PPE 2

ANCELIN Lorick
BTS SIO 26
PPE 2

Traçabilité et supervision de la santé et de la sécurité du système d'information

1. Introduction

1.1 Présentation du projet
1.2 Objectif

2. Présentation

2.1 Organisation du SI
2.2 Besoins identifiés

3. Analyse des besoins

3.1 Besoins en supervision
3.2 Risques identifiés
3.3 Solutions envisagées

4. Mise en place de l'environnement

4.1 Installation des machines virtuelles
4.2 Installation d'Active Directory
4.3 Présentation de l'Active Directory

5 Mise en place de la supervision du SI

5.1 Présentation de PRTG
5.2 Installation et configuration
5.3 Supervision des machines
5.4 Mise en place des alertes

6. Tests et validation

6.1 Scénarios de test
6.2 Résultats obtenus

1.1 Présentation du projet

L'entreprise « PROMPLUS », spécialisée dans les services numériques, possède un système d'information basé sur un environnement Windows avec un contrôleur de domaine Active Directory et plusieurs postes clients.

Dans le cadre de son développement, l'entreprise souhaite améliorer la sécurité et la disponibilité de son système d'information. En effet, aucune solution de traçabilité n'est actuellement en place, ce qui rend difficile l'identification des actions réalisées par les utilisateurs et les administrateurs.

De plus, l'entreprise ne dispose pas d'outil de supervision permettant de surveiller l'état de santé des serveurs et des postes de travail, ce qui peut entraîner des interruptions de service non anticipées.

L'objectif de ce projet est donc de mettre en place :

- Un système d'audit Active Directory permettant de tracer les actions sensibles (création de comptes, modifications de groupes, connexions)

- Une solution de supervision permettant de surveiller les performances des machines (CPU, mémoire, disque) et d'anticiper les incidents

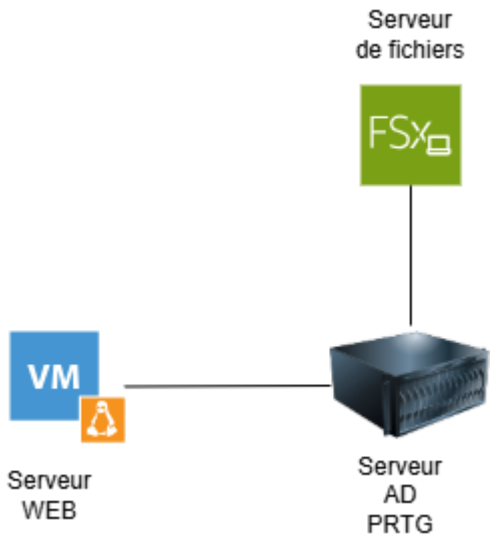
Ce projet a été réalisé dans un environnement virtualisé reproduisant l'infrastructure de l'entreprise.

1.2 Objectif

Les objectifs de ce projet sont les suivants :

- Mettre en place un contrôleur de domaine Active Directory
- Activer et configurer l'audit des événements de sécurité
- Identifier et analyser les événements critiques (création de comptes, connexions, modifications de groupes)
- Déployer une solution de supervision du système d'information
- Surveiller les performances des machines (processeur, mémoire, disque, réseau)
- Mettre en place des alertes en cas d'anomalie
- Proposer une solution permettant d'améliorer la sécurité et la disponibilité du système d'information

2.1 Organisation du SI



Adresse IP des machines virtuelles :

AD + PRTG : 192.168.200.5

Serveur WEB : 192.168.200.22

Serveur de fichiers : 192.168.200.21

2.2 Besoins identifiés

Suite à l'analyse du système d'information de l'entreprise, plusieurs besoins ont été identifiés afin d'améliorer la sécurité et la disponibilité des services.

Tout d'abord, l'entreprise ne dispose d'aucun mécanisme de traçabilité des actions réalisées dans l'environnement Active Directory. Il est donc impossible de savoir quel utilisateur a effectué une action sensible, comme la création d'un compte, la modification d'un groupe ou une tentative de connexion échouée. Ce manque de visibilité représente un risque important en termes de sécurité.

