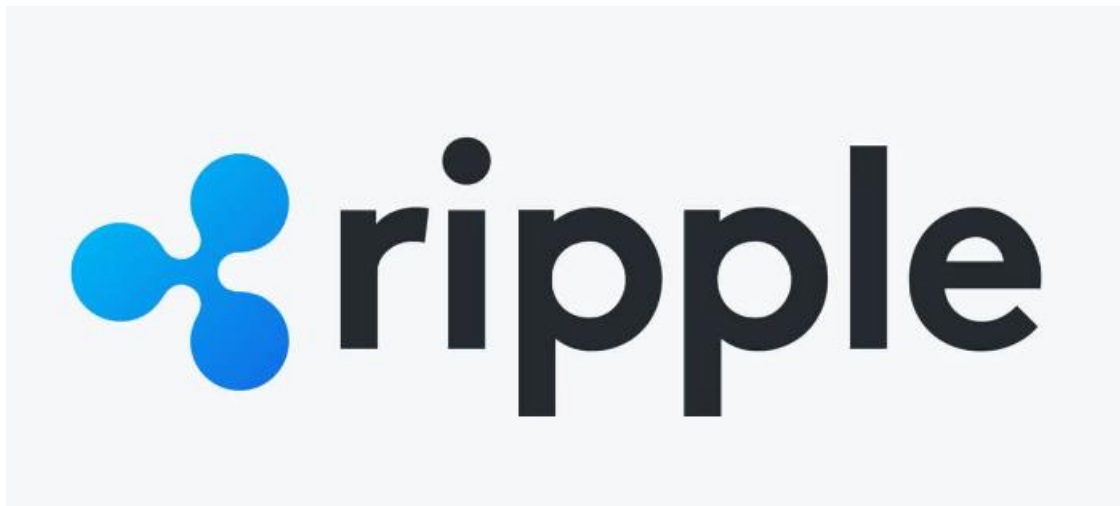


Projet Ripple
-
BTS SIO 2023 Option SISR



Epreuve 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 : BOLIDUM Théo		N° candidat : 02243995880
Épreuve ponctuelle <input type="checkbox"/> Contrôle en cours de formation <input checked="" type="checkbox"/>		Date : 26/04/2023
Organisation support de la réalisation professionnelle La situation professionnelle consiste à mettre en place une nouvelle infrastructure entre deux sites distants. Elle vise à implanter sur le réseau de l'association, en intégrant des services comme : Authentification forte, Portail Captif, Tunnel VPN, Redondance.		
Intitulé de la réalisation professionnelle Projet Ripple		
Période de réalisation : 14/09/2022 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"> • 2 serveurs comme serveur principal de Mulhouse et Strasbourg (annuaire, serveur de noms) • 2 serveurs comme serveur secondaire de Mulhouse et Strasbourg • 2 routeurs/pare-feux pour l'accès à internet et le tunnel VPN entre les sites (sécurisé / chiffré) • 2 serveurs de stockage pour le stockage des données et la mise en place du DFS • Postes client 		
Description des ressources documentaires, matérielles et logicielles utilisées² <ul style="list-style-type: none"> • 4 Windows Server 2019 • 2 routeurs, Pare-feux Pfsense • 2 serveurs TrueNAS • Postes client 		
Modalités d'accès aux productions³ et à leur documentation⁴ https://theo-bolidum.github.io/portfolio/		

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 de réseau mis en place et configurations des services.

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

Table des matières

Contexte.....	5
Besoins et contraintes.....	5
Solutions retenues et argumentations.....	6
Schéma réseau	8
Coût du projet	10
Planning prévisionnel	11
Planning réel	11
Planning prévisionnel vs réel	12
Conclusion.....	12
Améliorations possibles	12

Contexte

L'amélioration du service aux utilisateur et faciliter l'administration en passant par la création d'un système d'information indépendant ainsi que l'uniformisation du Système Informatique.

Une liaison inter-sites entre le site de Strasbourg et Mulhouse par le biais d'un VPN et une redondance des services pour une haute disponibilité des services informatique.

Réduire les couts de possession et d'exploitation en ayant une documentation complète de l'installation, la configuration ainsi que l'exploitation et cela facilitera l'administration.

Faciliter le travail collaboratif au niveau régional en utilisant des Serveurs VPN Site a Site afin de partager les données qui seront accessible depuis le site de Strasbourg et Mulhouse en connexion sécurisé ainsi qu'un serveur de redondance pour une haute disponibilité.

