

PROJET ECP



AP3

CAHIER DES CHARGES

*Création d'un système d'information
hautement disponible et interconnecté*

Propriétés	Description								
Intitulé	Fourniture d'un système d'information hautement disponible et d'une connexion inter-sites pour un centre de formation.								
Présentation Rapide	Le projet consiste à mettre en place la solution technique sur le réseau de l'entreprise, en intégrant les différents serveurs sur le LAN et en activant les différentes techniques de sécurisation : authentification forte, redondance des services, chiffrement des données, filtrage des services par le firewall								
Positionnement	<table><tr><td>Semestre 1</td><td>Semestre 2</td><td>Semestre 3</td><td>Semestre 4</td></tr><tr><td></td><td></td><td>>>>></td><td></td></tr></table>	Semestre 1	Semestre 2	Semestre 3	Semestre 4			>>>>	
Semestre 1	Semestre 2	Semestre 3	Semestre 4						
		>>>>							
Durée estimée en SEMAINE	10 semaines								
Documents joints	Cahier des charges, ANNEXES 1 A 8								
Modalités de réception	Présentation d'un système opérationnel – recettage solution stephane.beteta@ecp-apprentissage.fr gabriel.beteta@ecp-apprentissage.fr								

Lancement : 01/09/2025 – Fin : 31/12/2025

1) CONTEXTE	3
1.1) PRESENTATION DE L'ECP	3
2) OBJECTIFS DU PROJET	3
2.1) Axes stratégiques à atteindre	3
2.2) Objectifs attendues	4
2.3) Solution recommandée par la DSI	5
2.4) Responsabilités	6
2.5) Transfert de compétences et accompagnement au changement	6
2.6) Démarche ITIL / Normes ISO 2700x	6
3) GROUPES ET EVALUATIONS	6
3.1) Constitution des groupes	6
3.2) Notations	6
3.3) Planning prévisionnel	7
3.4) Aide à l'ordonnancement des tâches	7
3.5) Description des lots	8
3.6) Livrables et Oraux	8
3.7) Pénalités et Bonus	10
ANNEXES	10
SITOGRAFIE	10
OUTILS	10

1) CONTEXTE

1.1) Présentation de l'ECP

L'ECP Apprentissage fait partie du Groupe GEFE (Groupe Europe Formation Education) ; depuis 2020, nous avons pour mission de former les professionnels de demain dans les domaines de l'Immobilier, de l'Assurance et de la Gestion Patrimoniale. Pour cette raison, nous vous apportons les savoir-faire et compétences qui vont vous permettre de rapidement intégrer le monde de l'entreprise dans les meilleures conditions et dans des métiers porteurs.

Nous avons un catalogue de formations, uniquement dispensées en apprentissage. Parce que l'expérience pratique et la théorie se marient à merveille, cette méthode d'alternance vous ouvre les portes des métiers de l'Informatique, l'Immobilier, de l'Assurance et de la Gestion de Patrimoine. Du Bac+2 au Bac+5, nos cursus en BTS, Bachelors (Bac+3) et Mastères (Bac+5) sont des Diplômes d'Etat et des Titres RNCP.

ECP est implantée sur 2 sites à Strasbourg (site Vauban et site Somme).

L'ouverture de 2 nouvelles classes (BTS SIO à Strasbourg), nécessite d'aménager de nouvelles salles informatiques et de répondre à plusieurs critères :

- Cahier des charges technique liés aux référentiels des formations
- Souhait des professeurs, intervenants et des apprenants
- Décisions de la direction générale et informatique
- Règlements et lois



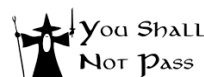
2) Objectifs du projet

2.1) Axes stratégiques à atteindre

La DSI en accord avec la Direction Générale a décidé de lancer un appel d'offres pour la création d'un réseau informatique indépendant, la création et l'équipement de nouvelles salles informatiques.

