

# Keynote

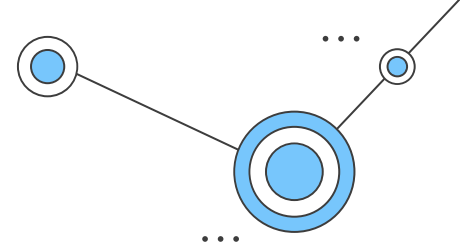
T-NSA\_800

# Sommaire

- ① Contexte du projet
- ② Présentation des outils
- ③ Architecture fonctionnelle
- ④ Dashboards
- ⑤ Alertes
- ⑥ Backup
- ⑦ Plan de gestion d'incidents
- ⑧ Retour d'expérience
- ⑨ Suggestions



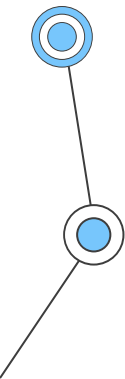
# Contexte

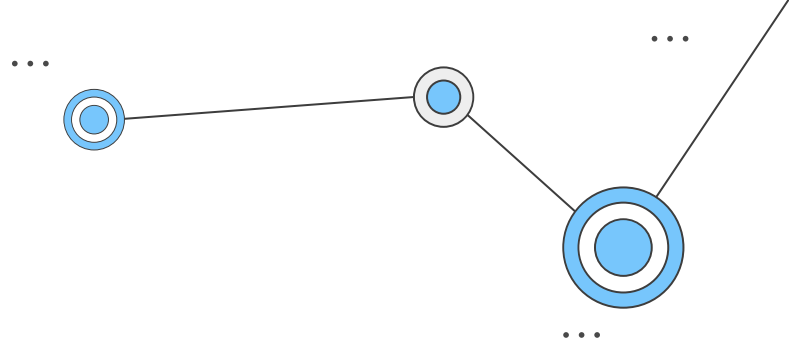


Le client cherche à avoir des métriques sur son infrastructure dans le but d'être réactif en cas d'incidents et de garantir un service hautement disponible.

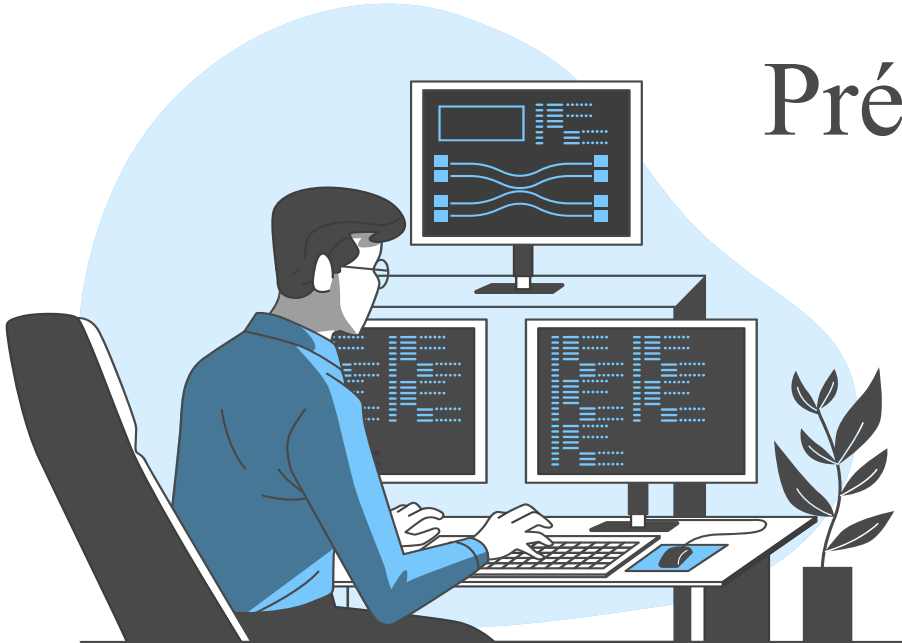
À cet effet, nous devons mettre en place:

- Des dashboards pratiques et concis;
  - Des alertes en cas d'anomalies;
- Des processus de sauvegarde de la bdd;
  - Un plan de gestion d'incident.





# Présentation des outils



# Outils de monitoring

1  
...

Prometheus

2  
...

Grafana

3  
...

Exporters

4  
...

Docker

5  
...

Alert manager



# Outil pour le monitoring



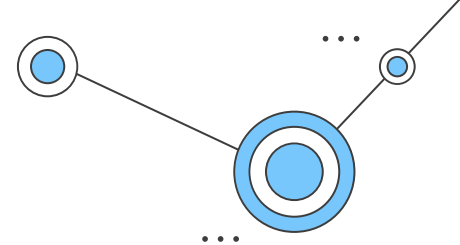
Prometheus

Prometheus est un outil de surveillance qui stocke des données numériques dans une base de données de séries temporelles.

