BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2023**

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle (recto)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : 1**
Nom, prénom : AKALAN Mahmut-Selim	**N° candidat : 02243943041**
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒	**Date :** 30 / 05 / 2023

Organisation support de la réalisation professionnelle
Entreprise cub-turquie

Intitulé de la réalisation professionnelle
Gestion d'une infrastructure de surveillance et de gestion des incidents informatiques.

Période de réalisation : 2021-2023 **Lieu :** CFA Robert Schuman, Metz.
Modalité : ☐ **Seul(e)** ☒ **En équipe**

Compétences travaillées
- ☒ Concevoir une solution d'infrastructure réseau
- ☒ Installer, tester et déployer une solution d'infrastructure réseau
- ☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation[1] (ressources fournies, résultats attendus)
Ressource fournies :
GLPI sur un serveur Linux Debian
RSYSLOG sur un serveur Linux Debian
PRTG sur le serveur de fichier.

Résultats attendus :
Supervision de l'infrastructure avec RSYSLOG (journaux d'événements sur le réseau) et PRTG (permet de créer des capteurs ou sondes en s'appuyant notamment sur l'ICMP, le SNMP, le WMI, les compteurs de performance, le Packet Sniffing, le NetFlow, le sFlow, le jFlow).
Gestion des incidents grâce aux outils de supervision ou à la demande des utilisateurs via GLPI en créant des tickets.

Description des ressources documentaires, matérielles et logicielles utilisées[2]
OS linux debian 11 x1
OS Windows server 2019 x2
2 logiciels de supervision (RSYSLOG et PRTG).
1 logiciel de gestion d'incident (GLPI).

Les sites informatiques sur internet (IT-connect, Rdr-it…)
Les vidéos sur youtube de la chaîne GeekAdvisor
Les aides et conseils des professeurs.

[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

Modalités d'accès aux productions[3] et à leur documentation[4]

Identifiant administrateur du domaine : cub-turquie.local\Administrateur
Mot de passe de l'administrateur du domaine : Bafrali55@
(vm PRTG : **AS WINDOWS SERVER 2019 V2**)

Identifiant administrateur du domaine : selim
Mot de passe de l'administrateur du domaine : bafrali@
(vm RSYSLOG et GLPI : **AS debian)**

La documentation des services cités précédemment est disponible ici : https://sa-portefolio.fr/projet/

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2023**

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)

[3] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[4] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

1. Objectifs

- L'objectif de cette réalisation professionnelle est de mettre en place une infrastructure de surveillance et de gestion des incidents informatiques basée sur les outils GLPI, SYSLOG et PRTG. Cette solution permettra de collecter les journaux d'événements (logs) de différents équipements du réseau informatique de l'entreprise, de les centraliser, d'analyser les anomalies, et de générer des alertes pour permettre une intervention rapide et efficace. Cette solution est essentielle pour garantir la disponibilité, la sécurité et la performance du système d'information de l'entreprise.

2. Compétence (s) principale (s)

En orange dans le **Erreur ! Source du renvoi introuvable.**

Concevoir une solution d'infrastructure réseau

- Déterminer et préparer les tests nécessaires à la validation de la solution.

Installer, tester et déployer une solution d'infrastructure réseau

- Installer et configurer des éléments nécessaires pour assurer la continuité des services.
- Installer et configurer des éléments nécessaires pour assurer la qualité de service.
- Rédiger ou mettre à jour la documentation technique et utilisateur d'une solution d'infrastructure.
- Tester l'intégration et l'acceptation d'une solution d'infrastructure.
- Déployer une solution d'infrastructure.

Exploiter, dépanner et superviser une solution d'infrastructure réseau

- Automatiser des tâches d'administration.
- Identifier, qualifier, évaluer et réagir face à un incident ou à un problème.