Ce projet doit permettre de mesurer des améliorations sur 4 axes principaux :

1. Amélioration du service aux utilisateurs et faciliter d'administration par la DSI
 - a. Création d'un Système d'Information indépendant
 - b. Uniformisation du SI
 - c. Liaison inter-sites entre les établissements de Strasbourg et Mulhouse
 - d. Redondance des services
2. Retour sur investissement par la réduction des coûts de possession et d'exploitation
 - d. Facilité d'administration
 - e. Documentation complète (installation, configuration, exploitation)
3. Faciliter le travail collaboratif au niveau régional
 - g. Partage et accessibilité des données inter-sites (sécurisé et redondé)
4. Sécurité des systèmes et des données
 - i. Faciliter la mise en place d'un plan de continuité d'activité (PCA)
 - j. Redondance des serveurs, services et des données
 - k. Sauvegarde régulière des serveurs



2.2) Objectifs attendues

Chaque groupe devra mettre en œuvre une solution technique répondant aux objectifs suivants :

- Respecter la date de début (01/09/25) et de fin de projet (31/12/25)
- La solution doit être à moindre coût et respecter un budget maximum de 100 000 € HT
- Rendre les livrables et effectuer les soutenances aux dates prévues

1. Etude du projet et réponse au cahier des charges (planning, coûts...)

- Mise en œuvre des solutions informatiques
- Equipements (Serveurs)
- Coût des licences **ANNEXES 3 et 4**
- Coût de la main d'œuvre



2. La mise en œuvre d'une liaison WAN inter-sites chiffrée

- Entre les nouvelles salles informatiques de Strasbourg Vauban et Strasbourg Somme (IPsec)

3. Harmoniser le plan d'adressage et de nommage sur l'ensemble des sites

- Segments réseaux, login, noms d'hôtes, serveurs etc.
ANNEXES 1 et 2

4. Création de serveurs et rôles/services suivants en haute disponibilité :

- Annuaire d'authentification (AD)-> SSO
- Résolution de noms (DNS)
- Distribution d'IP dynamique (DHCP)
- Systèmes de fichiers distribués (DFS) et réplica (DFSR) / données utilisateurs
- Données accessibles via un partage SMB (droits et permissions adaptés)
- Clichés instantanés (Shadow Copy) du disque contenant les DATAS stockés sur le SAN
- Sauvegarde complète (Sur un espace disque SAN via un point de montage iSCSI)

5. Accès aux données stockant les dossiers personnels des enseignants et des élèves à partir des 2 sites :

- Redondances des données
- Droits et permissions adaptés (*j'accède à mes données, pas à celles des autres*)

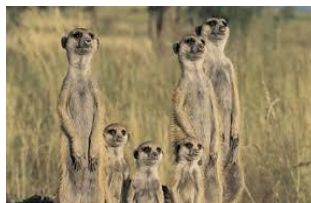
6. Création à minima d'1 poste client Windows 11 Pro à Strasbourg Vauban et Somme dans le domaine AD

7. Vous prendrez connaissances des recommandations de l'ANSSI

ANNEXES 5 à 8

La haute disponibilité (ou High Availability ou HA) permet d'assurer et de garantir le bon fonctionnement des applications ou services procurés, et ce, 24h/24 et 7j/7 ".

L'Active Directory sera l'unique moyen d'authentification et de contrôle des habilitations (droits/permissions) et permettra le déploiement du SSO (Single Sign-On).



2.3) Solution recommandée par la DSI

Informations techniques complémentaires en ANNEXES 1 et 2

Suite à l'Audit réalisée par la DSI ; elle estime qu'il faut au moins 8 serveurs pour la réalisation du projet :