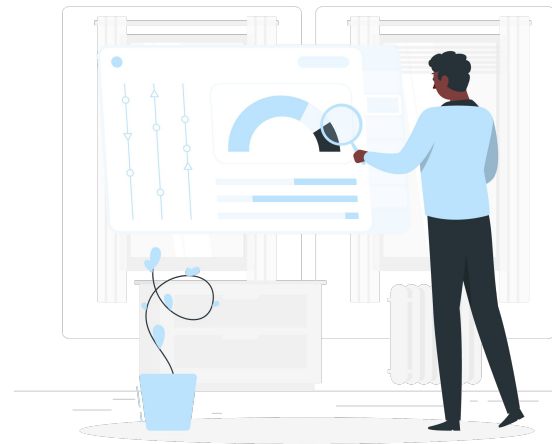


Collecte des métriques

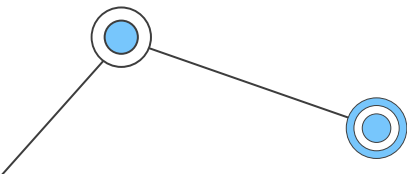
# Outil pour le monitoring



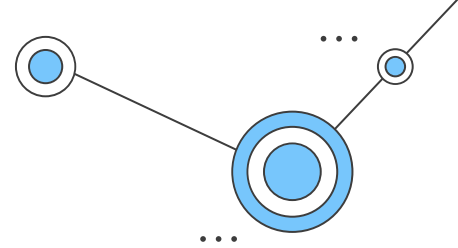
Grafana est une plateforme open source  
de visualisation de données et de  
surveillance.



Création des dashboards



# Exporters



Métriques systèmes

**Node exporter**



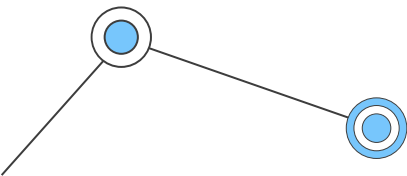
Métriques du serveur de bdd

**Postgres exporter**



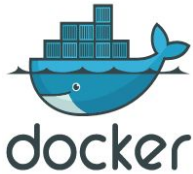
Métriques Docker

**Docker, cAdvisor**

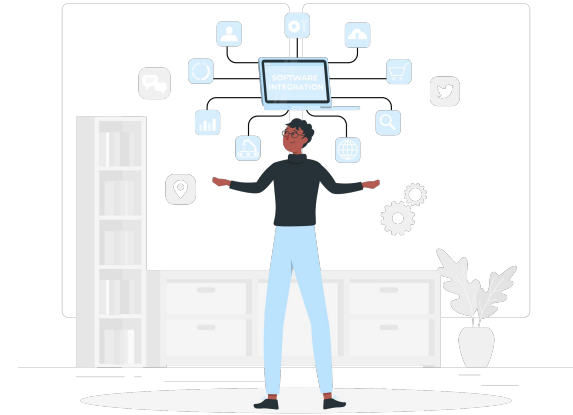
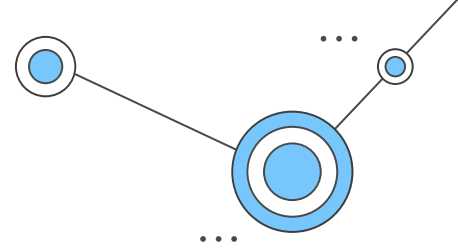




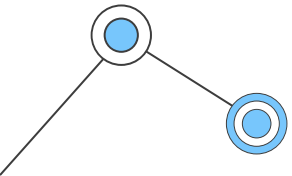
# Outil pour le monitoring



Docker est une plateforme de virtualisation et de gestion de conteneurs qui permet d'emballer une application et ses dépendances.



