



DOSSIER PROFESSIONNEL (DP)

Nom de naissance ➤ RODRIGUES DOS SANTOS
Nom d'usage ➤ RODRIGUES DOS SANTOS
Prénom ➤ Mylène
Adresse ➤ 211 chemin de la pépinière, 13600 La Ciotat

Titre professionnel visé

[Cliquez ici pour entrer l'intitulé du titre professionnel visé.](#)

MODALITÉ D'ACCÈS :

- ☐ Parcours de formation
- ☐ Validation des Acquis de l'Expérience (VAE)

Présentation du dossier

Le dossier professionnel (DP) constitue un élément du système de validation du titre professionnel. **Ce titre est délivré par le Ministère chargé de l'emploi.**

Le DP appartient au candidat. Il le conserve, l'actualise durant son parcours et le présente **obligatoirement à chaque session d'examen.**

Pour rédiger le DP, le candidat peut être aidé par un formateur ou par un accompagnateur VAE.
Il est consulté par le jury au moment de la session d'examen.

Pour prendre sa décision, le jury dispose :

1. des résultats de la mise en situation professionnelle complétés, éventuellement, du questionnaire professionnel ou de l'entretien professionnel ou de l'entretien technique ou du questionnement à partir de productions.
2. du **Dossier Professionnel** (DP) dans lequel le candidat a consigné les preuves de sa pratique professionnelle
3. des résultats des évaluations passées en cours de formation lorsque le candidat évalué est issu d'un parcours de formation
4. de l'entretien final (dans le cadre de la session titre).

[Arrêté du 22 décembre 2015, relatif aux conditions de délivrance des titres professionnels du ministère chargé de l'Emploi]

Ce dossier comporte :

- pour chaque activité-type du titre visé, un à trois exemples de pratique professionnelle ;
- un tableau à renseigner si le candidat souhaite porter à la connaissance du jury la détention d'un titre, d'un diplôme, d'un certificat de qualification professionnelle (CQP) ou des attestations de formation ;
- une déclaration sur l'honneur à compléter et à signer ;
- des documents illustrant la pratique professionnelle du candidat (facultatif)
- des annexes, si nécessaire.

Pour compléter ce dossier, le candidat dispose d'un site web en accès libre sur le site.

DOSSIER PROFESSIONNEL ^(DP)



<http://travail-emploi.gouv.fr/titres-professionnels>

Sommaire

Exemples de pratique professionnelle

Analyse de la conformité et des normes de sécurité

p.

- RGPD p. p. 7
- normes ISO27xxx p. p. 20

Mise en place et sécurisation d'un réseau simulé

p.

- Cisco Packet Tracer p. p. 23

Administrer et sécuriser les infrastructures systèmes et virtualisés

p.

- Conteneurisation et déploiement de services avec Docker p. p. 34
- Docker Swarm p. p. 39

Déploiement d'une solution de supervision centralisée

p.

- SIEM ELK p. p. 50

Titres, diplômes, CQP, attestations de formation *(facultatif)*

p. 56

Déclaration sur l'honneur

p. 57

Documents illustrant la pratique professionnelle *(facultatif)*

p. 58

Annexes *(Si le RC le prévoit)*

p. 59

DOSSIER PROFESSIONNEL ^(DP)

EXEMPLES DE PRATIQUE PROFESSIONNELLE

Activité-type 1 Analyse de la conformité et des normes de sécurité

Exemple n°1 - RGPD

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Lors de mon apprentissage cette année, j'ai dû faire des recherches sur les bonnes pratiques à adopter dans l'administration des infrastructures. Ceci inclut des recherches et des mises en place dans des entreprises fictives des normes du RGPD ainsi que de la gestion de risque.

Nous avons d'abord fait un registre de traitement des données personnelles pour trois clients de notre entreprise fictive. Nous avons défini des sécurités à mettre en place, cela nous a permis d'identifier les types de données collectées, les finalités du traitement, les durées de conservation comme: le chiffrement des données (AES-256), l'authentification à deux facteurs (2FA), le contrôle d'accès basé sur les rôles (RBAC) et la durée de conservation des données (ex: 10 ans pour des données médicales).

