ITWay

"ITWay : Sécuriser, Innover, Simplifier votre IT"

Samy SCANNA – Sept. 2024 – Projet d’infrastructure épreuve E5 – Campus de la CCI de Vaucluse

Table des matières

Contexte ITWay

Secteur d'activité : Fournisseur de services informatiques (externalisation de la gestion informatique, développement de solutions logicielles, cybersécurité)

Historique : Créée en 2005, **ITWay** a commencé comme une petite entreprise de conseil en informatique. Avec l'augmentation des besoins en services numériques et la complexification des

infrastructures IT, l'entreprise a rapidement élargi ses activités pour offrir des services d'intégration, de maintenance de réseaux, de gestion des systèmes informatiques et de cybersécurité. En 2018, ITWay a ouvert une antenne régionale pour mieux desservir ses clients en France et à l'international.

Statistiques :

- **Nombre d'employés** : 110 au total
- **Siège social (Marseille)** : 80 employés
- **Antenne régionale (Lille)** : 30 employés
- **Chiffre d'affaires annuel** : 15 millions d'euros
- **Clients** : Majoritairement des PME, quelques grands comptes et des administrations publiques • **Infrastructure actuelle** : En croissance constante, l'entreprise cherche à améliorer son infrastructure réseau pour répondre aux besoins croissants de ses clients, avec une meilleure sécurité, des temps de réponse plus rapides et une disponibilité accrue.

Structure de l'entreprise

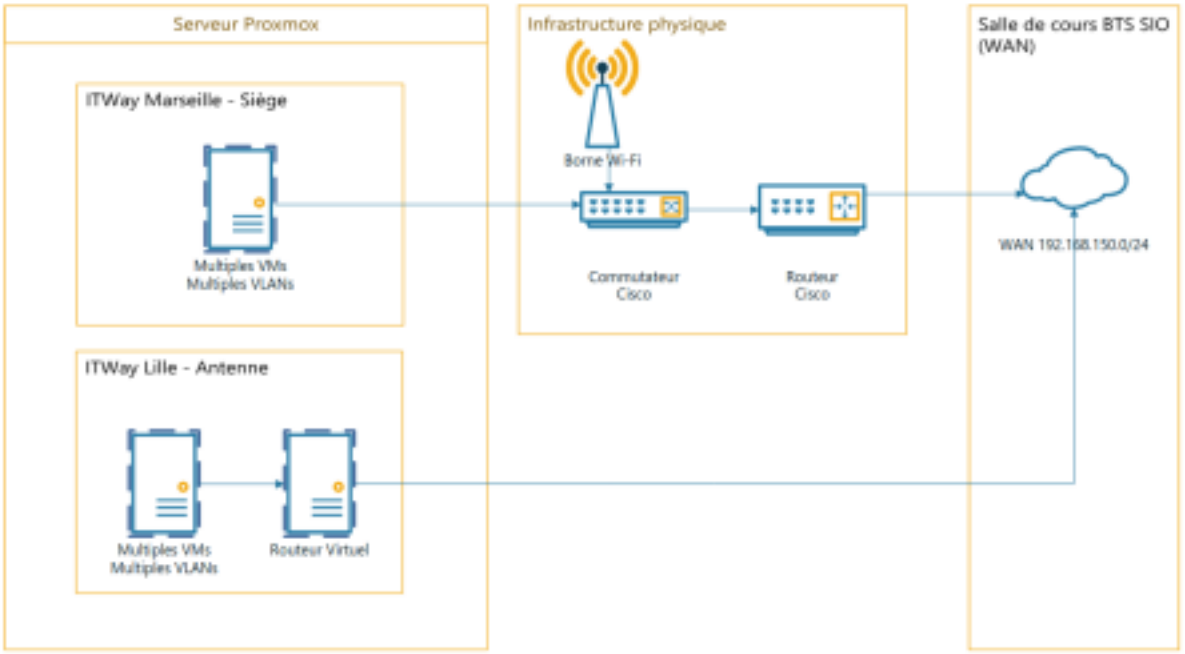
- **Siège social (Marseille)** :
    - **Services clés** :
        - Département IT (administration des systèmes, réseaux, sécurité) – 20 personnes
        - Département développement logiciel – 15 personnes
        - Support technique – 15 personnes
        - Services administratifs (RH, finance, direction générale) – 20 personnes
        - Commercial – 10 personnes
- **Antenne régionale (Lille)** :
    - **Services clés** :
        - Support technique - 10
        - Développement logiciel - 10
        - Commercial – 10