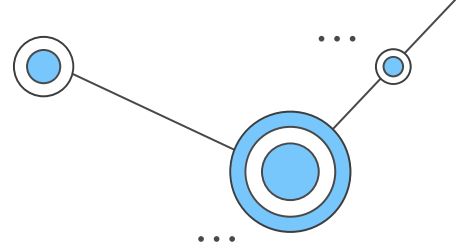
Intégration des outils de monitoring



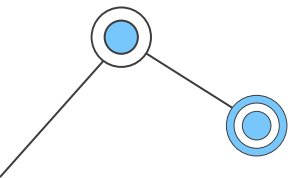
# Outil pour le monitoring



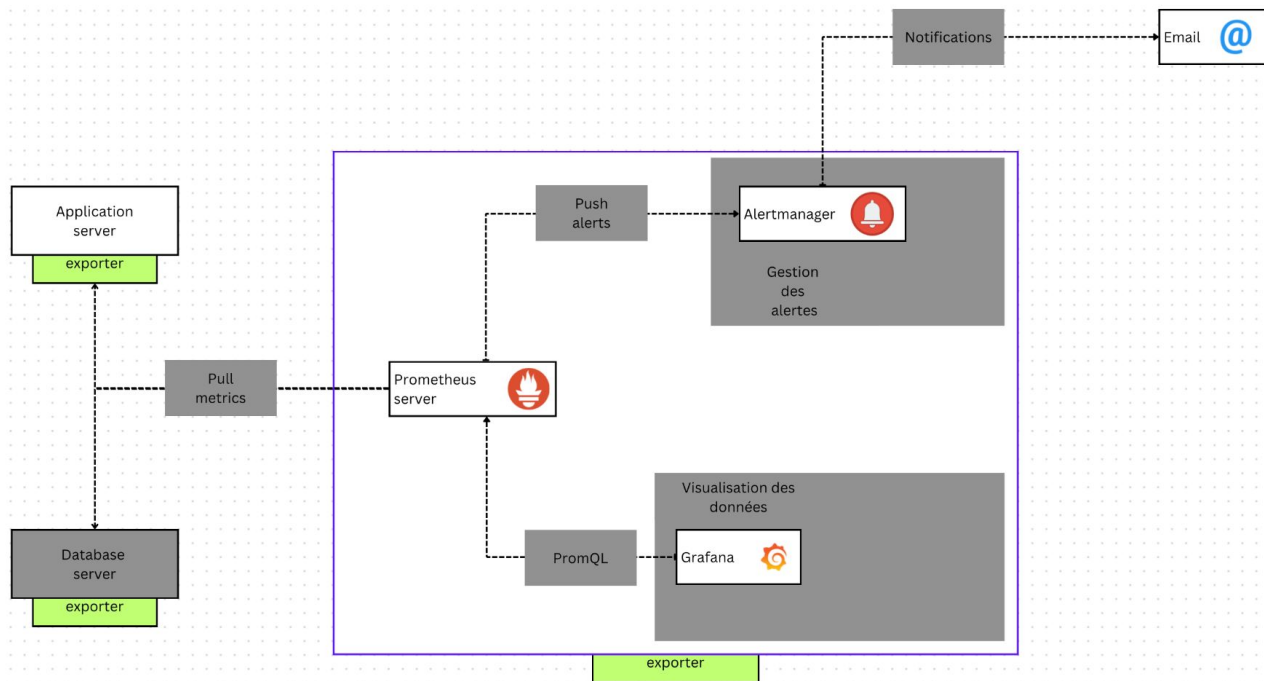
AlertManager est un composant de Prometheus qui gère les alertes envoyées par le serveur Prometheus



Configuration des alertes



# Architecture fonctionnelle



# Dashboards



Métriques systèmes

[https://tinyurl.com/  
yckw8mum](https://tinyurl.com/yckw8mum)

...



Métriques du serveur de bdd

[https://tinyurl.com/  
yc7sdtvx](https://tinyurl.com/yc7sdtvx)

...



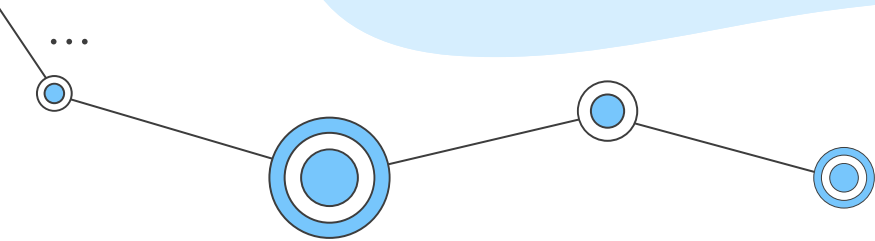
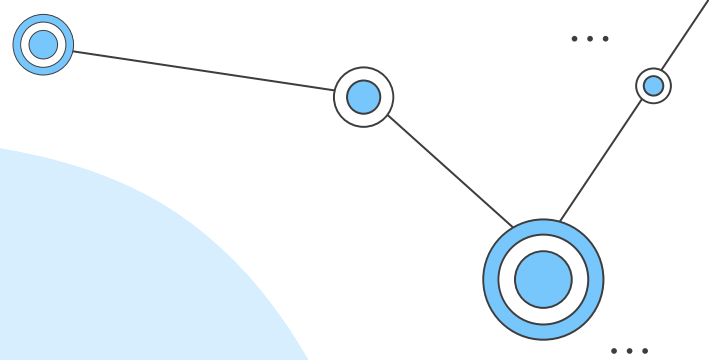
Métriques Docker

[https://tinyurl.com/  
mrynrv6m](https://tinyurl.com/mrynrv6m)

...