Ensuite, aucun outil de supervision n'est actuellement en place pour surveiller l'état de santé des machines. L'entreprise ne peut pas suivre l'utilisation des ressources systèmes telles que le processeur, la mémoire ou le disque, ce qui peut entraîner des dégradations de performance ou des interruptions de service non anticipées.

De plus, l'absence d'alertes empêche les administrateurs d'être informés rapidement en cas de problème, comme une surcharge du processeur, un manque d'espace disque ou une activité suspecte.

Enfin, l'entreprise souhaite centraliser les informations afin de faciliter l'analyse et la prise de décision. Une solution permettant de regrouper les données de sécurité et de performance est donc nécessaire.

Les besoins identifiés sont les suivants :

- Mettre en place un système de traçabilité des actions dans Active Directory
- Surveiller les connexions et les activités des utilisateurs
- Superviser l'état de santé des machines (CPU, mémoire, disque, réseau)
- Détecter les anomalies et les comportements suspects
- Mettre en place des alertes en temps réel
- Centraliser les informations pour faciliter leur analyse

3.1 Besoins en supervision

En complément de la traçabilité, l'entreprise a besoin de superviser l'état de santé de son système d'information afin d'assurer la disponibilité des services.

Il est nécessaire de surveiller les performances des machines, notamment l'utilisation du processeur, de la mémoire, de l'espace disque et du réseau. Cette supervision permet de détecter les anomalies avant qu'elles n'impactent les utilisateurs.

De plus, la mise en place d'alertes est indispensable pour informer rapidement les administrateurs en cas de dépassement de seuil critique.

Les besoins en supervision sont donc :

- Surveiller les performances des serveurs et des postes clients
- Mesurer l'utilisation des ressources système (CPU, RAM, disque)
- Détecter les anomalies de fonctionnement
- Mettre en place des alertes en cas de seuil critique
- Visualiser les données sous forme de graphiques

3.2 Risques identifiés

L'absence de traçabilité et de supervision expose le système d'information à plusieurs risques.

Sur le plan de la sécurité, l'absence de journalisation des événements empêche de détecter les actions malveillantes ou les erreurs humaines. Un utilisateur pourrait effectuer des modifications critiques sans être identifié.

Sur le plan technique, l'absence de supervision peut entraîner des pannes non anticipées, liées à une surcharge du processeur, un manque de mémoire ou un espace disque insuffisant.

Ces situations peuvent provoquer une indisponibilité des services, une perte de données ou une dégradation des performances.

Les principaux risques identifiés sont :

- Impossibilité de tracer les actions des utilisateurs
- Difficulté à détecter les attaques ou comportements suspects
- Surcharge des ressources système
- Pannes imprévues
- Interruption des services
- Perte de données

3.3 Solutions envisagées

Pour la supervision, l'utilisation d'un outil dédié comme PRTG permet de surveiller en temps réel les performances des machines et de recevoir des alertes en cas d'anomalie. Cet outil offre une interface graphique facilitant la visualisation des données.

La solution retenue repose donc sur :

- La mise en place d'un outil de supervision (PRTG)
- La configuration de capteurs pour surveiller les ressources système
- La mise en place d'alertes en cas de dépassement de seuil

Cette approche permet d'améliorer la sécurité et la disponibilité du système d'information.

4.1 Installation des machines virtuelles

Un Windows Server est configuré avec l'Active Directory d'installé.

Un autre Windows Server qui serra aussi dans le même domaine, sera configuré en tant que serveur de fichiers

4.2 Installation d'Active Directory

Le nom de domaine est : lancelinppe2.local

Une OU PPE est créée pour pouvoir créer à l'intérieur une OU POSTES et UTILISATEURS pour pouvoir organiser au mieux les postes et utilisateurs du domaine.

4.3 Présentation de l'audit Active Directory

L'audit Active Directory permet de tracer les actions réalisées au sein du domaine afin d'assurer la sécurité du système d'information.

Dans un environnement Windows, les événements liés à la sécurité sont enregistrés dans les journaux du système, notamment dans le journal de sécurité du contrôleur de domaine. Ces événements permettent de suivre les connexions des utilisateurs, les modifications des comptes, ainsi que les changements de permissions.

