serveurs (web, base de données, applications).
- **Réseau** : Des sondes ICMP ou SNMP sont utilisées pour surveiller l'état des équipements réseau (commutateurs, routeurs).
- **Interface web** : Les administrateurs consultent les alertes et les rapports via un tableau de bord interactif.

2.3. Définir les éléments de l'infrastructure à superviser

Une fois l'outil de supervision installé, il est crucial de définir les éléments spécifiques à superviser. Ces éléments varient en fonction des besoins de l'organisation, mais certains composants sont essentiels :

2.3.1. Les serveurs

Les serveurs physiques et virtuels doivent être surveillés de près pour assurer leur disponibilité. Voici des éléments à surveiller :

- **État général du serveur** (est-il allumé et fonctionnel ?)
- **Mémoire et CPU** : Les ressources système doivent être surveillées en permanence pour éviter les surcharges.
- **Disques durs** : L'utilisation de l'espace disque, les erreurs de disque et les températures doivent être surveillées.

2.3.2. Les services et applications

Les services critiques, tels que les serveurs web, les bases de données, ou les services DNS doivent être surveillés pour garantir leur fonctionnement :

- **Serveurs web** : Vérification de l'état des services HTTP/HTTPS.
- **Bases de données** : Vérification de l'accessibilité, de la performance et de l'intégrité des bases de données.
- **Applications métiers** : Les applications spécifiques doivent également être surveillées pour s'assurer qu'elles fonctionnent correctement.

2.3.3. Les équipements réseau

Il est important de surveiller la connectivité et les performances des équipements réseau pour éviter toute interruption de service :

- **Routeurs et commutateurs** : Vérification de leur disponibilité et de leur état général.
- **Connexion Internet** : Surveillance de la latence et des interruptions de service.

2.4. Définir des seuils d'alerte

2.4.1. Qu'est-ce qu'un seuil d'alerte ?

Un seuil d'alerte est une valeur prédéfinie qui, lorsqu'elle est atteinte ou dépassée, déclenche une notification d'alerte. Les seuils peuvent concerner différents aspects de la performance ou de la disponibilité :

- **Disponibilité** : Si un service ou un hôte est inaccessible pendant un certain temps.
- **Performance** : Si l'utilisation du CPU, de la mémoire, ou du disque dépasse un seuil critique.
- **Réseau** : Si la bande passante ou le temps de réponse du réseau dépasse un certain seuil.

2.4.2. Exemple de seuils d'alerte :

- **Serveur Web** : Si le serveur web met plus de 5 secondes à répondre à une requête HTTP, cela déclenche une alerte.
- **Mémoire** : Si l'utilisation de la mémoire dépasse 90 % pendant plus de 5 minutes, une alerte de type "avertissement" est envoyée.
- **Disque** : Si l'espace disque utilisé dépasse 85 %, une alerte "critique" est déclenchée.

2.5. Suivi et gestion des alertes

2.5.1. Suivi en temps réel

La surveillance en temps réel des alertes permet aux administrateurs de détecter les incidents dès qu'ils se produisent. L'outil de supervision affiche une vue en direct de l'état de l'infrastructure et met à jour les informations dès qu'un problème est détecté.

2.5.2. Gestion des alertes

Une fois l'alerte reçue, l'administrateur doit décider des actions à entreprendre. Par exemple :

- **Réinitialiser un service** qui a échoué.
- **Rechercher la cause de la panne** (panne matérielle, saturation de ressource, etc.).
- **Réparer le problème** pour rétablir la disponibilité du service.

Module 3 : La mise à niveau – Superviser la disponibilité de l'infrastructure : Centreon

Objectif du module :

Ce module est consacré à l'utilisation du logiciel de supervision **Centreon** pour surveiller la disponibilité de l'infrastructure informatique. Les participants apprendront à installer, configurer et utiliser Centreon pour suivre la disponibilité des serveurs, des applications, et des équipements réseau, et ainsi garantir la continuité des services.

3.1. Introduction à Centreon

3.1.1. Qu'est-ce que Centreon ?

Centreon est une solution de supervision open-source très populaire dans les environnements d'entreprise. Elle permet de surveiller l'état des composants de l'infrastructure IT (serveurs, services, applications, équipements réseau) en temps réel. Centreon est conçu pour :

- **Suivre la disponibilité des ressources** (serveurs, réseaux, applications),
- **Mesurer les performances** (utilisation CPU, mémoire, stockage, etc.),
- **Envoyer des alertes** en cas de problème,
- **Fournir des rapports et des historiques** pour l'analyse des tendances et la gestion proactive des ressources.

Centreon repose sur une architecture modulaire et flexible qui lui permet d'intégrer une grande variété d'équipements et de protocoles de supervision.

