![Une image contenant texte, Police, logo, Graphique

Description générée automatiquement]()

**Mots-clés**

Table des matières

[Prosit 1 2](#_Toc149729857)

[Prosit 2 3](#_Toc149729858)

[Prosit 3 4](#_Toc149729859)

[Prosit 4 6](#_Toc149729860)

[Prosit 5 7](#_Toc149729861)

[Prosit 6 8](#_Toc149729862)

[Prosit 7 9](#_Toc149729863)

[Prosit 8 10](#_Toc149729864)

## Prosit 1

DNS (Domain Name System) : Le DNS est un système utilisé sur Internet pour traduire les noms de domaine en adresses IP. Il permet aux utilisateurs d'accéder aux sites web en utilisant des noms conviviaux au lieu de devoir se souvenir des adresses IP numériques.

S.I (Système d'Information) : Le Système d'Information englobe l'ensemble des ressources informatiques et des processus utilisés pour collecter, stocker, gérer et diffuser des informations au sein d'une organisation.

ERP (Enterprise Resource Planning) : Un ERP est un système informatique intégré utilisé par les entreprises pour gérer efficacement leurs opérations, y compris la gestion des ressources humaines, des finances, de la production et de la logistique.

AD (Active Directory) : Active Directory est un service de répertoire développé par Microsoft, principalement utilisé pour gérer les identités et les droits d'accès des utilisateurs dans un environnement informatique Windows.

Powershell : Powershell est un langage de script et un environnement de ligne de commande développé par Microsoft, principalement utilisé pour l'automatisation des tâches administratives dans les systèmes Windows.

ANSSI (Agence nationale de la sécurité des systèmes d'information) : L'ANSSI est une agence gouvernementale française chargée de la sécurité des systèmes d'information en France. Elle joue un rôle essentiel dans la protection contre les cybermenaces.

Tableau Kanban : Le Tableau Kanban est une méthode de gestion de projet visuelle qui permet de suivre les tâches et les activités à l'aide de cartes et de colonnes pour représenter le flux de travail.

Administrateur système : Un administrateur système est une personne responsable de la gestion, de la maintenance et de la sécurité des systèmes informatiques au sein d'une organisation.

Serveur d'annuaire : Un serveur d'annuaire est un système qui stocke et gère des informations sur des objets tels que des utilisateurs, des groupes et des ressources au sein d'un réseau informatique, généralement utilisé pour l'authentification et l'autorisation.

Infrastructure : L'infrastructure désigne l'ensemble des composants matériels, logiciels, réseau et de communication qui permettent à un système informatique ou à une organisation de fonctionner.

Base Keepass : Une base Keepass est une base de données sécurisée utilisée pour stocker des mots de passe et d'autres informations sensibles.

## Prosit 2

ADDS : ADS peut signifier "Active Directory Domain Services", qui est un service de gestion des identités et des services d'annuaire développé par Microsoft. Il est couramment utilisé pour la gestion des utilisateurs, des groupes et des ressources au sein d'un réseau informatique.

FSMO : FSMO signifie "Flexible Single Master Operations". C'est un concept utilisé dans les services Active Directory de Microsoft pour désigner les rôles maîtres qui sont responsables de certaines opérations spécifiques au sein d'un domaine ou d'une forêt Active Directory.

SIO : SIO peut signifier "Systèmes d'Information et d'Organisation", ce qui fait référence à une discipline qui étudie la gestion des systèmes d'information au sein des organisations.

ADSL : ADSL signifie "Asymmetric Digital Subscriber Line". Il s'agit d'une technologie de communication de données qui permet de fournir une connexion Internet à haut débit sur des lignes téléphoniques traditionnelles.

OS : OS signifie "Système d'Exploitation" en informatique. C'est le logiciel qui gère les ressources matérielles d'un ordinateur et permet l'exécution d'autres programmes.

