Supervision de l'Infrastructure

Table des matières

Module 1 : L'administration superviseur 2
Module 2 : L'introduction au Serveur Syslog et NTP 5
Module 3 : L'installation d'un serveur Syslog 8
Module 4 : La création d'un Monitor 12
Module 5 : Les fonctionnalités d'un MDM (Mobile Device Manager) 16
Module 6 : Hypervision des systèmes et équipements réseau, journalisation 19
Module 7 : Hypervision de l'infrastructure : Syslog, protocoles de supervision et d'analyse 23

Module 1 : L’administration superviseur

Objectifs pédagogiques

À la fin de ce module, les apprenants seront capables de :

- Comprendre le rôle d'un administrateur superviseur dans une organisation.
- Identifier les tâches principales et les responsabilités d'un administrateur superviseur.
- Maîtriser les outils et les compétences nécessaires pour superviser efficacement une infrastructure.
- Comprendre les principes de gestion des incidents et de la performance dans une infrastructure.

1. Rôle et responsabilité de l’administrateur superviseur

A. Qu’est-ce qu’un administrateur superviseur ?

Un **administrateur superviseur** (ou **administrateur systèmes et réseaux**) est responsable de la gestion et de la surveillance de l’infrastructure informatique d’une organisation. Cela inclut les serveurs, les équipements réseau, les bases de données, les systèmes de stockage et autres ressources IT.

B. Responsabilités principales

Les administrateurs superviseurs ont plusieurs missions essentielles :

- **Gestion des systèmes informatiques** : Installation, configuration et maintenance des serveurs, des systèmes d'exploitation et des applications.
- **Surveillance de l’infrastructure** : Suivi des performances des ressources, détection et résolution des incidents, gestion des alertes.
- **Gestion des utilisateurs** : Création, modification et suppression des comptes utilisateurs, gestion des permissions d’accès.
- **Automatisation des tâches** : Mise en place de processus automatisés pour la gestion des ressources et des tâches répétitives (ex. : mise à jour de logiciels, backup).
- **Sécurisation de l’infrastructure** : Implémentation de politiques de sécurité, gestion des pare-feu, des antivirus, des systèmes de détection d’intrusion (IDS).
- **Planification de la capacité et de la scalabilité** : Prévision des besoins futurs en infrastructure pour s'assurer que l'organisation puisse évoluer sans risques de défaillance.

2. Outils utilisés par l’administrateur superviseur

A. Outils de surveillance et de gestion des systèmes

Les administrateurs superviseurs utilisent des outils variés pour surveiller, gérer et maintenir l'infrastructure. Ces outils permettent de visualiser en temps réel l'état des ressources, de prévenir les incidents et d’automatiser les tâches.

Quelques exemples d’outils populaires :

- **Nagios** : Outil de supervision des infrastructures IT, permettant de surveiller les équipements réseau, les serveurs et les services.
- **Zabbix** : Outil de surveillance open-source permettant de collecter des métriques, de générer des alertes et de produire des rapports sur les systèmes et les applications.

- **Prometheus + Grafana** : Utilisé pour la surveillance des métriques des systèmes, notamment dans des architectures de microservices.
- **Ansible** : Outil d'automatisation des tâches d'administration, comme l'installation de logiciels et la configuration des systèmes.
- **SolarWinds** : Outil commercial offrant une suite complète pour la surveillance des performances réseau, des serveurs, et de la gestion des incidents.

B. Outils de gestion des incidents

Un autre aspect important du rôle de l'administrateur superviseur est la gestion des incidents, qui permet de résoudre rapidement les problèmes pouvant affecter la continuité des services :

- **ServiceNow** : Plateforme permettant de gérer les incidents et les demandes de service, utilisée dans des environnements ITIL.
- **JIRA Service Management** : Utilisé pour la gestion des tickets et des incidents en relation avec les services informatiques.

🧹 3. La gestion des incidents et des problèmes

A. Gestion des incidents

L'une des tâches essentielles d'un administrateur superviseur est de **gérer les incidents**. Les incidents sont des événements qui perturbent ou affectent la performance des systèmes, des applications ou du réseau. Cela inclut des pannes de serveur, des attaques de sécurité, des pannes réseau, etc.

Étapes principales dans la gestion des incidents :

1. **Identification** : La détection d'un incident peut se faire par un système de surveillance ou par une notification d'un utilisateur.
2. **Priorisation** : Une fois l'incident identifié, il est crucial de déterminer sa gravité et de prioriser sa résolution.
3. **Résolution** : L'administrateur cherche à résoudre l'incident en diagnostiquant les causes sous-jacentes et en appliquant les correctifs nécessaires.
4. **Suivi et retour d'expérience** : Une fois l'incident résolu, un suivi est réalisé pour s'assurer qu'il ne se reproduise pas. Un rapport détaillé est souvent généré pour évaluer l'incident.

B. Gestion des problèmes

Les **problèmes** sont des causes sous-jacentes récurrentes ou complexes qui provoquent des incidents. Ils nécessitent une analyse approfondie pour identifier les causes profondes et éviter leur réapparition.

- **Exemple de problème** : Un serveur qui plante fréquemment en raison d'un manque de ressources (mémoire ou CPU). Un administrateur pourrait mettre en œuvre une solution à long terme comme l'optimisation des ressources ou la migration vers un autre serveur.

Processus de gestion des problèmes :

1. **Identification du problème récurrent**.
2. **Analyse approfondie** (enquête sur les causes racines).
3. **Résolution du problème** (ex. : mise à jour de la configuration, ajout de ressources matérielles, patching des systèmes).
4. **Documentation des solutions** : Mise en place de solutions à long terme et documentation pour éviter la réapparition.

4. Planification et gestion de la capacité

A. Planification des ressources

L'administrateur superviseur doit évaluer en permanence la capacité des ressources actuelles et prévoir les besoins futurs. Cela inclut les serveurs, la bande passante réseau, les applications, et les systèmes de stockage. Une planification efficace de la capacité permet d'éviter des goulots d'étranglement, des pannes ou des dégradations de performance.

Exemples de tâches de planification :

- **Analyse des tendances** : Analyser les tendances d'utilisation des ressources sur plusieurs mois pour prévoir les besoins en augmentation de capacité.
- **Planification de la scalabilité** : Assurer la capacité d'adaptation rapide en cas de forte demande (ex. : montée en charge des serveurs, virtualisation des ressources).

B. Scalabilité et élasticité

En fonction de la croissance des besoins, l'administrateur superviseur doit planifier la **scalabilité** et l'**élasticité** de l'infrastructure :

- **Scalabilité verticale** : Augmenter les ressources d'un serveur (ajout de mémoire RAM, de processeurs).
- **Scalabilité horizontale** : Ajouter davantage de serveurs ou d'instances pour équilibrer la charge et améliorer les performances.
- **Elasticité dans le Cloud** : Les solutions Cloud comme **AWS**, **Azure** ou **Google Cloud** permettent de scaler les ressources automatiquement en fonction de la demande via des services comme **Auto Scaling**.

5. Sécurisation de l'infrastructure

A. Principes de base de la sécurité des systèmes

La sécurité des infrastructures informatiques est un aspect essentiel du rôle d'un administrateur superviseur. Il doit protéger l'intégrité des données, des applications et des services contre les cyberattaques et les intrusions.