Schéma simplifié de l'infrastructure ITWay

Le réseau « WAN » ou Internet sera représenté par le réseau local de la salle de cours (192.168.150.0/24), ainsi vos deux sites (Marseille et Lille) disposeront tous deux d'une adresse IP publique dans le plan d'adressage de la salle. Ces adresses seront fixes et vous seront communiquées par groupe.

En complément, deux autres adresses IP fixes vous seront attribuées et seront destinées à l'hyperviseur et à la carte HP iLO.

Plus précisément, le site de Marseille disposera d'un routeur Cisco physique, le site de Lille disposera d'un routeur virtualisé et dont le choix de la technologie est laissé à votre appreciation.



PROJET D'INFRASTRUCTURE ITWAY – ÉPREUVE E5 BTS SIO SISR

Technologies à mettre en place en commun dans vos infrastructures

Le référentiel du diplôme BTS SIO option SISR demande qu'un certain nombre d'éléments soient présents dans les infrastructures de chaque équipe projet, ces éléments sont à mettre en œuvre **en commun**, en respectant bien les réunions régulières, comptes rendus de réunion, documentation techniques associées (tout ceci à mettre dans le drive d'équipe).

Éléments à mettre en œuvre	**Description**
1.1 - (Commun SLAM/SISR) L'environnement comporte l'ensemble de ces éléments :	
Service d'authentification	Rôle AD-DS (ou OpenLDAP sous GNU/Linux)
SGBD	MySQL, MariaDB, PostgreSQL (ou autre moteur de base de données)
Accès sécurisé à internet	Les PCs doivent disposer d'un antivirus et d'un pare-feu logiciel tous deux actif**.**
Environnement de travail collaboratif	Déjà en place : Suite Microsoft 365
Deux serveurs basés sur des systèmes d'exploitation différents (virtualisation possible et un sur un logiciel open source)	A minima une VM Windows Serveur et une VM GNU/Linux.

Solution de sauvegarde	A mettre en œuvre pour sauvegarder vos VMS. Soit la sauvegarde intégrée à Proxmox, soit un autre logiciel de votre choix type Veeam Backup…
Ressources dont l'accès est sécurisé et soumis à habilitation	Une VM pour les dossiers partagés, que ce soit avec Samba ou Windows Server. Les dossiers partagés remontent automatiquement (GPO), et sont gérés via des groupes de sécurité. Chaque service doit disposer de ses dossiers partagés.
Deux types de terminaux dont un mobile	PC fixe, portable, tablette, smartphone. L'accès de type mobile se fera via la mise en œuvre d'une borne Wi-Fi sur le site de Marseille, cette borne fonctionnera avec un mécanisme d'authentification Radius (802.1X).
1.2 - (Commun SLAM/SISR) Outils mobilisés pour la gestion de la sécurité :	
Gestion des incidents	Solution GLPI.
Détection et prévention des intrusions	A minima Fail2ban sur un serveur SSH + centralisation des logs ou Snort/Wazuh/Suricata etc…
Chiffrement	HTTPS obligatoire – Autorité de certification (PKI) locale sur un serveur dédié. Les certificats seront déployés sur l'ensemble des services utilisant HTTPS.
Analyse de traffic	Suite ELK et Packetbeat, Graphana ou autre.
2.1 - (Spécifique SISR) L'environnement comporte l'ensemble de ces éléments :	
Réseau comportant plusieurs périmètres de sécurité	Mise en œuvre d'un pare-feu (Cisco pour le site de Marseille), technologie au choix pour le site de Lille. A minima filtrage par IP/Ports.
Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité.	Tableaux de bord de la disponibilité des services via Nagios ou autre solution de supervision le proposant.
Logiciel d'analyse de trames	Wireshark doit être présent sur tous les serveurs et PCs de l'infrastructure.