Sous-domaine : Un sous-domaine est une partie d'un domaine de réseau plus vaste. Il permet une organisation hiérarchique des ressources et des utilisateurs au sein d'un réseau.

Mono forêt : Une forêt Active Directory est une structure de gestion des identités dans les environnements Windows. "Mono forêt" pourrait faire référence à une forêt unique, ce qui signifie qu'il n'y a qu'une seule instance de la forêt dans un environnement donné.

Relation d’approbation : Une relation d'approbation est une relation établie entre deux domaines ou forêts dans un environnement Active Directory. Elle permet à ces entités de partager des ressources et de collaborer de manière sécurisée.

Paradigme : Un paradigme est un modèle ou une approche générale utilisée pour résoudre des problèmes ou aborder des sujets spécifiques. En informatique, cela peut faire référence à des modèles de programmation ou à des approches de conception.

## Prosit 3

ACL : « Access control list » Ensemble de règles qui définissent les opérations (lire, écrire, exécuter…) que pourra réaliser un utilisateur sur une ressource (un fichier, le plus souvent, mais aussi une adresse ou un port réseau).

Proxy : Un proxy est un serveur intermédiaire qui agit en tant qu'intermédiaire entre un utilisateur et un serveur de destination. Il peut être utilisé pour diverses raisons, notamment pour la sécurité, la gestion du cache, ou l'anonymat (en masquant l’ip).

Zone démilitarisée (DMZ) : DMZ: En informatique, une zone démilitarisée est un sous-réseau séparé du réseau local et isolé de celui-ci ainsi que d'Internet par un pare-feu.

Filtrage : Le filtrage fait référence au processus de surveillance et de gestion du trafic réseau en fonction de certaines règles prédéfinies. Cela peut inclure le filtrage du contenu web, le filtrage des e-mails indésirables, etc.

Bac à sable : Un bac à sable (sandbox en anglais) est un environnement sécurisé et isolé où les fichiers ou les applications peuvent être exécutés et analysés sans risque pour le système hôte. Il est souvent utilisé pour tester des logiciels potentiellement dangereux.

UTM : UTM signifie "Unified Threat Management". C'est une approche de la sécurité réseau qui combine plusieurs fonctions de sécurité, telles que le pare-feu, l'antivirus, le filtrage web, etc., dans un seul appareil ou système.

DMZ : Veuillez noter que "DMZ" a déjà été défini comme "Zone démilitarisée". Il s'agit d'une redondance dans votre liste.

IPS/IDS : IPS (Système de Prévention d'Intrusion) et IDS (Système de Détection d'Intrusion) sont des technologies de sécurité réseau. IDS détecte les activités suspectes, tandis que IPS tente de bloquer activement les intrusions ou les menaces.

NAT/PAT : NAT (Traduction d'Adresse Réseau) et PAT (Traduction d'Adresse Port) sont des techniques utilisées pour attribuer des adresses IP et des ports aux appareils sur un réseau privé, permettant ainsi la communication avec le réseau public, généralement via un seul adresse IP publique.

Firewall : Un pare-feu est un dispositif ou un logiciel qui contrôle le trafic réseau en fonction de règles de sécurité définies, en permettant ou en bloquant le trafic en fonction de ses caractéristiques.

SOC : SOC signifie "Centre de Sécurité Opérationnelle". Il s'agit d'une équipe ou d'un centre qui surveille en permanence la sécurité informatique, détecte les menaces et réagit en temps réel pour protéger les systèmes informatiques.

SIEM : SIEM signifie "Système de Gestion des Informations et des Événements de Sécurité". C'est une solution logicielle ou matérielle qui permet de collecter, d'analyser et de gérer les données de sécurité pour détecter les menaces.

PFsense : pfSense est un système d'exploitation open-source basé sur FreeBSD, principalement utilisé comme pare-feu et routeur pour les réseaux informatiques.

Malwares : Les malwares sont des logiciels malveillants, tels que les virus, les vers, les chevaux de Troie, les spywares, etc., conçus pour causer des dommages ou voler des informations sur un système informatique.