Les principes de sécurité incluent :

- **Contrôle des accès** : Gérer les utilisateurs et leurs permissions à travers des outils comme **Active Directory** ou **LDAP**.
- **Patching et mise à jour** : Mettre à jour régulièrement les systèmes pour corriger les vulnérabilités.
- **Surveillance de la sécurité** : Utiliser des outils comme **Snort** ou **OSSEC** pour la détection d'intrusions (IDS).

B. Mesures de sécurité courantes

Les administrateurs mettent en œuvre des pratiques de sécurité telles que :

- **Pare-feu** (Firewalls) : Mettre en place des règles de pare-feu pour contrôler le trafic réseau entrant et sortant.
- **Chiffrement des données** : Assurer le chiffrement des données sensibles au repos et en transit (par exemple, avec **SSL/TLS**).
- **Audit de sécurité** : Effectuer des audits réguliers pour détecter d'éventuelles vulnérabilités ou manquements.

6. Outils de gestion des configurations et automatisation

A. Outils de gestion de configuration

Les administrateurs utilisent des outils d'automatisation pour garantir la cohérence et la rapidité des déploiements d'infrastructure, comme **Ansible**, **Puppet** ou **Chef**. Ces outils permettent de déployer automatiquement des configurations sur des serveurs en minimisant les erreurs humaines.

B. Automatisation des tâches

L'automatisation des tâches répétitives permet à l'administrateur superviseur de se concentrer sur des activités à plus forte valeur ajoutée :

- **Mises à jour automatiques** des serveurs.
- **Déploiement de scripts** pour la gestion des configurations.
- **Automatisation des sauvegardes**.

Module 2 : L'introduction au Serveur Syslog et NTP

Objectifs pédagogiques

À la fin de ce module, vous serez capable de :

- Comprendre le rôle d'un serveur **Syslog** dans la centralisation et la gestion des logs.
- Configurer un serveur **Syslog** pour collecter et analyser les logs générés par les systèmes et équipements réseau.
- Appréhender l'importance du protocole **NTP** dans la gestion du temps au sein d'un réseau informatique.
- Configurer un serveur et un client **NTP** pour synchroniser les horloges dans un réseau.

---

1. Serveur Syslog : Introduction et fonctionnement

A. Qu'est-ce que Syslog ?

Syslog (System Logging Protocol) est un protocole standard utilisé pour envoyer, stocker et gérer les messages de journalisation (logs) générés par les systèmes, applications et équipements réseau. Un serveur **Syslog** est donc un système centralisé qui reçoit les logs d'autres machines pour faciliter leur gestion et analyse.

Objectifs de Syslog :

- **Centralisation des logs** : Collecter les logs générés par différents serveurs, équipements réseau (comme les routeurs, switches, etc.), et applications.
- **Suivi des événements** : Aider à la détection des incidents, à la résolution de problèmes et à la surveillance des performances.
- **Conformité** : Assurer que les logs sont correctement enregistrés pour les besoins d'audit et de conformité.

B. Structure des messages Syslog

Un message Syslog est composé de plusieurs éléments :

- **Priorité (PRI)** : Indicateur de la gravité du message.

- **Timestamp (Horodatage)** : Heure à laquelle le message a été généré.
- **Nom de l'hôte** : Le nom de la machine ou de l'équipement qui a généré le message.
- **Tag** : Le nom du processus ou de l'application qui a généré le message.
- **Message** : Le contenu détaillé du message de log.

Exemple d'un message Syslog : pgsql

```
<34>Jan  1 12:34:56 server1 sshd[12345]: Failed password for root from 192.168.1.1 port 22 ssh2
```

C. Fonctionnement d'un serveur Syslog

Un serveur **Syslog** reçoit des messages de journaux de différents périphériques via le réseau. Les équipements et serveurs envoient leurs logs à une adresse IP spécifique et un port dédié (habituellement le port **514** en UDP).

Exemple de flux Syslog :

1. **Un périphérique ou serveur** génère un message de log.
2. **Le message est envoyé** au serveur Syslog via UDP ou TCP.
3. **Le serveur Syslog** centralise ces messages dans des fichiers journaux (logs) pour une consultation ultérieure.

D. Utilisation de Syslog dans la gestion des incidents

Syslog est un outil précieux dans la gestion des incidents et des problèmes. Les logs peuvent fournir des informations détaillées sur les causes d'une panne ou d'un dysfonctionnement.

- **Alertes en temps réel** : En configurant des règles spécifiques, il est possible d'envoyer des alertes lorsqu'un événement critique se produit.
- **Archivage des logs** : Stocker les logs pour des analyses futures, ce qui est essentiel pour des investigations après incident.

2. Installation et configuration d'un serveur Syslog

A. Installation d'un serveur Syslog sous Linux (rsyslog)

1. **Installer rsyslog (serveur Syslog sur Linux) :** `rsyslog` est l'une des implémentations les plus populaires de Syslog sous Linux.
    - Pour installer `rsyslog` sur une machine Linux (Debian/Ubuntu) :

      ```
      sudo apt-get update
      sudo apt-get install rsyslog
      ```

2. **Activer la réception des logs distants :** Par défaut, `rsyslog` peut être configuré pour recevoir des logs d'autres machines. Modifiez le fichier `/etc/rsyslog.conf` pour activer la réception des logs via UDP :

   ```
   module(load="imudp")    # Charge le module UDP
   input(type="imudp" port="514")  # Active la réception des logs sur le port 514 UDP
   ```

3. **Redémarrer rsyslog pour appliquer les modifications :**

   ```
   sudo systemctl restart rsyslog
   sudo systemctl enable rsyslog
   ```

4. **Vérifier que rsyslog fonctionne correctement :**

   ```
   sudo systemctl status rsyslog
   ```

B. Configurer un périphérique pour envoyer des logs au serveur Syslog

Sur vos périphériques réseau (comme les routeurs ou switches), vous devrez configurer l'adresse IP du serveur Syslog pour envoyer les messages de log. Cela se fait généralement via une interface de ligne de commande (CLI) ou une interface graphique, en fonction de l'équipement.

Exemple sur un **routeur Cisco** :

```
logging 192.168.1.100    # IP du serveur Syslog
logging trap warnings    # Niveau de gravité des logs
```

---

3. Le protocole NTP (Network Time Protocol)

A. Qu'est-ce que NTP ?

Le **Network Time Protocol (NTP)** est un protocole de synchronisation de l'heure qui permet de synchroniser l'horloge des systèmes informatiques sur un réseau avec une source de temps de référence. Cela est crucial pour garantir que tous les systèmes et équipements d'un réseau aient la même heure, ce qui est essentiel pour l'intégrité des logs, le diagnostic des incidents et la sécurité.

Utilité de NTP :

- **Synchronisation précise de l'heure** : Assurer une heure correcte sur tous les serveurs et périphériques du réseau.
- **Gestion des logs** : Les logs doivent être horodatés de manière précise pour corréler les événements et résoudre les incidents.
- **Sécurité** : La plupart des protocoles de sécurité, comme le SSL/TLS, nécessitent que les horloges des systèmes soient synchronisées pour éviter des problèmes avec les certificats et les mécanismes d'authentification.

B. Fonctionnement de NTP

Le protocole NTP fonctionne en interrogeant un serveur de temps (souvent un serveur **NTP public** ou un **serveur de temps local**) pour ajuster l'heure du client afin qu'elle corresponde à une source de temps fiable.

- **Architecture hiérarchique** : NTP utilise une hiérarchie de serveurs, où un serveur de niveau 0 (souvent une source de temps fiable comme une horloge atomique) se synchronise avec un serveur de niveau 1, et ainsi de suite.
- **Délai de transmission** : NTP tient compte des délais de transmission pour ajuster l'heure en conséquence.