3. Description du contexte

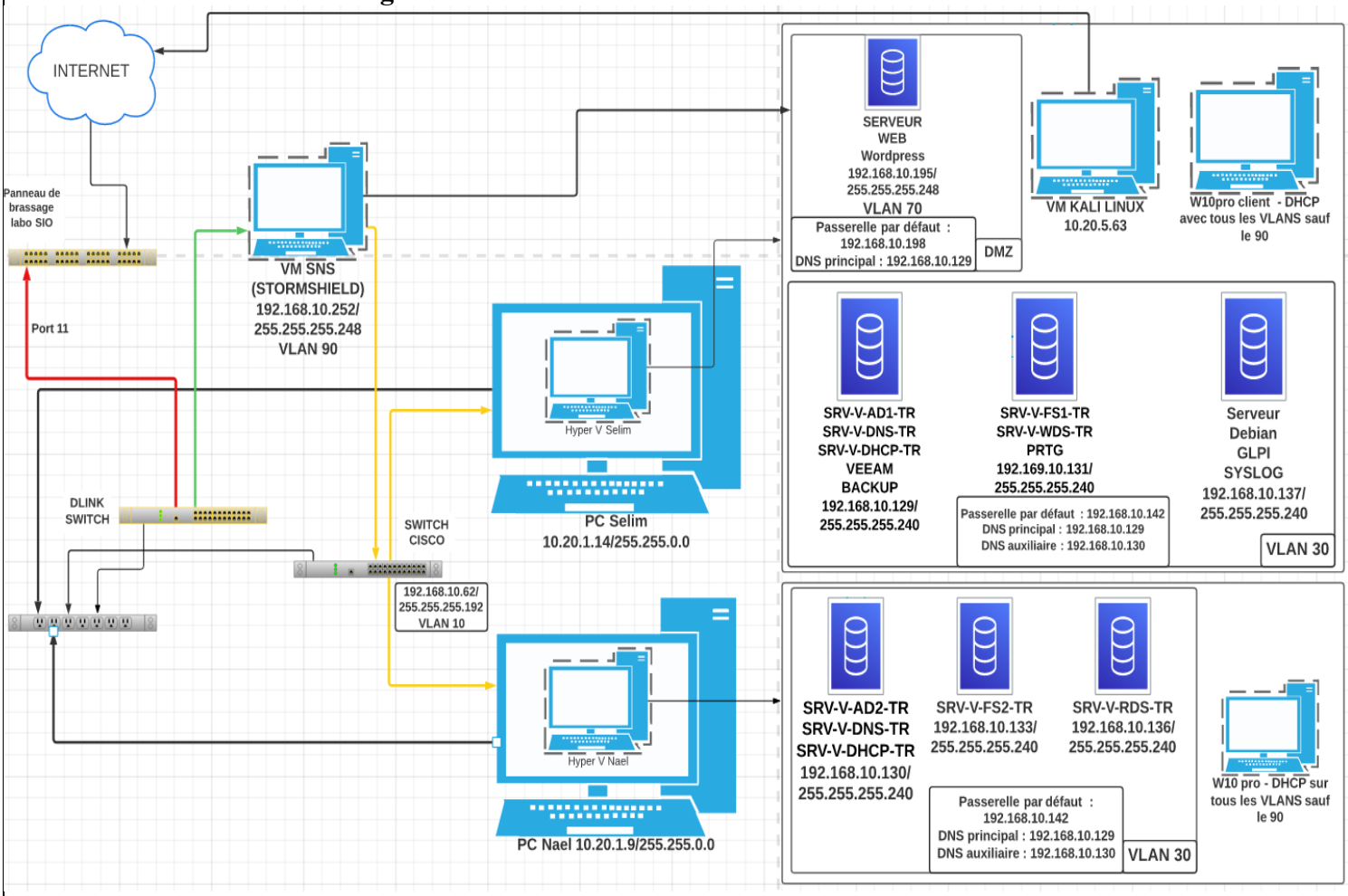
- Dans mon infrastructure, l'installation de GLPI (logiciel libre et open-source de gestion d'actifs informatiques) sur un serveur Linux (Debian) et avec l'installation de XAMPP, on peut utiliser la base de données MySQL fournie avec XAMPP pour installer et exécuter GLPI. Donc GLPI sert à gérer et suivre l'inventaire des matériels et logiciels et les demandes de support technique.

- L'installation de RSYSLOG par ligne de commande sur un serveur Linux (Debian) sert à centraliser la gestion des journaux de différents appareils et systèmes, afin de faciliter le suivi des événements système, le dépannage des problèmes et l'analyse des performances. Rsyslog est un protocole de journalisation de messages qui permet aux appareils informatiques de différents types et systèmes d'exploitation de générer, enregistrer et transmettre des messages de journalisation vers un serveur centralisé appelé un "syslog serveur". Les messages Rsyslog peuvent inclure des informations sur les événements système, les erreurs, les avertissements, les opérations de maintenance… J'ai donc paramétrer mon switch et pare-feu afin d'avoir un suivi et être averti en cas de risque.