# Alertes



# Différents types d'alertes

## Etat des serveurs

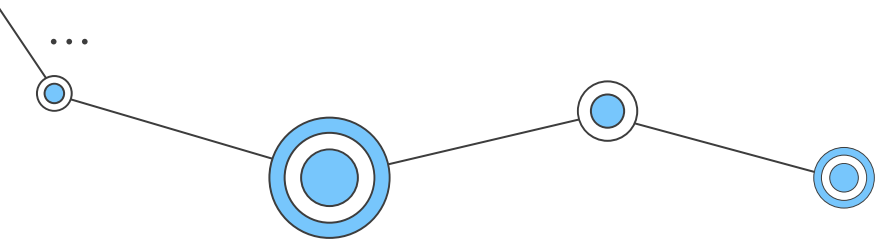
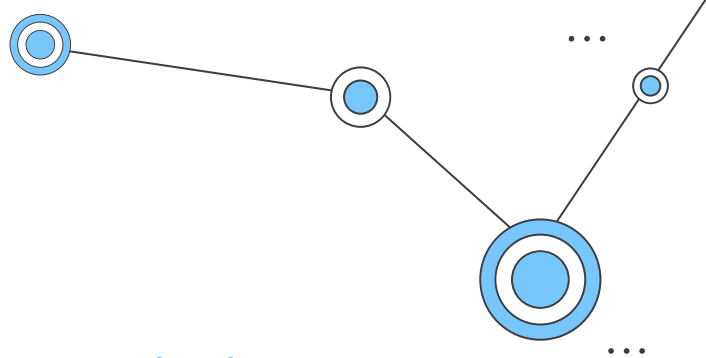
Cette alerte surveille l'état des différents serveurs hébergeant les applications.

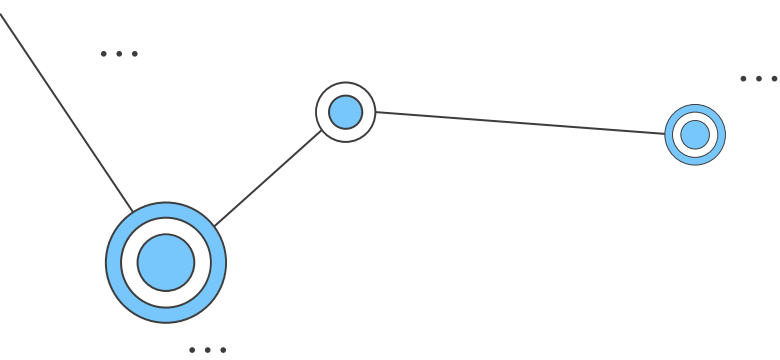
## Etat des services

Ce groupe d'alerte permet de surveiller l'état des différents services et applications ( Postgresql, application web ).

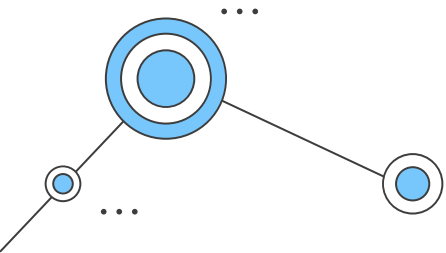
## Consommation des ressources

Ce groupe d'alerte permet de notifier une utilisation excessive des ressources des différents serveurs.





## Backups



# Outil pour le backup



Outil open source de sauvegarde et de  
restauration de bases de données  
PostgreSQL







# Fonctionnement



01


## Postgresql

Des backups complets de la base de données postgresql sont effectués chaque jour à 4h du matin avec une durée de rétention de 2 jours.

02

## Redis

La base de données redis a été configurée avec une procédure de sauvegarde automatique en cas de modification. Cette procédure génère un fichier de sauvegarde qui est exporté chaque jour vers un serveur de sauvegarde.





# Gestion des incidents



## Matrice des risques

Identifiant	Description	Impact	Probabilité	Criticité	Conséquences si avérées
R1	Non-détection de l'indisponibilité du service d'alerte	Elevé	Probable	Critique	Non-détection des incidents de la plateforme
R2	Indisponibilité de l'administrateur pour la résolution d'un problème sur la plateforme	Elevé	Probable	Critique	Indisponibilité de la plateforme de vote
R3	Perte de données du au crash de la base de données	Elevé	Probable	Critique	Dysfonctionnement du système de vote
R4	Attaque de la plateforme web	Elevé	Très probable	Critique	Corruption des votes et /ou dysfonctionnement de la plateforme
R5	Perte d'un des serveurs	Elevé	Peu probable	Critique	Arrêt du fonctionnement de la plateforme
R6	Crash du système de sauvegarde des bases de données	Elevé	Peu probable	Critique	Perte définitive des données en cas de crash de la base de données

# Traitement des risques

- **R1:** Pour mitiger ce risque, une alerte de test a été configurée. Cette alerte signale que le serveur d'alerte est actif chaque 2 jours. En cas de non-envoi de cette alerte, le service d'alerting sera considéré comme dysfonctionnant.
- **R2:** Ce risque est mitigé par la mise à disposition de trois 03 administrateurs compétents pour la résolution des incidents en rapport avec la plateforme.
- **R3:** Pour atténuer le risque, des systèmes de sauvegarde des bases de données (postgres et redis) ont été déployées
- **R4:** Ce risque est inacceptable et a donc été délégué à SOC qui s'occupe de la sécurité de la plateforme.
- **R5:** Pour mitiger ce risque, des systèmes d'automatisation ont été mises en place afin qu'une réinstallation rapide et conforme à l'état pré-incident.