C. Installation et configuration de NTP

1. **Installation de NTP sur un serveur Linux :**

   ```
   sudo apt-get install ntp
   ```

2. **Configurer le serveur NTP pour qu'il se synchronise avec un serveur de temps :** Modifiez le fichier de configuration `/etc/ntp.conf` pour ajouter des serveurs NTP :

   ```
   server 0.pool.ntp.org
   server 1.pool.ntp.org
   server 2.pool.ntp.org
   ```

3. **Redémarrer le service NTP :**

```
sudo systemctl restart ntp
sudo systemctl enable ntp
```

4. **Vérifier la synchronisation NTP :** Utilisez la commande suivante pour vérifier que votre serveur est bien synchronisé avec les serveurs NTP :

```
ntpq -p
```

5. **Configurer un client NTP pour se synchroniser avec le serveur NTP :** Sur les clients (serveurs, équipements réseau), configurez NTP pour qu'ils se synchronisent avec votre serveur NTP :

```
sudo apt-get install ntpdate
sudo ntpdate 192.168.1.100  # IP du serveur NTP
```

---

4. Conclusion et bonnes pratiques

A. Avantages de la centralisation des logs avec Syslog

- **Efficacité** : Une gestion centralisée des logs permet de surveiller facilement l'ensemble du réseau.
- **Sécurité** : Les logs peuvent être analysés pour détecter des tentatives d'intrusion ou des comportements suspects.
- **Audit** : Les logs peuvent être utilisés pour des audits de sécurité ou des analyses post-incident.

B. Importance de la synchronisation horaire avec NTP

- **Cohérence des logs** : Une synchronisation de l'heure est essentielle pour que les logs provenant de différents équipements soient fiables et facilement corrélables.
- **Précision dans la gestion des événements** : Des horodatages cohérents facilitent le diagnostic des problèmes et des attaques.
- **Sécurité renforcée** : Des horloges synchronisées permettent de valider des signatures numériques et d'éviter des conflits dans les mécanismes de sécurité.

Module 3 : L'installation d'un serveur Syslog

Objectifs pédagogiques

À la fin de ce module, vous serez capable de :

- Installer un serveur **Syslog** sur un système Linux (ex. : Ubuntu/Debian).
- Configurer un serveur Syslog pour recevoir des logs de différentes sources (serveurs, équipements réseau, applications).
- Gérer et analyser les logs centralisés pour surveiller et diagnostiquer l'infrastructure.
- Mettre en place des règles pour filtrer et organiser les logs collectés.

---

1. Introduction à Syslog

A. Qu'est-ce qu'un serveur Syslog ?

Un serveur **Syslog** centralise les journaux d'événements (logs) envoyés par différents systèmes, applications et périphériques réseau. Cela permet de faciliter la gestion et l'analyse des logs pour :

- La surveillance de l'infrastructure.
- La détection d'incidents ou d'attaques.
- La conformité aux normes de sécurité (audit logs).

B. Architecture de Syslog

Le **protocole Syslog** suit une architecture client-serveur. Les équipements, serveurs et applications envoient des logs au serveur Syslog via le réseau. Le serveur Syslog reçoit ces logs, les centralise et les stocke pour un traitement ultérieur.

- **Client Syslog** : Tout dispositif ou logiciel qui génère des messages de journalisation et les envoie à un serveur Syslog.
- **Serveur Syslog** : Le système qui reçoit, collecte et analyse les messages de log envoyés par les clients.

---

2. Installation d'un serveur Syslog sur un serveur Linux

Dans cette section, nous allons installer **rsyslog**, l'une des implémentations les plus populaires du serveur Syslog sous Linux.

A. Prérequis

- Un système Linux fonctionnant (Ubuntu/Debian, CentOS/RHEL).
- Des droits administratifs (sudo) sur le système.

B. Installer rsyslog sur Ubuntu/Debian

1. **Mise à jour du système** : Avant toute installation, il est essentiel de mettre à jour votre système :

   ```
   sudo apt-get update
   sudo apt-get upgrade
   ```

2. **Installer rsyslog** : Utilisez la commande suivante pour installer rsyslog sur votre serveur Linux :

   ```
   sudo apt-get install rsyslog
   ```

3. **Vérifier l'installation** : Une fois l'installation terminée, vérifiez que `rsyslog` est actif et fonctionne correctement :

   ```
   sudo systemctl status rsyslog
   ```

   Vous devriez voir une sortie indiquant que le service `rsyslog` est en cours d'exécution.

---

3. Configurer le serveur Syslog pour recevoir des logs distants

Après l'installation de `rsyslog`, vous devez le configurer pour recevoir les logs provenant d'autres systèmes.

A. Modifier la configuration de rsyslog pour accepter les logs distants

1. **Éditez le fichier de configuration rsyslog** : Le fichier de configuration principal de `rsyslog` se trouve à l'emplacement suivant :

   ```
   sudo nano /etc/rsyslog.conf
   ```

2. **Activer la réception de logs via UDP (port 514)** : Par défaut, `rsyslog` écoute le port **514** en UDP pour recevoir des messages de log. Pour l'activer, décommentez ou ajoutez les lignes suivantes dans le fichier **`/etc/rsyslog.conf :`**

   ```
   # Chargement du module UDP pour recevoir des logs
   module(load="imudp")  # Charge le module UDP
   input(type="imudp" port="514")  # Active la réception de logs via UDP sur le port 514
   ```

3. **Configurer pour accepter les logs via TCP (optionnel)** : Si vous souhaitez également recevoir des logs via TCP (plus sécurisé que UDP), ajoutez les lignes suivantes :

   ```
   # Chargement du module TCP pour recevoir des logs
   module(load="imtcp")  # Charge le module TCP
   input(type="imtcp" port="514")  # Active la réception des logs via TCP sur le port 514
   ```

B. Configurer l'emplacement de stockage des logs

Vous pouvez personnaliser l'emplacement où les logs sont enregistrés sur votre serveur. Par exemple, dans le fichier **`/etc/rsyslog.conf`**, vous pouvez définir des règles de filtrage qui spécifient où les logs de différents niveaux de priorité seront stockés.

Exemple de configuration pour stocker les logs dans `/var/log/syslog` :

```
*.*    /var/log/syslog
```

C. Redémarrer rsyslog pour appliquer les modifications

Après avoir modifié le fichier de configuration, vous devez redémarrer `rsyslog` pour appliquer les modifications :

```
sudo systemctl restart rsyslog
```

D. Activer rsyslog au démarrage :

Pour vous assurer que `rsyslog` redémarre automatiquement après un redémarrage de votre serveur, exécutez la commande suivante :

```
sudo systemctl enable rsyslog
```

---

4. Configurer les périphériques pour envoyer des logs au serveur Syslog

Maintenant que le serveur Syslog est configuré pour recevoir des logs, il est temps de configurer les autres périphériques et serveurs pour envoyer leurs logs au serveur Syslog.

A. Configurer un serveur Linux pour envoyer des logs

Sur un serveur Linux, vous pouvez configurer l'envoi de logs à un serveur Syslog distant en modifiant le fichier de configuration de `rsyslog` ou `syslog`.

1. **Éditez le fichier de configuration de rsyslog** :

   ```
   sudo nano /etc/rsyslog.conf
   ```

2. **Ajoutez la ligne suivante pour envoyer les logs au serveur Syslog distant** : Remplacez `192.168.1.100` par l'adresse IP de votre serveur Syslog.