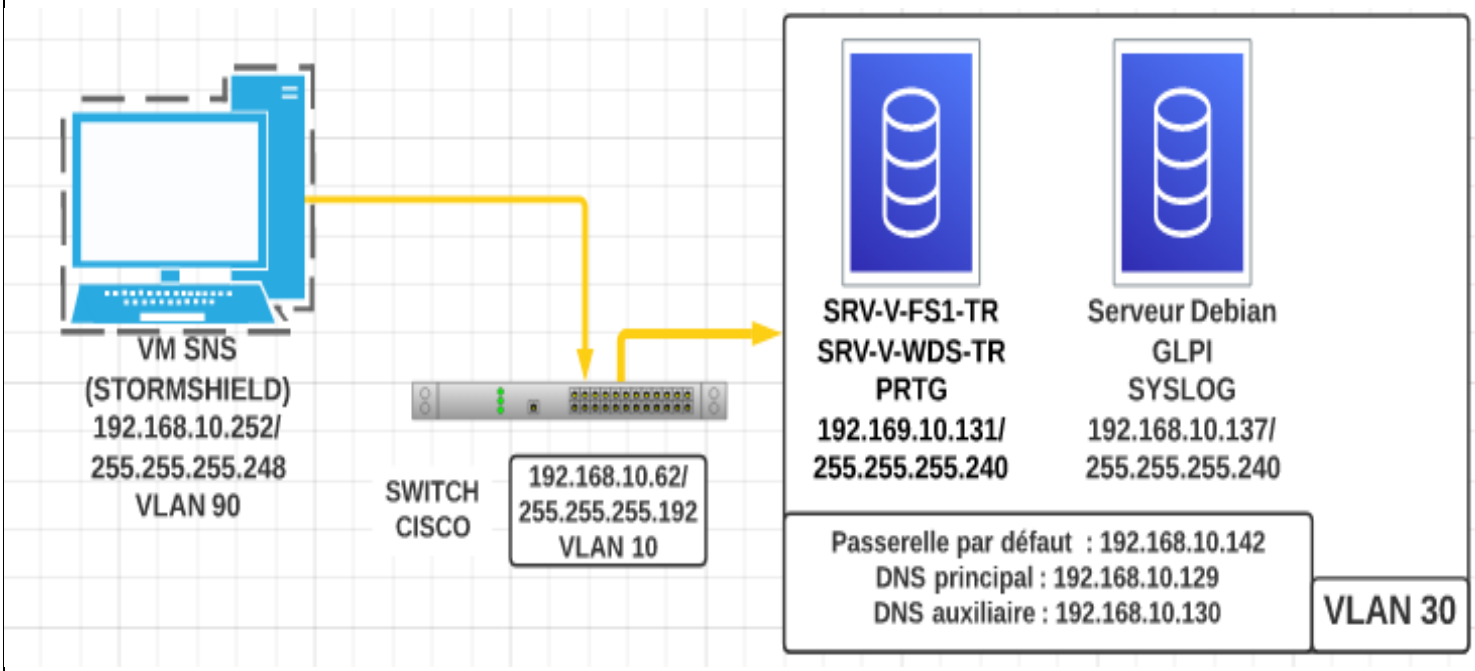
- L'installation de PRTG (PRTG Network Monitor est un logiciel de surveillance réseau commercial) sur mon serveur AD à débuter par le téléchargement du fichier d'installation de PRTG à partir du site web de l'éditeur de logiciels. Une fois le fichier télécharger il faut l'installer et lors de l'installation il faut paramétrer PRTG (le port 80…). Ensuite c'est au tour de la configuration initiale comme la création d'un compte utilisateur. Et une fois le PRTG est accessible il nous reste juste à ajouter des appareils avec la création des sondes (exemple : une sonde WMI pour l'espace disque sur le serveur AD).

