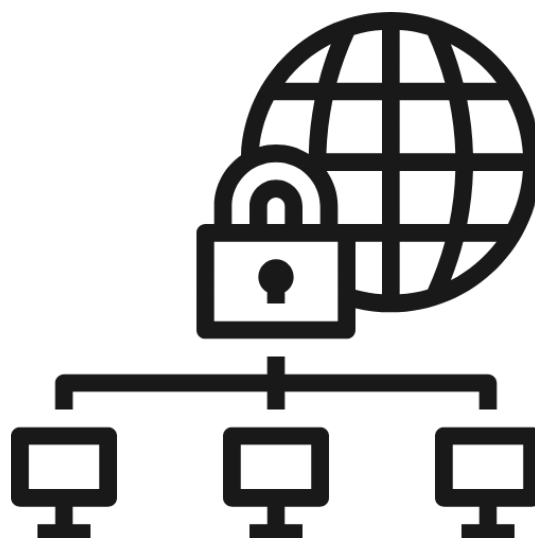


PROJET STARKINDUSTRIES

**Système d'information hautement disponible et
interconnecté**

SIO 2023 – Option SISR



Épreuve E5
-
Situation professionnelle 1

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 : RAKOTOZAFY Winness		N° candidat : 02243995935
Épreuve ponctuelle <input type="checkbox"/>	Contrôle en cours de formation <input checked="" type="checkbox"/>	Date : 26 / 04 / 2023
Organisation support de la réalisation professionnelle Cette situation professionnelle consiste à mettre en place deux infrastructures LAN hautement disponible et interconnecté entre deux sites : Strasbourg et Mulhouse à travers Internet. Compte tenu de l'analyse des risques que l'interconnexion par Internet, ce projet intègre l'implémentation d'un VPN site à site, des serveurs de fichiers hautement disponibles et d'une solution de sauvegarde.		
Intitulé de la réalisation professionnelle Projet STARKINDUSTRIES		
Période de réalisation : 02/09/2022 au 31/12/2022 Lieu : Strasbourg Modalité : <input type="checkbox"/> Seul(e) <input checked="" type="checkbox"/> En équipe		
Compétences travaillées <input checked="" type="checkbox"/> Concevoir une solution d'infrastructure réseau <input checked="" type="checkbox"/> Installer, tester et déployer une solution d'infrastructure réseau <input checked="" type="checkbox"/> Exploiter, dépanner et superviser une solution d'infrastructure réseau		
Conditions de réalisation¹ (ressources fournies, résultats attendus) <ul style="list-style-type: none"> - Des pare-feux pour sécuriser le réseau intranet - Une connexion intersite sécurisée qui passe par Internet - Des contrôleurs de domaine redondés sur les deux sites avec un SEUL domaine - Des serveurs de fichiers redondés sur les deux sites - Des serveurs de contrôle d'accès Internet sécurisé avec authentification centralisée - Des serveurs de sauvegarde complète des contrôleurs de domaine - Des postes clients 		
Description des ressources documentaires, matérielles et logicielles utilisées² <ul style="list-style-type: none"> - 2 pare-feux sous pfSense FreeBSD - 1 tunnel VPN site à site avec protocole IPsec - 4 serveurs AD, DNS, DHCP, DFS-R, et RADIUS dont : 2 Windows Server 2019 en GUI, et 2 en version Core - 2 serveurs de sauvegarde sous TrueNAS FreeBSD : 1 sous Strasbourg / 1 sous Mulhouse - 2 Clients Windows 10 : 1 Strasbourg / 1 Mulhouse 		
Modalités d'accès aux productions³ et à leur documentation⁴ Les documentations de présentations et technique du projet sont accessibles depuis la section E4-E5 de mon portfolio via le lien suivant : https://www.winness-rakotozafy.fr		

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.

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

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

Table des matières

Contexte.....	4
Besoins et objectifs.....	4
Solutions retenues et argumentations.....	5
Annuaire authentification : Microsoft Active Directory	5
Accès des données sur le réseau et redondance des données : DFS et DFSR.....	5
Solution de sauvegarde complète : SAN, cible iSCSI avec TrueNAS.....	5
Solution de clichés instantanés : Volume Shadow Copy.....	6
Routeur/pare-feu : pfSense.....	6
Solution VPN Site à Site : IPSec.....	6
Solution portail captif : pfSense + Active Directory.....	7
Schéma réseau	9
Coût du projet.....	10
Planning prévisionnel	12
Planning réel	12
Planning prévisionnel vs réel	13
Résultats attendus vs Résultats obtenus	14
Conclusion.....	15
Améliorations possibles	15

Contexte

L'entreprise STARKINDUSTRIES souhaite élargir son activité en France dans la région de l'Alsace. Son site principal dans ce pays sera donc basé à Strasbourg et une extension à Mulhouse.