Logiciel de gestion des configurations	Ansible, Chef, Puppet sinon à minima GLPI + Agent déployé sur l'ensemble des machines.
Solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès.	SSH, Powershell, MSTSC (Bureau à distance), console MMC. Les serveurs doivent être administrables par l'un des protocoles communs ci-dessus.

Solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes	Nagios + Cartographie, Eyes of Network, Centreon ou autre solution équivalente.
Solution garantissant des accès sécurisés à un service interne au périmètre de sécurité du CFAI (intranet) ou externes (extranet)	**Mise en place d'une DMZ et d'un serveur Proxy** Tout le monde doit savoir agir dans la DMZ, y placer des équipements, ajuster les ACL qui vont avec. Tout le monde doit être capable d'agir sur le proxy.
Solution garantissant la continuité d'un service	AD redondant, DHCP redondant, DNS redondant, GLPI redondant, EON redondant, pare-feu redondant… et bien d'autres.
Solution garantissant la tolérance de panne de systèmes ou équipements réseau	Commutateurs en redondance, routeurs en redondance.
Solution permettant la répartition de charges entre services, serveurs ou équipements réseau	Mise en place d'un TSE en équilibrage de charge, citrix, LTSP…. Nginx/Reverse proxy en répartition de charge
2.2 - (Spécifique SISR) Au moins UNE solution opérationnelle parmi les suivantes :	
Une solution permettant la connexion sécurisée entre deux sites distants	VPN site-à-site (VPN IPSec, OpenVPN…) ← Obligatoire car il faut interconnecter le site de Marseille avec le site de Lille.
Solution permettant le déploiement des PCs (solutions techniques d'accès)	WDS, MDT, FOGProject… Ces situations ne sont jamais évaluées, car jugées trop longues à évaluer. Toutefois c'est intéressant à mettre en place en commun, car tellement utile dans la vraie vie…Très utile pour ceux qui veulent chercher du travail à la suite du BTS.
Solution gérée à l'aide de procédures automatisées écrites avec un langage de scripting	Réalisation de scripts de gestion d'un service (par exemple Active Directory) : Création d'un utilisateur, configuration de dossiers partagés, configuration automatique de la session, script d'extraction et mise en forme des journaux d'évènements…
Solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau	Dans cette solution, ce n'est plus simplement de l'Host/Network IDS/IPS mais l'ensemble de ces systèmes couplés à une solution de type SIEM (Security Information & Event Monitoring), le SIEM permet d'effectuer la corrélation des évènements remontés par un IDS/IPS de type réseau et un IDS/IPS de type hôte. SecurityOnion par exemple.

Tous les apprentis doivent impérativement mettre en œuvre, et maîtriser tous les éléments du tableau ci-dessus, ils serviront de base à l'épreuve E5. La meilleure façon de maîtriser ces éléments est que chacun s'applique à faire/refaire le travail x fois !!!

Les situations individuelles

Chaque apprenti devra mettre en œuvre sur l'infrastructure commune (les éléments du premier tableau) deux situations individuelles (supplémentaires et indépendantes de l'infrastructure commune) et sera interrogé :

- Sur l'une d'entre elle
- Sur les deux, si les deux situations sont jugées « trop simples » ou « pas assez développées, ce qui implique des pénalités pour le candidat !
- Deux apprentis d'un même plot ne peuvent pas mettre en œuvre le même produit en commun

LA MISE EN ŒUVRE D'UNE SITUATION N'EST PAS UN SIMPLE TP ; IL NE SUFFIT PAS D'INSTALLER UN PRODUIT POUR QUE LA SITUATION SOIT TERMINÉE ; LE PRODUIT DOIT ÊTRE COMPRIS ET COMPLÈTEMENT ASSIMILÉ.

