

CONTRÔLE DE L'ENVIRONNEMENT TECHNOLOGIQUE

Annexe II.E – Environnement technologique pour la certification du référentiel du BTS SIO

Nom et adresse du centre d'examen	CFI-CCI LAVAL 5 Boulevard de l'Industrie 53940 SAINT-BERTHEVIN	Cachet et signature du responsable du centre d'examen accueillant l'épreuve E5	SISR
--	--	---	-------------

1. Environnement commun aux deux options

1.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation ¹
Un service d'authentification	L' Active Directory est mon service centralisé d'identification et d'authentification. _srv-ad2 et _srv-ad1 (serveurs Active Directory, Windows serveur 2019) : 2CPU, 2GB de ram et 80GB de stockage.	
Un SGBD	Un serveur MariaDB est utilisé pour centraliser les requêtes SQL. Il est installé sur _srv-node02 (Debian, 1 CPU, 1GB de ram, 16GB de stockage)	
Un accès sécurisé à Internet	Création de règles de pare-feu pour autoriser une connexion sécuriser à Internet. La solution opnSense à été installée sur _firewall-opnsense (Debian, 2 CPU, 4GB de ram, 20GB de stockage)	
Un environnement de travail collaboratif	La solution Nextcloud a été installée sur _srv-node01 (Debian, 1CPU, 1GB de ram, 16GB de stockage)	
Deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel <i>open source</i>	_srv-node01 : Debian 11. _srv-ad1 : Windows server 2019. _dmz-srv-mail : Debian 11 avec serveur mail sous docker.	

¹²⁸ À renseigner pour les personnes candidates passant l'épreuve sous forme ponctuelle.

ANNEXE 8-A (suite) : Modèle d'attestation de respect de l'annexe II.E – Environnement technologique pour la certification du référentiel

Épreuve E5 - Administration des systèmes et des réseaux (option SISR) - Coefficient 4

Une solution de sauvegarde	Afin de sécuriser les données de mon serveur de fichier, j'utilise un serveur de sauvegarde. _srv-urbackup (Debian, 1CPU, 1GB de ram, 16GB de stockage pour l'OS + 100GB de stockage pour les sauvegardes)	
Des ressources dont l'accès est sécurisé et soumis à habilitation	Via le serveur ad1 et ad2 , chaque utilisateur possède un répertoire personnel ou il est le seul à avoir accès en lecture et écriture.	
Deux types de terminaux dont un mobile (type <i>smartphone</i> ou encore tablette)	Une connexion filaire entre les serveurs est disponible. Il est aussi possible d'administrer l'infrastructure via le réseau sans fil.	

1.2 Les logiciels de simulation ou d'émulation sont utilisés en réponse à des besoins de l'organisation. Ils ne peuvent se substituer complètement à des équipements réels dans l'environnement technologique d'apprentissage.

1.3 Des outils sont mobilisés pour la gestion de la sécurité :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation ²
Gestion des incidents	Un serveur GLPI est installé sur _srv-node01 , ou les utilisateurs peuvent créer des tickets afin de remonter leurs incidents auprès des techniciens.	
Détection et prévention des intrusions	Le système d'IDS de opnSense est activé et configuré.	
Chiffrement	Le HTTPS des pages web assure un chiffrement sécurisé. Un certificat généré est diffusé sur toutes les machines.	
Analyse de trafic	L'analyse de trafic du réseau est effectuée avec l'outil « journal » du Firewall _firewall-opnsense .	

²²⁸ À renseigner pour les personnes candidates passant l'épreuve sous forme ponctuelle.

ANNEXE 8-A (suite) : Modèle d'attestation de respect de l'annexe II.E – Environnement technologique pour la certification du référentiel

Épreuve E5 - Administration des systèmes et des réseaux (option SISR) - Coefficient 4

2. Éléments spécifiques à l'option « Solutions d'infrastructure, systèmes et réseaux » (SISR)

Rappel de l'annexe II.E du référentiel : « *Une solution d'infrastructure réduite à une simulation par un logiciel ne peut être acceptée.* »

2.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation ³
Un réseau comportant plusieurs périmètres de sécurité	L'infrastructure est scindée en 4 sous-réseaux et gérée par le serveur de pare-feu _firewall-opnsense : WAN : DHCP, passerelle : 10.192.0.0 ; Réseau WANCCI53 , considéré comme le FAI LAN : DHCP possible, réseau 10.192.45.0/24 ; Réseau 545 , DMZ : réseau 10.192.44.0/24 ; Réseau 544 , SRV : réseau 10.192.43.0/24 ; Réseau 543 , utilisé pour tous les serveurs	
Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité	Un contrat de maintien en conditions opérationnel de l'infrastructure pendant 3 ans.	
Un logiciel d'analyse de trames	Le logiciel Wireshark est installé sur _lan-win-mgmt afin de pouvoir analyser les trames réseaux.	
Un logiciel de gestion des configurations	L'agent GLPI est installé via GPO sur tous les postes dans la zone LAN. Les données remontent sur _srv-node01 , et permettent ainsi de faire l'inventaire automatiquement.	
Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès	Une machine de rebond basé sur Windows 10 est installée (_lan-win-mgmt) dans la zone LAN, elle dispose du logiciel mRemoteNG et lui permet d'accéder à tous les autres serveurs.	
Une 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	Le logiciel Grafana est installé sur _srv-supervision avec le gestionnaire de données Prometheus. On y retrouve toutes les machines qui y sont superviser.	
Une solution garantissant des accès sé-	Dans la zone DMZ , un serveur web sous IIS est installé afin de proposer un Intranet.	

³²⁸ À renseigner pour les personnes candidates passant l'épreuve sous forme ponctuelle.

curisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet)	Sur _dmz-IIS-server (Windows Server, 2CPU, 4GB de ram, 80GB de stockage)	
Une solution garantissant la continuité d'un service	Les sauvegardes effectuées sont transmises sur le serveur de backup (_srv-urbackup) afin de maintenir entièrement les services fournis par les différents serveurs.	
Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion	La réplication de mon contrôleur de domaine _srv-ad1 par _srv-ad2 permet de maintenir opérationnel les tâches de l' AD1 même s'il tombe en panne.	
Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion	La réplication de mon contrôleur de domaine _srv-ad1 par _srv-ad2 va permettre d'équilibrer la charge entre les contrôleurs de domaine. Le serveur DHCP est en mode équilibre de charge en 50/50 avec l' AD2 .	

2.2 La structure et les activités de l'organisation s'appuient sur au moins une solution d'infrastructure opérationnelle parmi les suivantes :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation ⁴
Une solution permettant la connexion sécurisée entre deux sites distants	Le pare-feu de Megaproduct _firewall-opnsense me permet de maintenir la connexion entre les différents sites opérationnel ou non et de manière sécurisée.	
Une solution permettant le déploiement des solutions techniques d'accès	Le serveur UrBackup permet la restauration d'image système (BMR – Bare Metal Restore).	
Une solution gérée à l'aide de procédures automatisées écrites avec un langage de <i>scripting</i>	L'AD à la possibilité d'être remonté qu'avec des scripts Powershell et des .csv , afin de faciliter la tâche. Les ordinateurs sont automatiquement mirés dans une OU « Ordinateurs » via un script appelé tous les jours à 04h00.	
Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau	Les alertes envoyées par l'IDS de _firewall-opnsense plus la journalisation de toutes les requêtes permettent de prévenir des intrusions.	

⁴²⁸ À renseigner pour les personnes candidates passant l'épreuve sous forme ponctuelle.