Soucieux de la sécurité de son système d'information, et dans le cadre de son Plan de Continuité d'Activité et de Reprise d'Activité, la DSI implémenté sur France souhaite harmoniser les deux sites, et rendre hautement disponible les données entre chaque site.

Ainsi, en cas de défaillance sur l'un des sites (incendies, sinistre, pannes matérielles, etc.), les données des utilisateurs pourront continuer à être accessibles, et restaurés avec un processus de restauration bien défini.

Enfin, sur la sécurité des accès, un portail captif est mis en place pour permettre aux utilisateurs de s'authentifier avant de pouvoir accéder à Internet.

Besoins et objectifs

Les **besoins du projet** selon les décisions prises par la DSI en accord avec la Direction Générale sont :

- Mise à disposition des équipements nécessaires à la création des nouvelles salles informatiques pour les activités de STARKINDUSTRIES en France.
- Installation des serveurs conformément à la décision de la direction générale et du DSI, et respect de tous règlements et lois du numérique de l'État français et l'Union européenne, tout en assurant l'optimisation et une facilitation d'administration au sein de l'équipe technique.
- Mise en place d'un système d'information harmonisé et ainsi interconnecté de manière sécurisée entre les deux sites.
- Adoption d'une approche cybersécurité sur les accès des utilisateurs et Internet

Ainsi, pour répondre à ces besoins, les **objectifs du projet** fixés par l'équipe technique sont :

- Mise en œuvre d'une liaison WAN inter-sites chiffrée entre Strasbourg et Mulhouse
- Mise en place des serveurs et rôles/services en haute disponibilité
- Mise en œuvre d'un portail captif avec authentification forte et sécurisé se basant sur les identifiants AD (SSO)
- Accès des données stockant les dossiers personnels à partir des deux sites par la redondance des données partagées.

Solutions retenues et argumentations

Dans l'élaboration de ce projet, compte tenu du cahier des charges établi, des besoins exprimés par l'entreprise, et les objectifs fixés du projet, ci-dessous les **solutions retenues** avec leurs avantages et inconvénients :

Annuaire authentification : Microsoft Active Directory

Pour l'annuaire d'authentification, nous recommandons de recourir à l'annuaire Active Directory sous Windows Server 2019. Le choix se justifie par le fait qu'il puisse satisfaire les besoins du client, par la présence d'une interface graphique interactive (user-friendly), qui facilite la création, la gestion et l'administration des objets de l'environnement.

Un serveur d'annuaire est un serveur qui fournit un service d'annuaire, permettant une gestion optimale des objets sur le réseau, normalisation, authentification et l'administration de plusieurs utilisateurs/groupes/services sur un large réseau d'un domaine.

Et encore de plus, étant sur un serveur sous Windows Server, primo le service DNS sera automatiquement installé avec le rôle AD DS, mais nous installerons également le service DHCP afin de permettre au client de s'attribuer une adresse IP de manière dynamique.

Accès des données sur le réseau et redondance des données : DFS et DFSR

Pour la solution d'accès des données (utilisateurs, éducatives, organisationnelles) sur le réseau, nous mettrons à disposition le système de fichiers distribués (DFS), disponible dans la licence Windows Server.

Ce système permet de structurer les fichiers partagés sur différents serveurs de réseau de façon logique. Il permet de référencer un ensemble de partages qui sera accessible de manière uniforme, puis de centraliser l'ensemble des espaces disponibles sur l'ensemble de partage. Le DFS fonctionne avec un système d'espace de noms, qui permet donc de faciliter la tâche de l'administrateur, sans recourir à l'utilisation des chemins UNC ([\\nomserver\nompartage](#)).

De plus, DFS se repose sur le partage SMB qui est implémenté de base dans les systèmes de fichiers de Windows, dont nous expliciterons plus spécifiquement dans une documentation technique à destination des administrateurs.

Solution de sauvegarde complète : SAN, cible iSCSI avec TrueNAS

La sauvegarde est un principe, une norme à mettre à disposition dans un environnement de production, et rentre dans un contexte de sécurité, et de disponibilité des données. Elle n'est pas à négliger, et doit être mise en place et redondée sur plusieurs sites, ce que nous vous proposerons dans cette solution.

La sauvegarde complète des données intégrales des serveurs seront stockés dans un stockage SAN montée par TrueNAS, accessible par les serveurs par un montage iSCSI, qui permettra de créer des disques virtuels pointant vers les disques physiques de TrueNAS.

L'intérêt et l'avantage est qu'en cas de panne de nos serveurs, les données seront encore disponibles sur nos serveurs TrueNAS, et encore, grâce au recours à des disques SAN, nous proposons un gain de performance considérable sur la lecture et l'écriture des disques de sauvegarde, facilitant ainsi la gestion et l'administration des sauvegardes par l'équipe technique.