   ```
   *.* @192.168.1.100:514  # Envoie tous les logs au serveur Syslog via UDP
   ```

   Pour TCP, utilisez le format suivant :

   ```
   *.* @@192.168.1.100:514  # Envoie tous les logs au serveur Syslog via TCP
   ```

3. **Redémarrer rsyslog sur le serveur client** :

   ```
   sudo systemctl restart rsyslog
   ```

B. Configurer un périphérique réseau (ex : routeur ou switch Cisco)

Sur les équipements réseau, comme un routeur Cisco, vous devez spécifier l'adresse IP du serveur Syslog pour envoyer les logs. Voici un exemple pour configurer un périphérique Cisco :

1. **Accéder à l'interface de ligne de commande (CLI) de l'équipement**.
2. **Configurer le serveur Syslog** :

   ```
   logging 192.168.1.100  # Adresse IP du serveur Syslog
   logging trap debugging  # Niveau de journalisation
   ```

Cela permettra au périphérique de commencer à envoyer les logs au serveur Syslog centralisé.

---

5. Analyser et gérer les logs reçus

A. Vérifier la réception des logs

Une fois que les périphériques et serveurs ont commencé à envoyer leurs logs, vous pouvez vérifier si les logs sont correctement reçus sur le serveur Syslog. Les logs seront stockés dans les fichiers configurés dans `/var/log`.

Pour consulter les logs dans un terminal, utilisez la commande suivante :

```
sudo tail -f /var/log/syslog
```

Cette commande vous permettra de suivre les derniers messages de log en temps réel.

B. Filtrer et organiser les logs

L'un des avantages de l'utilisation de Syslog est la possibilité de filtrer et d'organiser les logs selon différents critères (niveau de gravité, source, type d'événement). Vous pouvez configurer `rsyslog` pour stocker des types de logs

spécifiques dans des fichiers séparés. Par exemple, vous pourriez vouloir que les logs d'erreur soient enregistrés dans un fichier séparé :

```
if $syslogseverity-text == 'err' then /var/log/errors.log
& stop
```

Cela permet de mieux organiser les logs pour faciliter leur consultation et analyse.

---

6. Conclusion

A. Avantages d'un serveur Syslog

L'installation d'un serveur Syslog permet de centraliser la gestion des logs de votre infrastructure, ce qui est essentiel pour :

- La détection d'incidents de sécurité et des problèmes techniques.
- La conformité aux normes et aux réglementations de sécurité.
- La gestion de la performance et l'optimisation des ressources.

B. Bonnes pratiques

- **Sécuriser les communications** entre les clients et le serveur Syslog, en privilégiant TCP plutôt que UDP.
- **Mettre en place une politique de rétention des logs** pour éviter qu'ils ne saturent les ressources du serveur.
- **Automatiser la gestion des logs** en utilisant des outils comme `Logrotate` pour gérer l'archivage et la suppression des logs anciens.

Module 4 : La création d'un Monitor

Objectifs pédagogiques

À la fin de ce module, vous serez capable de :

- Comprendre l'importance d'un système de monitoring dans une infrastructure.
- Créer et configurer un monitor pour surveiller la performance et la disponibilité des systèmes et services.
- Mettre en place des alertes pour être averti en cas de problème.
- Utiliser des outils de monitoring comme **Nagios**, **Zabbix**, **Prometheus** ou **Grafana** pour créer des monitors efficaces.

---

1. Introduction au Monitoring

A. Qu'est-ce qu'un système de monitoring ?

Le monitoring (ou surveillance) d'une infrastructure informatique consiste à surveiller en temps réel les performances, la disponibilité, et l'état des différents composants du système : serveurs, applications, bases de données, équipements réseau, etc. Un **monitor** est un outil ou un processus qui permet de suivre ces paramètres pour détecter les anomalies ou défaillances.

B. Pourquoi est-il important de surveiller l'infrastructure ?

La surveillance continue permet de :

- **Assurer la disponibilité** des services et applications critiques.
- **Identifier rapidement** les problèmes de performance ou les pannes.
- **Anticiper les incidents** en analysant les tendances de performance.
- **Optimiser l'utilisation des ressources** (CPU, mémoire, espace disque, etc.).
- **Améliorer la sécurité** en détectant les activités suspectes ou non autorisées.

C. Types de monitoring

Il existe plusieurs types de monitoring que vous pouvez configurer pour surveiller différents aspects de votre infrastructure :

- **Surveillance des hôtes** : Suivi de la disponibilité et des performances des serveurs et autres équipements.
- **Surveillance des services** : Surveillance de la disponibilité des services (Web, base de données, email, etc.).
- **Surveillance des réseaux** : Surveillance des équipements réseau (routeurs, switches, etc.), de la bande passante et des erreurs réseau.
- **Surveillance de la sécurité** : Suivi des logs, des tentatives d'intrusion et des comportements suspects.

---

2. Création d'un Monitor : Processus étape par étape

A. Définir les objectifs de surveillance

Avant de commencer à créer un monitor, il est essentiel de définir les objectifs de la surveillance :

- **Quels systèmes doivent être surveillés ?** (serveurs, bases de données, équipements réseau).
- **Quels paramètres de performance doivent être mesurés ?** (utilisation du CPU, mémoire, espace disque, latence réseau).
- **Quels seuils déclencheront des alertes ?** (par exemple, 90% d'utilisation du CPU ou moins de 10% d'espace disque libre).

Exemple : Si vous souhaitez surveiller un serveur Web, vous pouvez vouloir suivre l'utilisation du CPU, la mémoire, l'espace disque et la disponibilité du service HTTP (port 80).

B. Choisir un outil de monitoring

Il existe de nombreux outils de monitoring disponibles pour aider à créer des monitors. Parmi les outils populaires, on trouve :

- **Nagios** : Un des outils les plus connus pour le monitoring des systèmes et services, très flexible et extensible.
- **Zabbix** : Un outil de surveillance open-source, avec une interface web et une configuration facile.
- **Prometheus** : Spécialisé dans la surveillance des systèmes basés sur des séries temporelles (très utilisé avec **Grafana** pour visualiser les données).
- **Grafana** : Un outil de visualisation des métriques, souvent utilisé avec Prometheus pour afficher des graphiques de performance.

C. Configurer un monitor avec un outil de monitoring

Nous allons maintenant détailler la création d'un monitor avec **Nagios** comme exemple, mais le processus est similaire avec d'autres outils.