- 2 routeurs
- 4 serveurs de production
- 2 serveurs de sauvegarde



Tableau : Répartition des serveurs et services par sites

SITES	RÔLES / SERVICES
A – Strasbourg Vauban	<p>Active Directory : 1 seule forêt et 4 contrôleurs de domaine (sites A et B) Les clients seront sous Windows 11 Pro</p> <p>1 routeur/pare-feu avec VPN Inter-sites (IPsec)</p> <p>Serveurs avec les rôles/services suivants :</p> <p>1^{er} serveur : Principal (WS 2022 Standard GUI)</p> <ul style="list-style-type: none"> ▪ AD DS, DNS, DHCP, DFS, cible DFSR (Réplica) <p>2nd serveur : Secondaire (WS 2022 Standard CORE)</p> <ul style="list-style-type: none"> ▪ AD DS secondaire, DNS secondaire, DHCP de basculement, DFS, cible DFSR (Réplica) <p>3^{ème} serveur : Serveur NAS/SAN contenant</p> <ul style="list-style-type: none"> ▪ Espace disque SAN accessible via un point de montage iSCSI, contenant la sauvegarde complète (OS + DATAS) du serveur STG1-SRVW-01 ▪ Clichés instantanés de la partition DATAS sur le même disque ou stockés sur un point de montage iSCSI
B – Strasbourg Somme	<p>1 routeur/pare-feu avec VPN Inter-sites (IPsec)</p> <p>Serveurs avec les rôles/services suivants :</p> <p>1^{er} serveur : Principal (WS 2022 Standard GUI)</p> <ul style="list-style-type: none"> ▪ AD DS (connecté à l'AD Strasbourg), DNS, DHCP, DFS, cible DFSR (Réplica) <p>2nd serveur : Secondaire (WS 2022 Standard CORE)</p> <ul style="list-style-type: none"> ▪ AD DS secondaire, DNS secondaire, DHCP de basculement, DFS, cible DFSR (Réplica) <p>3^{ème} serveur : Serveur NAS/SAN contenant</p> <ul style="list-style-type: none"> ▪ Espace disque SAN accessible via un point de montage iSCSI, contenant la sauvegarde complète (OS + DATAS) du serveur STG2-SRVW01 ▪ Clichés instantanés de la partition DATAS sur le même disque ou stockés sur un point de montage iSCSI

Tableau : Nombre d'utilisateurs estimé

Sites	Utilisateurs	PC Fixes	PC Portables*
Strasbourg	60	40	60
Mulhouse	30	20	30
Total	90	60	90

**avec la multiplication du AVEC / BYOD, il y a potentiellement autant de PC Portables que d'utilisateurs à prendre en compte. On peut également supposer l'utilisation de smartphones/tablettes...*

2.4) Responsabilités

- Le commanditaire fournira à la demande toute information sur le contexte nécessaire à la mise en place de l'infrastructure.
- Le prestataire est à l'initiative de toute proposition technique.
- Le prestataire fournira un système opérationnel sous forme de machines virtuelles
- Le prestataire présentera une maquette

2.5) Transfert de compétences et accompagnement au changement

La prestation dans sa globalité devra être entièrement documentée et un mémoire technique fonctionnel, rédigé impérativement en Français, devra être remis pour chaque élément technique de la solution mis en place. Il pourra être demandé la fourniture de mode opératoire concis pour les utilisateurs.

2.6) Démarche ITIL / Normes ISO 2700x

La DSI de la CCI Grand-Est a initiée une démarche de mise en place des bonnes pratiques de l'informatique basée sur le référentiel ITIL V3. La DSI vise à terme une certification du service sur les normes ISO 20000 et ISO 27000.

Dans ce contexte, la solution mise en place devra faciliter la mise en place de la démarche et permettre d'identifier des indicateurs précis quant au bon fonctionnement des équipements.



3) Groupes et évaluations

3.1) Constitution des groupes

- Chaque groupe sera composé de 2 apprenants
- Le cas échéant, le dernier groupe (à trois ou seul) sera composé sur avis des formateurs
- Chaque apprenant du groupe aura un site affecté dont il sera responsable (A ou B)

SITE A : Apprenant 1, SITE B : Apprenant 2

L'apprenant qui met en œuvre est responsable de la production de la documentation

A l'examen, l'épreuve technique est individuelle, chaque partie de cet AP peut constituer un sujet d'examen

**Le jour de l'épreuve, vous pouvez réutiliser vos machines virtuelles et snapshots !
Il est impératif que chacun puisse être autonome et sache réaliser l'ensemble de AP.**

3.2) Notations

La notation est individuelle.