Aussi, avec les deux disques physiques de notre serveur SAN, nous appliquerons une tolérance aux pannes en

configurant et mettant en place un RAID 1 (miroir) afin de garantir la sécurité et la disponibilité des données de STARKINDUSTRIES Inc.

Solution de clichés instantanés : Volume Shadow Copy

Shadow Copy utilise l'utilitaire Volume Shadow Copy Service (VSS) afin de restaurer un fichier, un dossier en volume sur un serveur de fichiers. L'intérêt est que VSS permet de prendre les clichés instantanés d'un disque physique entier sans pour autant nuire aux activités du serveurs/disques cibles.

A priori, nous considérerons que les clichés instantanés permettent de faire « une sauvegarde » d'une partition en ne stockant que les fichiers modifiés. Toutefois, les snapshots ne sont pas considérés comme une réelle sauvegarde, dans la mesure où les snapshots seront tout de même stockés sur le disque en usage, en différence d'une sauvegarde délocalisée, et donc n'est pas tolérable aux pannes hormis une configuration permettant de stocker les clichés instantanés sur un point de montage disque virtuel délocalisé.

En tenant compte de la demande et des besoins du clients, l'implémentation de la solution de clichés instantanés est une alternative intéressante en matière de sauvegarde, permettant de dépanner le plus rapidement possible l'utilisateur finale en cas d'une mauvaise manipulation effectuée par ledit utilisateur.

Routeur/pare-feu : pfSense

Afin de sécuriser votre réseau interne, nous vous proposons d'installer un routeur, qui sera également votre pare-feu afin de minimiser les coûts.

La solution que nous vous recommandons est pfSense, qui est une solution open-source, gratuit, et englobe diverses fonctionnalités. Pfsense a pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD.

PfSense utilise le pare-feu à états qui garde en mémoire l'état de connexions réseau, comme les flux TCP, ou les communications UDP qui le traversent. Le fait de garder en souvenir les états de connexions précédents permet de mieux détecter et écarter les intrusions et assurer une meilleure sécurité), introduisant ainsi une fonctionnalité d'IDS/IPS.

Le pare-feu utilisé par pfSense est Packet Filtre, (pare-feu logiciel et officiel d'OpenBSD, écrit à l'origine par « Daniel Hartmeier » qui est un logiciel libre gratuit).

PfSense comporte des fonctions de routage et de NAT, lui permettant de connecter plusieurs réseaux informatiques. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires, et convient aussi bien pour la sécurisation d'un réseau domestique ou d'entreprise.

Solution VPN Site à Site : IPSec

IPSec, pour Internet Protocol Security, est un protocole développé par un groupe de travail à l'IETF (Internet Engineering Task Force) depuis 1992 afin de sécuriser le protocole IP. IPSec a l'avantage d'offrir l'ensemble des services de sécurité attendus sur un VPN :

Pour la solution du VPN site à site, nous avons fait le choix de recourir au protocole **IPSec/IKEv2** par le fait que :

- IPSec est supporté et natif sur une majorité d'équipements réseaux
- IPSec est un standard ouvert : adapté sur plusieurs protocoles d'authentification et algorithmes de

chiffrement ;

- IPSec est sécurisé : chiffrement de point à point des communications, et intervient à une couche basse du modèle OSI et TCP/IP (niveau 3) opérant ainsi une sécurité dès le protocole IP avant de transporter les données.

Solution portail captif : pfSense + Active Directory

Pour répondre aux besoins demandés par l'entreprise, nous avons fait le choix de partir sur la solution du portail captif de pfSense avec AD RADIUS.

En effet, le choix s'est porté par le fait que :

- L'outil est gratuit et open-source
- L'équipe de prestataire informatique a des connaissances dans la mise en place de la solution, nous permettant ainsi d'être plus efficace dans le déploiement de la solution.
- Avoir une seule machine dédiée pour pfSense nous permet d'amenuiser les coûts d'achats de matériel ou de consommation pour le projet

PfSense intègre nativement une fonctionnalité de portail captif qui peut être utilisé soit en utilisant la base de données locale des utilisateurs, soit en redirigeant l'authentification des utilisateurs vers un serveur externe disposant d'un protocole RADIUS (dans notre cas, les serveurs Active Directory).

L'authentification RADIUS nécessite que l'on soit dans un domaine administré par un contrôleur de domaine qui définit les utilisateurs et leur mot de passe. Ainsi, pour mettre en place le portail captif en utilisant les mêmes identifiants Active Directory, en réponse à vos besoins et à votre demande, le serveur RADIUS (avec AD) et le routeur/pare-feu pfsense doivent être dans le même domaine, et ils communiquent dans le but d'autoriser ou non les utilisateurs à se connecter.