La sécurité des systèmes et des données en mettant en place la conformité légale de la mise à disposition d'un accès internet.

Une redondance des serveurs pour une haute disponibilité des Services et des données ainsi qu'une sauvegarde régulière des serveurs pour avoir un backup.

Besoins et contraintes

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 formations des employés de Ripple basé à Mulhouse et à Strasbourg
- Aménagement des nouvelles salles informatiques pour répondre au cahier des charges techniques, souhait des professeurs et apprenants.
- 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'Etat français et l'Union Européenne, tout en assurant l'optimisation et une facilitation d'administration au sein de l'équipe technique.

Solutions retenues et argumentations

Solution VPN site-à-site

J'ai choisi IPsec via pfSense comme solution de VPN site à site sécurisé pour notre projet car c'est une solution éprouvée et stable pour les grandes infrastructures d'entreprise. IPsec est un protocole de sécurité réseau largement utilisé pour sécuriser les communications entre les réseaux privés. pfSense est une solution open-source qui permet de déployer facilement un VPN site à site et de gérer les politiques de sécurité pour protéger les communications réseau. En utilisant IPsec via pfSense, nous pouvons garantir une haute sécurité et une haute disponibilité pour les communications entre les sites distants. De plus, cette solution est économique et évolutive, ce qui répond à nos besoins pour le projet.

Solution Portail captif & Pare-feu

J'ai choisi pfSense comme pare-feu et comme portail captif pour notre projet car il offre une gamme de fonctionnalités de sécurité avancées et une grande flexibilité pour la configuration. PfSense est une solution open-source qui permet de déployer facilement un pare-feu personnalisé et de gérer les règles de sécurité pour protéger les réseaux. Le portail captif de pfSense permet également de fournir un accès Internet sécurisé aux utilisateurs externes, tout en contrôlant et en surveillant leur accès à la ressource tout cela connecté via RADIUS à l'AD. Enfin, pfSense est une solution économique et évolutive qui répond à nos besoins pour le projet.

Solution annuaire d'authentification

J'ai choisi Active Directory comme annuaire d'authentification pour notre projet car c'est une solution largement utilisée en entreprise pour la gestion des utilisateurs, des groupes et des permissions d'accès. Active Directory permet de centraliser la gestion des identités et des accès à l'ensemble des ressources de l'entreprise. Cette solution offre également une haute disponibilité et une grande sécurité pour les informations d'authentification des utilisateurs. De plus sa réputation n'est plus à prouver, la solution est parfaitement intégré dans Windows serveur.

Accès des données sur le réseau (DFS) et redondance des données (DFSR)

J'ai choisi Windows Server pour la solution DFS (Accès des données sur le réseau) et DFSR (Redondance des données) pour notre projet car c'est une solution largement utilisée en entreprise pour la gestion de la distribution et de la réplication des données entre les serveurs. DFS et DFSR permettent de fournir une haute disponibilité et une redondance des données pour les applications critiques. En utilisant Windows Server, nous pouvons bénéficier d'une solution éprouvée et stable pour la gestion des données en entreprise. Cette solution est également facilement intégrable avec d'autres services Windows tels que Active Directory, ce qui répond à nos besoins pour le projet.

Solution de sauvegarde complète (SAN, cible iSCSI)

J'ai choisi TrueNAS comme solution de sauvegarde complète pour notre projet car c'est une solution open-source éprouvée pour la gestion de données en entreprise. TrueNAS offre une gamme de fonctionnalités avancées pour la sauvegarde et la récupération des données, y compris la prise en charge de SAN et de cibles iSCSI. Cette solution permet également de mettre en place une politique de sauvegarde personnalisée pour répondre aux besoins spécifiques de notre entreprise.

Solution de clichés instantanés (Shadow Copy)

L'utilisation de Shadow Copy présente de nombreux avantages pour notre entreprise. Shadow Copy est une fonctionnalité de sauvegarde intégrée à Windows Server qui permet de créer des instantanés de volumes de données en lecture seule à des intervalles réguliers. Ces instantanés peuvent être utilisés pour récupérer des versions antérieures de fichiers ou de dossiers qui ont été modifiés ou supprimés, sans avoir besoin de restaurer une sauvegarde complète. Cela permet de réduire considérablement le temps de récupération des données et de minimiser les pertes de données en cas de problème. De plus, l'utilisation de Shadow Copy est simple à mettre en place et n'entraîne pas de coûts supplémentaires pour l'entreprise, car c'est une fonctionnalité intégrée à Windows Server.