- Coeff. 1 pour chaque soutenance, démonstrations techniques, QCM, Badges CISCO et éventuels bonus ou défis individuels
- Coeff. 2 pour chaque production écrite
- Coeff. 3 pour la démonstration technique finale (maquette de l'ORAL-2)

3.3) Planning prévisionnel – 8 Séances

- | | |
|----------------------------------|---|
| 1. Lundi 01/09/2025 matin : | LANCEMENT DU PROJET + Présentation des épreuves informatiques à l'examen de BTS SIO / Présentation du sujet / Validation des solutions en séance |
| 2. Vendredi 05/09/25 matin : | Etudes CdC + Maquettage LOT1 |
| 3. Vendredi 03/10/25 matin : | Livraison du 1 ^{er} LOT – MAQUETTAGE LOT1 + QCM1 |
| 4. Vendredi 17/10/25 matin : | Séance de travail en groupe |
| Lundi 20 octobre 25 : | Livraison du LIVRABLE 1 (avant 23h59) |
| 5. Vendredi 31/10/25 matin : | ORAL 1 |
| 6. Jeudi 13/11/25 matin : | Réalisation maquette/expérimentation |
| 7. Vendredi 28/11/25 matin : | Livraison 2nd LOT- MAQUETTAGE LOT2 + QCM2 |
| 8. Mardi 09/12/25 matin : | ORAL 2- MAQUETTE COMPLETE (LOTS 1 à 4) |
| 31/12/25 : | Livraison du LIVRABLE 2 et 3 (avant 23h59) |
| Mardi 06/01/26 matin | BTS Blanc – Epreuve technique (sujets AP3) |

3.4) Aide à l'ordonnancement des tâches

Aide méthodologique :

1. Lire le sujet
2. Relevé des objectifs pour chaque site (A, et B,)
3. Relevé les dates importantes du projet (Début, Fin, livrables, oraux...)
4. Etudes / Analyse par le groupe (Discussions, échanges, recherches...)
5. Réaliser un agenda partagé et fixer vous des dates de « réunions teams/discord » pour avancer progressivement
6. Découper le projet en objectifs intermédiaires et créer une liste de tâches (Méthode SMART)
7. Evaluer la durée de chaque tâche en heures (Cible 2h par tâches)
8. Définir l'ordre chronologique des tâches (tâches en parallèles ou après qu'une soit terminée)
9. Calculer la planification du projet (combien d'heures, jours ?) et prévoir les marges nécessaires.
10. Créer le planning prévisionnel puis transposer le sur un logiciel de type Gantt Project
11. Editer le diagramme de Gantt du projet
12. Affecter les tâches aux personnes

NB : Vous avez le droit d'organiser des sessions de travail en ligne sous forme de « soutien » / réaliser un travail collaboratif entre les groupes



3.5) Description des lots

- LOT 1 :
 - 2 Routeurs/Pare-Feu avec 1 VPN site à site (IPsec) entre les sites A et B
 - Documentation d'installation et de configuration en V1 du LOT 1
- LOT 2 :
 - 4 serveurs Windows Serveur 2022 Standard avec les rôles suivants fonctionnels et configurés : ADDS, DNS, DHCP et DHCP de basculement
(2 serveurs sur le Site A et 2 serveurs sur le site B)
 - Documentation d'installation et de configuration en V1 du LOT 2
- LOT 3 :
 - DFS + DFSR (Réplica) fonctionnel sur les quatre serveurs des sites A et B
 - Sauvegarde et Shadow Copy sur un espace de stockage séparé (serveur SAN avec montage iSCSI)
 - Documentation d'installation et de configuration en V1 du LOT 3
- LOT 4 :
 - Appliquer les consignes et GPO de l'Annexe 2
 - Règles de pare-feu configurées (WAN, LAN, VPN et SAN)

3.6) Livrables et Oaux

- Chaque groupe déposera sur le dossier partagé avec les formateurs les différents livrables, dans les délais.
- A chaque séance, il faudra compléter le tableau de suivi partagé avec les formateurs sur Teams.
- Rendre compte de problèmes par courriel aux formateurs ou conversation Teams (avec les deux formateurs invités dans la conversation).

LIVRABLE 1 : PROPOSITION TECHNIQUE ET COMMERCIALE

A RENDRE AVANT LE LUNDI 20 OCTOBRE 2025, 23h59

- Rédaction d'un document de réponse argumentée au Cahier des Charges, selon le modèle proposé :
« LIVRABLE_1_Reponse_CDC_GROUPE_X_YYYYMMJJ_HHMM.docx ».