Toutefois, le portail captif sous pfSense présente des défauts en termes de pratique et d'administration, notamment lié à la conformité à la RGPD et de la CNIL.

Pour plus de détails, la journalisation des activités (logs) de connexion des utilisateurs ne sont pas supprimés automatiquement au bout d'un an (durée maximale de conservation des traces de connexions des utilisateurs), mais surtout dans le fait que les utilisateurs ne sont pas avertis à chaque consultation des journaux d'activités des administrateurs pouvant ainsi porter atteinte au respect de la vie privée de ces derniers.

Pour synthétiser l'étude des solutions retenues pour le projet, ci-dessous un tableau récapitulatif avec les avantages et les inconvénients de chaque solution :



Solutions retenues		
Annuaire authentification : Active Directory	<ul style="list-style-type: none"> - Administration en interface graphique - Authentification unifiée - Gestion des services et utilisateurs simplifiés 	<ul style="list-style-type: none"> - Nécessite des ressources matérielles importantes - Coûteux (Licence Windows)
Accès des données sur le réseau et redondance des données : DFS – DFSR	<ul style="list-style-type: none"> - Tolérances aux pannes - Performant - Sécurité - Scalabilité 	<ul style="list-style-type: none"> - Coûteux (Licence Windows) - Solution propriétaire
Solution de sauvegarde complète : Cible iSCSI → SAN	<ul style="list-style-type: none"> - Tolérances aux pannes - Performant (vitesse de lecture accrue) - Système d'exploitation TrueNAS : gratuit 	<ul style="list-style-type: none"> - Configuration méticuleuse - Nécessite beaucoup de ressources matérielles
Solution de clichés instantanés : Shadow Copy	<ul style="list-style-type: none"> - Flexibilité - Vitesse de restauration 	<ul style="list-style-type: none"> - N'équivaut pas une vraie sauvegarde - Non tolérable aux pannes matérielles (sauf délocalisation des clichés) - Solution propriétaire Microsoft
OS routeur/pare-feu : pfSense	<ul style="list-style-type: none"> - Gratuit et open-source - Intègre des solutions VPN natifs - Peu gourmand en ressources - Intègre des plugins IDS/IPS - Intègre le NAT/PAT 	<ul style="list-style-type: none"> - Prise en main de l'interface difficile au début - Langue du clavier en ENG par défaut (difficile à prendre en main pour les adeptes du clavier FR) - Pas de mise à jour régulier en comparaison de ses concurrents
Solution VPN site à site : IPSec	<ul style="list-style-type: none"> - Natif sur une grande majorité d'équipement réseau - Optimale pour une communication site-a-site - Protocole sécurisé dès l'échange IP entre deux sites 	<ul style="list-style-type: none"> - Peut facilement être bloqué par les règles de pare-feux si les ports spécifiques au tunnel ne sont pas autorisés. - Requiert l'ouverture de certains ports : 50, 51, 500 et 4500
Solution portail captif : pfSense + AD Radius	<ul style="list-style-type: none"> - Open-source et gratuit - Natif dans le routeur/pare-feu - Centralisation des authentifications par RADIUS - Diverses documentations disponibles sur Internet - Facilité de mise en production 	<ul style="list-style-type: none"> - RADIUS n'est disponible que sur la version graphique de Windows Server

Schéma réseau

Pour mieux comprendre la réalisation du projet, ci-dessous le schéma du réseau complet :