La mise en place d'un audit Active Directory est essentielle pour détecter les comportements anormaux, identifier les actions malveillantes et répondre aux exigences de traçabilité.

Dans le cadre de ce projet, l'audit a été configuré afin de surveiller les actions sensibles réalisées dans le domaine Active Directory.

5.1 Présentation de PRTG

PRTG Network Monitor est un outil de supervision réseau développé par Paessler AG. Il permet de surveiller en temps réel les équipements informatiques comme les serveurs, routeurs, applications et services.

Son fonctionnement repose sur des capteurs, chacun mesurant un élément précis (CPU, bande passante, disponibilité, etc.). Un même appareil peut avoir plusieurs capteurs pour une surveillance détaillée.

PRTG offre des tableaux de bord, des graphiques en temps réel et un système d'alertes en cas de problème. Il utilise différents protocoles comme SNMP, WMI ou SSH pour collecter les données.

Il est utile en cybersécurité pour détecter des anomalies réseau ou des comportements suspects. Facile à installer et à utiliser, il convient aussi bien aux petites qu'aux grandes infrastructures, bien qu'il soit principalement orienté Windows.

5.2 Installation et configuration

L'installation de PRTG a été réalisée sur le serveur Windows utilisé comme contrôleur de domaine.

Le logiciel a été téléchargé depuis le site officiel de l'éditeur puis installé en suivant les étapes de l'assistant. Une fois l'installation terminée, l'accès à l'interface web s'effectue via un navigateur, en utilisant l'adresse IP du serveur.

Lors du premier lancement, un compte administrateur a été configuré afin d'accéder à l'interface de gestion.

La configuration initiale comprend la création d'un environnement de supervision, permettant d'ajouter des équipements et de configurer les capteurs nécessaires.

5.3 Supervision des machines

La supervision des machines a été mise en place en ajoutant des capteurs sur le serveur et le poste client.

Les capteurs configurés permettent de surveiller les éléments suivants :

- L'utilisation du processeur (CPU)

- L’utilisation de la mémoire (RAM)

- L’espace disque disponible

- Le trafic réseau

Ces capteurs permettent d’obtenir une vision en temps réel de l’état de santé des machines.

Les données sont affichées sous forme de graphiques dans l’interface de PRTG.

5.4 Mise en place des alertes

Afin d’être informé en cas d’anomalie, des alertes ont été configurées dans PRTG.

Des seuils ont été définis pour certains capteurs, par exemple :

- Utilisation du processeur supérieure à 90 %

- Espace disque inférieur à 10 %

- Utilisation de la mémoire élevée

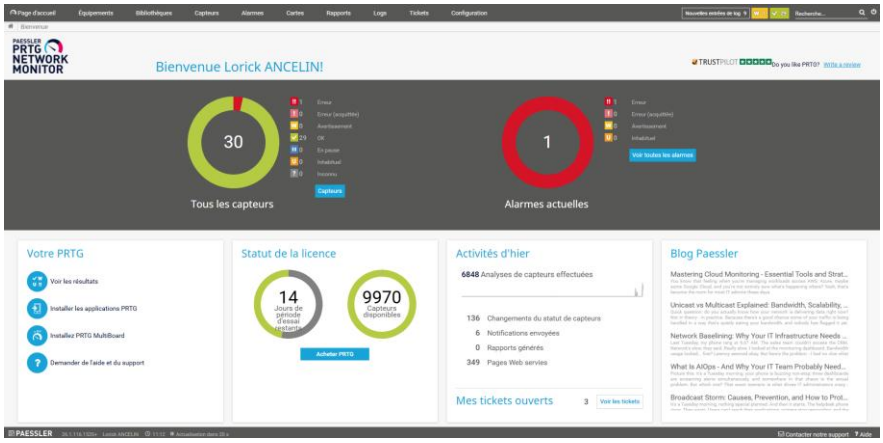
Lorsque ces seuils sont dépassés, PRTG génère automatiquement une alerte.

Ces alertes permettent aux administrateurs d’intervenir rapidement afin de corriger les problèmes et d’éviter une dégradation des performances ou une interruption de service.