Ce document contiendra à minima :

- La composition et présentation de votre groupe
- Le rappel des besoins et objectifs du projet
- Votre solution argumentée :
 - *Présentation de chaque solution + arguments du choix par rapport au cahier des charges*
 - *Tableau comparatif ou un tableau de synthèse sur des points clés avec des smileys ou coches vertes/rouges afin d'orienter immédiatement vers les points clés et la solution que vous retenez.*
(Les serveurs Windows étant imposés, il n'est pas demandé une alternative)
- Schéma réseau complet
(Contenant : les pare-feux, serveurs, rôles/fonctionnalités, versions OS et logiciels, noms, adresses IP, équipements réseaux et connexions / liens et toutes informations utiles).
 - *Utiliser plutôt Microsoft VISIO ou un logiciel similaire pour réaliser vos schémas (Draw.io).*
- Budget / Coût du projet
(Devis et/ou un tableau complet reprenant les différentes ressources (humaines, financières, matérielles) nécessaires à la réalisation de votre projet et le coût global s'approchant du réel).
 - *N'oubliez pas les licences CAL (Annexe 4)*
 - *Comment est justifié la main d'œuvre ?*

- La liste des tâches prévisionnelle de votre projet
(Lister les tâches dans l'ordre chronologique ; pour vous aider, identifier les tâches que vous pouvez réaliser sans attendre qu'une autre soit terminée)
- Diagramme de Gantt prévisionnel de votre projet
Spécifiant les tâches, durées et ressources nécessaires
 - *Le diagramme de Gantt doit permettre de déterminer le temps nécessaire à la réalisation du projet et son ordonnancement.*
 - *Combien de jours/heures sont nécessaires ? -> coût de la main d'œuvre*

ORAL 1 : LE VENDREDI 31 OCTOBRE 2025, 8h30

- **PHASE 1 - PRESENTATION ORALE : 15 minutes**
10 minutes de présentation puis 5 minutes de questions / réponses
Le diaporama sera déposé dans le dossier partagé avec les formateurs

Chaque groupe présentera aux formateurs sa réponse au cahier des charges à l'aide d'un support projeté selon le modèle proposé « ORAL_1_Reponse_CDC_GROUPE_X_YYYYMMJJ_HHMM.pptx »

Le contenu reprendra les éléments du livrable 1, bien que complet, cela doit être concis pour respecter le temps.

ORAL 2 : LE MARDI 09 DECEMBRE 2025, 8h30

- **PHASE 1 - PRESENTATION ORALE : 15 minutes**
10 minutes de présentation puis 5 minutes de questions / réponses
Chaque groupe présentera à l'oral son rapport de clôture de projet, à l'aide d'un support projeté, selon le modèle proposé « ORAL_2_Rapport_de_cloture_du_projet_GROUPE_X_YYYYMMJJ_HHMM .pptx »
Ce sera une synthèse qui permettra d'évoquer les écarts entre les éléments prévisionnels de votre livrable 1 et la réalité.
- **PHASE 2 - DEMONSTRATION TECHNIQUE : 30 minutes**
Chaque groupe présentera techniquement la solution validée dans le Livrable 1.
Les maquettes devront permettre aux formateurs de vérifier le bon fonctionnement de l'ensemble de la solution ainsi que la cohérence des éléments entre eux dans la solution.

LIVRABLES 2 et 3 : FICHE DE SITUATION PROFESSIONNELLE N°1 ET DOCUMENTATION TECHNIQUE

A RENDRE AVANT LE MARDI 31 DECEMBRE 2025, 23H59

Ces livrables au format éditable devront être partagés dans le groupe pour être réutilisés ultérieurement

- « LIVRABLE_2_GROUPE_X_Fiche_situation_professionnelle_1_BTS-SIO 2025 ».
 - Reprise du livrable 1 et tenir compte des remarques et demandes de modifications
 - Analyse prévisionnel vs réel / Conclusion et améliorations possibles du projet
- « LIVRABLE_3_GROUPE_X_Documentation_technique_situation_professionnelle_1_BTS-SIO 2025 »
 - Documentation technique complète du projet à la façon d'un mode d'emploi, rédigée et mise en forme à rendre sous format électronique .DOCX et .PDF, obligatoire.