3.1.2. Architecture de Centreon

L'architecture de Centreon se compose de plusieurs composants essentiels :

1. **Centreon Web** : Interface graphique permettant aux administrateurs de configurer, gérer et visualiser la supervision de l'infrastructure.
2. **Centreon Engine** : Moteur de supervision qui exécute les contrôles de disponibilité et de performance sur les hôtes et services.
3. **Centreon Broker** : Composant responsable de la transmission des informations entre le moteur de supervision et la base de données.
4. **Base de données** : Stocke les informations relatives à la configuration, aux données de supervision et aux historiques.

3.2. Installation de Centreon

3.2.1. Prérequis

Avant d'installer Centreon, il est important de vérifier les prérequis suivants :

- **Système d'exploitation** : Centreon peut être installé sur diverses distributions Linux, comme CentOS ou Debian.
- **Dépendances logicielles** : Assurez-vous que les paquets nécessaires (Apache, MySQL, PHP, etc.) sont installés sur le système cible.

3.2.2. Installation de Centreon (sur CentOS 7)

Voici les étapes de base pour installer Centreon sur un serveur CentOS :

1. **Installer les dépendances** :

```
yum install -y httpd mariadb-server php php-mysqlnd php-gd php-mbstring php-xml
```

2. **Télécharger et installer Centreon** : Téléchargez le fichier d'installation depuis le site officiel de Centreon ou le dépôt.

```
wget https://download.centreon.com/releases/stable/centreon-20.x.rpm
rpm -ivh centreon-20.x.rpm
```

3. **Configurer la base de données** : Créez la base de données nécessaire à Centreon :

```
mysql -u root -p
CREATE DATABASE centreon;
GRANT ALL PRIVILEGES ON centreon.* TO 'centreon'@'localhost' IDENTIFIED BY 'your_password';
FLUSH PRIVILEGES;
```

Démarrer les services Centreon : Activez et démarrez les services nécessaires à Centreon :

```
systemctl enable httpd mariadb
systemctl start httpd mariadb
systemctl start centreon
```

4. **Accéder à l'interface Web** : Une fois l'installation terminée, accédez à l'interface de configuration de Centreon via un navigateur web en allant sur `http://<IP-du-serveur>/centreon` et suivez le processus d'installation via l'assistant Web.

3.3. Configuration de Centreon pour surveiller la disponibilité

3.3.1. Ajouter des hôtes et des services

Une fois Centreon installé et accessible via l'interface web, la configuration commence par l'ajout d'hôtes (serveurs, équipements réseau, etc.) et de services (applications, bases de données, services web, etc.).

1. **Ajouter un hôte** :
   - Accédez à l'interface Web de Centreon.
   - Allez dans le menu **Configuration** > **Hôtes**.
   - Cliquez sur **Ajouter un hôte** et remplissez les informations nécessaires :
     - **Nom de l'hôte** : Le nom que vous souhaitez donner au serveur ou à l'équipement.
     - **Adresse IP** : L'adresse IP de l'hôte à surveiller.
     - **Groupe d'hôtes** : Choisissez un groupe ou créez-en un nouveau.
     - **Modèle d'hôte** : Sélectionnez un modèle d'hôte pour appliquer des vérifications préconfigurées (disque, mémoire, CPU, etc.).
2. **Ajouter un service à un hôte** :
   - Une fois l'hôte ajouté, vous pouvez configurer les services associés (par exemple, pour surveiller les services web ou bases de données).
   - Allez dans **Configuration** > **Services**.
   - Cliquez sur **Ajouter un service**, puis sélectionnez l'hôte et spécifiez le type de service à surveiller (HTTP, FTP, MySQL, etc.).

Exemple :
Pour surveiller un serveur web, vous ajouterez un service HTTP sur l'hôte correspondant. Vous pourrez ainsi vérifier sa disponibilité en temps réel.

3.4. Définir des seuils d'alerte

Une fois les hôtes et services configurés, il est essentiel de définir des seuils d'alerte afin de recevoir des notifications lorsque certains critères de performance ou de disponibilité sont dépassés.

1. **Configurer les seuils d'alerte** :
    - Allez dans **Configuration** > **Services**.
    - Sélectionnez un service et configurez les seuils d'alerte pour la disponibilité ou la performance (par exemple, si un serveur HTTP met plus de 5 secondes à répondre).
2. **Exemple de seuils de performance** :
    - **Mémoire** : Si l'utilisation de la mémoire dépasse 90 %, une alerte sera générée.
    - **Disque** : Si l'espace disque est inférieur à 10 %, une alerte critique sera déclenchée.
    - **Réseau** : Si la latence du réseau dépasse 100 ms, une alerte sera envoyée.