VOUS DEVEZ VOUS APPROPRIER CE PRODUIT AU MAXIMUM DE VOS POSSIBILITÉS. Les

deux situations combinées doivent couvrir les modules (référentiel BTS SIO) suivants :

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

Exemple de situations déjà observées les années précédentes

Sont listées ci-dessous plusieurs situations observées les années précédentes.

Situation	Description
Exchange ou autre messagerie	Routage extérieur des mails non exigé. Savoir administrer (groupes de diffusion, agents d'absence, BALs communes, sauvegarde/restauration des BAL, délégation). La mise en œuvre de DAG est fortement appréciée
PostFix	Pour les plus courageux, Postfix avec Dovecot, SpamAssassin, Amavis, ClamAV, OpenSPF/DKIM est excellent et très utilisé en tant que serveur mail, à coupler à une interface graphique type Roundcube (ou autre)
Asterisk	Serveur de téléphonie IP (savoir créer des groupements, appels circulaires, BAL, gestion du nombre de sonneries, mise en œuvre des répondeurs)
EON avancé	Avec test de service, cartographie avancée, scripts pour effectuer des checks personnalisés.

Serveur Citrix/TSE	Toujours intéressant à faire, faire des groupes d'utilisateurs, avec des bureaux différents
BIND	Serveur DNS sous Bind (GNU/Linux) redondant avec le serveur DNS de l'AD + zones personnalisées pour l'extranet + implémentation de DNSSEC.
Administration avec PowerShell	Intéressant….Voir très intéressant, se passer de l'interface graphique au bout d'un moment çà deviens très très rapide !
Hardening réseau	Blinder d'ACL, filtrage fin des réseaux.
ReverseProxy Nginx avec équilibrage de charge	Mise en œuvre de Nginx en tant que Reverse Proxy + équilibrage de charge sur plusieurs serveurs.

Intégration LDAP à AD	Couplage de LDAP à Active Directory, sécurisation d'un site
Docker/ Kubernetes	Situation intéressante
Stack ELK ou Graylog	Centralisation des logs des différents hôtes sur une stack ELK + création de tableaux de bords personnalisés.
GPOs	Intéressant si vous creusez au maximum le fonctionnement des GPO, cad re modélisation complète des GPO à partir d'un plan de sécurité informatique

Exemples de situation jamais retenues, ou impliquant souvent des pénalités

Situation	Le pourquoi
WDS / MDT	Trop long pour être évalué
Bitlocker	Trop simple
Files d'impression	Trop simple, pénalités
DFS	Trop simple, pénalités
RemoteApp	Trop simple si pas assez poussé, souvent pénalités
Partage de fichier	Beaucoup trop simple
PRTG et équivalents	Produit très utilisé en entreprise pour monitorer, mais la mise en

	œuvre consiste à faire clic clic suivant clic suivant….

Exemples de situation préparant mieux que d'autres au passage en DSNS/M2I ou autre.

Situation	Le pourquoi
SNORT	Détection d'intrusion, créer des règles « maison », très belle activité, pour les motivés
Stack ELK ou Graylog	Centralisation des logs, création de dashboard personnalisés…
Défense en profondeur	Voir « sécurisation à outrance », proxy/pare-feu, ACLs, durcissement des postes, un vaste sujet, chronophage et très intéressant
Infrastructure Security Onion	Détection, prévention d'intrusion au niveau réseau et système.

Préparation de l'architecture, nommage, sous-réseaux

Avant de se lancer le déploiement des différentes machines virtuelles il faut déjà réfléchir à l'architecture réseau à mettre en œuvre.