Schéma réseau

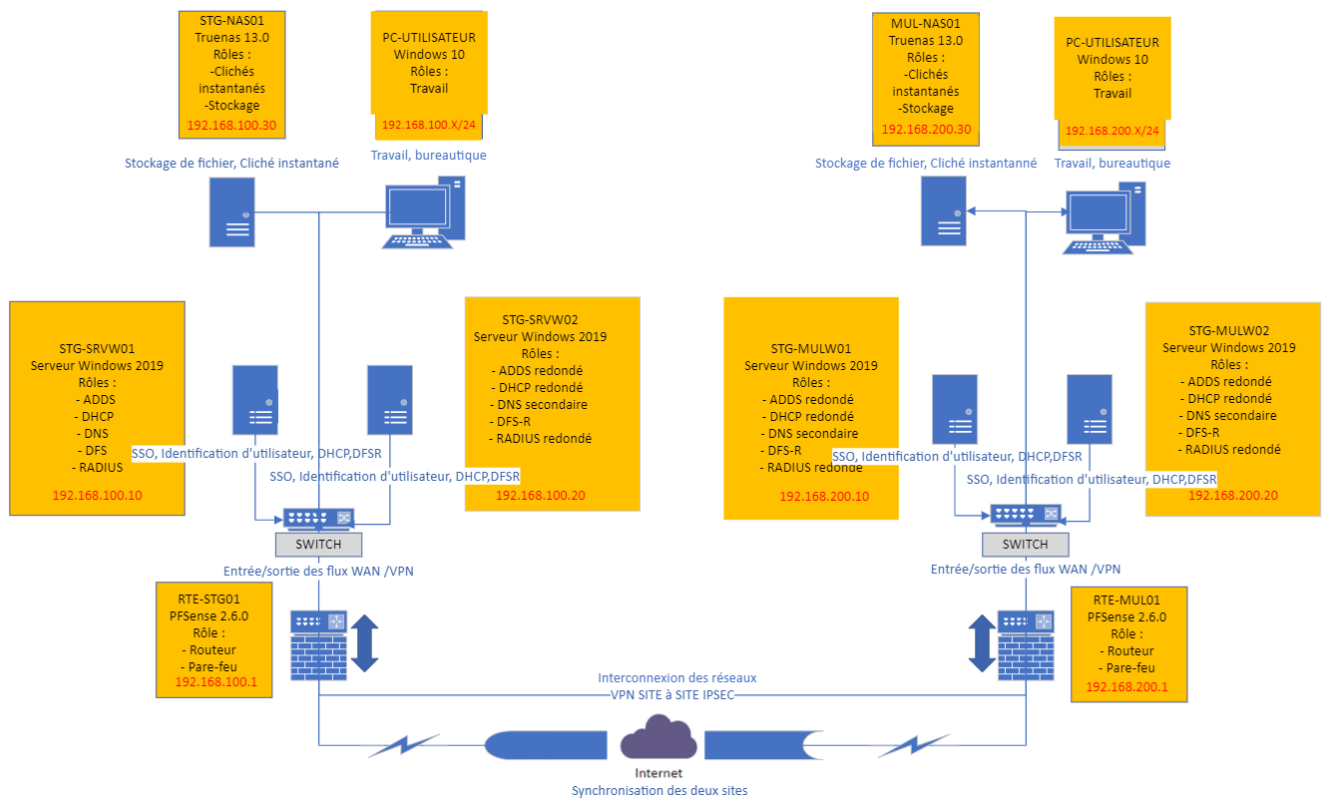


Tableau de configuration réseau

NOM	Adresse IP	Role	Version OS
RTE-STG01	192.168.100.1	- Routeur - Pare-feu	PFSense 2.6.0
RTE-MUL01	192.168.200.1	- Routeur - Pare-feu	PFSense 2.6.0
STG-SRVW01	192.168.100.10	- ADDS - DHCP - DNS - DFS - RADIUS	Windows Serveur 2019
STG-MULW01	192.168.200.10	- ADDS redondé - DHCP redondé - DNS secondaire - DFS-R - RADIUS redondé	Windows Serveur 2019
STG-SRVW02	192.168.100.20	- ADDS redondé - DHCP redondé - DNS secondaire - DFS-R - RADIUS redondé	Windows Serveur 2019
STG-MULW02	192.168.200.20	- ADDS redondé - DHCP redondé - DNS secondaire - DFS-R - RADIUS redondé	Windows Serveur 2019
MUL-NAS01	192.168.200.30	-Clichés instantanés -Stockage	Truenas 13.0
STG-NAS01	192.168.100.30	-Clichés instantanés -Stockage	Truenas 13.0
PC-UTILISATEUR	192.168.200.X/24 192.168.100.X/24	Travail, bureautique	Windows 10