3.1. Schémas et maquettes

- **Schéma du réseau global de votre contexte.**



- **Schéma précis de la partie mise en œuvre dans la réalisation.**



- **Schéma précis de l'adressage réseau (doit permettre de faire un « traceroute » manuel)**

			FROM	TO	Brodc	128	64	32	16	8	4	2	1
T 1	60	192.168.10.0/26	192.168.10.1	192.168.10.62	192.168.10.63	0	0	1	1	1	1	1	1
T 2	60	192.168.10.64 /26	192.168.10.65	192.168.10.126	192.168.10.127	0	0	1	1	1	1	1	1
veur	14	192.168.10.128 /28	192.168.10.129	192.168.10.142	192.168.10.143	0	0	0	0	1	1	1	1
FI	14	192.168.10.144 /28	192.168.10.145	192.168.10.158	192.168.10.159	0	0	0	0	1	1	1	1
P	14	192.168.10.160	192.168.10.161	192.168.10.174	192.168.10.175	0	0	0	0	1	1	1	1
min	10	192.168.10.176 /28	192.168.10.177	192.168.10.190	192.168.10.191	0	0	0	0	1	1	1	1
Z1	6	192.168.10.192 /29	192.168.10.193	192.168.10.198	192.168.10.199	0	0	0	0	0	1	1	1
Z2	6	192.168.10.200 /29	192.168.10.201	192.168.10.206	192.168.10.207	0	0	0	0	0	1	1	1

/26= 255.255.255.192	/26= 255.255.255.192
10	20
ENT 1	ENT 2
192.168.10.1	192.168.10.65
192.168.10.2	192.168.10.66
192.168.10.3	192.168.10.67
192.168.10.4	192.168.10.68
192.168.10.5	192.168.10.69
192.168.10.6	192.168.10.70
192.168.10.7	192.168.10.71
192.168.10.8	192.168.10.72
192.168.10.9	192.168.10.73
192.168.10.10	192.168.10.74
192.168.10.11	192.168.10.75
192.168.10.12	192.168.10.76
192.168.10.13	192.168.10.77
192.168.10.14	192.168.10.78
192.168.10.15	192.168.10.79
192.168.10.16	192.168.10.80
192.168.10.17	192.168.10.81
192.168.10.18	192.168.10.82
192.168.10.19	192.168.10.83
192.168.10.20	192.168.10.84
192.168.10.21	192.168.10.85
192.168.10.22	192.168.10.86
192.168.10.23	192.168.10.87
192.168.10.24	192.168.10.88
192.168.10.25	192.168.10.89
192.168.10.26	192.168.10.90
192.168.10.27	192.168.10.91
192.168.10.28	192.168.10.92
192.168.10.29	192.168.10.93
192.168.10.30	192.168.10.94
192.168.10.31	192.168.10.95
192.168.10.32	192.168.10.96
192.168.10.33	192.168.10.97
192.168.10.34	192.168.10.98
192.168.10.35	192.168.10.99
192.168.10.36	192.168.10.100
192.168.10.37	192.168.10.101
192.168.10.38	192.168.10.102
192.168.10.39	192.168.10.103
192.168.10.40	192.168.10.104
192.168.10.41	192.168.10.105
192.168.10.42	192.168.10.106
192.168.10.43	192.168.10.107
192.168.10.44	192.168.10.108
192.168.10.45	192.168.10.109
192.168.10.46	192.168.10.110
192.168.10.47	192.168.10.111
192.168.10.48	192.168.10.112
192.168.10.49	192.168.10.113
192.168.10.50	192.168.10.114
192.168.10.51	192.168.10.115
192.168.10.52	192.168.10.116
192.168.10.53	192.168.10.117
192.168.10.54	192.168.10.118
192.168.10.55	192.168.10.119
192.168.10.56	192.168.10.120
192.168.10.57	192.168.10.121
192.168.10.58	192.168.10.122
192.168.10.59	192.168.10.123
192.168.10.60	192.168.10.124
192.168.10.61	192.168.10.125
192.168.10.62 IP pour se connecter au cisco	192.168.10.126 IP pour se connecter au

Les postes W10 pro sont en DHCP sur tous les VLAN et une connexion au Web est disponible.

Démarrer la VM SNS + la VM DHCP pour avoir une connexion internet sur les machines.

Brancher les câbles jaune sur le switch Cisco.