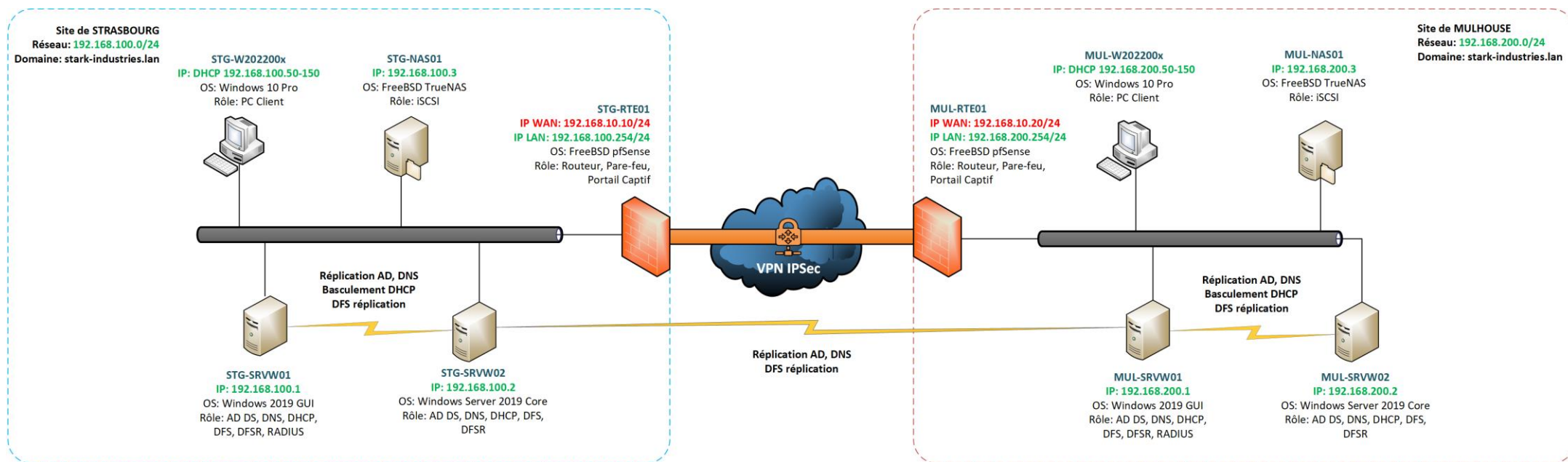


Figure 1 : Schéma réseau complet

Pour compléter le schéma, veuillez trouver le tableau d'adressage établi pour chaque ressource numérique :

SITES	NOM	ADRESSE IP	MASQUE	PASSERELLE	DNS
STRASBOURG	RTE-STG01	LAN :192.168.100.254 WAN :192.168.10.10	255.255.255.0	WAN :192.168.10.254	192.168.100.1 192.168.100.2
	STG-SRVW01	192.168.100.1	255.255.255.0	192.168.100.254	192.168.100.1 192.168.100.2
	STG-SRVW02	192.168.100.2	255.255.255.0	192.168.100.254	192.168.100.1 192.168.100.2
	STG-NAS01	192.168.100.3	255.255.255.0	192.168.100.254	192.168.100.1 192.168.100.2
	STG-W2022xx	DHCP	255.255.255.0	192.168.100.254	192.168.100.1 192.168.100.2
MULHOUSE	RTE-MUL01	LAN :192.168.200.254 WAN :192.168.10.20	255.255.255.0	WAN :192.168.10.254	192.168.200.1 192.168.200.2
	MUL-SRVW01	192.168.200.1	255.255.255.0	192.168.200.254	192.168.200.1 192.168.200.2
	MUL-SRVW02	192.168.200.2	255.255.255.0	192.168.200.254	192.168.200.1 192.168.200.2
	MUL-NAS01	192.168.200.3	255.255.255.0	192.168.200.254	192.168.200.1 192.168.200.2
	MUL-W2022xx	DHCP	255.255.255.0	192.168.200.254	192.168.200.1 192.168.200.2

Coût du projet

Pour l'entreprise STARKINDUSTRIES, l'utilisation de ces ressources impliquerait des frais. Afin de clarifier la situation, un tableau présentant le coût total des équipements à acheter et le coût des services nécessaires pour la réalisation du projet est fourni ci-dessous.

DEVIS

STARKINDUSTRIES INC.