Ne vous contentez pas de créer un VLAN par service, pensez qu'il faudra un VLAN dédié aux serveurs internes, un VLAN dédié à la DMZ, un VLAN pour le Wi-Fi. Est-ce qu'on fait la même chose sur le site de Lille ?

C'est à vous de démarrer un travail de réflexion et de préparer un tableau des différents réseaux que vous allez créer et qui alimentera votre documentation technique.

Tout ça en respectant certaines normes, la première c'est la convention de nommage, ci-dessous un exemple de convention de nommage, à vous de déterminer la votre ou réutiliser celle-ci : Pour les serveurs de Marseille : **SRVM-XXX**
Pour les serveurs de Lille : **SRVL-XXX**
Pour les VLANs de Marseille : **VLNM-XXX**
Pour les VLANs de Lille : **VLNL-XXX**
Pour les ordinateurs : **PC-XX-XX** avec par exemple pour le premier XX = numéro de VLAN et le second une numérotation incrémentée.

Ensuite vient la définition des plans d'adressage, mixez l'utilisation des plans d'adressage, par exemple :
10.X.X.X pour les serveurs
172.X.X.X pour les DMZ
192.168.X.X pour les utilisateurs

Et utilisez des masques adaptés au contexte, ne mettez pas du /24 à tout va.

Ça fait pas mal de VLANs, profitez-en pour les propager entre commutateurs via **VTP**.

Chaque apprenti doit s'amuser à casser/recréer les VLANs via VTP, vous devez tous être capables de

créer un nouveau VLAN et s'assurer qu'il soit propagé correctement.

Démarche de mise en œuvre des services

1) Vous devrez dans un premier temps mettre en œuvre le contrôleur de domaine (Active Directory).
2) Puis reproduire dans l'arborescence Active Directory des OU représentant la structure de l'entreprise.

Ex : **OU-COMMERCIAL**, sous **OU-DIRECTION**, sous **OU-MARSEILLE** et **OU-LILLE**.

Faites de même pour les groupes de sécurité, qui eux commenceront par GRP-SECU, Ex : **GRP-SECU MRS-COMMERCIAL**, **GRP-SECU-LIL-COMMERCIAL, GRP-SECU-MRS-WIFI-EXT, GRP-SECU-MRS-WIFI INT.**

3) Mise en route des services DHCP, débrouillez vous pour mettre en place un relais DHCP pour chaque réseau.
4) Commencez à modéliser quelques GPO, ON NE MODIFIE JAMAIS LA STRATEGIE PAR DEFAUT. On crée une stratégie spécifique pour chaque besoin QUI RESPECTERA ELLE AUSSI UN PLAN DE NOMMAGE ! Remarque : la stratégie par défaut impose un modèle unique, plutôt bien sécurisé « out of the box » aux entreprises, si la politique de l'entreprise demande certains changements (ex : politique de rotation des mots de passe), il reste préférable de créer une GPO spécifique puis en demander son application inconditionnelle (**enforce** en anglais, et la mauvaise traduction « **appliquer** » en français).
5) C'est l'heure de créer des lecteurs réseaux de les mapper automatiquement par GPO/groupe de sécurité ou encore OU.

Une fois arrivé ici, vous pouvez commencer à déployer tous les services de base (tableau des éléments communs indispensables).

La sécurité des communications (ACL/Parefeu/proxy) ne sera appliquée qu'une fois l'ensemble des services de base mis en place. Cela n'empêche pas de commencer à réfléchir aux ACLs, de déployer

un Proxy, mais on applique quand l'infrastructure de base fonctionne.

Mise en œuvre des situations

Les technologies imposées à mettre en œuvre dans l'infrastructure commune, à savoir : Le tableau des éléments indispensable (technologies à mettre en place en commun) sont généralement opérationnelles en fin d'année calendaire (FIN 2024).

Il restera de Janvier jusqu'à la fin de l'année scolaire pour mettre en œuvre les deux situations par apprenti.