/28=255.255.255.240	/28=255.255.255.240	/28=255.255.255.240	/28=255.255.255.240	/28=255.255.255.240
30		40	50	60
Serveur		WIFI	VoIP	Admin
192.168.10.129	vm selim ad 1	192.168.10.145	192.168.10.161	192.168.10.177
192.168.10.130	vm nael ad 2	192.168.10.146	192.168.10.162	192.168.10.178
192.168.10.131	vm selim fs 1	192.168.10.147	192.168.10.163	192.168.10.179
192.168.10.132	windows 10 pro selim fs	192.168.10.148	192.168.10.164	192.168.10.180
192.168.10.133	vm nael fs2	192.168.10.149	192.168.10.165	192.168.10.181
192.168.10.134		192.168.10.150	192.168.10.166	192.168.10.182
192.168.10.135		192.168.10.151	192.168.10.167	192.168.10.183
192.168.10.136	vm nael RDS	192.168.10.152	192.168.10.168	192.168.10.184
192.168.10.137	vm selim DEBIAN glpi	192.168.10.153	192.168.10.169	192.168.10.185
192.168.10.138		192.168.10.154	192.168.10.170	192.168.10.186
192.168.10.139		192.168.10.155	192.168.10.171	192.168.10.187
192.168.10.140		192.168.10.156	192.168.10.172	192.168.10.188
192.168.10.141		192.168.10.157	192.168.10.173	192.168.10.189
192.168.10.142		192.168.10.158 IP pour se connecter au cisc	192.168.10.174 IP pour se connecter au cisc	192.168.10.190 IP pour se connecter au cisc

/29=255.255.255.248	/29=255.255.255.248	/29=255.255.255.248
70	80	90
DMZ1	DMZ2	lien
192.168.10.193	192.168.10.201	192.168.10.249
192.168.10.194	192.168.10.202	192.168.10.250
192.168.10.195 vm selim serveur web	192.168.10.203	192.168.10.251
192.168.10.196	192.168.10.204	192.168.10.252 vm selim sns (stormshield)
192.168.10.197	192.168.10.205	192.168.10.253
192.168.10.198 IP pour se connecter au cisc	192.168.10.206 IP pour se connecter au cisc	192.168.10.254

4. Planification

Installation et configuration

- Créer deux VM : Génération 1 (prend en charge les OS de 32 bits et 64 bits), Mémoire de démarrage 2048MO,
  30GO pour le disque dur virtuel, installer l'OS à partir d'un CD de démarrage (insérer l'ISO de Windows server 2019 et l'ISO debian 11 pour la 2ème machines).
- Les tâches effectuées pour mettre en œuvre complètement cette réalisation ont été les suivantes :
- Installation et configuration de GLPI sur debian par ligne de commande (créer la base de données et ensuite on peut installer GLPI),
- Configuration de la gestion des incidents dans GLPI.
- Installation et configuration de RSYSLOG sur debian par ligne de commande (créer la base de données et ensuite on peut installer RSYSLOG),
- Configuration de la collecte des logs des serveurs et des équipements réseau.
- Installation et configuration de PRTG (télécharger sur le site officiel le dossier d'installation et lancer l'installation),
- Configuration des alertes et de la surveillance du réseau.

Configuration Réseau

- Création du VLAN 30 sur l'interface CISCO et configuration de l'IP (passerelle, masque…) selon la documentation,
- Configuration de l'IPV4 de chaque machine virtuelle des serveurs selon la documentation technique (passerelle, masque…).
- Ne pas oublier de mettre les machines en LAN et activer l'identification LAN virtuelle sur le VLAN 30.

5. Définitions et Normes

Les protocoles et normes utilisés pour cette réalisation sont :

- TCP/IP (Transmission Control Protocol/Internet Protocol) est un ensemble de protocoles de communication utilisés pour la transmission de données entre des ordinateurs sur Internet ou un réseau local. Il s'agit d'une suite de protocoles standard qui définit comment les données sont envoyées, reçues et routées sur le réseau. TCP est responsable de l'assurance de la fiabilité de la transmission des données tandis que IP est responsable de la transmission de ces données de manière efficace entre différents réseaux. TCP/IP est le fondement de la communication sur l'Internet et est utilisé pour une variété d'applications, y compris la navigation Web, la messagerie électronique, la voix sur IP, et plus encore.

- SNMP (Simple Network Management Protocol) est un protocole de gestion de réseau qui permet aux administrateurs réseau de surveiller et de gérer les équipements réseau à distance. Il s'agit d'un protocole standard utilisé pour gérer les équipements réseau tels que les routeurs, les commutateurs, les imprimantes et les serveurs. SNMP permet aux administrateurs de surveiller les performances du réseau, de détecter les erreurs et les pannes, et de configurer les équipements réseau à distance. Il utilise un modèle de données hiérarchique pour organiser les informations de gestion en tant que variables, qui peuvent être lues et écrites à distance à l'aide de commandes SNMP. Les équipements réseau doivent être compatibles avec SNMP pour pouvoir être gérés à distance à l'aide de ce protocole.