1. **Installer Nagios (sur un serveur Linux)** :
   - Installez le serveur Nagios et les plugins nécessaires pour surveiller les services et les hôtes.

```
sudo apt update
sudo apt install nagios3 nagios-plugins
```

2. **Configurer les hôtes à surveiller** :
   - Les **hôtes** représentent les serveurs ou périphériques réseau que vous souhaitez surveiller. Pour chaque hôte, vous devez définir les services que vous voulez surveiller (ex : SSH, HTTP, ICMP).
   - Dans Nagios, vous définissez les hôtes dans un fichier de configuration situé dans `/etc/nagios3/conf.d/` (par exemple `hosts.cfg`). Exemple de configuration d'un hôte (un serveur Web) :

```
define host{
    use                     generic-host
    host_name               webserver1
    alias                   Serveur Web 1
    address                 192.168.1.10
    }
```

3. **Définir les services à surveiller** : Vous pouvez définir quels services seront surveillés sur chaque hôte (par exemple, HTTP, SSH, utilisation du disque). Exemple pour surveiller le service HTTP :

```
define service{
    use                     generic-service
    host_name               webserver1
    service_description     HTTP
    check_command           check_http
    }
```

4. **Configurer des alertes** : Configurez des alertes pour chaque service ou hôte. Vous pouvez définir des seuils à partir desquels Nagios enverra une notification par email ou SMS (par exemple, si l'utilisation du CPU dépasse 90% ou si le service HTTP est en panne). Exemple pour configurer une alerte par email :

```
define contact{
    contact_name            admin
    alias                   Administrator
    email                   admin@monentreprise.com
    service_notification_period   24x7
    }
```

5. **Redémarrer Nagios pour appliquer les modifications** : Après avoir modifié la configuration, redémarrez le service Nagios pour appliquer les nouveaux paramètres :

```
sudo systemctl restart nagios3
```

6. **Vérifier les services surveillés** : Utilisez l'interface web de Nagios pour voir les statistiques et les alertes générées par les services surveillés. Par défaut, l'interface web est accessible via :

   http://<IP_du_serveur_Nagios>/nagios3

---

3. Types de Monitoring à mettre en place

A. Surveillance de la performance du serveur

Les systèmes doivent être surveillés pour des paramètres tels que :

- **Utilisation du CPU** : Suivi de la charge processeur pour détecter les pics d'activité.
- **Mémoire** : Suivi de l'utilisation de la mémoire pour détecter les fuites ou les surcharges.
- **Espace disque** : Surveillance de l'utilisation de l'espace disque pour éviter les interruptions de service.
- **Charge du système** : Calcul de la charge moyenne du système sur 1, 5 et 15 minutes.

B. Surveillance de la disponibilité des services

Vous devez également vérifier la disponibilité des services critiques sur vos serveurs :

- **HTTP/HTTPS** : Suivi de l'état du serveur Web (port 80/443).
- **SSH** : Vérification de l'accès SSH pour les administrateurs.
- **Base de données** : Vérification que les services de base de données (MySQL, PostgreSQL, etc.) sont actifs.
- **Mail** : Surveillance des services de messagerie (SMTP, IMAP, etc.).

C. Surveillance des équipements réseau

Les équipements réseau tels que les routeurs, switches et firewalls peuvent être surveillés pour les paramètres suivants :

- **Disponibilité** : Ping du périphérique pour vérifier qu'il est accessible.
- **Utilisation de la bande passante** : Vérification de l'utilisation de la bande passante pour éviter les goulots d'étranglement.
- **Erreurs réseau** : Surveillance des erreurs de transmission de données.

D. Surveillance des logs

Surveiller les logs des systèmes et applications pour détecter des anomalies de sécurité, des erreurs ou des comportements suspects. Cela inclut l'utilisation de **Syslog** et d'outils comme **ELK Stack** (Elasticsearch, Logstash, Kibana).

---

4. Configurer des alertes et notifications

A. Niveaux de gravité des alertes

Les alertes peuvent être classées selon leur gravité :

- **Critical** : Des problèmes majeurs affectent la disponibilité du service.
- **Warning** : Des problèmes mineurs qui n'affectent pas encore la disponibilité.
- **Info** : Informations générales qui peuvent être utilisées pour le diagnostic.

B. Canaux de notification

Les alertes peuvent être envoyées par :

- **Email** : Notification par courrier électronique.
- **SMS** : Via un service SMS pour les alertes urgentes.
- **Slack/Teams** : Notifications dans des canaux de messagerie d'équipe.
- **Webhook/Rest API** : Notifications via des APIs pour l'intégration avec d'autres outils.

Module 5 : Les fonctionnalités d'un MDM (Mobile Device Manager)

Objectifs pédagogiques

À la fin de ce module, vous serez capable de :

- Comprendre le rôle et l'importance d'un MDM dans la gestion des appareils mobiles.
- Identifier les fonctionnalités clés d'un MDM.
- Configurer et administrer un MDM pour gérer les appareils mobiles dans une organisation.
- Implémenter des politiques de sécurité et de gestion via un MDM.
- Assurer la conformité et la sécurité des appareils mobiles dans l'entreprise.

1. Introduction au MDM (Mobile Device Management)

A. Qu'est-ce qu'un MDM ?

Un **MDM** (Mobile Device Management) est un système ou un logiciel qui permet aux entreprises de gérer, sécuriser et contrôler les appareils mobiles (smartphones, tablettes, ordinateurs portables, etc.) utilisés par les employés. Ces appareils peuvent être fournis par l'entreprise (BYOD - Bring Your Own Device) ou appartenir à l'entreprise.

L'objectif principal d'un MDM est de :

- **Gérer les appareils mobiles** : Assurer que tous les appareils respectent les normes et politiques de l'entreprise.
- **Sécuriser les appareils** : Protéger les données de l'entreprise et assurer la conformité.
- **Optimiser la gestion des appareils** : Réduire les risques, améliorer l'efficacité et faciliter la maintenance des appareils.

B. Pourquoi utiliser un MDM ?

L'utilisation d'un MDM présente plusieurs avantages, notamment :

- **Sécurisation des données** : Protection des informations sensibles, surtout dans un environnement mobile où les appareils peuvent être facilement perdus ou volés.
- **Gestion centralisée** : Permet de gérer tous les appareils à partir d'une interface centralisée, réduisant ainsi la complexité de gestion des appareils mobiles dans l'entreprise.
- **Conformité** : Le MDM assure que les appareils respectent les normes de sécurité de l'entreprise, ce qui est crucial pour la conformité avec les réglementations telles que le RGPD.
- **Optimisation des coûts** : Une gestion efficace des appareils peut réduire les coûts liés à la maintenance et à la gestion des appareils.

2. Fonctionnalités principales d'un MDM

A. Enrôlement et gestion des appareils

Une des premières étapes dans l'utilisation d'un MDM est l'enrôlement des appareils mobiles dans le système.

1. **Enrôlement automatique ou manuel des appareils** :
    - **Enrôlement manuel** : L'utilisateur doit saisir un code ou utiliser un processus pour enregistrer son appareil dans le MDM.

- **Enrôlement automatique** : L'entreprise peut configurer des systèmes de gestion qui permettent d'enrôler les appareils en masse via un serveur ou une plateforme dédiée.

2. **Gestion des profils d'appareils** :
   - Les profils de configuration permettent de définir les paramètres et restrictions des appareils (Wi-Fi, VPN, gestion des applications, etc.). Ces profils peuvent être appliqués à un groupe d'appareils selon des critères définis par l'entreprise.
3. **Type d'enrôlement** :
   - **Enrôlement basé sur l'entreprise** : L'entreprise gère entièrement les appareils (contrôle total).
   - **Enrôlement basé sur l'utilisateur** : L'utilisateur gère ses propres appareils, mais l'entreprise peut appliquer des restrictions et des politiques de sécurité.

B. Sécurisation des appareils

L'une des fonctionnalités clés du MDM est la sécurité. Un MDM permet de déployer des stratégies de sécurité sur les appareils mobiles.