Durant la mise en œuvre de vos situations, vous êtes **autonomes.** Ceci implique que vous ne devez pas attendre de vos formateurs qu'ils puissent vous faire un cours sur chaque aspect du produit que vous avez choisi, ceci implique de longs moments d'appropriation, d'expérimentations, de mettre hors service/refaire. Les formateurs sont là pour vous conseiller sur les démarches à mettre en œuvre, vous donner un avis sur la qualité des réalisations, et vous aiguiller en cas de difficultés techniques (mais pas forcément solutionner). Toutefois vous ne devez pas rester « bloqués » trop longtemps sur un même sujet, à un moment donné, il faut savoir dire à l'aide.

PROJET D'INFRASTRUCTURE ITWAY – ÉPREUVE E5 BTS SIO SISR

FAQ/Conseils

- Ⓟ Il est autorisé de changer de situation, à éviter « au dernier moment », la dead-line pour le choix des situations interviendra fin décembre.
- Ⓟ Vous devez MAITRISER la technologie que vous présentez en situation, ce n'est pas un simple TP avec réalisation de « tuto ».
- Ⓟ Vos deux solutions doivent être documentées techniquement (serveur, IP, mot de passe, étapes suivies dans la réalisation, planning de mise en œuvre, difficultés majeures rencontrées et solutions apportées).

Ⓟ Une partie des documentations techniques sera à mettre sur le portfolio (pour l'épreuve E4) Ⓟ Vous allez impacter le travail des autres apprentis, souvent négativement (une partie du réseau ou serveurs sera inopérant), il faut absolument communiquer au sein du groupe. Ⓟ Vous ne pouvez pas exiger d'un autre apprenti de ne pas faire x ou y chose, sous prétexte qu'à cause de cela, votre situation ne fonctionne plus, ou vous demande une adaptation, c'est toujours le cas en entreprise, il faut apprendre à le faire intelligemment.

Ⓟ Ne vous battez pas ! Pas d'embrouille, faites des réunions lorsqu'une situation impacte négativement trop souvent la situation des autres apprentis

Ⓟ N'hésitez pas à vous inspirer/reproduire des technologies que vous avez utilisées dans votre entreprise !

Ⓟ Documentez, suivez votre projet régulièrement, c'est indispensable. Vous ne pouvez pas faire une journée d'implémentation sans avoir apporté votre contribution à la documentation. Ⓟ Bloquez l'expiration des mots de passe.

Ⓟ Ne travaillez qu'en SSH/RDP avec les équipements actifs du réseau.

Ⓟ FAITES DES SAUVEGARDES TRÈS SOUVENT.

Ⓟ FAITES DES SNAPSHOT/SAUVEGARDES de vos VMs avant de tester telle ou telle fonctionnalité que vous ne maîtrisez pas.

Ⓟ La mise en œuvre d'Exchange modifie en profondeur le schéma AD, ce qui est l'objet chaque année de pleurs quand Exchange est en ruine (AD le sera aussi !) et il faudra tout recommencer.

Ⓟ Documentez vos GPO.

Ⓟ GLPI est là pour le suivi de vos incidents lors de la mise en œuvre de vos technologies, vous DEVEZ l'utiliser, il n'est pas là pour la déco.

Ⓟ La câble console, c'est pour mettre en service les équipements actifs, ensuite on ne s'en sert plus (ou presque) !

Ⓟ Faites un schéma de câblage (telle interface du switch sert à tel équipement, elle est dans tel VLAN).

Ⓟ Il ne sert à rien d'étiqueter les câbles, quand ils sont débranchés, çà n'aide pas à rebrancher (le schéma de câblage si) ; c'est l'erreur la plus classique de tous les candidats…

Ⓟ Communiquez, communiquez, communiquez au sein de votre équipe !!!!

Ⓟ Si vous avez du temps, n'hésitez pas à expérimenter d'autres situations, puis retenir vos deux favorites.