DOSSIER PROFESSIONNEL (DP)

Nom du traitement	Description	Responsable	Finalité du traitement	Base légale	Données traitées	Catégories de personnes concernées	Durée de conservation	Mesures de sécurité
Gestion des clients pour <u>Retail Co</u>	Collecte, organisation et gestion des données clients pour la chaîne	X-corp	Personnalisation des offres et promotions, amélioration de	Consentement des clients	Noms, adresses, emails, numéros de téléphone, historique	Clients de <u>Retail Co</u>	5 ans après le dernier contact	- Pseudonymisation - Chiffrement AES-256

DOSSIER PROFESSIONNEL (DP)

Analyse de l'usage pour EduLearn	Collecte et analyse des données d'utilisation pour améliorer les parcours d'apprentissage	X-corp	Amélioration des parcours d'apprentissage, recommandations de cours, suivi des progrès	Consentement des utilisateurs	Identifiants utilisateurs, adresse email, parcours d'apprentissage, résultats d'examen	Utilisateurs de la plateforme EduLearn	2 ans après la fin de l'utilisation de la plateforme	- Pseudonymisation - Chiffrement AES-256 - Contrôle d'accès basé sur les rôles (RBAC)
---	---	--------	--	-------------------------------	--	--	--	---

Analyse de l'usage pour EduLearn	Collecte et analyse des données d'utilisation pour améliorer les parcours d'apprentissage	X-corp	Amélioration des parcours d'apprentissage, recommandations de cours, suivi des progrès	Consentement des utilisateurs	Identifiants utilisateurs, adresse email, parcours d'apprentissage, résultats d'examen	Utilisateurs de la plateforme EduLearn	2 ans après la fin de l'utilisation de la plateforme	- Pseudonymisation - Chiffrement AES-256 - Contrôle d'accès basé sur les rôles (RBAC)
---	---	--------	--	-------------------------------	--	--	--	---

Nous avons ensuite rédigé une DPIA (digital privacy impact assessment) pour notre entreprise fictive afin d'anticiper et d'analyser les risques de traitements des données avant leur mise en œuvre. Nous avons donc relevé des potentiels problèmes dans notre entreprise fictive et trouvé des solutions adaptées afin



de réduire le risque de fuite de données et de proposer des mesures directrice: gestion des consentements, sécurité des données, formations et sensibilisations, documentation et traçabilité, réponse aux incidents.

1. Gestion des consentements :

- Problème : Difficultés à gérer les consentements des utilisateurs pour le marketing.
- Amélioration : Mettre en place un système clair pour donner, modifier ou retirer le consentement.

2. Sécurité des données :

- Problème : Risques de fuites de données lors de transferts.

-
- Amélioration : Renforcer le chiffrement des données et effectuer des audits réguliers de sécurité.

3. Formation et sensibilisation :

- Problème : Risques humains liés à la manipulation des données.
- Amélioration : Mettre en place un programme de formation régulier sur la protection des données pour tous les employés.

4. Documentation et traçabilité :

- Problème : Difficulté à retracer les décisions sur le traitement des données.
- Amélioration : Documenter systématiquement les demandes d'accès aux données et les modifications apportées.

5. Réponse aux incidents :

- Problème : Failles dans la gestion des incidents après une fuite de données.
- Amélioration : Établir un plan de réponse robuste avec des étapes claires à suivre en cas de violation.

Comment réduire votre délai de réponse aux violations de données
Nous savons à présent que plus la réponse est rapide, plus l'impact est limité. Voici quelques façons de réduire le délai de réponse aux violations de données et de permettre à votre entreprise de gagner du temps et de faire des économies.

6. Transferts internationaux de données :

- Problème : Risques associés aux transferts vers des pays tiers.
- Amélioration : Évaluer les garanties en place pour chaque transfert et s'assurer que les partenaires hors UE respectent le RGPD.

Conclusion : Ces améliorations renforcent la conformité de X-corp au RGPD, protégeront les données des clients et réduisent les risques de violations. Une approche proactive installe la confiance des clients et préserve la réputation de l'entreprise.

Une fois notre DPIA rédigé, nous avons simulé une gestion de violation de données de notre entreprise fictive en plusieurs étapes:

La première étape consiste à établir une politique de sécurité des données, donc la mise en place de protocole sur la gestion des données et leur accès en plus d'une formation régulière des employés sur la sécurité des données.