777 Avenue de l'Europe, 67000 Strasbourg

07 07 07 07 07

tony-stark@stark-industries.com

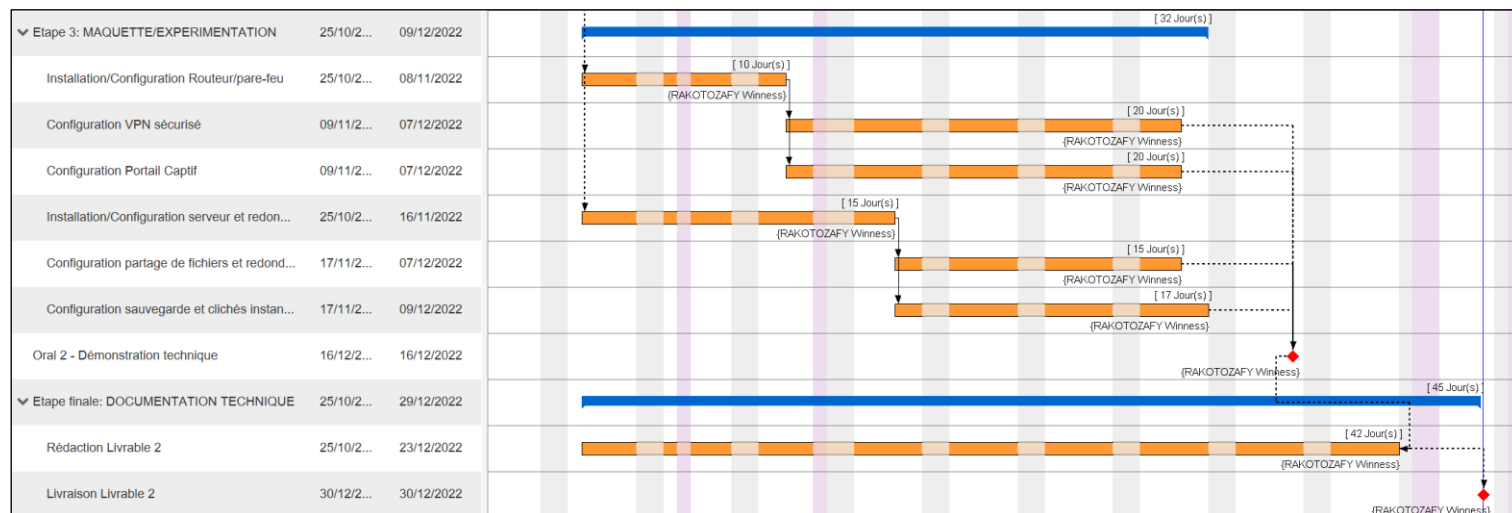
Objet : Coût total du projet

Description	Quantité (unité/jours)	Prix Unitaire HT	TVA	Total HT
TP-Link TL-SF1024 Switch 24 Ports 10/100 Mbps	10	75,20 €	20 %	752,00 €
Routeur/Pare-feu NetGate 7100 1U BASE Pfsense+	2	959,20 €	20 %	1 918,40 €
Serveur Smart Value PowerEdge T150	6	1 124,90 €	20 %	6 749,40 €
Lenovo M80t Celeron G7400 - Sans OS	60	224,50 €	20 %	13 470,00 €
Moniteur LED 21,5" Philips 223V5LSB2/10 - 1920 x 1080 - VGA	60	74,80 €	20 %	4 488,00 €
Clavier USB Lenovo 300	60	9,60 €	20 %	576,00 €
Souris Lenovo	60	7,68 €	20 %	460,80 €
Câble réseau RJ45-Cat6 10 m	200	3,50 €	20 %	700,00 €
Licence Windows Server 2019 (+10 CALs Users Pack)	4	1 344,00 €	20 %	5 376,00 €
Licence Windows 10 Pro Retail	60	119,99 €	20 %	7 199,40 €
Licence Windows CALs Pack 5 Users	12	104,79 €	20 %	1 257,48 €
Etude du marché et solutions technique	5	300,00 €	20 %	1 500,00 €
Installation et configuration des serveurs Windows en haute disponibilité	30	300,00 €	20 %	9 000,00 €
Installation et configuration des routeurs/pare-feu	30	500,00 €	20 %	15 000,00 €
Mise en place d'une solution de sauvegarde	20	300,00 €	20 %	6 000,00 €
Mise à disposition des équipements en salle de formation	10	300,00 €	20 %	3 000,00 €
Brassage des équipements reseaux	5	300,00 €	20 %	1 500,00 €

Montant Total HT	78 947,48 €
Total TVA	15 789,50 €
Montant Total TTC	94 736,98 €

Planning prévisionnel

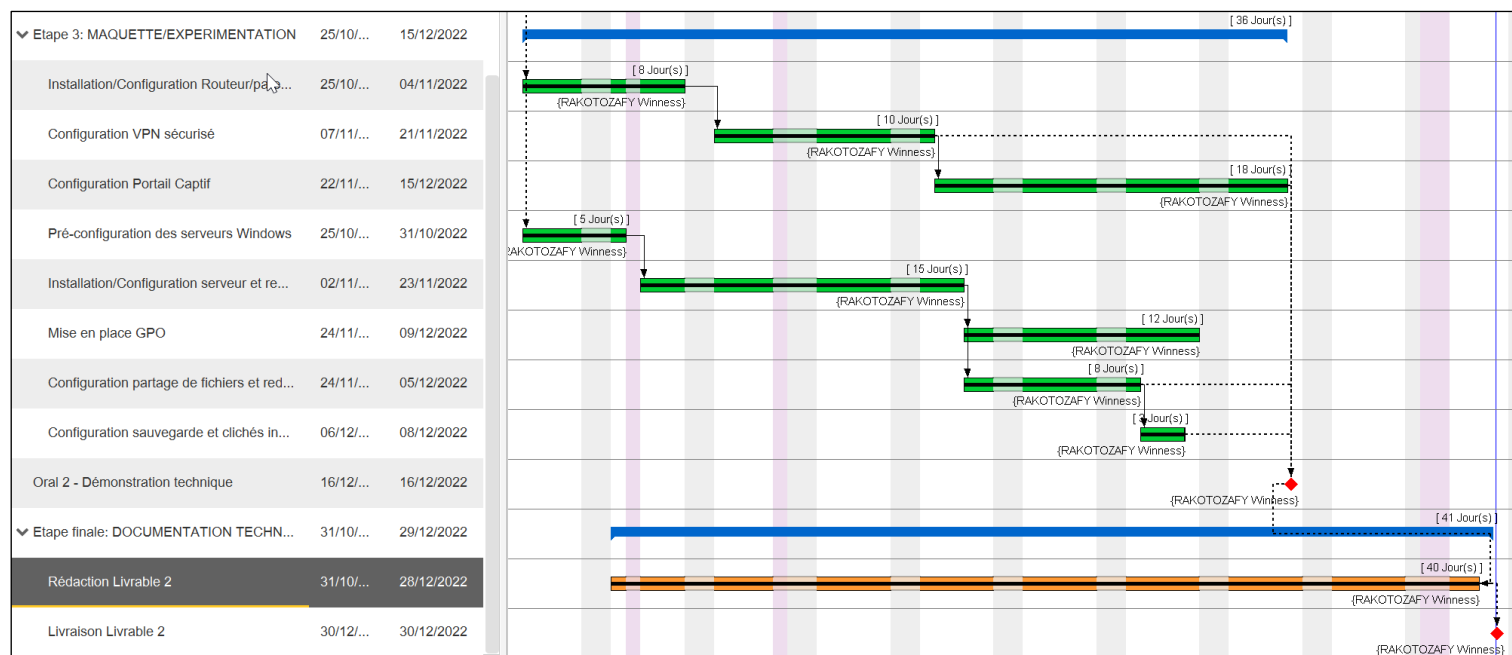
Pour la réalisation du projet, ci-dessous le planning prévisionnel établi avec les différentes tâches à effectuer pour atteindre les objectifs fixés :