1. **Authentification et gestion des mots de passe** :
   - Le MDM impose des politiques de mots de passe (longueur, complexité, expiration) et peut également activer l'authentification biométrique ou par code PIN.
2. **Chiffrement des données** :
   - Le MDM peut activer le chiffrement des données stockées sur l'appareil (telles que les fichiers, les emails, les messages) pour protéger les informations sensibles en cas de perte ou vol de l'appareil.
3. **Gestion des applications** :
   - Le MDM permet de contrôler les applications installées sur les appareils. Par exemple, il est possible de :
     - Déployer des applications sur les appareils.
     - Restreindre l'installation d'applications non approuvées.
     - Mettre à jour ou supprimer des applications à distance.
4. **Protection contre la perte ou le vol** :
   - **Localisation des appareils** : En cas de vol ou de perte, l'administrateur peut localiser l'appareil à distance via GPS.
   - **Effacement à distance (Remote Wipe)** : Si un appareil est perdu ou volé, l'administrateur peut effacer les données sensibles à distance pour éviter les fuites d'informations.
   - **Verrouillage à distance** : L'administrateur peut verrouiller l'appareil pour empêcher son utilisation non autorisée.

C. Gestion des connexions réseau

Le MDM peut gérer les connexions réseau des appareils mobiles pour garantir que les utilisateurs se connectent à des réseaux sécurisés.

1. **VPN (Virtual Private Network)** :
   - Le MDM peut déployer et configurer un VPN sur les appareils pour garantir que toutes les connexions à des réseaux externes soient sécurisées.
2. **Wi-Fi et réseaux mobiles** :
   - Le MDM permet de configurer automatiquement les paramètres Wi-Fi et les connexions mobiles (APN, paramètres de proxy, etc.) sur les appareils.

D. Gestion des politiques et des restrictions

Les politiques de sécurité et de gestion permettent de contrôler les actions possibles sur les appareils mobiles.

1. **Restrictions d'utilisation** :
    - Interdire l'accès à certaines applications (comme les réseaux sociaux) ou fonctionnalités (par exemple, l'appareil photo, le Bluetooth).
2. **Gestion des mises à jour** :
    - Forcer les mises à jour des systèmes d'exploitation et des applications pour s'assurer que tous les appareils soient à jour avec les derniers patchs de sécurité.
3. **Définir des politiques de géolocalisation** :
    - Implémenter des politiques basées sur la géolocalisation pour restreindre l'accès à certains services ou applications en fonction de la localisation de l'appareil.

E. Suivi et rapports

Les solutions MDM offrent des capacités de suivi et de génération de rapports sur l'utilisation des appareils, leur état de sécurité, les applications installées et bien plus.

1. **Suivi des appareils** :
    - Le MDM fournit une vue d'ensemble sur l'état des appareils (en ligne/hors ligne, dernières connexions, etc.).
    - Statistiques sur l'utilisation des applications, la consommation de batterie, et l'état de la sécurité des appareils.
2. **Rapports de conformité** :
    - Générer des rapports réguliers pour vérifier si les appareils respectent les politiques de sécurité et de gestion définies par l'entreprise.

---

3. Intégration avec d'autres systèmes

A. Intégration avec des systèmes de gestion des identités (IAM)

Les MDM modernes peuvent s'intégrer avec des systèmes de gestion des identités et d'accès (IAM) pour garantir que seuls les utilisateurs autorisés peuvent accéder aux ressources de l'entreprise via leurs appareils mobiles.

B. Intégration avec des outils de sécurité supplémentaires

Un MDM peut être couplé avec des solutions de sécurité supplémentaires, telles que des systèmes de prévention des intrusions (IDS/IPS), des solutions antivirus et des firewalls pour garantir une sécurité optimale des appareils.

C. Intégration avec des systèmes de gestion des applications mobiles (MAM)

Certains MDM offrent également des fonctionnalités de gestion des applications mobiles (MAM), permettant de gérer les applications installées sur les appareils, de contrôler les accès à ces applications, et de les sécuriser.

---

4. Exemples d'outils MDM populaires

- **Microsoft Intune** : Un MDM très utilisé dans les environnements Microsoft, qui permet de gérer les appareils mobiles, les applications et les politiques de sécurité.
- **VMware Workspace ONE** : Un MDM tout-en-un qui combine la gestion des appareils, des applications et des utilisateurs.
- **MobileIron** : Une solution de gestion des appareils et des applications mobiles, avec une forte orientation vers la sécurité.
- **AirWatch (acquis par VMware)** : Un autre produit MDM populaire, souvent utilisé dans des environnements BYOD.

5. Conclusion

A. Importance du MDM dans la sécurité et la gestion des appareils

Les appareils mobiles sont désormais essentiels pour le travail quotidien, mais leur gestion et leur sécurité sont cruciales. Un MDM est une solution indispensable pour garantir que tous les appareils utilisés dans l'entreprise respectent les politiques de sécurité, sont protégés contre les risques (perte, vol, attaques) et restent conformes aux normes internes.

B. Meilleures pratiques

- **Former les utilisateurs** à la gestion sécurisée de leurs appareils.
- **Appliquer des politiques de sécurité strictes**, mais équilibrées pour ne pas nuire à la productivité.
- **Effectuer des audits réguliers** des appareils et des données pour assurer la conformité.
- **Tenir les systèmes à jour** pour éviter les failles de sécurité.

Module 6 : Hypervision des systèmes et équipements réseau, journalisation

Objectifs pédagogiques

À la fin de ce module, vous serez capable de :

- Comprendre le rôle de l'hypervision dans la gestion des systèmes et des équipements réseau.
- Mettre en place des outils et des techniques d'hypervision pour suivre l'état des équipements.
- Utiliser des outils de journalisation pour suivre les événements système et réseau.
- Analyser les logs pour détecter les problèmes et assurer la sécurité.
- Gérer les alertes et les notifications liées aux événements enregistrés.

1. Introduction à l'Hypervision

A. Qu'est-ce que l'hypervision ?

L'**hypervision** est la pratique de surveiller et de gérer en temps réel tous les composants d'une infrastructure informatique, notamment les serveurs, les équipements réseau (commutateurs, routeurs, pare-feu), les services et les applications. Elle permet de garantir la disponibilité, la performance et la sécurité de l'infrastructure IT.

L'hypervision est souvent mise en œuvre via des outils qui collectent des données sur l'état des systèmes et les services afin de fournir une vue d'ensemble et des alertes en cas de défaillance ou d'anomalie.

B. Objectifs de l'hypervision

- **Suivre en temps réel** l'état des composants de l'infrastructure.
- **Identifier et résoudre les problèmes rapidement** avant qu'ils n'affectent les utilisateurs finaux.
- **Optimiser les performances** du réseau et des systèmes en analysant les données recueillies.
- **Améliorer la sécurité** en détectant les anomalies, comme les attaques ou les tentatives d'intrusion.

C. Exemples d'outils d'hypervision

Parmi les outils les plus populaires d'hypervision, on trouve :

- **Nagios** : Un outil de surveillance des systèmes et des services très flexible.
- **Zabbix** : Un outil de monitoring avec une interface web pour la gestion centralisée.
- **Prometheus** : Utilisé principalement pour la surveillance des infrastructures basées sur des séries temporelles.
- **Grafana** : Un outil de visualisation de données, souvent intégré à Prometheus pour une surveillance détaillée.

---

2. Surveillance des systèmes et des équipements réseau

A. Types de systèmes et équipements à surveiller

1. **Les serveurs** : Surveillance de l'utilisation des ressources comme le CPU, la mémoire, le disque et la charge du système.
2. **Les équipements réseau** :
    - **Commutateurs (switches)** : Vérification de la disponibilité, de la performance du port, de l'utilisation de la bande passante.
    - **Routeurs** : Surveillance de la latence réseau, des erreurs de transmission et de la qualité de service.
    - **Pare-feu** : Suivi des règles de filtrage, de la charge du pare-feu et des alertes de sécurité.
3. **Les applications** : Surveillance des services web, des bases de données, des serveurs de messagerie, etc.