Ⓟ N'hésitez pas à faire tester vos situations par votre binome.

Ⓟ Aidez-vous, même entre équipes !

Ⓟ N'attendez SURTOUT PAS les dernières semaines pour vous y mettre, beaucoup ont essayé, très peu ont réussi, la somme de travail est très importante.

Ⓟ Ne jouez pas les durs à cuire, en implémentant au dernier moment des fonctionnalités complexes que vous ne maîtrisez pas.

Dossiers de situations

Vous devrez présenter, avant votre épreuve, et pour preuve auprès du rectorat, deux dossiers distincts pour vos deux situations.

Ces deux dossiers sont une synthèse de vos travaux, ils doivent tenir sur 8 pages max, pas beaucoup plus, respecter un formalisme précis, et ne rien omettre d'essentiel (nom des serveurs, VLANs

présents, plans d'adressage, IP des serveurs, mots de passe des serveurs et équipements, schéma réseau global, fonctionnalités mises en œuvre, **démarche entreprise pour la réalisation**)

Le jury se base quasi exclusivement sur ce document pour réaliser votre sujet d'examen, aussi il faut y apporter un soin très important. Si vous avez bien documenté les fonctionnalités mises en œuvre et qu'il transparaît que vous maîtrisez, le jury saura sur quoi vous interroger.

La construction des sujets par le jury

Le jury prend connaissance de vos situations une fois les deux dossiers remis, pour rappel le jury est extérieur à la CCI et ne vous connaît pas. TOUT DOIT FONCTIONNER.

Les règles pour établir un sujet son très simples :

- Vos situations sont mal documentées dans les dossiers E5 que vous remettez : Le jury se rabat sur un sujet « à minima », et ce ne sera jamais à votre avantage. Il faudra en une heure faire des GPOs, des dossiers partagés, des ACL un peu de partout, voir du routage, en plus de poser plusieurs questions sur vos situations : on ne sait pas ce que vous avez fait-> on demande un peu de tout, et c'est compliqué à réaliser en un heure
- Vos situations sont très minimalistes ou ne fonctionnent pas: Vous risquez de très fortes pénalités (-15 points), ou en plus d'avoir un sujet « à minima » de devoir agir sur vos deux situations.

Pour les deux cas précédent, le but n'est pas de mettre le candidat en difficulté, mais de lui poser plein de problèmes pour voir ce qu'il sait faire, s'il sait gérer ses priorités, donc son temps, et au final si il mérite le titre de technicien systèmes et réseaux.

- Vos situations sont bien documentées, vous avez expérimenté plein de choses, les avez retournées un peu dans tous les sens. Le questionnement dans ce cas portera principalement sur l'exploitation de votre situation, et on sera moins tenté de demander trop de GPO et d'ACL (mais il y en aura toujours un peu).

Dans tous les cas, il y aura forcément une question soit sur l'AD, soit sur les ACL, et on sondera si vous savez faire quelque chose avec la supervision, ou bien un autre élément au hasard (n'importe quoi qui fait partie du schéma que vous présentez).

A propos du schéma de votre infrastructure, **joint aux deux dossiers de situation**

Votre schéma doit faire apparaître tous les éléments obligatoires, et à minima **un** des éléments « optionnels » parmi la liste des éléments optionnels (en clair il doit être conforme au tableau de l'annexe 10 et ne rien avoir omis).

Les serveurs ou services mis en œuvre par votre binôme dans le cadre de ses deux situations personnelles, NE DOIVENT PAS APPARAÎTRE SUR CE SCHÉMA. En effet, le jury est susceptible de vous demander d'intervenir sur n'importe quel élément présent dans ce schéma.

Ex : Vous avez mis un serveur Exchange qui provient d'une situation de votre collègue, mais vous n'avez jamais touché Exchange ? Erreur, on pourrait vous demander de déplacer ce serveur dans la DMZ…. et vérifier qu'il fonctionne toujours !