# Méthodologie de détection et de résolution d'un incident

## Détection

### Mesures prises pour la détection des incidents

- Configuration des alertes mails pour au minimum 3 administrateurs en cas d'incidents
- Surveillance active de l'état du système sur grafana (de jours et de nuit) par un soc
- Aussi, des incidents peuvent être détectés par les utilisateurs de la plateforme

# Résolution

Après la détection d'un incident, sa résolution sera faite avec un outil de gestion des comme GLPI et suivra les étapes suivantes :

**Enregistrement** : Création d'un ticket permettant d'enregistrer les informations en rapport avec un incident.

**Classification** : La classification permet de déterminer la gravité de l'incident et les services touchés.

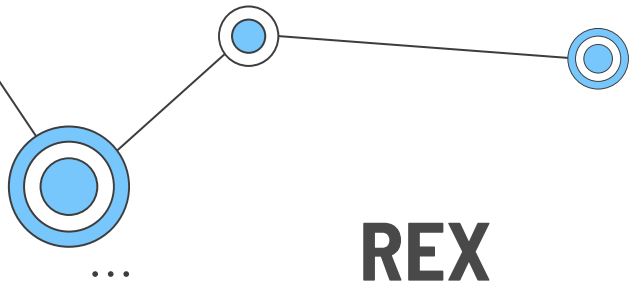
**Traitement** : A cette étape, le ticket créé sera attribué à la personne compétente pour résoudre l'incident.

**Solution** : Ici, le technicien estime avoir résolu l'incident.

**Validation** : A ce niveau, le groupe d'administrateur valide que l'incident est bel et bien résolu.

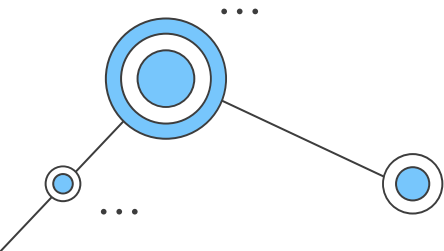
**Remédiation** : Ici, toutes les mesures possibles sont prises pour éviter la réapparition de l'incident.

**Clôture** : À cette étape, le ticket est clôturé et l'incident est considéré comme totalement résolu.



# REX

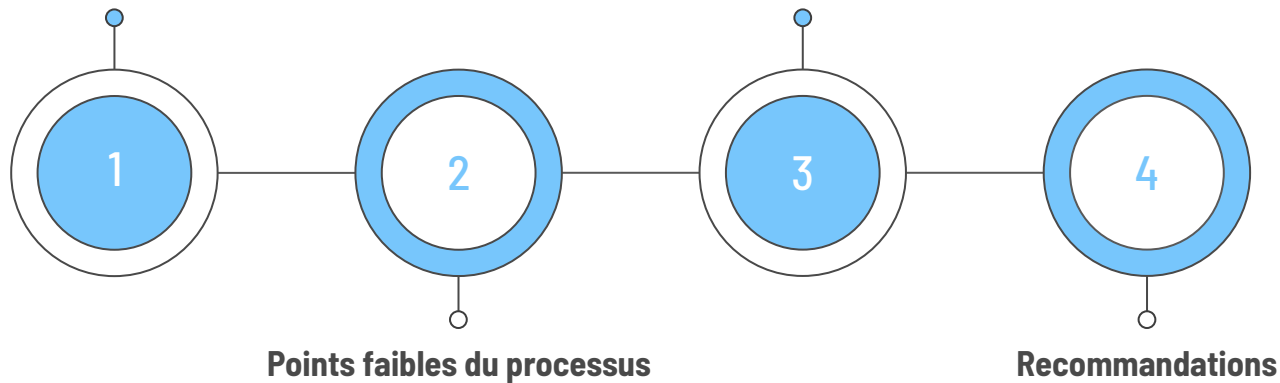
- Arrêt du service postgresql
- Crash de l'application web



# REX

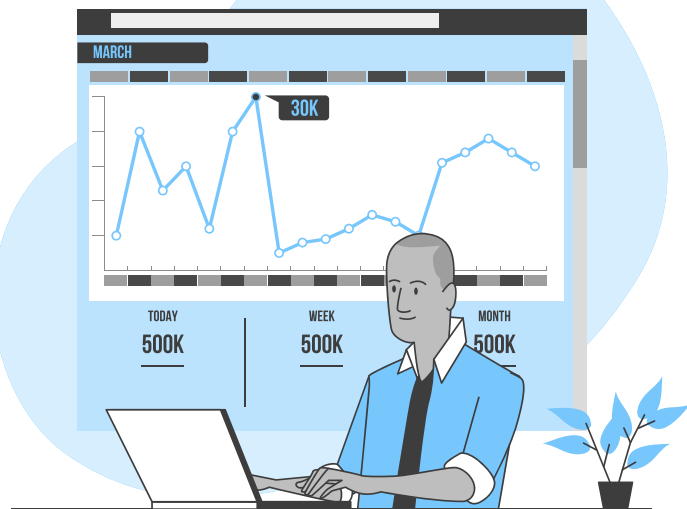
Déroulement de l'incident

Actions correctrices mises en oeuvre / prévues  
par le plan de gestion d'incidents