B. Collecte de données de performance

Les données de performance permettent de surveiller la santé des systèmes et des équipements réseau. Elles comprennent généralement :

- **Utilisation du CPU** : Indicateur de la charge de traitement des serveurs.
- **Utilisation de la mémoire** : Indicateur de la capacité mémoire disponible pour le système.
- **Espace disque** : Indicateur de l'espace utilisé et libre sur les disques.
- **Bande passante réseau** : Indicateur de l'utilisation des réseaux et des connexions.
- **Latence et temps de réponse** : Mesure de la réactivité des systèmes et des services.

C. Surveillance des services réseau

Les services sont des applications essentielles qui tournent sur des serveurs et des équipements réseau. Leur surveillance est essentielle pour s'assurer que l'infrastructure fonctionne correctement. Par exemple :

- **HTTP/HTTPS** : Vérification de la disponibilité des serveurs web.
- **DNS** : Surveillance de la résolution des noms de domaine.
- **SSH** : Vérification de l'accessibilité des serveurs via le protocole sécurisé SSH.

D. Alertes et notifications

L'hypervision permet de définir des seuils d'alerte pour chaque paramètre surveillé. Si un seuil est dépassé (par exemple, l'utilisation du CPU dépasse 90 %), le système déclenche une alerte. Ces alertes peuvent être envoyées via :

- **Email** : Envoi automatique d'un email en cas d'anomalie.
- **SMS** : Alerte via un service de messagerie pour les incidents critiques.
- **Applications de messagerie** : Intégration avec des plateformes comme Slack ou Microsoft Teams.
- **SNMP (Simple Network Management Protocol)** : Utilisation de ce protocole pour les équipements réseau afin d'envoyer des alertes.

3. Journalisation des événements système et réseau

A. Qu'est-ce que la journalisation ?

La **journalisation** consiste à enregistrer les événements et les actions effectuées sur un système informatique ou un réseau. Les logs (ou journaux) contiennent des informations détaillées sur les événements, erreurs, avertissements, et autres messages système importants qui se produisent sur l'infrastructure.

Les logs sont essentiels pour :

- **Analyser les incidents** : Comprendre la cause d'une défaillance ou d'une intrusion.
- **Auditer les actions des utilisateurs** : Suivre les activités des utilisateurs pour des raisons de sécurité et de conformité.
- **Détecter les anomalies** : Repérer les comportements suspects ou anormaux.

B. Types de journaux à collecter

1. **Logs des serveurs** :
    - **Logs système** : Contiennent des informations sur l'état du système d'exploitation.
    - **Logs des applications** : Relèvent des événements spécifiques liés à une application (par exemple, les erreurs de base de données).
2. **Logs des équipements réseau** :
    - **Logs de pare-feu** : Contiennent des informations sur les tentatives d'accès et les filtres appliqués.
    - **Logs de switches et de routeurs** : Incluent des informations sur la performance du réseau et les erreurs de transmission.
3. **Logs de sécurité** :
    - **Authentification** : Tentatives de connexion réussies ou échouées.
    - **Accès aux fichiers** : Journaux détaillant les accès aux fichiers et aux répertoires partagés.

C. Collecte et centralisation des logs

Il est essentiel de centraliser la collecte des logs afin de faciliter leur gestion et leur analyse. Voici quelques solutions pour cela :

- **Syslog** : Un protocole standard de journalisation utilisé pour collecter des logs d'équipements réseau, de serveurs, etc.
- **SIEM (Security Information and Event Management)** : Outils comme **Splunk** ou **ELK Stack (Elasticsearch, Logstash, Kibana)** permettent de centraliser, analyser et visualiser les logs.

  Par exemple, **Logstash** collecte et transmet les logs à **Elasticsearch**, où ils sont indexés et stockés. Puis, **Kibana** est utilisé pour visualiser et analyser les logs via des dashboards interactifs.

D. Analyse des logs

Les logs contiennent des informations essentielles pour diagnostiquer les problèmes. Une analyse efficace des logs peut aider à :

- **Trouver la cause racine des problèmes** (pannes, erreurs d'application, etc.).
- **Détecter les tentatives d'intrusion** et autres événements de sécurité.
- **Optimiser les performances** en identifiant les goulots d'étranglement.

L'analyse des logs se fait en recherchant des motifs spécifiques ou des anomalies dans les journaux. Cela inclut :

- **Analyse des codes d'erreur** : Identifier les erreurs fréquentes et leur origine.
- **Suivi des anomalies de performance** : Rechercher des périodes de latence ou d'utilisation excessive des ressources.
- **Audit de sécurité** : Vérifier les logs de connexion pour détecter des tentatives d'intrusion ou des actions non autorisées.

E. Mise en place des alertes sur les logs

Une autre fonctionnalité clé des systèmes de journalisation est la capacité à configurer des alertes automatiques sur certains événements. Par exemple :

- **Événements critiques** : Échecs de connexion répétés, attaques par déni de service (DoS), ou problèmes de serveur.
- **Avertissements** : Utilisation élevée du disque ou du CPU, par exemple.

Ces alertes peuvent être envoyées par email, SMS, ou via une application de messagerie, et permettent une intervention rapide en cas de problème.

---

4. Intégration de l'hypervision et de la journalisation dans une stratégie de gestion d'incidents

A. Processus de gestion des incidents

Lorsqu'un incident survient, il est crucial de disposer d'un processus bien défini pour :

- **Recevoir les alertes** générées par l'hypervision ou la journalisation.
- **Diagnostiquer rapidement** l'incident en analysant les logs et les données de performance.
- **Prendre des mesures correctives** pour résoudre l'incident et restaurer le service.
- **Documenter l'incident** pour les audits futurs et l'amélioration continue.

B. Automatisation de la gestion des incidents

Certains outils de gestion des incidents peuvent automatiser le processus, en utilisant les données d'hypervision et les logs pour :

- **Ouvrir un ticket automatiquement** lorsqu'une alerte est déclenchée.
- **Exécuter des scripts correctifs** pour résoudre des problèmes récurrents ou simples.
- **Notifier les équipes** concernées pour qu'elles interviennent rapidement.

Module 7 : Hypervision de l'infrastructure : Syslog, protocoles de supervision et d'analyse

Objectifs pédagogiques

À la fin de ce module, vous serez capable de :

- Comprendre les rôles de Syslog et des protocoles de supervision dans l'hypervision d'une infrastructure.
- Installer et configurer un serveur Syslog pour la collecte des logs.
- Mettre en place des solutions de supervision d'infrastructure (SNMP, ICMP, WMI, etc.).
- Analyser les données collectées pour détecter des anomalies et améliorer la gestion des incidents.

1. Introduction à l'Hypervision de l'infrastructure

A. Qu'est-ce que l'hypervision de l'infrastructure ?

L'**hypervision de l'infrastructure** est une approche qui permet de suivre en temps réel l'état et la performance de tous les composants d'une infrastructure informatique, incluant les serveurs, les équipements réseau, les services et les applications. Elle vise à garantir la disponibilité, la sécurité, et la performance de l'ensemble du système.

Cela inclut :

- La **collecte des données de performance** de chaque composant.
- L'utilisation de **protocoles de supervision** pour obtenir des informations détaillées.
- La **centralisation des logs** pour faciliter la détection des incidents et des anomalies.

Les principaux protocoles utilisés pour l'hypervision sont **Syslog**, **SNMP**, **ICMP**, et **WMI**, chacun ayant des fonctions spécifiques dans la collecte et la supervision des données.