La seconde étape consiste à mettre en place des outils de surveillance accompagné d'un système d'alerte pour repérer rapidement des activités suspectes.



La troisième étape consiste à isoler le système affecté pour éviter toute propagation et que le système entier soit affecté.

La quatrième étape consiste à informer les autorités compétentes (la CNIL) dans les délais requis dans le but de transparence de l'entreprise.

La cinquième étape consiste à analyser la cause de la violation, comprendre comment cela c'est produit et appliquer des mesures correctives pour y remédier.

La sixième étape consiste à mettre à jour ses protocoles de sécurité et effectuer des tests réguliers de pentests et d'audits de sécurité.

La septième étape consiste à documenter l'événement de manière détaillée en tenant un registre des mesures prises et de faire une nouvelle évaluation post-événement.

Enfin, l'entreprise doit restaurer la confiance de ses clients en menant des actions et communiquant sur les initiatives de sécurité ajoutées.

Nous avons après travaillé sur la mise en conformité du RGPD de notre entreprise en prenant en compte de l'analyse des données (type de données collectées, des bases légales, de la conservation des données, des mesures de sécurité), des risques identifiés et des actions correctives (documentation consentement, vulnérabilité de sécurité, gestion d'accès), de la cartographie des processus opérationnels (collecte de données, stockage et accès aux données, utilisation des données, suppressions des données), et répertorier les traitements de données et suivre l'évolution du registre. Nous avons donc fait une liste des actions prioritaires pour assurer la conformité RGPD et une liste des actions à entreprendre.

Pour évaluer le niveau de conformité de X-corp au RGPD, nous devons examiner l'ensemble des données à caractère personnel collectées et les pratiques associées.

Analyse des Données :

- **Types de Données Collectées :**
 - Données clients (RetailCo) : noms, adresses, emails, numéros de téléphone, historique d'achats, préférences de produits.
 - Données de santé (HealthMed) : noms, adresses, emails, numéros de téléphone, historique médical, prescriptions.
 - Données utilisateurs (EduLearn) : identifiants utilisateurs, adresses email, parcours d'apprentissage, résultats d'examen.
- **Bases Légales :**
 - Vérifier que toutes les données sont collectées sur la base du consentement explicite et documenté des individus.
- **Conservation des Données :**
 - Évaluer si les périodes de conservation des données respectent les exigences du RGPD.
- **Mesures de Sécurité :**
 - Vérifier l'efficacité des mesures de sécurité en place (pseudonymisation, chiffrement, authentification à deux facteurs, contrôle d'accès basé sur les rôles).

2. Identifier les Risques et Prioriser les Actions Correctives

Après avoir mesuré le niveau de conformité, il est essentiel d'identifier les risques potentiels.

Risques Identifiés :

- **Manque de Documentation sur le Consentement :**
 - Difficultés à prouver que le consentement a été obtenu pour l'utilisation des données, en particulier pour les campagnes via AutoMail.
- **Vulnérabilités de Sécurité :**
 - Lacunes révélées lors de la fuite de données précédente (2 000 enregistrements exposés), suggérant des failles dans les protocoles de sécurité.
- **Gestion des Demandes d'Accès :**
 - Volume élevé de demandes de droit d'accès (50 à 100 par mois) pouvant entraîner des retards ou des erreurs dans la réponse.

Actions Correctives Priorisées :

1. **Améliorer la Gestion du Consentement** : Mettre en place un système robuste pour suivre et documenter les consentements.
2. **Renforcer les Mesures de Sécurité** : Réévaluer et améliorer les protocoles de sécurité suite à la fuite de données.
3. **Optimiser la Réponse aux Demandes d'Accès** : Mettre en place un processus standardisé pour gérer efficacement ces demandes.

3. Cartographier les Processus Opérationnels

La cartographie des processus opérationnels aidera à identifier les ajustements nécessaires pour garantir la conformité.

Processus à Cartographier :

- **Collecte de Données** :
 - Comment et où les données sont collectées (formulaires en ligne, interactions client).
- **Stockage et Accès aux Données** :
 - Identifier où les données sont stockées et qui y a accès.
- **Utilisation des Données** :
 - Déterminer comment les données sont utilisées dans les produits (DataManage, MarketInsight, AutoMail).
- **Suppression des Données** :
 - Évaluer les processus de suppression des données après la période de conservation.