Planning réel

Toutefois, dans la conduite du projet, plusieurs facteurs ont influencé notre mode opératoire, la divergence entre le temps prévu sur le planning prévisionnel, et le planning final du projet.

Pour avoir plus d'éclaircissement sur ce contexte, ci-dessous le planning réel du projet :



Pour faciliter la lecture et l'analyse de la comparaison, le décalage et les tâches modifiées sur le planning réel sont marqués en **couleur verte**.

Planning prévisionnel vs réel

De ce fait, par ces diagrammes, nous pouvons constater que, en premier lieu, quelques tâches ont été rajoutées, notamment sur la partie de l'installation et configuration des serveurs Windows, impactant ainsi la planification initiale en temps et en ressources utilisés, mais qui sera à la charge de l'équipe de projet, et non du client.

En second lieu, nous pouvons constater un léger décalage sur la tâche du **Portail Captif**, lié à diverses causes, notamment sur la redondance, et le dépannage réseau sur l'un des routeur/pare-feu, étant le client RADIUS.

Tout d'abord, le rajout des tâches a été réalisée en cause de la non-précision du planning prévisionnel sur les différentes à effectuer au cours du projet, pouvant ainsi troubler l'organisation de l'équipe du projet.

Toutefois, cette initiative rentre également dans un objectif d'alléger le chef de projet en termes d'administration des serveurs afin d'aboutir à une délégation de tâches vers un technicien notamment marqué sur les **configurations et mises en place des GPO**. La tâche pré-configuration des serveurs (changement de nom, configuration réseau, association des cartes réseaux...) a été rajoutée pour un besoin de conformité et d'harmonisation afin que les serveurs soient prêts avant tout **Ajout des rôles et fonctionnalités**.

Par la suite, comme mentionné précédemment, nous avons également rencontré un léger décalage sur la tâche de **configuration du portail captif**.

En effet, ce retard est dû à des problèmes rencontrés pour la mise en service du portail captif qui sont : l'ouverture des ports exploités par RADIUS sur les serveurs Windows dont les **ports UDP 1812, 1813, 1645 et 1646**, mais aussi l'autorisation des flux à travers le pare-feu pfSense en lui-même. Diverses solutions ont été sollicités pour pallier et rendre fonctionnel les solutions.

Enfin, le retard est également dû à la recherche d'alternative quant à la non-disponibilité du service NPAS sur le serveur Core (cf. [Documentation officielle de Microsoft](#)).

Enfin, nous avons constaté que certaines tâches ont été réalisées plus tôt que prévu, notamment sur la tâche de « **Mise en place de sauvegarde et des clichés instantanés** ». Cette tâche, au départ prévu pour 20 jours, et donc **160 heures** (taux de travail 8h/jour ouvrable) a pu être concrétisée en **24 heures**. La planification principale de 160 heures a été imposée compte tenu du temps d'adaptation, et de la difficulté de mise en place jugé initialement « difficile », car ce fut une découverte de technologie pour tous les membres du projet.

Cependant, lors de la mise en application et configuration, la configuration et la mise en application ont pu être entamée le plus tôt possible.

Résultats attendus vs Résultats obtenus

De manière générale les résultats attendus sont homogènes avec les résultats obtenus. Nos lots ont été testés en amont avant la présentation finale.