B. Rôle des protocoles de supervision

Les protocoles de supervision sont des mécanismes utilisés pour collecter et transmettre des informations depuis les systèmes surveillés (serveurs, équipements réseau, applications). Ils permettent de centraliser la gestion des événements et de fournir une vue d'ensemble sur l'état de l'infrastructure.

Les protocoles de supervision les plus utilisés sont :

- **Syslog** : Pour la gestion des logs des équipements réseau et des serveurs.
- **SNMP (Simple Network Management Protocol)** : Utilisé principalement pour surveiller les équipements réseau tels que les routeurs, commutateurs, et autres appareils réseau.
- **ICMP (Internet Control Message Protocol)** : Utilisé pour vérifier la disponibilité d'un périphérique (via des "pings").
- **WMI (Windows Management Instrumentation)** : Permet la supervision des systèmes Windows à distance.

2. Le rôle de Syslog dans l'hypervision

A. Qu'est-ce que Syslog ?

Syslog est un protocole standard de journalisation des événements sur un réseau informatique. Il permet de collecter et de transmettre des informations de logs provenant de diverses sources (serveurs, équipements réseau, systèmes d'exploitation, etc.). Les logs générés peuvent inclure des événements systèmes, des alertes de sécurité, des erreurs, et d'autres types de messages utiles pour la gestion et la surveillance de l'infrastructure.

B. Composants d'un système Syslog

Un système Syslog se compose de trois composants principaux :

1. **Émetteur (ou générateur de logs)** : Il s'agit des serveurs, des équipements réseau ou des applications qui génèrent les logs.
2. **Serveur Syslog** : Ce serveur reçoit et centralise les logs envoyés par les émetteurs. Il peut également stocker les logs dans un fichier ou une base de données pour une analyse ultérieure.
3. **Client Syslog** : Le client est l'application ou le système qui envoie les logs au serveur Syslog.

C. Configuration d'un serveur Syslog

Pour mettre en place un serveur Syslog, vous devez :

1. Installer un serveur Syslog (par exemple, **rsyslog** ou **syslog-ng**).
2. Configurer les périphériques ou serveurs à envoyer leurs logs vers ce serveur.
3. Configurer les filtres et les règles sur le serveur Syslog pour gérer et stocker les logs de manière efficace.

Exemple de configuration avec rsyslog :

- Installer rsyslog : `sudo apt install rsyslog`
- Configurer le fichier `/etc/rsyslog.conf` pour activer la réception des logs à distance.

```
Graphql

# Activer la réception des logs via UDP (port 514)
module(load="imudp")
input(type="imudp" port="514")
```

- Redémarrer le service : `sudo systemctl restart rsyslog`

Les équipements (routeurs, commutateurs, serveurs) doivent être configurés pour envoyer leurs logs vers le serveur Syslog en utilisant des outils comme `logger` sur Linux ou `Eventlog` sur Windows.

---

3. Protocoles de supervision d'infrastructure

A. SNMP (Simple Network Management Protocol)

SNMP est un protocole de gestion utilisé principalement pour surveiller les équipements réseau. Il permet aux administrateurs de réseau de récupérer des informations sur l'état des équipements réseau, tels que la disponibilité, l'utilisation du processeur, l'utilisation de la bande passante, etc.

Les versions de SNMP :

- **SNMPv1 et SNMPv2c** : Peu sécurisé, car les informations de gestion (comme les mots de passe) sont envoyées en texte clair.
- **SNMPv3** : Offre des fonctionnalités de sécurité améliorées, comme le chiffrement et l'authentification.

Fonctionnement de SNMP :

1. **Agent SNMP** : Un agent est installé sur l'équipement réseau et collecte des informations sur l'état de l'équipement.
2. **Gestionnaire SNMP** : Le gestionnaire est un serveur ou une station de travail qui interroge les agents SNMP pour collecter les informations.

Exemple de configuration d'un agent SNMP sur un switch :

```
pgsql
# Activer SNMP v2c avec la communauté "public"
snmp-server community public ro
```

B. ICMP (Internet Control Message Protocol)

ICMP est un protocole utilisé pour envoyer des messages de contrôle, tels que les "pings", afin de vérifier la connectivité et la latence entre des équipements sur le réseau.

Les pings sont utilisés pour tester si un équipement est joignable et mesurer le temps de réponse, ce qui est essentiel pour vérifier l'état d'un réseau.

Exemple de commande ping :

```
Nginx

ping 192.168.1.1
```

Cela enverra des paquets ICMP au périphérique avec l'adresse IP spécifiée et affichera le temps de réponse.

C. WMI (Windows Management Instrumentation)

WMI est un ensemble d'outils Microsoft permettant de surveiller et de gérer des systèmes Windows à distance. WMI fournit des informations détaillées sur les composants matériels, les applications et les services d'un système Windows.

WMI peut être utilisé pour :

- Vérifier l'utilisation des ressources (processeur, mémoire, disque).
- Surveiller les journaux d'événements du système.
- Lancer des scripts et des actions à distance.

D. NetFlow et sFlow

Ces deux protocoles sont utilisés pour la surveillance du trafic réseau. **NetFlow** (de Cisco) et **sFlow** permettent de collecter des informations détaillées sur les paquets de données circulant dans le réseau, afin de surveiller les performances du réseau, la bande passante utilisée, et les anomalies de trafic.

---

4. Collecte et Analyse des données

A. Centralisation des données de supervision

Pour une gestion efficace des événements, il est essentiel de centraliser les données collectées via Syslog, SNMP, ICMP, et autres protocoles. Cela peut être réalisé à l'aide d'outils comme :

- **Splunk** : Outil de collecte, d'analyse et de visualisation des logs.
- **Elasticsearch/Logstash/Kibana (ELK Stack)** : Permet de centraliser, d'analyser et de visualiser les logs de manière très efficace.
- **Grafana** : Utilisé pour la visualisation des métriques en temps réel, notamment en combinaison avec Prometheus pour la collecte de données de performance.

B. Analyse des données de supervision

Une fois que les données sont centralisées, il est crucial de les analyser pour détecter des anomalies, résoudre des problèmes ou optimiser les performances. Voici quelques techniques d'analyse :

- **Suivi des anomalies de performance** : Analyse des graphiques de bande passante, de latence ou de charge des serveurs pour détecter les goulots d'étranglement.
- **Audit de sécurité** : Recherche des événements suspects dans les logs système et réseau (tentatives d'accès non autorisées, défaillances des services de sécurité).
- **Analyse des erreurs** : Identification des messages d'erreur dans les logs Syslog et des équipements SNMP pour résoudre rapidement les pannes.

---

5. Conclusion

A. Récapitulatif des points clés

- **Syslog** permet la centralisation des logs et est essentiel pour l'analyse des événements dans l'infrastructure.
- **SNMP** est un protocole clé pour surveiller les équipements réseau.
- **ICMP** est utilisé pour vérifier la connectivité réseau de base.
- **WMI** permet de surveiller les systèmes Windows à distance.
- La **centralisation et l'analyse** des données collectées via ces protocoles sont cruciales pour garantir la sécurité et la performance de l'infrastructure.

B. Meilleures pratiques

- **Centraliser les logs** et les données de performance pour faciliter leur gestion.
- **Utiliser plusieurs protocoles de supervision** en fonction des types d'équipements (Syslog, SNMP, ICMP, etc.).
- **Analyser régulièrement les données** pour détecter rapidement les anomalies.
- **Mettre en place des alertes** pour être informé immédiatement en cas de problème.