Pour plus de précision sur le serveur web, un capteur a été configuré pour vérifier uniquement l'état de la page web http://192.168.200.22 (qui est l'ip du serveur web et à la fois l'ip qui sert à accéder à la page web). Grâce à ce capteur, uniquement le service Apache est supervisé.

6.1 Scénario de test

Une alerte (indiqué comme erreur) est remontée indiquant une anomalie sur le serveur web.



L'erreur indique : Connection refused Socket Error # 10061 Connection refused. (erreur de socket # 10061)

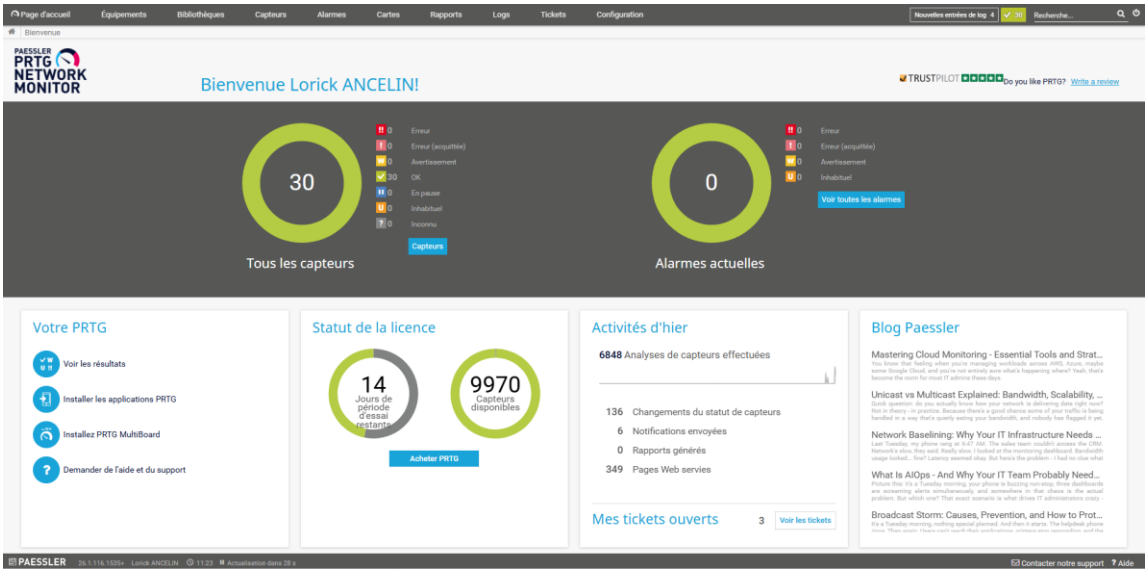
On peut voir que tous les autres capteurs concernant le serveur web sont « ok ». La machine virtuelle est toujours en fonctionnement. C'est donc le service Apache qui a un problème.

6.2 Résultats obtenus

```
root@srv-web:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: inactive (dead) since Thu 2026-04-02 11:17:28 CEST; 3min 47s ago
   Duration: 2min 29.167s
 Invocation: 587f2a408fa7466192e59c0d7e6f3d4e
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 1506 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Process: 1575 ExecStop=/usr/sbin/apachectl graceful-stop (code=exited, status=0/SUCCESS)
   Main PID: 1509 (code=exited, status=0/SUCCESS)
   Mem peak: 7M
        CPU: 41ms

avril 02 11:14:58 srv-web systemd[1]: Starting apache2.service - The Apache HTTP Server...
avril 02 11:14:58 srv-web systemd[1]: Started apache2.service - The Apache HTTP Server.
avril 02 11:17:28 srv-web systemd[1]: Stopping apache2.service - The Apache HTTP Server...
avril 02 11:17:28 srv-web systemd[1]: apache2.service: Deactivated successfully.
avril 02 11:17:28 srv-web systemd[1]: Stopped apache2.service - The Apache HTTP Server.
root@srv-web:~#
```

Sur le serveur web, en faisant « systemctl status apache2 » on peut voir l'état du service. A la 3eme ligne « Acive : inactive », le service est donc désactivé. Pour le ractiver : systemctl start apache2.



Plus aucune erreur n'est remontée, et le service Apache est de nouveau fonctionnel.