Coût du projet

DEVIS

Date d'émission : 09/05/2022

Valide jusqu'au : 08/07/2022

De la part de : Network & InfraStras

234 avenue de Colmar, 67021 Strasbourg - FRANCE

SIRET : 13002267600030

N°TVA : FR 123456789

À l'attention de : Heumann

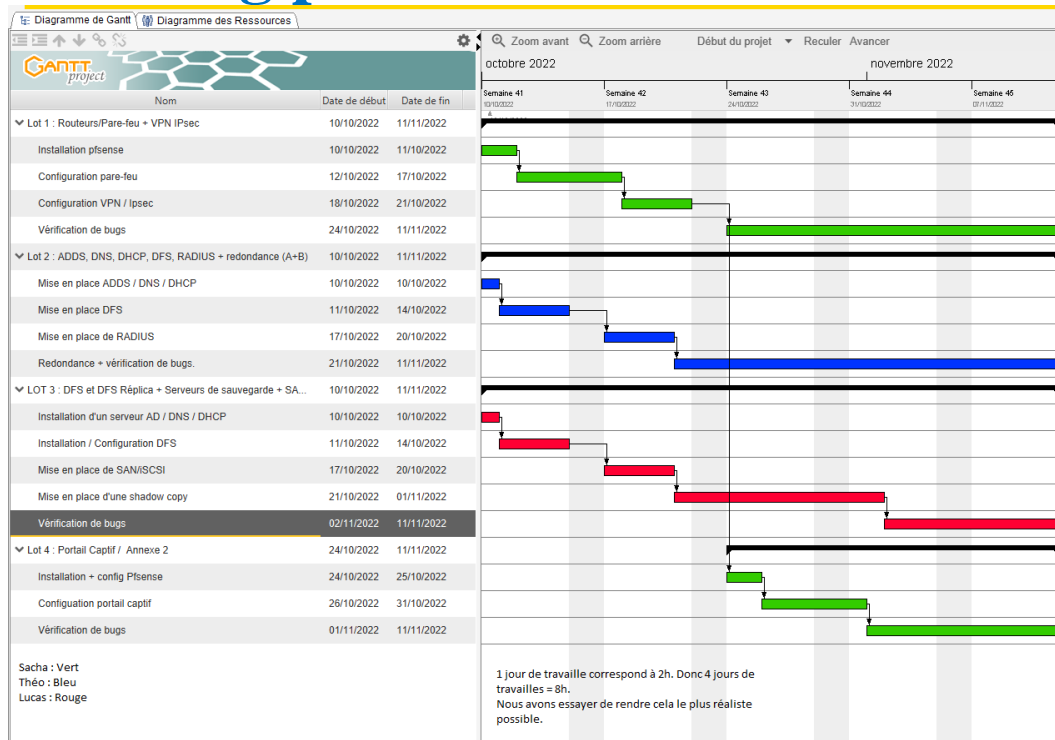
Numéro de devis : 06768

N° Client : 670

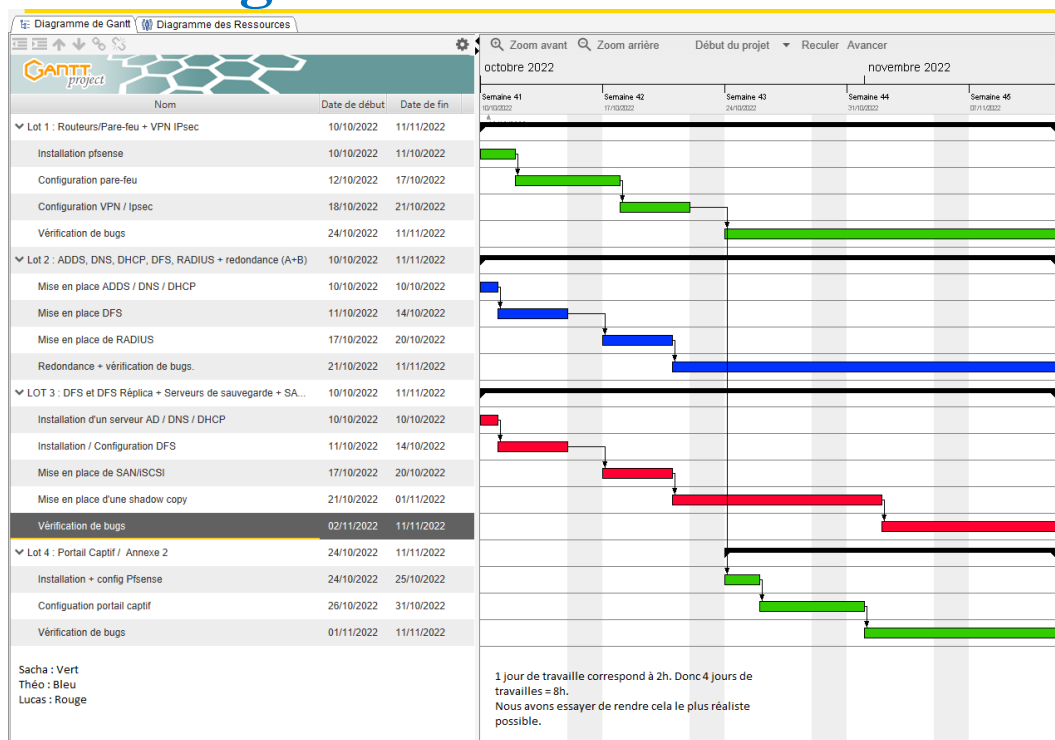
Quantité	Description	Réduction	Prix Unitaire HT	Prix TTC
	Ressources matérielles			
6	Licence Microsoft Windows Server Standard 2019 (16 Coeurs) 64 Bits	-	799,96€	4 799,76€
2	License Acronis	-	50.00€	100.00€
6	Serveur Dell PowerEdge T140 (5JV1T) Intel Xeon E-2224G, 16 Go, 1 To, Graveur DVD	-	879,95€	5 279,70€
2	Onduleur APC Back-UPS Pro 1500VA – 6 Prises	-	367,96€	919,90€
150	Cable RJ45 Cat6 – 5M	-	5,90€	885.00€
60	Pack clavier souris Logitech MK120	-	17.99€	1 079,4€
60	HP Pavilion TP01-3279nf	-	699.00€	41 940€
60	Ecran iiyama 24 pouces X2481HS-B1	-	134.93€	8 095,80€
	Ressources humaines			
6	Installation et configuration de serveur Dell	-	99,80€	
5		-		
78	Frais de main d'œuvre pour l'intervention (78 Heures)		49,90	3 892,20€
TOTAL HT			0,00€	
Total TVA 20%			0,00€	
Total TTC				0,00€
Net à payer				66 991.76€

TVA non applicable - article 293 B du CGI : CGI : Code général des impôts

Planning prévisionnel



Planning réel



Planning prévisionnel vs réel

Le planning prévisionnel a bien été respecté pour les délais, cependant nous avons été confrontés à des ralentissements pendant la période de test et de configurations. Ce temps a été rattrapé lors de la phase de test finale.