Ajustements Nécessaires :

- Créer un diagramme de flux pour chaque processus, permettant d'identifier les points faibles et les améliorations à apporter.

4. Répertoire des Traitements de Données et Suivre l'Évolution du Registre

Il est crucial d'établir un registre des traitements de données et d'assurer son suivi.

Pour assurer la conformité RGPD, voici les actions prioritaires :

1. Suivi et Documentation des Consentements :

- Créer un **registre de traitement** pour documenter chaque traitement de données, précisant les données utilisées, la finalité, la base légale, la durée de conservation et les mesures de sécurité.

- **Mise à jour régulière** du registre (minimum une fois par an) pour rester conforme.
- **Formation continue des employés** pour garantir leur compréhension des enjeux et des procédures RGPD.

2. Automatisation et Gestion des Demandes d'Accès :

- Mettre en place un **portail automatisé** pour que les utilisateurs puissent soumettre, suivre, et télécharger leurs informations, ce qui réduit la charge de travail.
- Utiliser des **outils de gestion RGPD** comme OneTrust ou BigID pour centraliser et automatiser les réponses.
- **Former les équipes** pour gérer efficacement les demandes et standardiser les réponses, en respectant les délais légaux de 30 jours.

3. Politiques de Conservation des Données :

- Mettre en œuvre une **politique de suppression régulière** des données non nécessaires afin de réduire le volume de données, facilitant la recherche et le traitement des demandes d'accès.

Ces mesures permettent de garantir une meilleure gestion des droits d'accès des utilisateurs et du suivi des consentements, tout en respectant les obligations RGPD de manière efficace.

Le suivi et la documentation des consentements, en particulier pour les campagnes marketing automatisées comme AutoMail, sont essentiels pour éviter les litiges potentiels et respecter les préférences des utilisateurs. Voici des solutions pour une meilleure gestion des consentements :

- **Création du Registre de Traitement :**
 - Documenter tous les traitements de données, y compris la nature des données, la finalité, la base légale, la durée de conservation, et les mesures de sécurité mises en place.
- **Mise à Jour Régulière :**
 - Établir un calendrier de révision (au moins une fois par an) pour mettre à jour le registre et s'assurer qu'il reste conforme.
- **Formation Continue :**
 - Former régulièrement les employés sur l'importance de la conformité RGPD et les procédures associées.

Pour une entreprise recevant entre 50 et 100 demandes de droit d'accès par mois, il est important de mettre en place une stratégie de réponse efficace pour gagner du temps,

réduire le risque d'erreur, et garantir le respect des délais RGPD (en général 30 jours). Voici des solutions possibles :

- **Automatisation des Processus :** Mettre en place un système automatisé pour gérer les demandes de droit d'accès. Un portail client où les utilisateurs peuvent soumettre leurs demandes, voir l'état de traitement et télécharger leurs données de manière sécurisée, pourrait diminuer la charge de travail. Des outils comme [OneTrust](#) ou [BigID](#) peuvent aider à automatiser ce processus.
- **Outils de Gestion des Demandes de RGPD :** Utiliser une solution de gestion des demandes d'accès spécifiquement dédiée à la RGPD, capable de centraliser et de suivre l'ensemble des demandes d'accès. Ces outils facilitent la réponse aux demandes en automatisant la collecte et la présentation des données demandées.
- **Formations des Équipes :** Former les employés à traiter ces demandes rapidement et conformément aux exigences légales peut aider à améliorer la rapidité et la cohérence des réponses. Il pourrait être judicieux de mettre en place des processus standards pour chaque type de demande.
- **Politiques de Conservation et de Suppression des Données :** En adoptant une politique de conservation stricte et en supprimant régulièrement les données non nécessaires, le volume de données à traiter lors des demandes d'accès peut être réduit, ce qui facilite la recherche et la préparation des réponses.

