

ICCMN



La sécurité cloud notre domaine

Inventaire

Composant	Quantité	Marque/Modèle	Caractéristiques
Disque dur	8	Western Digital	1 To, SATA 6 Gbit/s, 5400 RPM
Barrette de RAM	11	Samsung	8 Go, DDR3
Barrette de RAM	1	Hynix	8 Go, DDR3
Serveur	1	Dell Poweredge R620	Numéro de série : 9HCFR22, Numéro de commande : 20639856314
Processeur	2	Intel Xeon E5-2650L v2	1,70 GHz, cache de niveau 2 de 10 x 250 Ko, cache de niveau 3 de 25 Mo
Chipset	1	Intel C600 series	
Switch réseau	1	Cisco Catalyst 2960G 48 ports	
Routeur sans fil	1	TP-Link Archer A5 AC1200 Wireless Dual Band Router	
Clavier	1	VicTsing PC132A	
Carte RAID	1	Dell PERC H710 Mini	
Carte réseau	4	Intel® Gigabit 4P I350-t rNDC	Adresses MAC : 24:6E:96:2F:90:2C ; 24:6E:96:2F:90:2D ; 24:6E:96:2F:90:2E ; 24:6E:96:2F:90:2F
Disques virtuels en RAID	7		Le dernier est celui du système

Tableau des taches à réaliser

Activités	Semaine1	Semaine2	Semaine3	Semaine4	Semaine5	Semaine6	Semaine7
NASSIM							
-TRUE NAS	2	2	2				
-SNORT		2	2	2			
Makhtar							
-GLPI	2	2					
-Cœur de réseau			3	3	2		
CORENTIN							
-DNS	2	2					
-Active Directory			3	3	2		
CLEMENT							
-Zabbix	2	2	2				
-HA proxy				2	2	2	
IMANE							
Pare-feu							

TACHE DE NASSIM : TRUENAS ET SNORT

TrueNAS est un système de stockage en réseau open source qui permet de stocker et de gérer des données à grande échelle. Snort est un système de détection d'intrusion open source qui permet de détecter et de prévenir les attaques sur le réseau.

Pour répondre aux besoins d'un client fictif qui aurait besoin de gérer son infrastructure de stockage et de sécurité, Nassim serait chargé d'installer et de configurer TrueNAS pour gérer efficacement les données du client. Il serait également responsable de l'installation et de la configuration de Snort pour détecter les tentatives d'intrusion sur le réseau et protéger les données stockées sur le serveur.



TACHE DE MAKHTAR : GLPI ET CŒUR DE RESEAU

GLPI est un système open source de gestion de parc informatique qui permet de suivre et de gérer les actifs matériels et logiciels de l'entreprise. Le cœur de réseau fait référence à l'ensemble des équipements réseau de base, tels que les routeurs, les commutateurs et les pare-feux.

Pour répondre aux besoins d'un client fictif qui aurait besoin de gérer son parc informatique et son réseau, Makhtar serait chargé d'installer et de configurer GLPI pour permettre une gestion efficace des actifs matériels et logiciels de l'entreprise. Il serait également responsable de l'installation et de la configuration des équipements de base du réseau, tels que les routeurs, les commutateurs et les pare-feu, pour garantir la sécurité et la stabilité du réseau.

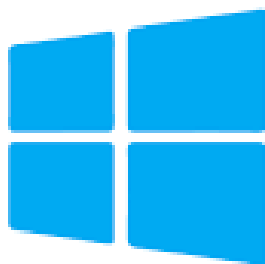


GLPI

TACHE DE CORENTIN : DNS ET ACTIVE DIRECTORY

DNS (Système de noms de domaine) est un système qui permet de résoudre les noms de domaine en adresses IP, tandis qu'Active Directory est un système de gestion d'annuaire qui permet de gérer les utilisateurs, les groupes et les ordinateurs d'un réseau.

Pour répondre aux besoins d'un client fictif qui aurait besoin d'une gestion efficace de son infrastructure réseau et de son annuaire d'utilisateurs, Corentin serait chargé d'installer et de configurer DNS pour permettre une résolution efficace des noms de domaine en adresses IP. Il serait également responsable de l'installation et de la configuration d'Active Directory pour permettre une gestion efficace des utilisateurs, des groupes et des ordinateurs du réseau.

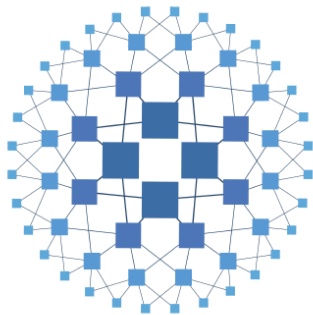


Active Directory

TACHE DE CLEMENT : ZABBIX ET HA PROXY

Zabbix est un système open source de surveillance et de suivi de la disponibilité des ressources informatiques, tandis que HA Proxy est un système open source de répartition de charge qui permet de répartir le trafic entre les serveurs.

Pour répondre aux besoins d'un client fictif qui aurait besoin d'une surveillance efficace de ses ressources informatiques et d'une répartition efficace de la charge, Clément serait chargé d'installer et de configurer Zabbix pour surveiller l'état des serveurs et des applications du client. Il serait également responsable de l'installation et de la configuration de HA Proxy pour répartir la charge entre les différents serveurs du client.



HAPROXY

ZABBIX

TACHE D'IMANE : OPENVPN ET PARE-FEU

La tâche d'Imane consiste à mettre en place un réseau privé virtuel (VPN) avec OpenVPN pour permettre aux utilisateurs distants de se connecter de manière sécurisée au réseau de l'entreprise. Elle aura également la charge de la configuration du pare-feu pour sécuriser l'accès au réseau et limiter les risques d'intrusion.

Plus spécifiquement, Imane devra :

- Installer et configurer le logiciel OpenVPN sur le serveur dédié afin de permettre la création d'un réseau privé virtuel ;
- Créer les certificats et clés d'authentification pour chaque utilisateur autorisé à se connecter au VPN ;
- Configurer le pare-feu pour permettre l'accès aux services nécessaires depuis le VPN, tout en bloquant les connexions non autorisées depuis l'extérieur ;
- Mettre en place des règles de filtrage pour protéger le réseau contre les attaques externes et les intrusions ;
- Tester et valider le fonctionnement du VPN et du pare-feu pour s'assurer que l'ensemble du système est sécurisé et fonctionne de manière optimale.

En somme, la tâche d'Imane vise à sécuriser l'accès au réseau de l'entreprise pour les utilisateurs distants en mettant en place un VPN avec OpenVPN et un pare-feu efficace pour limiter les risques d'intrusion.



Ces tâches permettent au bon fonctionnement et à assurer la sécurité d'une quelconque entreprise si elle venait à faire à nos services.