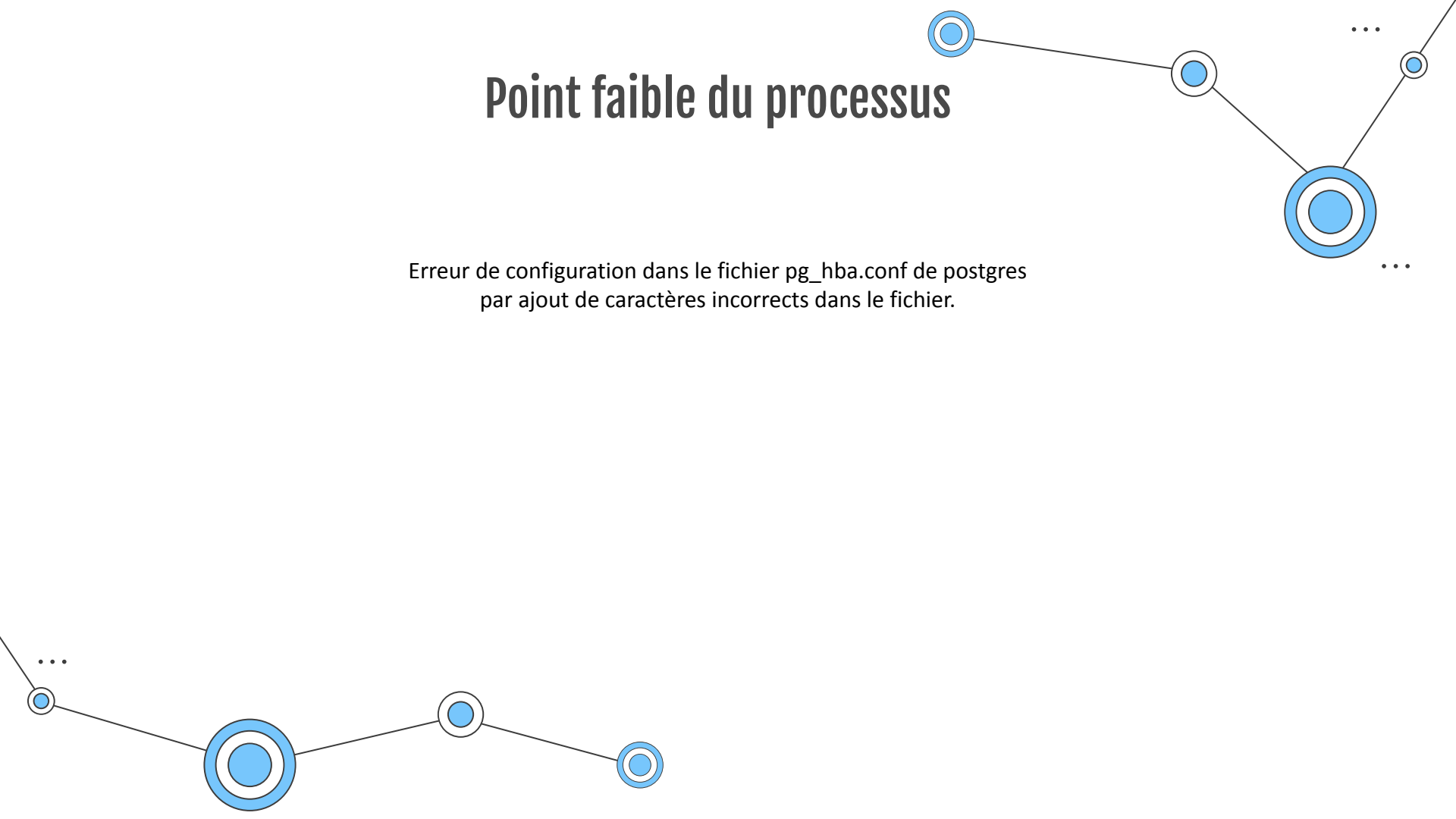
# Déroulement de l'incident 1



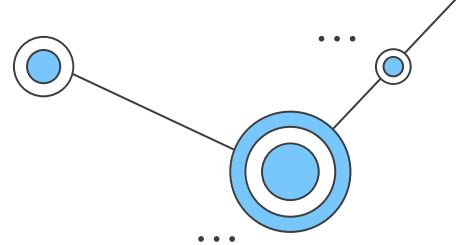
Cet incident s'est manifesté par l'arrêt du service postgresql empêchant l'enregistrement des votes dans la base de données

# Point faible du processus

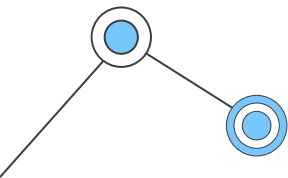
Erreur de configuration dans le fichier pg\_hba.conf de postgres  
par ajout de caractères incorrects dans le fichier.



