Scénario

I. Contexte

L'entreprise NetSecure, spécialisée dans le support informatique pour les PME, dispose d'un système d'information composé de plusieurs serveurs Windows et Linux.

Afin d'assurer la disponibilité des services, l'entreprise a mis en place une solution de supervision permettant de surveiller l'état des équipements et des services.

Cependant, plusieurs limites ont été identifiées dans l'infrastructure actuelle :
- Absence de centralisation des journaux systèmes
- Supervision partielle des ressources
- Utilisation du protocole SNMPv2, qui présente des faiblesses de sécurité
- Absence de mécanismes avancés d'analyse des événements

Ces limites compliquent la détection rapide des incidents et peuvent représenter un risque pour la sécurité du système d'information.

Le projet consiste donc à concevoir et à mettre en place une infrastructure de supervision permettant d'améliorer la surveillance du système d'information.

II. Objectifs du projet

Le projet doit répondre à plusieurs objectifs.

1- Supervision

Mettre en place une supervision centralisée permettant de surveiller les équipements et services critiques de l'infrastructure.

2- Santé du système d'information

Afin de détecter les anomalies et les problèmes de performance nous avons besoin de surveiller les ressources systèmes :
- CPU
- mémoire
- espace disque
- disponibilité des services

3- Traçabilité

Centraliser et analyser les journaux systèmes afin de pouvoir retracer les événements et identifier l'origine d'un incident.

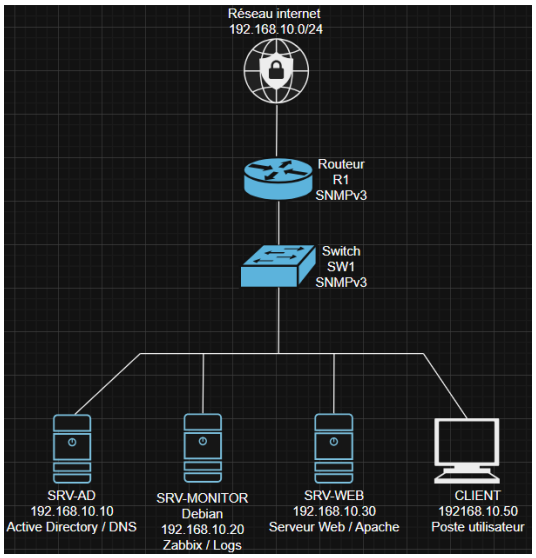
4- Sécurité

Renforcer la sécurité de l'infrastructure en améliorant les mécanismes de supervision et en sécurisant les communications de monitoring.

III. Architecture du projet

L'infrastructure repose sur un environnement virtualisé utilisant VMware Workstation.
Le réseau est composé de plusieurs machines virtuelles simulant l'infrastructure d'une entreprise :
- un serveur Active Directory
- un serveur de supervision
- un serveur applicatif
- un poste client

La supervision est réalisée à l'aide d'un serveur centralisé capable de collecter les informations provenant des différentes machines.



IV. Machines virtuelles utilisées

Machines virtuelles utilisées	Serveur Active Directory	Serveur de supervision	Serveur applicatif	Poste client
Nom	SRV-AD	SRV-MONITOR	SRV-WEB	CLIENT
Système	Windows Server 2019	Debian	Debian	Windows 10
Rôle	Contrôleur de domaine Authentification des utilisateurs Service DNS	Supervision des machines Collecte des informations système Centralisation des journaux	Hébergement d'un service web interne	Poste utilisateur Accès aux services du domaine
Services installées	---------- ---------- ---------- ----------	Zabbix Server Outils de supervision Serveur de logs	Apache	---------- ---------- ---------- ----------
Configuration	192.168.10.10 netsecure.local	192.168.10.20	192.168.10.30	192.168.10.50 Membre du domaine netsecure.local

V. Amélioration mises en place

Améliorations 1 – Sécurisation de SNMP

L'entreprise utilise actuellement SNMPv2 pour superviser certains équipements.

Cependant, cette version présente des faiblesses de sécurité car elle utilise uniquement une communauté servant de mot de passe.

Afin d'améliorer la sécurité de la supervision, il a été décidé de migrer vers SNMPv3, qui offre :
- authentification des utilisateurs
- chiffrement des communications
- protection contre certaines attaques réseau

Cette amélioration permet de sécuriser les échanges entre les équipements et le serveur de supervision.

Amélioration 2 – Supervision des performances

Une supervision des performances système est mise en place afin de surveiller :
- l'utilisation du processeur
- la mémoire
- l'espace disque
- la disponibilité des services

Ces informations permettent de détecter les anomalies et d'anticiper les incidents.

Amélioration 3 – Supervision des services applicatifs

Le serveur web est supervisé afin de vérifier :
- la disponibilité du service Apache
- la réponse du server web

Cela permet de détecter rapidement une interruption de service.

Amélioration 4 – Centralisation des journaux

Afin d'améliorer la traçabilité, les journaux systèmes sont centralisés sur le serveur de supervision.

Cette centralisation permet :
- une analyse simplifiée des événements
- la détection d'activités suspectes
- une meilleure gestion des incidents

VI. Tests et simulation d'incidents

Afin de vérifier l'efficacité de la supervision, plusieurs incidents sont simulés :
- arrêt du service web
- saturation de l'espace disque
- tentatives de connexion échoués

- anomalies de performance

Ces tests permettent de vérifier la capacité du système du système de supervision à détecter les incidents.

VII. Résultats attendus

La solution mise en place doit permettre :
- une meilleure visibilité sur l'état du système d'information
- une détection rapide des incidents
- une amélioration de la sécurité de la supervision
- une meilleure traçabilité des événements