Ex 2 : Vous avez placé deux routeurs en redondance, mais çà ne fait pas l'objet d'une de vos deux situations ? Erreur, le jury va penser que vous maîtrisez la redondance des routeurs, et pourra vous demander d'intervenir dessus….

Soyez donc encore une fois extrêmement vigilants sur la qualité des deux documents que vous rendez. PROJET

Jury

Un jury extérieur à la CCI sera présent pour évaluer votre travail, il ne vous connaît pas.

Rappels sur l'épreuve

Phases

Phase 1 : (quelques minutes) Remise du sujet au candidat, si le candidat a des questions, c'est le seul moment durant lequel il pourra le faire.

Phase 2 : Préparation sur table : 30 minutes. Accès internet autorisé, toute forme de communication interdite (éliminatoire). Le candidat prépare sur papier la démarche qu'il souhaite entreprendre pour résoudre les besoins exprimés.

Phase 3 : 20 minutes : le candidat présente sa démarche au Jury. Ce dernier pourra attirer l'attention du candidat sur des points cruciaux, ou l'aide à remodeler son plan d'action si ce dernier n'est pas suffisant. Une démarche est une succession d'étapes avec tests associés en fin d'étape.

Phase 4 : 1 heure : Le candidat est en autonomie sur son environnement, et réalise son plan d'action.

Phase 5 : jusqu'à 20 minutes : Le candidat présente le travail réalisé, en structurant sa présentation autour des étapes qu'il a prévues de réaliser. Le Jury questionne le candidat (les questions peuvent prendre n'importe quelle forme). Le candidat, une fois interrogé doit impérativement remettre l'infrastructure dans l'état initial avant le prochain candidat.

Phase 6 : Chaque Jury ayant effectué sa propre notation, un temps d'harmonisation est nécessaire afin de s'assurer de la justesse de la note proposée.

La note n'est pas communiquée au candidat, elle est directement transmise au rectorat, avec les feuilles de notation, le jury d'attribution des titres BTS se réservant le droit d'altérer cette note (ex : sur ou sous notation d'un centre d'examen).

Cas des 1/3 temps

Certains candidats peuvent bénéficier d'un tiers temps (dossier à mettre en œuvre rapidement). Cas

classiques :

Ⓟ Tiers temps sur l'écrit : Seule la partie « travail sur table » sera impacté (1/3 de temps en plus), puisque c'est la seule phase durant laquelle un écrit est nécessaire.
Ⓟ Tiers temps type « oral », dans ce cas, le candidat disposer d'un tiers de temps en plus durant la phase devant le jury (avant pratique), puis dans la phase de restitution.
Ⓟ Tiers temps type « pratique », dans ce cas, le candidat disposera d'un tiers temps durant sa phase de réalisation.

Certains candidats peuvent disposer de plusieurs types de tiers temps, en fonction de ses difficultés.

VPN

Vous devrez mettre en œuvre un serveur VPN au sein de votre infrastructure pour y accéder à distance, il faudra me communiquer votre adresse IP WAN sur lequel le VPN sera en écoute (192.168.150.X) ainsi que le port et on se chargera de rediriger un port de l'IP publique de la CCI vers votre serveur VPN.

Point d'attention : En cas d'utilisation inappropriée, la CCI se réserve le droit de révoquer définitivement l'accès à un apprenti, ou à toute la section, et ceci sans rappel à l'ordre.

En particulier :

- Ⓟ Ne pas surcharger la connexion lorsque vous utilisez le VPN durant les heures habituelles de formation (pour ne pas impacter la formation des autres sections quand vous êtes en entreprise).
- Ⓟ Accéder au VPN avec un système d'exploitation légitime (non piraté), ne contenant pas de logiciel piraté, ni virus, l'ordinateur utilisé avec le VPN doit être dûment protégé. Ⓟ Pas de téléchargement de logiciels illégaux via la connexion de la CCI.
- Ⓟ Pas de P2P.