- Rsyslog est un logiciel de gestion de journaux (logs) open source qui permet de collecter, traiter et router des logs depuis différents équipements et systèmes d'exploitation. Il est couramment utilisé pour collecter des logs système, d'applications, de bases de données et de sécurité provenant de diverses sources telles que des serveurs, des commutateurs, des pare-feux et des routeurs. Rsyslog dispose d'une architecture modulaire qui permet une configuration et une personnalisation avancées. Il prend en charge divers protocoles de collecte de logs tels que Syslog, SNMP, RELP, et TCP/UDP. Il dispose également de fonctionnalités avancées telles que la compression de logs, la journalisation de débogage, la filtre et le partitionnement de logs.
  En résumé, Rsyslog est un outil flexible et puissant de gestion de journaux qui permet aux administrateurs système de collecter et de traiter efficacement les logs de leur infrastructure, ce qui facilite la détection des pannes, des erreurs et des cyberattaques.

- GLPI est un outil de gestion des services informatiques qui permet aux organisations de suivre et de gérer efficacement leur parc informatique, de gérer les demandes des utilisateurs et de suivre les ressources matérielles et logicielles.

- PRTG (Paessler Router Traffic Grapher) est un outil de supervision réseau qui permet aux administrateurs de surveiller les performances des équipements réseau tels que les routeurs, les commutateurs, les serveurs et les applications et il permet de surveiller les performances de leur réseau, d'identifier les problèmes et d'y remédier de manière proactive.

- WMI est utilisé par les administrateurs système pour surveiller les performances du système, configurer des paramètres de sécurité, collecter des informations sur les applications et les services installés sur un ordinateur, ainsi que pour la gestion des comptes utilisateurs et la configuration des stratégies de groupe. WMI est une technologie de gestion de système puissante pour les systèmes d'exploitation Windows, qui permet aux administrateurs système de surveiller et de gérer efficacement les ressources, les services et les processus du système.

- DNS (Domain Name System) est un système de noms de domaine qui permet de traduire les noms de domaine en adresses IP numériques. Le DNS fonctionne en associant des noms de domaine à des adresses IP numériques. Lorsqu'un utilisateur saisit une URL dans son navigateur Web, le navigateur envoie une demande de résolution DNS au serveur DNS de l'utilisateur. Le serveur DNS va alors chercher dans sa base de données de noms de domaine pour trouver l'adresse IP correspondante, et retourner l'information au navigateur Web. Ce processus est invisible pour l'utilisateur, qui est simplement redirigé vers le site web demandé.

6. Tableau comparatif des solutions possibles

- Il existe d'autres outils de gestion d'incidents et de surveillance de réseau tels que Zabbix, Nagios, Centreon, etc. Cependant, nous avons choisi GLPI, SYSLOG et PRTG en raison de leur facilité de mise en place et de configuration, ainsi que de leur compatibilité avec notre environnement.

7. Documentation

7.1. Doc Technique

7.1.1.1. Comptes-rendus

https://sa-portefolio.fr/

8. Résultats attendus

- En combinant l'installation de GLPI, SYSLOG et PRTG, on peut améliorer la gestion globale de notre infrastructure informatique, en réduisant les temps d'arrêt, en améliorant les performances et en améliorant la sécurité globale de notre réseau.
- Avec GLPI, on peut créer un ticket avec un utilisateur qui se trouve dans notre Active Directory.
- Avec Rsyslog, on a accès aux journaux donc on voit l'ensemble des activités sur notre switch et pare-feu.
- Avec PRTG, j'ai créé des sondes SNMP, sur notre Cisco il y a une sonde qui contrôle la charge CPU et pour le stormshield il y a une sonde qui contrôle la charge CPU, une sonde PING et des sondes qui contrôle le trafic par interface réseau (LAN et WAN). Des sondes WMI ont été créé sur l'ensemble de notre matériel, sur mon serveur Active Directory, j'ai créé un capteur pour l'espace disque libre et un capteur pour voir les erreurs sur la réplication de mon active directory qui se trouve sur la machine de mon collègue. Sur les autres serveurs comme : FS, AD2, FS2 et RDS il y une sonde WMI pour l'espace disque libre.