3.5. Gestion des alertes et notifications

Centreon permet de configurer des notifications et des alertes par différents moyens pour informer les administrateurs en cas de problème de disponibilité.

3.5.1. Configurer les notifications

1. **Créer des contacts** :
   Allez dans **Configuration** > **Contacts** pour créer des contacts auxquels les alertes seront envoyées (email, SMS, etc.).
2. **Configurer les règles de notification** :
    - Allez dans **Configuration** > **Notifications**.
    - Définissez les critères pour les notifications : type d'alerte, seuils, fréquence des alertes, etc.
3. **Exemple de notification** : Vous pouvez configurer une notification par email lorsqu'un serveur devient indisponible ou lorsque l'utilisation du CPU dépasse un seuil critique.

3.6. Visualisation des données avec Centreon

Une fois la supervision configurée, Centreon offre des outils puissants pour visualiser les données collectées et analyser la disponibilité et les performances de l'infrastructure.

3.6.1. Tableaux de bord et graphiques

Centreon propose des tableaux de bord interactifs qui permettent de suivre en temps réel la disponibilité des équipements et services. Vous pouvez personnaliser ces tableaux pour afficher des informations pertinentes pour votre infrastructure.

- **Tableau de bord** : Visualisez l'état global de votre infrastructure en un coup d'œil (hôtes en ligne, services disponibles, etc.).
- **Graphiques** : Centreon permet de générer des graphiques détaillés pour suivre l'évolution de l'utilisation des ressources (CPU, mémoire, disque).

3.6.2. Rapports et historiques

Centreon permet de générer des rapports détaillés qui permettent d'analyser la disponibilité au fil du temps. Cela aide à identifier des tendances, des points faibles ou des opportunités d'amélioration.

Module 4 : La mise en œuvre et l'exploitation d'une solution de supervision

Objectif du module :
Ce module est destiné à guider les participants à travers les étapes pratiques de la mise en œuvre et de l'exploitation d'une solution de supervision. Il couvre la planification, la configuration, la gestion et l'optimisation de la solution de supervision afin de garantir une surveillance efficace, proactive et réactive de l'infrastructure informatique.

4.1. Introduction à la mise en œuvre d'une solution de supervision

La mise en œuvre d'une solution de supervision permet aux administrateurs système de suivre l'état de santé des équipements, des applications et des services critiques. Ce processus comprend l'intégration de la solution de supervision dans l'environnement IT existant et la configuration des paramètres nécessaires pour détecter les anomalies ou les défaillances.

4.1.1. Les objectifs de la mise en œuvre de la supervision

- **Proactivité** : Anticiper et prévenir les défaillances en surveillant les indicateurs de performance.
- **Réactivité** : Être capable de réagir rapidement en cas de panne ou d'anomalie, grâce à des alertes précoces.
- **Optimisation des ressources** : Analyser les tendances pour ajuster la capacité des ressources en fonction des besoins réels.
- **Gouvernance et conformité** : Garantir que l'infrastructure respecte les normes de sécurité, de performance et de disponibilité exigées.

4.1.2. Enjeux d'une solution de supervision efficace

- **Visibilité complète de l'infrastructure** : Une solution de supervision doit être capable de surveiller l'ensemble des composants de l'infrastructure IT, y compris les serveurs, le réseau, les applications et les bases de données.
- **Réduction des coûts et des risques** : Une surveillance proactive permet de réduire les coûts associés à des défaillances non détectées et minimise les risques de temps d'arrêt imprévus.
- **Amélioration des performances** : L'analyse continue des performances permet d'identifier et de résoudre les problèmes avant qu'ils n'affectent la productivité.

4.2. Planification de la mise en œuvre de la supervision

4.2.1. Identifier les besoins et les objectifs

Avant de commencer l'implémentation d'une solution de supervision, il est important de définir clairement :

- **Les services critiques à surveiller** : Identifiez les éléments de votre infrastructure qui sont essentiels au bon fonctionnement de l'entreprise (serveurs web, bases de données, équipements réseau, etc.).
- **Les objectifs de performance** : Définir les objectifs de performance pour chaque service ou hôte (par exemple, la disponibilité du réseau doit être de 99,9 %).
- **Les types de surveillance nécessaires** : Quelle supervision mettre en place (disponibilité, performance, utilisation des ressources, sécurité, etc.) et sur quels éléments spécifiques.

4.2.2. Choisir une solution adaptée

Selon les besoins identifiés, il faut choisir la solution de supervision qui correspond aux exigences :

- **Solutions open-source** : Comme Centreon, Nagios, ou Zabbix, qui sont adaptées pour les entreprises ayant des compétences techniques internes.
- **Solutions commerciales** : Comme SolarWinds, PRTG, ou Datadog, qui offrent des interfaces conviviales et des options avancées, mais à un coût supérieur.

