

# BLOC Administration SI

A saturation

# Contexte :

Les serveurs qui stockent les informations médicales ne sont plus disponibles

# Mots à définir / mots Clés :

Log : Un log est un enregistrement chronologique des événements, des actions ou des messages générés par un système informatique, un logiciel ou un dispositif. Les logs sont souvent utilisés pour le dépannage, la surveillance et la sécurité.

Fichier temporaire : Un fichier temporaire est un fichier créé par un programme pour stocker des données de manière temporaire, souvent dans le but de traiter ou de transférer des informations entre les différentes étapes d'un processus.

Outils de monitoring : Les outils de monitoring sont des logiciels ou des dispositifs utilisés pour surveiller en temps réel les performances, l'état ou la disponibilité des systèmes informatiques, des réseaux ou des applications.

Protocole de supervision : Un protocole de supervision est un ensemble de règles et de normes permettant aux systèmes de collecter des données de supervision, de les envoyer à un outil de monitoring et de les interpréter pour évaluer la santé d'un système.

SNMP/ MIB : SNMP (Simple Network Management Protocol) est un protocole de supervision réseau, tandis que MIB (Management Information Base) est une structure de données hiérarchique utilisée pour organiser des informations de supervision dans le cadre de SNMP.

Centreon : Centreon est une plateforme open source de surveillance informatique qui permet de collecter, d'analyser et de visualiser des données de supervision pour assurer la disponibilité et les performances des systèmes.

Nagios : Nagios est un logiciel de surveillance informatique open source très populaire qui permet de surveiller des services réseau, des hôtes et d'envoyer des alertes en cas de problèmes.

Syslogs : Les syslogs sont des messages d'événements générés par les systèmes d'exploitation, les serveurs et les applications. Ils sont utilisés pour la journalisation, le dépannage et la surveillance des systèmes.

# Problématique :

**Comment mettre en place un outil de remontée d’alertes et d’escalade d’incidents ?**

# Contraintes :

Utilisation ne doit pas être impactée

# Généralisation :

Utiliser un outil de supervision

# Livrable :

Ensemble de protocoles supervision

Analyse et choix de protocole de supervision

Référencée des solutions, avantages et inconvénients, pourquoi cet outil est le plus adapté

# Hypothèses / Pistes de solution :

Centreon

# Plan d’actions :

Réaliser le WS

Se renseigner sur les différents outils de supervision

Comparatif des outils

# Réalisation du plan d’actions :

## Ensemble de protocoles supervision

SNMP, ICMP, SSH, WMI, HTTP/HTTPS, Syslog, FTP, Telnet, SNMP Traps, JMX

## Analyse et choix de protocole de supervision

Centreon : Centreon est une solution de supervision open source qui utilise divers protocoles de communication, tels que SNMP, NRPE, NSClient, SSH, pour superviser et gérer les performances des systèmes, des réseaux et des applications. Il offre une interface conviviale pour la configuration et la visualisation des données de surveillance.

SNMP (Simple Network Management Protocol) : Un protocole standard pour la gestion et la supervision des périphériques réseau.

ICMP (Internet Control Message Protocol) : Utilisé pour les opérations de ping et de détection d'hôtes actifs sur un réseau.

SSH (Secure Shell) : Pour superviser et gérer des serveurs à distance de manière sécurisée.

WMI (Windows Management Instrumentation) : Principalement utilisé pour superviser des systèmes Windows.

HTTP/HTTPS : Pour surveiller les serveurs web et les services en ligne.

Syslog : Pour la collecte de journaux et de données de plusieurs dispositifs réseau.

FTP (File Transfer Protocol) : Souvent utilisé pour transférer des fichiers de journalisation et des données de surveillance.

Telnet : Bien que moins sécurisé que SSH, il est parfois utilisé pour la gestion à distance.

SNMP Traps : Des messages d'alerte envoyés par les périphériques réseau pour signaler des événements importants.

JMX (Java Management Extensions) : Principalement utilisé pour la supervision d'applications Java.

## Référencée des solutions, avantages et inconvénients, pourquoi cet outil est le plus adapté

Centreon est considéré comme l'un des meilleurs outils de supervision informatique pour plusieurs raisons :

Interface conviviale : Centreon offre une interface utilisateur conviviale et intuitive, ce qui facilite la configuration et la visualisation des données de surveillance. Cela le rend accessible même aux utilisateurs non techniques.

Polyvalence : Centreon prend en charge de nombreux protocoles de communication, ce qui lui permet de superviser une grande variété de systèmes, de réseaux et d'applications, y compris des environnements hétérogènes.

Personnalisation : Il offre de nombreuses options de personnalisation pour adapter la surveillance aux besoins spécifiques de l'entreprise. Vous pouvez créer des tableaux de bord, des alertes et des rapports personnalisés.

Gestion des alertes : Centreon permet de configurer des alertes en temps réel en cas de problème, ce qui aide à réagir rapidement aux incidents et à minimiser les temps d'arrêt.

Intégration : Il peut être intégré à d'autres outils et systèmes, ce qui en fait une solution polyvalente pour l'intégration dans des environnements complexes.

Communauté active : Centreon bénéficie d'une communauté active d'utilisateurs et de développeurs, ce qui signifie qu'il est constamment mis à jour et amélioré.

Support professionnel : En plus de la version open source, Centreon propose des services de support professionnel pour les entreprises qui ont besoin d'une assistance plus avancée.