La documentation est autorisée à l'examen technique et peut-être demandée à l'examen « oral pro »

3.7) Pénalités et Bonus

- Les productions à livrer (déposer) sur le dossier partagé avec les formateurs ont des dates de remise à respecter.
- Chaque jour de retard entraîne le retrait d'1 point sur 20 par jour.
- La remise en retard des livrables 2 et 3 seront sanctionnés d'un 0/20 (Date de fin du projet).
- La remise aux formateurs des attestations de réussite des MOOC suivants seront comptabilisés (note sur 20 coeff. 1, pondéré selon le volume horaire théorique).

CISCO : S'inscrire/être authentifié avec son adresse électronique personnelle ou réutiliser un compte existant avant de cliquer sur les liens.

P1 : Introduction à la Cybersécurité /rapide 6h

https://www.netacad.com/courses/introduction-to-cybersecurity?courseLang=fr-FR&instance_id=8a0c0dbf-6bfd-4246-bede-8b4a4aef7ea7



P2 : CCNA1 : Présentation des réseaux

https://www.netacad.com/courses/ccna-introduction-networks?courseLang=fr-FR&instance_id=c7b77b94-ba98-4b06-86dd-da50987b3798

P3 : Principes de cybersécurité

https://www.netacad.com/courses/cybersecurity-essentials?courseLang=fr-FR&instance_id=1fd2a67c-d8de-4f78-811f-2ec6689dc817

P4 : CCNA2 : Switching, Routing, and Wireless Essentials (SRWE)

https://www.netacad.com/courses/ccna-switching-routing-wireless-essentials?courseLang=fr-FR&instance_id=4071adba-3b66-495f-bc55-662ffc6934c5

Rapide / ½ journée :

<https://secnumacademie.gouv.fr/>



SecNumacadémie.gouv.fr
Formez-vous à la sécurité du numérique

<https://atelier-rgpd.cnil.fr/>



ANNEXES

ANNEXE 1 : SPECIFICATIONS TECHNIQUES

ANNEXE 2 : CONSIGNES AD ET GPO

ANNEXE 3 : LICENCES CLIENTS WINDOWS

ANNEXE 4 : LICENCES SERVEURS 2016 ET CAL + DOCS-MICROSOFT.zip

ANNEXE 5 : RECOMMANDATIONS DE SECURITE RELATIVES A IPSEC, ANSSI

ANNEXE 6 : RECOMMANDATIONS DE SÉCURISATION D'UN PARE-FEU STORMSHIELD NETWORK SECURITY, ANSSI

ANNEXE 7 : RECOMMANDATIONS DE SECURITE RELATIVES AUX MOTS DE PASSE, ANSSI

ANNEXE 8 : RECOMMANDATIONS À L'ADMINISTRATION SÉCURISÉE DES SYSTÈMES D'INFORMATION, ANSSI

SITOGRAPHIE

<https://www.ecp-apprentissage.fr/>

<https://gefe-strasbourg.fr/>

<https://www.ssi.gouv.fr/administration/bonnes-pratiques/>

OUTILS

<https://trello.com>

<https://www.notion.so/fr-fr/product/projects>

ANNEXE 1

Indications techniques des machines virtuelles (À adapter...)

SITE A (VMNET1)

PLAN D'ADRESSAGE :

SITE A : 192.168.100.0 /24 (LAN)

RTE-STG01 : 512 Mo RAM – FreeBSD Unix – Pfsense / OPNsense

- 1 disque de 20 Go
- 3 interfaces Ethernet :
 - o WAN = VBR01
 - o LAN = AP3-TRIGRAMME-ELEVE
 - o SAN = SAN-ELEVE / réservé réseau local pour liaison/montage iSCSI
- VPN SITE A vers SITE B

STG-SRVW01 : 2 Go RAM - Microsoft Windows 2022 Standard (GUI)

- 2 disques durs :
 - o 1 disque de 60 Go (OS)
 - o 1 disque de 60 Go (**DATAS01**)
- SMBV3 à activer (chiffrement à démontrer avec une analyse de trames Wireshark)
- Serveur Active Directory (contrôleur principal du domaine)
- Serveur de fichiers racine (Espace de Noms DFS) et Réplica (DFSR)
 - o Clichés instantanés DATAS01
 - o Fonctionnalité déduplication de fichiers DATAS01
- Partage réseau DATAS01
- Montage du disque iSCSI **Backup01** (STG-SAN01) / sauvegarde complète de STG-SRVW-01
(Possibilité de déplacer les clichés instantanés sur la cible iSCSI également)
(Option) sécurisation d'accès/montage de la cible iSCSI avec un mot de passe ou IPSEC