4.2.3. Préparer l'infrastructure de supervision

L'architecture d'une solution de supervision doit être adaptée à l'infrastructure de l'entreprise. Il faut :

- **Choisir les serveurs pour l'outil de supervision** : Identifier la capacité nécessaire (CPU, RAM, stockage) en fonction du nombre d'éléments à superviser.
- **Planifier la bande passante nécessaire** : Estimer la quantité de données qui seront transmises par les agents ou sondes vers le serveur central.
- **Vérifier la compatibilité avec l'infrastructure existante** : Assurez-vous que la solution choisie fonctionne avec les équipements et systèmes existants.

4.3. Installation et configuration de la solution de supervision

4.3.1. Installation de l'outil de supervision

La mise en œuvre de la supervision commence par l'installation de la solution choisie. Cette étape peut varier en fonction du logiciel utilisé, mais elle inclut généralement les étapes suivantes :

- **Installer le serveur de supervision** (Centreon, Nagios, Zabbix, etc.) sur un serveur dédié.
- **Configurer la base de données** pour stocker les informations de supervision.
- **Installer des agents sur les hôtes** à surveiller, ou bien utiliser des sondes réseau pour surveiller les équipements sans agents.

Par exemple, si vous utilisez **Centreon**, vous devrez installer le serveur Centreon ainsi que le moteur de supervision, la base de données, et éventuellement des plugins supplémentaires pour surveiller des services spécifiques.

4.3.2. Configuration initiale de la supervision

Une fois le logiciel installé, configurez les éléments de l'infrastructure à surveiller :

- **Ajouter des hôtes** à superviser (serveurs, équipements réseau, etc.).
- **Configurer les services à surveiller** (HTTP, FTP, DNS, MySQL, etc.).
- **Définir les modèles de supervision** pour appliquer des vérifications standardisées sur plusieurs hôtes.

Il est important de prendre le temps de bien définir les paramètres de chaque service, notamment :

- Les **seuils d'alerte** pour chaque service (ex. : serveur HTTP en panne, utilisation du CPU > 90%).
- Les **intervals de vérification** pour déterminer la fréquence des contrôles (par exemple, vérifier toutes les 5 minutes l'état d'un serveur web).

4.3.3. Tester la configuration

Avant de déployer la solution sur toute l'infrastructure, il est recommandé de tester la configuration sur un nombre limité d'hôtes et services pour vérifier que la supervision fonctionne comme prévu. Lors des tests, vous pourrez ajuster les seuils d'alerte et les notifications pour éviter un excès d'alertes ou des alertes manquées.

4.4. Exploitation et gestion de la solution de supervision

4.4.1. Surveillance en temps réel

Une fois la solution en place, la surveillance en temps réel est la première tâche des administrateurs. Cela implique :

- **Suivre les alertes en temps réel** sur le tableau de bord pour détecter immédiatement toute anomalie.
- **Utiliser des outils de visualisation** pour analyser l'état global de l'infrastructure et prioriser les actions à prendre.

Les outils modernes, comme Centreon, offrent une interface graphique qui centralise toutes les alertes et fournit des visualisations claires sur l'état de santé de l'infrastructure.

4.4.2. Gestion des alertes et incidents

La gestion des alertes est cruciale pour répondre rapidement aux pannes ou aux problèmes. Cela inclut :

- **Réagir aux alertes** : Lorsqu'une alerte est déclenchée, il faut diagnostiquer rapidement le problème et y remédier (par exemple, redémarrer un service, libérer de l'espace disque, etc.).
- **Enregistrer les incidents** : Garder une trace des incidents et des actions entreprises dans un registre d'incidents pour une analyse ultérieure.
- **Exploiter les notifications** : Configurer des notifications par email, SMS ou d'autres moyens pour avertir les équipes responsables.

4.4.3. Optimisation et maintenance continue

La supervision de l'infrastructure doit être un processus continu d'optimisation et de réévaluation des performances :

- **Analyser les tendances** : Utiliser les rapports générés pour analyser les tendances de performance et la disponibilité des services. Cela permet d'anticiper les besoins futurs en termes de ressources ou d'infrastructure.
- **Ajuster les seuils d'alerte** : Réévaluer régulièrement les seuils d'alerte en fonction des changements dans l'infrastructure ou des exigences de l'entreprise.
- **Mettre à jour la solution de supervision** : Il est important de maintenir à jour la solution de supervision, y compris les agents et les plugins, pour garantir une supervision optimale.

