

Architectures distribuées

Master 1 génie de l'informatique logicielle

Maintenance et monitoring

Présenté par : Lydia KAHOUADJI & Luc Perin PANTA

20 mars 2024



UFR Sciences
et **Techniques**

- 1 Contexte
- 2 Problématique
- 3 Définitions
- 4 Maintenance des Applications
- 5 Stratégies de Mise à Jour
- 6 Gestion des Configurations
- 7 Monitoring des Applications
- 8 Pourquoi le monitoring ?
- 9 Différents types de monitoring
- 10 Différents types de monitoring
- 11 Métriques et logs
- 12 Alerting dans le Monitoring des Applications
- 13 Outils de Monitoring

- L'informatique moderne repose de plus en plus sur l'utilisation d'applications déployées dans des environnements dynamiques et évolutifs.
- Les entreprises adoptent des architectures basées sur les microservices et utilisent des plateformes de conteneurisation telles que Docker et Kubernetes pour gérer leurs applications.

- Avec la complexité croissante des architectures logicielles, la maintenance et le monitoring des applications deviennent des défis majeurs pour les équipes informatiques.
- Comment assurer la disponibilité, la performance et la sécurité des applications déployées dans des environnements dynamiques comme Kubernetes ?

Maintenance

La maintenance des applications dans un environnement Kubernetes fait référence aux actions préventives et correctives nécessaires pour garantir que les applications fonctionnent de manière fiable, sécurisée et optimale. Cela comprend la mise à jour des logiciels, la gestion des configurations et la résolution des problèmes de performance.

Monitoring

Le monitoring des applications dans un environnement Kubernetes consiste à surveiller en temps réel les performances, la disponibilité et la santé des applications. Cela implique la collecte et l'analyse de métriques, de journaux et d'événements pour identifier les problèmes potentiels et prendre des mesures correctives.

La maintenance des applications est un processus essentiel pour garantir leur bon fonctionnement, leur sécurité et leur évolutivité tout au long de leur cycle de vie. Cela implique une série d'activités préventives et correctives visant à identifier, résoudre et prévenir les problèmes potentiels.

- **La maintenance proactive** vise à prévenir les incidents et les pannes avant qu'ils ne se produisent, en surveillant et en corrigeant les signes avant-coureurs de dysfonctionnement.
- **La maintenance corrective** intervient après qu'un problème est survenu, visant à restaurer les fonctionnalités normales de l'application dans les plus brefs délais.

- **Mises à jour automatiques** : Les mises à jour sont appliquées automatiquement dès leur disponibilité, ce qui permet de maintenir les applications à jour sans intervention manuelle.
- **Mises à jour planifiées** : Les mises à jour sont programmées pour être appliquées à des moments spécifiques, généralement en dehors des heures de pointe, pour minimiser les perturbations.
- **Mises à jour progressives** : Les mises à jour sont déployées de manière progressive sur un sous-ensemble d'utilisateurs ou de machines, ce qui permet de détecter et de corriger rapidement les problèmes potentiels.

Utilisation de la Gestion des Configurations

- **Gestion centralisée des configurations** : Les outils de gestion des configurations permettent de stocker et de gérer toutes les configurations d'application de manière centralisée, ce qui facilite la gestion des environnements complexes.
- **Versionnement des configurations** : Les modifications apportées aux configurations sont versionnées, ce qui permet de suivre les changements, de revenir à des versions précédentes si nécessaire, et d'appliquer des configurations spécifiques à différentes branches ou environnements.
- **Distribution des configurations** : Les configurations peuvent être distribuées de manière fiable et cohérente à travers différents environnements, ce qui garantit que toutes les instances de l'application fonctionnent avec la même configuration.

- Le monitoring d'applications est la pratique de collecter et d'analyser des données pour surveiller la santé et les performances des applications. Il permet de détecter les problèmes avant qu'ils ne impactent les utilisateurs. Il aide à identifier les goulots d'étranglement et les points d'amélioration.

Pourquoi le monitoring ?

- Améliorer la fiabilité et la disponibilité des applications.
- Réduire les temps d'arrêt et les coûts de maintenance.
- Optimiser les performances et l'utilisation des ressources.
- Assurer la sécurité et la conformité des applications.
- Meilleure prise de décision basée sur des données.

Différents types de monitoring

- **Monitoring des performances** : Surveiller les temps de réponse, l'utilisation du CPU, la mémoire, etc.
- **Monitoring de la disponibilité** : Détecter les pannes et les interruptions de service.
- **Monitoring de l'expérience utilisateur** : Mesurer la satisfaction des utilisateurs et identifier les points d'amélioration.
- **Monitoring de la sécurité** : Surveiller les menaces et les incidents de sécurité.
- **Monitoring des logs** : Analyser les logs pour identifier les erreurs et les problèmes potentiels.

Le monitoring des performances vise à surveiller et à mesurer les performances des systèmes informatiques, notamment :

- Temps de réponse des applications.
- Utilisation du CPU, de la mémoire et du disque.
- Taux de transfert réseau.