Cependant, quelques jours avant le rendu final du projet, un incident électrique a corrompu une grande partie de nos données nous avons dû refaire tout au plus vite.

Conclusion

Nous reconnaissons l'importance de la préparation et de la planification pour minimiser les risques de perte de données et d'interruption des activités. Nous avons pris conscience des conséquences négatives pour nous, de la perte de données causée par une panne électrique imprévue. En tirant les leçons de cette expérience, nous avons réalisé que l'achat d'un onduleur aurait permis de protéger nos données sensibles en cas de panne de courant. Cela aurait également évité une interruption prolongée de nos activités, une perte de temps et d'argent ainsi qu'un impact potentiel sur la livraison du projet à notre client. En conséquence, nous prenons désormais des mesures proactives pour garantir la sécurité et la continuité de nos activités, en nous assurant que nous disposons des équipements et des plans nécessaires pour faire face à toute situation d'urgence.

Améliorations possibles

Deux axes sont envisageables pour l'amélioration de l'infrastructure.

En premier lieu il serait préférable de mettre en place un certificat SSL pour le portail captif afin d'utiliser une connexion sécurisée pour les utilisateurs via le protocole HTTPS.

En second temps, nous recommandons la mise en place d'un deuxième routeur/firewall PfSense sur chaque site en redondance afin d'éviter toute coupure intersites en cas de panne d'un routeur.