4.5. Reporting et analyse des performances

4.5.1. Générer des rapports détaillés

Les rapports sont essentiels pour l'analyse de la performance de l'infrastructure. Ces rapports peuvent inclure :

- **Disponibilité des services** : Évaluer le temps de disponibilité des services pendant une période donnée.
- **Historique des pannes** : Analyser les incidents passés pour identifier des patterns récurrents ou des points faibles.
- **Utilisation des ressources** : Suivre l'évolution de l'utilisation des ressources comme la mémoire, le CPU, le stockage, etc.

4.5.2. Analyser les résultats

L'analyse des résultats permet de prendre des décisions informées sur l'optimisation des performances et des ressources. Par exemple :

- **Revoir les capacités** : Si un service approche constamment des seuils d'alerte, il peut être nécessaire d'ajouter des ressources (augmentation de la capacité serveur, etc.).
- **Réévaluer les stratégies de sauvegarde** : Si un problème récurrent est détecté dans une partie de l'infrastructure, il peut être nécessaire de revoir les stratégies de sauvegarde et de redondance.

Module 5 : La mise en œuvre d'une solution de centralisation des journaux d'événements

Objectif du module :
Ce module est conçu pour guider les participants à travers les étapes de la mise en œuvre d'une solution de centralisation des journaux d'événements (ou **logs**). Les journaux d'événements contiennent des informations cruciales sur l'état de l'infrastructure informatique, et leur centralisation permet une gestion efficace des incidents, une surveillance proactive, ainsi qu'une meilleure conformité aux normes de sécurité et de réglementation.

5.1. Introduction à la centralisation des journaux d'événements

5.1.1. Pourquoi centraliser les journaux d'événements ?

Les journaux d'événements sont générés par divers composants de l'infrastructure IT, tels que les serveurs, les applications, les équipements réseau, et les dispositifs de sécurité. Ces journaux contiennent des informations sur l'activité des systèmes, les erreurs, les alertes, et les événements critiques.

Les principaux avantages de la centralisation des logs :

- **Faciliter la détection des incidents** : Unifier les journaux permet une vue d'ensemble pour détecter des comportements anormaux, comme des tentatives de pénétration, des pannes de service, ou des erreurs système.
- **Analyser efficacement les incidents** : En regroupant les logs de différentes sources, il devient plus facile de faire des corrélations entre les événements (par exemple, une erreur dans un service peut être liée à une défaillance dans un autre service).
- **Conformité et audit** : De nombreuses entreprises doivent répondre à des normes de sécurité ou des régulations qui imposent la conservation des journaux pour une période donnée. La centralisation facilite la gestion de ces logs à des fins d'audit et de conformité.
- **Améliorer la sécurité** : Une analyse centralisée permet de détecter des attaques potentiellement passées inaperçues si elles étaient stockées localement sur chaque hôte.

5.1.2. Les sources de journaux d'événements

Les journaux d'événements peuvent provenir de :

- **Systèmes d'exploitation** (Windows, Linux) : Journaux de sécurité, erreurs système, informations sur les connexions.
- **Applications** : Logs d'accès, erreurs d'application, logs des transactions.
- **Équipements réseau** : Routeurs, switchs, pare-feu, qui enregistrent des informations sur l'activité du réseau.
- **Dispositifs de sécurité** : IDS/IPS (systèmes de détection et de prévention d'intrusion), antivirus, VPN.

5.2. Choisir une solution de centralisation des journaux d'événements

5.2.1. Critères de choix d'une solution de centralisation des logs

Le choix de la solution dépendra de plusieurs facteurs :

- **Volume de logs à traiter** : Le système doit être capable de gérer le volume de journaux générés par l'infrastructure.
- **Facilité de déploiement et de configuration** : Une bonne solution doit être simple à mettre en place et à configurer.
- **Scalabilité** : Il faut que la solution puisse évoluer pour intégrer plus de sources de logs ou supporter une croissance du volume de données.
- **Analyse et corrélation des logs** : Certaines solutions permettent d'effectuer des analyses avancées et de corréler les événements provenant de différentes sources.
- **Conformité aux normes** : Assurez-vous que la solution de centralisation respecte les exigences de conservation des logs imposées par les réglementations (ex : GDPR, HIPAA).

5.2.2. Exemples de solutions de centralisation des logs

- **Syslog-ng** : Un serveur de logs très répandu, compatible avec plusieurs types de logs et capable de les centraliser à partir de différentes sources. Il permet d'acheminer, de filtrer et de stocker les logs sur une base centralisée.
- **Graylog** : Outil open-source qui centralise, analyse et visualise les logs. Il offre une interface utilisateur pour rechercher et analyser les logs en temps réel, avec une bonne capacité de mise à l'échelle.
- **Elasticsearch, Logstash, Kibana (ELK Stack)** : Solution open-source très populaire pour la gestion et l'analyse des logs. **Logstash** collecte, filtre et transforme les logs, **Elasticsearch** permet de les indexer et de les rechercher, et **Kibana** fournit une interface pour les visualiser et les analyser.
- **Splunk** : Une solution payante mais très performante pour la gestion des logs, offrant des capacités avancées d'analyse et de visualisation des données.