STG-SRVW02 : 1 Go RAM - Microsoft Windows 2022 Standard (CORE)

- 2 disques durs :
 - o 1 disque de 60 Go (OS)
 - o 1 disque de 60 Go (**DATAS02**)
- Serveur Active Directory (contrôleur supplémentaire)
- Serveur de fichiers (Espace de Noms DFS) et Réplica (DFSR)
- Partage réseau DATAS02

STG-SAN01 : 512 Mo RAM

(Attention aux versions récentes de TrueNas gourmandes en mémoire vive. D'autres solutions sont envisageables, 1 serveur Windows Core supplémentaire avec diffusion de cible iSCSI. Ou bien encore... Xpenology / RR / Veeam Backup....

- 1 disque de 20Go
- iSCSI services : **Backup01**

Attention, pour les sites A et B.

- La version de Windows Serveur doit être identique sur l'ensemble des serveurs
- Active Directory : 1 seule forêt, 1 contrôleur de domaine principal, 3 contrôleurs de domaine supplémentaires.
- **DFS : 1 espace de nom « INTRANET » accessible à :**
 - \\IEF.LOCAL\INTRANET ou \\IEF.LOCAL\DFS\INTRANET
- **4 cibles DFSR** (les données seront répliquées en maille pleine et accessibles à partir des 4 cibles) :
 - \\STG-SRVW-01\DATAS01
 - \\STG-SRVW-02\DATAS02
 - \\STG2-SRVW-01\DATAS03
 - \\STG2-SRVW-02\DATAS04

SITE B (VMNET2)

PLAN D'ADRESSAGE :

SITE B : 192.168.200.0 /24 (LAN)

RTE2-STG01 : 512 Mo RAM – FreeBSD Unix – Pfsense / OPNsense

- 1 disque de 20 Go
- 3 interfaces Ethernet :
 - WAN = VBR01
 - LAN = AP3-TRIGRAMME-ELEVE
 - SAN = SAN-ELEVE / réservé réseau local pour liaison/montage iSCSI
- VPN SITE B vers SITE A

STG2-SRVW01 : 2 Go RAM - Microsoft Windows 2022 Standard (GUI)

- 2 disques durs :
 - 1 disque de 60 Go (OS)
 - 1 disque de 60 Go (**DATAS03**)
- SMBV3 à activer (à démontrer avec une analyse de trames Wireshark)
- Serveur Active Directory (contrôleur supplémentaire)
- Serveur de fichiers (Espace de Noms DFS) et Réplica (DFSR)
 - Clichés instantanés DATAS03
 - Fonctionnalité déduplication de fichiers DATAS03
- Partage réseau DATAS03
- Montage du disque iSCSI **Backup02** (STG2-SAN01) / sauvegarde complète de STG2-SRVW01
 (Possibilité de déplacer les clichés instantanés sur la cible iSCSI également)
 (Option) sécurisation d'accès/montage de la cible iSCSI avec un mot de passe ou IPSEC

STG2-SRVW02 : 1 Go RAM - Microsoft Windows 2022 Standard (CORE)

- 2 disques durs :
 - 1 disque de 60 Go (OS)
 - 1 disque de 60 Go (**DATAS04**)
- Serveur Active Directory (contrôleur supplémentaire)
- Serveur de fichiers (Espace de Noms DFS) et Réplica (DFSR)
- Partage réseau DATAS04

STG2-SAN01 : 512 Mo RAM

(Attention aux versions récentes de TrueNas gourmandes en mémoire vive. D'autres solutions sont envisageables, 1 serveur Windows Core supplémentaire avec diffusion de cible iSCSI. Ou bien encore Xpenology / RR / Veeam Backup....