## Prosit 4

Chiffrement par substitution : Le chiffrement par substitution est une méthode de cryptage où chaque lettre d'un texte clair est remplacée par une autre lettre selon une règle spécifique. Le chiffrement César est un exemple célèbre de chiffrement par substitution.

Cryptographie : La cryptographie est l'art et la science de sécuriser des informations en les transformant en un format illisible, puis en les rendant lisibles uniquement pour les personnes disposant de la clé de déchiffrement appropriée.

Cryptanalyse : La cryptanalyse est l'analyse des systèmes de chiffrement dans le but de les casser ou de les décrypter sans avoir la clé de déchiffrement. C'est l'art de casser les codes.

Hashage : Le hashage est le processus de conversion de données (comme un mot de passe) en une valeur de hachage, généralement une chaîne de caractères alphanumériques, à l'aide d'une fonction de hachage. Le résultat est souvent utilisé pour vérifier l'intégrité des données.

Signature de mot de passe (MDP) : Une signature de mot de passe est une technique de stockage des mots de passe dans une base de données de manière sécurisée en utilisant des fonctions de hachage et des méthodes de salage pour protéger les informations sensibles.

Signature électronique : Une signature électronique est l'équivalent numérique d'une signature manuscrite. Elle est utilisée pour authentifier un document ou une transaction électronique, garantissant son origine et son intégrité.

Chiffrement César : Le chiffrement César est une technique de chiffrement par substitution où chaque lettre dans le texte clair est déplacée d'un certain nombre de positions dans l'alphabet. Il porte le nom de Jules César, qui l'aurait utilisé pour protéger des messages.

Chiffrement de Hill : Le chiffrement de Hill est une méthode de chiffrement qui utilise des matrices pour transformer le texte clair en texte chiffré. Il a été inventé par Lester S. Hill.

Enigma : Enigma était une machine de chiffrement mécanique utilisée par les forces armées allemandes pendant la Seconde Guerre mondiale. Elle était célèbre pour sa complexité et a été décryptée par les Alliés, ce qui a eu un impact significatif sur l'issue de la guerre.

## Prosit 5

SSO : SSO signifie "Single Sign-On", ce qui se traduit en français par "Authentification Unique". C'est un mécanisme qui permet à un utilisateur de se connecter une seule fois à un système ou à une application et d'accéder ensuite à plusieurs services sans avoir à se reconnecter à chaque fois.

MiM : MiM signifie "Man-in-the-Middle", soit "L'homme du milieu" en français. Il s'agit d'une attaque où un attaquant intercepte et modifie les communications entre deux parties, souvent sans que ces dernières en aient conscience.

Keyloggers : Les keyloggers, ou "enregistreurs de frappe" en français, sont des programmes ou des dispositifs matériels conçus pour enregistrer les frappes du clavier d'un utilisateur à son insu. Cela peut être utilisé pour voler des informations sensibles, telles que des mots de passe.

Extranet : Un extranet est un réseau privé étendu qui permet à des partenaires, clients ou fournisseurs autorisés d'accéder à certaines ressources ou informations internes d'une organisation, généralement via Internet.

PKI : PKI signifie "Infrastructure à Clé Publique" en français. C'est un ensemble de technologies et de pratiques de sécurité qui permettent de gérer des clés de chiffrement, de certificats numériques et d'assurer l'authentification et la confidentialité des données.

SSL : SSL signifie "Secure Sockets Layer", soit "Couche de Sockets Sécurisée" en français. C'est un protocole de sécurité qui garantit la confidentialité et l'intégrité des données échangées entre un serveur et un client, souvent utilisé pour sécuriser les connexions Web.

TLS : TLS signifie "Transport Layer Security", ou "Sécurité de la Couche de Transport" en français. Il s'agit d'une version plus récente et plus sécurisée du protocole SSL, utilisée pour sécuriser les communications sur Internet.