# Action menée



Suppression des caractères incorrects insérés  
dans le fichier suivi d'un redémarrage du  
service.

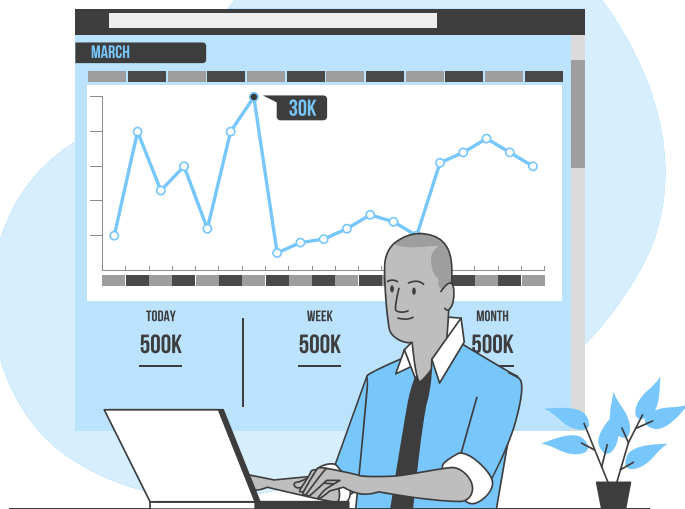


# Recommandations

Être vigilant quand on effectue des modifications sur des fichiers de configuration