Il permet d'identifier les goulots d'étranglement, d'optimiser les ressources et d'améliorer les performances globales du système.

Le monitoring de la disponibilité vise à détecter et à signaler les pannes et les interruptions de service, en surveillant :

- Disponibilité des serveurs et des services.
- Temps de réponse des requêtes.
- Statut des connexions réseau.

Il permet de garantir que les applications et les services sont accessibles et fonctionnels pour les utilisateurs finaux.

Le monitoring de l'expérience utilisateur vise à mesurer la satisfaction des utilisateurs et à identifier les points d'amélioration, en surveillant :

- Temps de chargement des pages web.
- Taux de conversion des transactions.
- Réactions des utilisateurs aux nouvelles fonctionnalités.

Il permet d'optimiser l'ergonomie et la convivialité des applications pour améliorer l'expérience globale des utilisateurs.

Le monitoring de la sécurité vise à surveiller les menaces et les incidents de sécurité, en analysant :

- Activités anormales sur le réseau.
- Tentatives d'accès non autorisées.
- Utilisation suspecte des comptes utilisateurs.

Il permet de détecter rapidement les violations de sécurité et de prendre des mesures pour protéger les systèmes et les données contre les attaques.

Le monitoring des logs vise à analyser les logs générés par les applications et les systèmes informatiques, en recherchant :

- Erreurs et exceptions dans les logs.
- Tendances et modèles d'utilisation.
- Activités suspectes ou malveillantes.

Il permet de diagnostiquer les problèmes, de suivre les performances et de détecter les anomalies dans les systèmes informatiques.

Métriques

Les métriques sont des mesures quantitatives des performances et de l'état d'une application. Elles fournissent des données précises sur différents aspects de l'application, tels que le temps de réponse, l'utilisation des ressources, le nombre de requêtes traitées, etc. Les métriques sont généralement collectées à intervalles réguliers et utilisées pour surveiller les performances et identifier les tendances au fil du temps.

Logs

Les logs sont des enregistrements d'événements et d'erreurs générés par une application. Ils fournissent une trace détaillée des activités de l'application, y compris les opérations effectuées, les erreurs rencontrées et les transactions effectuées. Les logs sont essentiels pour le débogage des applications, la gestion des incidents et la conformité réglementaire. Ils permettent aux administrateurs système et aux développeurs de comprendre le comportement de l'application et de diagnostiquer les problèmes potentiels.

Les deux métriques et les logs sont essentiels pour une surveillance efficace des applications et des systèmes informatiques.

Alerting dans le Monitoring des Applications

Définition

L'alerting est un processus automatisé de détection et de notification des anomalies ou des événements indésirables dans le système. Il permet d'informer les opérateurs ou les administrateurs système des problèmes potentiels, afin qu'ils puissent prendre des mesures correctives rapidement.

Fonctionnement

L'alerting repose sur la surveillance continue des métriques ou des logs. Lorsqu'une condition prédéfinie est déclenchée, généralement basée sur des seuils de performance ou des motifs d'anomalie, un système d'alerting envoie des notifications aux personnes concernées, par exemple par e-mail, SMS ou intégration avec des outils de communication comme Slack.

Importance

L'alerting permet une réponse proactive aux incidents, réduisant ainsi les temps d'arrêt et minimisant l'impact sur les utilisateurs finaux. Il aide également à garantir que les problèmes critiques sont identifiés et traités rapidement, ce qui contribue à maintenir la disponibilité et les performances des applications.

Prometheus

Prometheus est un système open-source de monitoring et d'alerting. Il collecte les métriques des cibles configurées, stocke les données dans une base de données de séries temporelles, et permet la création de règles d'alerte pour détecter les anomalies. Prometheus est souvent utilisé pour surveiller les performances des applications et des infrastructures, en fournissant des métriques telles que le temps de réponse des requêtes, l'utilisation des ressources et le nombre de requêtes traitées.

Grafana

Grafana est une plateforme open-source de visualisation et de création de tableaux de bord. Elle est souvent utilisée en conjonction avec Prometheus pour créer des tableaux de bord personnalisés et des graphiques interactifs, permettant aux utilisateurs de surveiller et d'analyser les métriques des applications et des infrastructures. Grafana offre une grande flexibilité dans la création de graphiques et de tableaux de bord, avec une variété de visualisations disponibles pour représenter les données de manière claire et compréhensible.

ELK Stack (Elasticsearch, Logstash, Kibana)

ELK Stack est un ensemble d'outils utilisé pour la collecte, le traitement, le stockage et la visualisation des logs. Il comprend Elasticsearch pour le stockage et la recherche des logs, Logstash pour l'ingestion et le traitement des logs, et Kibana pour la visualisation et l'analyse des données. ELK Stack est souvent utilisé pour surveiller les logs des applications et des infrastructures, en permettant aux utilisateurs de rechercher, d'analyser et de visualiser les logs pour diagnostiquer les problèmes et détecter les anomalies.