5.3. Mise en œuvre de la centralisation des journaux d'événements

5.3.1. Architecture de la solution de centralisation des logs

L'architecture de la solution de centralisation des logs implique généralement plusieurs composants :

- **Sources de logs** : Serveurs, équipements réseau, applications, dispositifs de sécurité.
- **Collecteurs de logs** : Agents ou services installés sur les hôtes qui collectent les journaux locaux.
- **Serveur central de collecte** : Un serveur dédié à l'agrégation des logs. Ce serveur peut également effectuer des analyses de base.
- **Base de données ou indexation** : Un composant comme Elasticsearch ou une base SQL qui stocke les logs pour une récupération rapide et une analyse efficace.
- **Interface de gestion** : Une interface web (comme Kibana ou Graylog) pour consulter, analyser et générer des rapports à partir des logs centralisés.

Exemple d'architecture avec Syslog-ng :

- **Sources de logs** : Serveurs Linux, dispositifs réseau (pare-feu, switches, etc.).
- **Collecteurs de logs** : Syslog-ng configuré pour collecter les logs à partir des différents équipements.
- **Serveur central de collecte** : Un serveur Syslog-ng qui reçoit tous les logs des différents collecteurs et les stocke.
- **Base de données** : Logs stockés dans une base de données SQL ou dans un système de fichiers pour un accès rapide.

5.3.2. Déploiement et configuration des collecteurs de logs

Une fois le serveur central configuré, vous devez déployer des collecteurs sur les hôtes ou équipements à superviser pour collecter les logs :

- **Configurer un collecteur Syslog** sur les serveurs Linux :
  - Modifier le fichier de configuration de **rsyslog** pour envoyer les logs vers le serveur central :

```
bash
*.* @<adresse_IP_du_serveur_central>:514
```

- **Configurer un collecteur Windows** avec **NXLog** ou **Winlogbeat** (si vous utilisez la stack ELK) pour envoyer les journaux d'événements Windows au serveur central.

5.3.3. Sécuriser la collecte des journaux

Il est essentiel de sécuriser la transmission des logs entre les sources et le serveur central pour éviter que des informations sensibles soient interceptées. Utilisez des protocoles sécurisés tels que **Syslog sur TLS** ou des connexions **VPN** pour assurer la confidentialité et l'intégrité des données.

5.4. Analyse des journaux d'événements centralisés

5.4.1. Visualisation des logs

Les outils de centralisation des journaux offrent souvent des interfaces graphiques pour rechercher et visualiser les logs en temps réel. **Kibana** (dans l'ELK Stack) ou **Graylog** permettent de créer des tableaux de bord interactifs pour suivre les événements en temps réel et effectuer des analyses.

Exemples de visualisations courantes :

- **Top des erreurs d'application** : Visualiser les erreurs récurrentes dans les applications.
- **Flux réseau** : Analyser les logs des équipements réseau pour détecter des anomalies (tentatives de pénétration, trafic suspect).
- **Surveillance des utilisateurs** : Surveiller les logs des serveurs Windows pour identifier des comportements inhabituels des utilisateurs.

5.4.2. Recherche et corrélation des logs

Une fois les logs centralisés, il devient plus facile de rechercher et de corréler des événements. Par exemple, l'identification d'une activité suspecte peut être faite en croisant les logs des équipements réseau, des pare-feu et des serveurs applicatifs.

Les outils comme **Logstash** (dans l'ELK Stack) permettent de filtrer et de transformer les logs avant qu'ils ne soient indexés pour faciliter la recherche. Par exemple, vous pouvez filtrer les logs pour ne retenir que ceux relatifs aux erreurs critiques ou aux événements liés à la sécurité.

5.5. Gestion des alertes et notifications

Les solutions de centralisation des logs permettent de configurer des alertes en fonction des événements observés dans les logs. Ces alertes peuvent être envoyées par email, SMS ou autres moyens de communication en cas d'incident.

5.5.1. Exemples de configurations d'alertes

- **Alertes de sécurité** : Par exemple, lorsqu'un certain type de tentative d'intrusion est détecté dans les logs du pare-feu.
- **Alertes de performance** : Si un service ou une application dépasse un seuil critique dans les logs de performance.
- **Alertes de défaillance** : Lorsqu'un serveur envoie un message d'erreur critique dans ses logs système.