- 1 disque de 20Go / iSCSI services : **Backup02**

ANNEXE 2 : CONSIGNES AD ET GPO

- Vous installerez Microsoft Windows 2022 Serveur Standard en mode GRAPHIQUE / GUI en tenant compte des informations suivantes :

Nom d'hôte : Voir annexe 1 ;

Nom de la société : IEF ;

Organisation : IEF ;

Disques durs / partitions : Voir annexe 1

Nombre de connexions simultanées : 100 ;

Adresses IP : Voir annexe 1

Password Administrateur recommandé dans le cadre de l'AP : P@ssword10

Nom de domaine : IEF.

Nom de domaine FQDN : IEF.LOCAL

Le mot de passe de restauration d'AD doit être identique à celui de l'administrateur (*recommandé dans le cadre de l'AP*)

Nom de zone DNS : IEF.LOCAL

Le serveur DNS devra être capable de résoudre les noms DNS de tous les hôtes du réseau. La/les station(s) seront membres de ce domaine.

- Créez les objets suivants :

- Unités Organisationnelles nommée VAUBAN et SOMME
- Les comptes utilisateurs : Paul, Pierre placés dans l'UO VAUBAN
- Les comptes utilisateurs : Isabelle, Nathalie placés dans l'UO SOMME
- Un compte utilisateur ADMIN (Administrateur de secours)
- Un groupe nommé GRP1, auquel appartiennent Paul et Pierre seront membres ;
- Un groupe nommé GRP2, dans lequel Isabelle et Nathalie seront membres ;

Seuls les comptes ADMIN et ADMINISTRATEUR ont tous les privilèges.

- La politique de mots de passe sera la suivante :

(Plus pratique pour les AP sinon se référer aux recommandations de l'ANSSI)

- Longueur de 12 caractères minimum, avec au minimum 1 chiffre, 1 caractère spécial, 1 majuscule.
- Verrouillage du compte utilisateur pendant 30 minutes après 3 tentatives de mot de passe erroné

- Créez une infrastructure réseau avec un seul et unique partage de type (utilisé pour DFS/DFSR)

\\IEF.LOCAL\\intranet

- Créer les dossiers GRP1, GRP2, TRANSFERT situés dans le répertoire INTRANET avec les dossiers personnels des utilisateurs en respectant le cahier des charges au niveau des droits et permissions.
- Tous les utilisateurs auront les droits lecture/écriture sur le partage TRANSFERT.
- Seuls les membres du groupe « Administrateurs du Domaine » auront le droit contrôle total sur tous les partages.

- Une stratégie de groupe affectera par défaut à tous les comptes de l'AD, les paramètres suivants :

- Création du lecteur réseau U: sur le répertoire personnel de chaque utilisateur (%username%)
- Création du lecteur réseau T: sur le répertoire TRANSFERT
- Déploiement d'un fond d'écran unique et bloquer sa personnalisation
- Redirection des dossiers Mes documents et Bureau vers le dossier personnel de l'utilisateur

Exemple : Dossier documents redirigé vers [\\ief.local\\intranet\\users\\%USERNAME%](\\ief.local\\intranet\\users\\%USERNAME%\\)

- **Une stratégie de groupe affectera uniquement les utilisateurs :**

- Interdiction d'accès au panneau de configuration
- Bloquer les ports USB
- Masquer **et** bloquer les accès aux disques locaux des postes
- Bloquer l'accès aux consoles Powershell et Invité de commande

Informations sur les Licences :

"Le nouveau modèle de licence inclut obligatoirement des licences par cœurs + des Licences d'Accès Client (CALs). Chaque utilisateur et/ou appareil accédant une licence de Windows Server 2016 édition Standard ou Datacenter a besoin d'une CAL Windows Server."

Il est bien nécessaire d'acheter des licences CAL (par utilisateur ou par device) en plus des licences Serveur et Windows 10. Confirmation de Microsoft par téléphone, 09 70 01 90 90 (support/infos gratuit)

Licence CAL par utilisateur : environ 50€/users et 40€/Device

Il n'y a pas d'installations à faire, c'est une simple "règle morale", il faut prouver l'achat en cas de contrôles (sauf licences CAL RDS).

Nota bene :

- Il existe également des CAL pour SQL Serveur, Exchange, Link, SharePoint... et bien sur RDS. (En supplément à chaque fois...)