## Prosit 6

Serveur RDP : Un serveur RDP est un serveur qui prend en charge le protocole RDP (Remote Desktop Protocol). Il permet aux utilisateurs de se connecter à distance à un ordinateur ou à un serveur et d'accéder à son bureau et à ses applications à partir d'un emplacement distant.

Hyper-V : Hyper-V est une plateforme de virtualisation développée par Microsoft. Elle permet de créer et de gérer des machines virtuelles sur un serveur physique, ce qui permet l'exécution de plusieurs systèmes d'exploitation sur une même machine.

Docker : Docker est une plateforme de conteneurisation qui permet d'emballer des applications et leurs dépendances dans des conteneurs légers et portables. Cela facilite le déploiement et la gestion d'applications dans des environnements différents.

ERP : ERP signifie "Enterprise Resource Planning", soit "Planification des ressources de l'entreprise" en français. Il s'agit de logiciels intégrés conçus pour aider les entreprises à gérer et à automatiser leurs processus métier, y compris la comptabilité, la gestion des ressources humaines, la logistique, etc.

Virtualisation : La virtualisation est la création d'environnements virtuels ou de ressources informatiques, tels que des machines virtuelles, des réseaux virtuels ou des serveurs virtuels, à partir d'une seule ressource matérielle.

Hyperviseur : Un hyperviseur est un logiciel ou un matériel qui permet la création et la gestion de machines virtuelles. Il agit en tant que couche d'abstraction entre le matériel physique et les machines virtuelles.

Oracle : Oracle est une entreprise spécialisée dans les bases de données et les solutions logicielles pour les entreprises. Elle est notamment connue pour sa base de données Oracle, largement utilisée dans le monde de l'informatique.

VMware : VMware est une entreprise qui fournit des solutions de virtualisation, notamment le logiciel VMware vSphere, qui permet la création et la gestion de machines virtuelles.

Windows Container : Un conteneur Windows est une forme de conteneurisation qui permet d'exécuter des applications Windows dans un environnement isolé et léger. Il est souvent utilisé pour le déploiement d'applications sur des serveurs Windows.

Ansible : Ansible est une plateforme d'automatisation open source utilisée pour déployer, gérer et configurer des infrastructures et des applications. Il permet d'automatiser des tâches de gestion informatique de manière efficace.

## Prosit 7

Log : Un log est un enregistrement chronologique des événements, des actions ou des messages générés par un système informatique, un logiciel ou un dispositif. Les logs sont souvent utilisés pour le dépannage, la surveillance et la sécurité.

Fichier temporaire : Un fichier temporaire est un fichier créé par un programme pour stocker des données de manière temporaire, souvent dans le but de traiter ou de transférer des informations entre les différentes étapes d'un processus.

Outils de monitoring : Les outils de monitoring sont des logiciels ou des dispositifs utilisés pour surveiller en temps réel les performances, l'état ou la disponibilité des systèmes informatiques, des réseaux ou des applications.

Protocole de supervision : Un protocole de supervision est un ensemble de règles et de normes permettant aux systèmes de collecter des données de supervision, de les envoyer à un outil de monitoring et de les interpréter pour évaluer la santé d'un système.

SNMP/ MIB : SNMP (Simple Network Management Protocol) est un protocole de supervision réseau, tandis que MIB (Management Information Base) est une structure de données hiérarchique utilisée pour organiser des informations de supervision dans le cadre de SNMP.

Centreon : Centreon est une plateforme open source de surveillance informatique qui permet de collecter, d'analyser et de visualiser des données de supervision pour assurer la disponibilité et les performances des systèmes.

Nagios : Nagios est un logiciel de surveillance informatique open source très populaire qui permet de surveiller des services réseau, des hôtes et d'envoyer des alertes en cas de problèmes.