5.5.2. Configurer les alertes avec ELK ou Graylog

- **ELK** : Utilisez **Watchers** dans Elasticsearch pour configurer des alertes basées sur les logs.
- **Graylog** : Définissez des règles d'alerte dans l'interface utilisateur pour détecter des patterns spécifiques dans les logs.

Module 6 : L'analyse des journaux d'événements

Objectif du module :
Ce module vise à détailler les processus d'analyse des journaux d'événements pour extraire des informations pertinentes et les utiliser pour améliorer la gestion de l'infrastructure. L'analyse des logs permet de détecter des anomalies, de résoudre des problèmes, d'améliorer la sécurité et de garantir la conformité aux politiques internes et aux normes de régulation.

6.1. Introduction à l'analyse des journaux d'événements

Les journaux d'événements, ou logs, sont des enregistrements détaillés des activités qui se déroulent au sein de l'infrastructure informatique. Ils contiennent des informations critiques, comme des erreurs systèmes, des transactions d'application, des événements de sécurité, des alertes réseau, etc. L'analyse des journaux d'événements permet de comprendre ces événements et d'en tirer des enseignements utiles pour la gestion de l'infrastructure.

6.1.1. Pourquoi analyser les journaux d'événements ?

- **Détection des incidents de sécurité** : La détection précoce d'intrusions, de malwares ou d'attaques.
- **Résolution de problèmes** : Identifier les causes profondes des pannes de systèmes ou des erreurs applicatives.
- **Optimisation des performances** : Analyser les logs pour identifier les goulets d'étranglement ou les ressources surutilisées.
- **Conformité et audit** : Garantir que les journaux sont correctement enregistrés, stockés et analysés selon les exigences réglementaires.

6.1.2. Types de journaux d'événements courants à analyser

- **Journaux système** : Contiennent des informations sur l'état du système d'exploitation, les processus système, et les erreurs.
- **Journaux d'application** : Enregistrent les événements générés par des applications spécifiques.
- **Journaux de sécurité** : Contiennent des événements liés à la sécurité, comme les connexions, les tentatives de connexion échouées, ou les activités suspectes.
- **Journaux réseau** : Enregistrent l'activité du réseau, comme les connexions ou les tentatives d'accès non autorisées.

6.2. Outils et techniques d'analyse des journaux d'événements

6.2.1. Outils d'analyse des logs

Il existe plusieurs outils pour analyser les journaux d'événements, chacun ayant des caractéristiques adaptées à différents types d'analyse. Les outils les plus courants incluent :

- **ELK Stack (Elasticsearch, Logstash, Kibana)** : Une solution puissante permettant de collecter, stocker, indexer, rechercher et visualiser les logs. Logstash collecte et filtre les logs, Elasticsearch les indexe pour une recherche rapide, et Kibana permet de visualiser les données sous forme de graphiques interactifs.
- **Graylog** : Un autre outil open-source permettant de collecter, analyser, et visualiser des logs avec une interface conviviale pour l'analyse et la recherche des journaux d'événements.
- **Splunk** : Une solution d'analyse de données qui permet de recueillir des logs, d'effectuer des recherches complexes et de visualiser les événements sous forme de tableaux de bord.
- **Syslog-ng** : Utilisé pour la collecte, le filtrage et l'acheminement des journaux d'événements vers un serveur de centralisation.

6.2.2. Techniques d'analyse des logs

Une analyse efficace des journaux d'événements repose sur plusieurs techniques fondamentales :

- **Filtrage** : L'extraction des événements les plus pertinents en fonction de critères spécifiques, tels que les erreurs, les avertissements, ou des codes d'événements particuliers.
- **Agrégation** : La collecte de plusieurs logs provenant de différentes sources dans un même endroit pour une analyse comparative.
- **Corrélation** : La recherche de relations entre différents événements provenant de diverses sources de journaux. Par exemple, corréler les tentatives d'accès dans les logs de pare-feu avec les logs d'authentification d'un serveur.
- **Analyse de tendances** : Analyser les logs sur des périodes prolongées pour identifier des patterns ou des anomalies récurrentes.
- **Alerting** : La mise en place d'alertes automatisées pour notifier les administrateurs des événements anormaux ou critiques.

6.3. Processus d'analyse des journaux d'événements

6.3.1. Collecte des journaux d'événements

La première étape dans l'analyse des logs est de collecter les journaux à partir des différentes sources. Cela peut inclure :

- **Les serveurs** : Journaux système (Linux, Windows), logs d'applications, logs de bases de données.
- **Les équipements réseau** : Logs des pare-feu, des routeurs, des switchs.
- **Les dispositifs de sécurité** : Logs des systèmes de détection d'intrusion (IDS), des VPN, des antivirus.