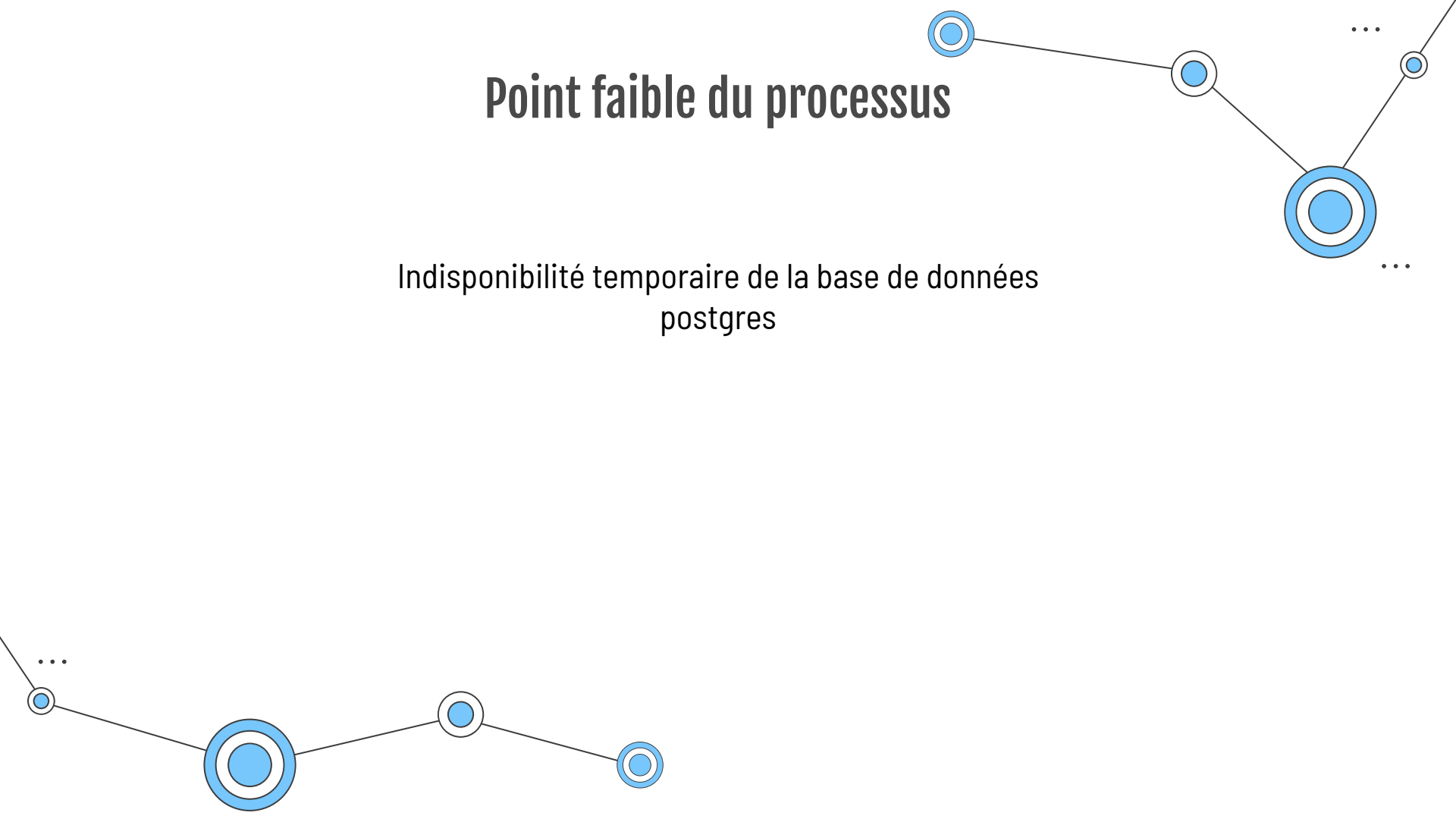
## Déroulement de l'incident 2



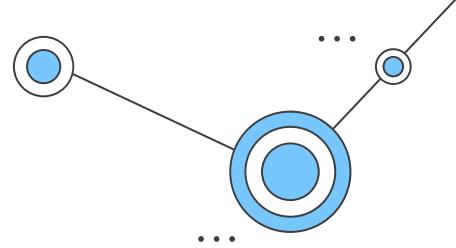
Cet incident s'est manifesté par l'indisponibilité de la page d'affichage du niveau d'évolution des votes.

# Point faible du processus

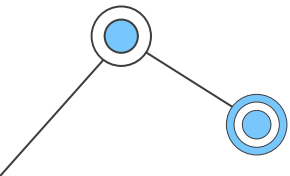
Indisponibilité temporaire de la base de données  
postgres



# Action menée



La résolution de cet incident n'a nécessité que le redémarrage des différents conteneurs dockers après le redémarrage de la bdd



# Recommandations

Prévoir un processus de reprise d'activité (failover)







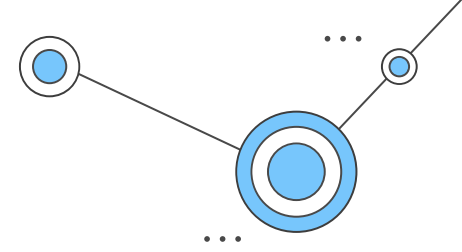
# Suggestions pour l'amélioration de la résilience de l'infrastructure



# Suggestions

- **Mise en de mécanismes de redondance :** En ajoutant des éléments redondants, tels que des serveurs de secours, des lignes de communication de secours, ou des alimentations de secours, on peut garantir que le système peut continuer à fonctionner même en cas de défaillance d'un élément clé.
- **Amélioration de la sécurité :** En renforçant les mesures de sécurité, telles que la mise en place de firewalls, de systèmes de détection d'intrusion et d'authentification forte, on peut réduire les risques d'attaques malveillantes qui pourraient causer des perturbations.
- **Développement d'un plan de reprise d'activité :** Un plan de reprise d'activité détaille les mesures à prendre pour restaurer le service après une interruption, qu'elle soit planifiée ou non.
- **Tests réguliers :** En effectuant des tests réguliers du système, on peut identifier les éventuels points faibles et les améliorer avant qu'ils ne provoquent des interruptions. Les tests doivent couvrir différents scénarios, y compris les pannes matérielles, les pannes logicielles, les attaques malveillantes, etc.

# Conclusion

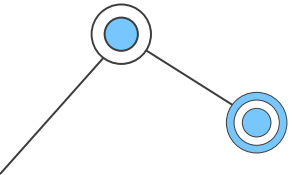
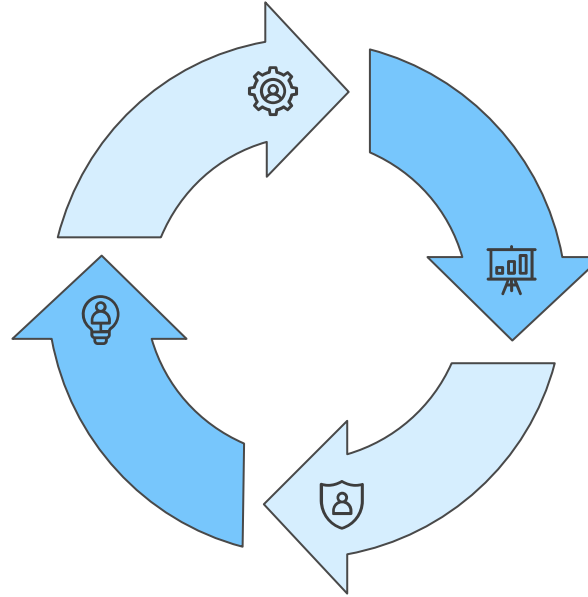


Monitoring

Gestion des incidents

Gestion des risques

Gestion de projets



# Merci!

Avez vous des questions

**CREDITS:** This presentation template was created by [Slidesgo](#), including icons by [Flaticon](#), infographics & images by [Freepik](#) and illustrations by [Stories](#)