Cependant nous pouvons noter un écart sur la mise en place du portail captif. En effet, nous avons du mal à le déployer sur le serveur Windows Core, car la version Core ne dispose pas du service NPS pour l'authentification. C'est pour cela que nous avons dû décaler la mise en place de ce lot. Après maintes recherches, nous avons constaté qu'il nous était impossible de le mettre en place et cela a été remonté à la présentation finale.

Après analyse de nos lots il aurait été judicieux de mieux les répartir, en effet Corentin avait pris en charge d'une partie du portail captif sous pfSense. Dylan ayant mis en place pfSense aurait pu prendre ce lot avec mais nous n'avions pas fait attention sur le coup pour la répartition des lots.

Toutefois, le **bilan fut très satisfaisant** puisque nous rentrons dans les délais en termes de résultats obtenus.

L'initiative proposée par le chef de projet de mettre en place des documents techniques en amont pour se partager les connaissances a été grandement utile, ce qui nous allège encore plus notre charge de travail post-présentation finale du projet.

Pour une visualisation comparative des résultats, veuillez-vous référer aux deux tableaux suivants :

Résultats attendus

LOTS	Résultats
Routeurs / Pare-feu + VPN IPSec	✓
ADDS, DNS, DHCP, DFS, RADIUS + Redondance (A+B)	✓
DFS et DFSR + Serveurs de sauvegarde + SAN/iSCSI + Shadows Copy	✓
Portail Captif	✓
GPO (Stratégie de groupe)	✓

Résultats obtenus

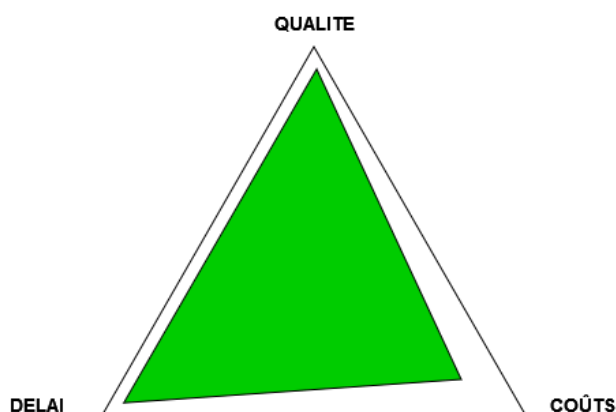
LOTS	Résultats
Routeurs / Pare-feu + VPN IPSec	✓
ADDS, DNS, DHCP, DFS, RADIUS + Redondance (A+B)	✓
DFS et DFSR + Serveurs de sauvegarde + SAN/iSCSI + Shadows Copy	✓
Portail Captif	✓ ✗
GPO (Stratégie de groupe)	✓

Conclusion

Le projet a été un succès grâce à la définition claire et précise de ses objectifs, à la mise en place d'un plan de projet détaillé, à une gestion efficace des ressources, hormis le léger décalage du budget final. Malgré une difficulté vis-à-vis de la communication et à un suivi régulier du progrès, des précautions ont été mis en œuvre pour la réussite de ce projet.

Tous les objectifs du projet ont été atteints en plus des propositions réalisés sur le projet. Les résultats ont été conformes aux attentes et ont contribué de manière significative à atteindre les objectifs, et les clients ont exprimé leur satisfaction lors de la présentation de clôture et de démonstration technique, dans lequel chaque spécificité technique a été réalisée correctement selon la perspective du client.

En termes de **Qualité-Coût-Délai**, pour schématiser l'état finale du projet, veuillez-vous référer au schéma suivant :



Améliorations possibles

Pour reprendre ce qui a été mentionné précédemment, notamment sur les solutions envisagées, les améliorations possibles ont été les suivants dans la conduite du projet :

- Amélioration de la communication interne
- Mise en place d'une plus grande répartition des tâches
- Prévoir une solution de sauvegarde des matériels d'expérimentation, et appliquer si possible la [règle du 3-2-1](#).
- Réajustement des coûts et calcul budgétaire sur la réalisation du projet

Et dans le cadre de la technique, afin de mieux sécuriser le SI (système d'information), diverses propositions sont mises en avant par l'équipe de projet dont :

- Mise en place d'un serveur proxy filtrant pour l'activation des blacklist/whitelist sur la navigation des utilisateurs → moins de risque de propagation de malware provenant d'Internet.
- Mettre en place une seconde méthode d'authentification avec LDAPS (communication chiffrée) pour le portail captif → Redondance du portail captif
- Mise en place des certificats SSL sur l'accès au portail captif (connexion HTTPS) afin que les identifiants utilisés par les utilisateurs, qui sont leur propre identifiant AD ne passent pas en clair sur le réseau interne.
- Mise en place d'une passerelle en très haute disponibilité → Redondance au niveau des routeurs et pare-feu car dans le contexte actuel, si l'un des routeurs tombent en panne, la communication inter site sera en panne. Cependant, de forts coûts supplémentaires seront à envisager de la part du client.