Les journaux doivent être collectés dans un format compatible avec l'outil d'analyse choisi, comme **Syslog** ou **JSON** pour les solutions basées sur ELK.

6.3.2. Normalisation et structuration des logs

Une fois les logs collectés, ils doivent être normalisés et structurés afin de faciliter leur analyse. Cela peut impliquer :

- **Transformation des formats** : Convertir les logs dans un format commun, comme JSON ou CSV, pour simplifier l'analyse.

- **Ajout de métadonnées** : Ajouter des informations supplémentaires aux logs, telles que les heures d'agrégation, les adresses IP des utilisateurs, ou les types d'événements.
- **Indexation** : Organiser les logs pour une recherche rapide en indexant des informations clés, comme les identifiants d'utilisateur, les erreurs, ou les codes d'état.

6.3.3. Analyse des logs

L'analyse proprement dite se déroule en plusieurs étapes :

- **Identification des événements critiques** : Chercher des erreurs, des échecs de connexion, ou des alertes de sécurité (tentatives de pénétration, malwares, etc.).
- **Corrélation des événements** : Relier des événements provenant de plusieurs sources pour identifier des incidents complexes. Par exemple, une tentative d'accès échouée suivie d'une modification de privilèges utilisateur dans les logs système pourrait indiquer une tentative d'escalade de privilèges.
- **Analyse des anomalies** : Utiliser des outils de visualisation pour détecter des anomalies dans les données. Cela peut inclure des pics inhabituels dans les connexions réseau, des augmentations soudaines de l'utilisation CPU, ou des erreurs applicatives fréquentes.

Exemple d'analyse dans ELK Stack :
Un administrateur peut utiliser **Kibana** pour visualiser les logs des serveurs web et détecter des erreurs HTTP 500 qui surviennent plus fréquemment à une heure spécifique. En croisant cette information avec les logs des pare-feu, il peut identifier que ces erreurs coïncident avec des tentatives d'attaque par force brute sur un serveur web.

6.3.4. Recherche et requêtes avancées

Dans des outils comme ELK, la recherche et l'utilisation de requêtes avancées permettent de trouver rapidement des événements spécifiques. Par exemple :

- **Requête pour trouver des erreurs spécifiques** : Dans Elasticsearch, une requête simple peut être utilisée pour extraire toutes les erreurs liées à un service particulier :

```
json
CopierModifier
{
  "query": {
    "match": {
      "level": "error"
    }
  }
}
```

- **Requête pour analyser les pics d'utilisation** : Vous pouvez rechercher les logs pour identifier des pics d'utilisation du CPU ou de la mémoire dans les logs systèmes, ce qui pourrait indiquer un problème avec une application.

6.3.5. Détection de menaces et incidents

L'une des principales raisons pour lesquelles on analyse les journaux d'événements est la détection de menaces potentielles. Les logs peuvent aider à repérer :

- **Tentatives d'intrusion** : Par exemple, plusieurs tentatives échouées de connexion SSH peuvent indiquer une tentative de piratage par force brute.
- **Comportement anormal des utilisateurs** : Comme des connexions hors des heures de travail ou depuis des adresses IP géographiques inhabituelles.

- **Éléments de compromission** : Les logs peuvent également signaler des actions effectuées par un utilisateur après qu'un compte ait été compromis, telles que la modification de fichiers de configuration ou l'escalade des privilèges.

6.4. Utilisation des résultats de l'analyse des journaux d'événements

6.4.1. Prise de décision basée sur l'analyse

Une fois les logs analysés, les informations collectées peuvent être utilisées pour :

- **Diagnostiquer et résoudre des problèmes** : Si des erreurs récurrentes sont détectées dans les logs d'application, elles peuvent être signalées à l'équipe de développement pour une correction.
- **Renforcer la sécurité** : Des anomalies de sécurité identifiées dans les logs peuvent conduire à une amélioration de la politique de sécurité (par exemple, mettre en place une authentification multi-facteurs, réviser les paramètres des pare-feu, etc.).
- **Optimiser les performances** : Si des pics d'utilisation des ressources sont détectés dans les logs système, des ajustements peuvent être faits pour augmenter la capacité des serveurs ou redistribuer la charge de travail.

6.4.2. Génération de rapports et alertes

Les résultats de l'analyse peuvent être utilisés pour générer des rapports réguliers sur la santé de l'infrastructure et des alertes en cas de détection de problèmes graves ou d'incidents de sécurité. Ces rapports peuvent être envoyés aux équipes responsables pour qu'elles prennent des mesures correctives rapidement.