Syslogs : Les syslogs sont des messages d'événements générés par les systèmes d'exploitation, les serveurs et les applications. Ils sont utilisés pour la journalisation, le dépannage et la surveillance des systèmes.

## Prosit 8

Raid : https://www.ontrack.com/fr-fr/recuperation-donnees/raid/configurations#:~:text=De%20toutes%20ces%20configurations%20RAID,inscrit%20les%20informations%20en%20double

RAID 0-5 : Les niveaux RAID 0 à 5 font référence à différentes configurations de stockage redondant utilisées pour améliorer la performance et la résilience des systèmes de stockage. Par exemple, le RAID 0 divise les données en bandes et les répartit sur plusieurs disques, tandis que le RAID 5 utilise une parité distribuée pour la tolérance aux pannes.

ESN : ESN signifie "Entreprise de Services du Numérique". C'est un terme utilisé en France pour désigner les entreprises qui fournissent des services liés à l'informatique, aux technologies de l'information et à la transformation numérique.

RTO : RTO signifie "Recovery Time Objective", soit l'objectif de temps de récupération en français. Il définit la durée maximale acceptable pour restaurer un service après une panne ou un incident.

RPO : RPO signifie "Recovery Point Objective", soit l'objectif de point de récupération en français. Il représente la quantité maximale de données qui peut être perdue en cas de sinistre, mesurée en fonction du temps.

Modèle de sauvegarde 3-2-1 : Le modèle de sauvegarde 3-2-1 est une méthode de sauvegarde recommandée qui consiste à avoir trois copies de vos données (2 copies sur site, 1 copie hors site) pour garantir leur sécurité.

Certification ISO : La certification ISO fait référence à la conformité d'une organisation à des normes établies par l'Organisation internationale de normalisation (ISO) pour garantir la qualité, la sécurité ou d'autres aspects liés aux processus et produits.

Norme ISO : Une norme ISO est un document qui spécifie des exigences, des recommandations ou des lignes directrices pour garantir la qualité, la sécurité ou d'autres aspects liés à un produit, un service ou un processus.

Sauvegarde différentielle : Une sauvegarde différentielle consiste à sauvegarder uniquement les données qui ont changé depuis la dernière sauvegarde complète. Cela permet de réduire l'espace de stockage nécessaire pour les sauvegardes.

PCI : PCI signifie "Payment Card Industry", soit l'industrie des cartes de paiement en français. Les normes de sécurité PCI définissent les exigences de sécurité pour les entreprises qui traitent des informations de paiement par carte de crédit.

PRI : PRI peut signifier "Primary Rate Interface" en anglais, ce qui se traduit en français par "Interface d'accès primaire". Il s'agit d'une interface numérique pour la transmission de données et de voix.

PCA : PCA peut signifier "Plan de Continuité d'Activité", qui est un ensemble de procédures et de ressources permettant à une organisation de maintenir ses opérations en cas de perturbations majeures.

PRA : PRA signifie "Plan de Reprise d'Activité", ce qui est similaire au PCA. Il s'agit des mesures et des procédures mises en place pour reprendre les activités après une interruption.

Contrat de maintenance : Un contrat de maintenance est un accord entre un fournisseur de services et un client qui spécifie les services de maintenance qui seront fournis, y compris la durée, les coûts et les obligations des parties.

Business Impact Analysis : L'analyse de l'impact sur l'activité (BIA) est un processus visant à évaluer les effets potentiels des perturbations sur les activités d'une organisation et à identifier les priorités de récupération.

Stockage PC : Le stockage PC fait référence à l'espace de stockage disponible sur un ordinateur sur ses différents disques, utilisé pour stocker des fichiers, des applications et des données.

Archivage : L'archivage consiste à stocker des données, des documents ou des informations de manière organisée et à long terme pour des raisons de conformité, de conservation ou d'historique.

T.I. : T.I. signifie "Technologies de l'Information", ce qui englobe l'informatique, les réseaux, la sécurité informatique et d'autres domaines liés à la technologie.