Le suivi et la documentation des consentements, en particulier pour les campagnes marketing automatisées comme AutoMail, sont essentiels pour éviter les litiges potentiels et respecter les préférences des utilisateurs. Voici des solutions pour une meilleure gestion des consentements :

- **Utilisation d'une Plateforme de Gestion des Consentements (CMP)** : Adopter un outil de gestion des consentements permet de centraliser les consentements recueillis via différents canaux (site web, application, emails) et de les mettre à jour automatiquement. Des plateformes comme [TrustArc](#), [ConsentManager](#) ou [Cookiebot](#) peuvent fournir cette fonctionnalité, tout en permettant un suivi en temps réel.
- **Mise en Place d'un Tableau de Bord RGPD** : Créer un tableau de bord qui enregistre et suit en temps réel les consentements des utilisateurs permet de visualiser et d'organiser les données de consentement. Cela permet de documenter les actions en cas d'audit et de répondre rapidement aux demandes de mise à jour des préférences.
- **Double Opt-In et Suivi des Consentements** : Pour s'assurer de la validité des consentements, mettre en place un processus de double opt-in (l'utilisateur reçoit un email de confirmation pour valider son consentement) et un historique de consentement pour chaque utilisateur. En cas de retrait de consentement, un

système automatisé doit pouvoir désinscrire immédiatement l'utilisateur des campagnes de marketing.

- **Paramètres de Préférences Personnalisés** : Ajouter une section de gestion des préférences pour que les utilisateurs puissent voir, modifier, ou retirer leur consentement directement depuis un portail dédié. Cela allège le volume de demandes de gestion de consentement et permet aux utilisateurs de gérer eux-mêmes leurs préférences.

DOSSIER PROFESSIONNEL (DP)

2. Précisez les moyens utilisés :

Pour ce projet, j'ai utilisé un ordinateur avec une connexion Internet.

Nous nous sommes appuyés sur le site de la CNIL et de l'ANSSI (cyber.gouv.fr) en plus de recherches complémentaires sur Internet

3. Avec qui avez-vous travaillé ?

Sur ce projet, j'ai travaillé en groupe avec deux camarades de ma classe

4. Contexte

Nom de l'entreprise, organisme ou association ▶ La Plateforme	
Chantier, atelier, service	▶ Dans le cadre de la formation administrateur système et réseau
Période d'exercice	▶ Du 24/09/24 au 29/09/24

5. Informations complémentaires (facultatif)

DOSSIER PROFESSIONNEL (DP)

Cliquez ici pour taper du texte.

Activité-type 1 Analyse de la conformité et des normes de sécurité

Exemple n°2 - normes ISO 27xxx

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Dans le cadre de mon apprentissage, j'ai étudié et appliqué plusieurs normes de la famille ISO 27xxx, notamment les normes ISO 27001, 27002, 27005, 27017, 27018 et 27701. Nous avons d'abord fait un travail de recherches et documentations sur les normes 27001, 27002, 27005, 27017-18 et 27701, respectivement système de management de la sécurité de l'information (SMSI), code de bonnes pratiques, gestion des risques, sécurité des services cloud, gestion de la protection de la vie privée conforme au RGPD.

ISO 27001: Système de Management de la Sécurité de l'Information (SMSI)

Elle définit un cadre méthodologique pour établir, mettre en œuvre, maintenir et améliorer un système de sécurité de l'information. Elle regroupe ces enjeux clés:

- les enjeux internes et externes de l'entreprise (définition du périmètre du SMSI),
- d'identifier et évaluer les risques liés à la sécurité et élaborer la politique de sécurité en respectant ses 7 points: identifier les actifs, identifier les personnes responsables, identifier les vulnérabilités, identifier les menaces, identifier les impacts, évaluer la vraisemblance et estimer les niveaux de risque.
- Traiter le risque et identifier le risque par un plan de gestion: il existe 4 traitements possibles pour chacun des risques identifiés: l'acceptation, l'évitement, le transfert et la réduction
- Sélection des mesures de sécurité à mettre en place
- Amélioration continu PDCA (Plan, Do, Check, Act)

ISO 27002: Code de bonnes pratiques

Cette norme complète la norme ISO 27001 en fournissant des recommandations concrètes pour la mise en œuvre des contrôles de sécurité. Elle regroupe:

- la gestion des accès (droits des utilisateurs, gestion des mots de passe et la restriction à certaines données ou accès)
- la gestion des actifs (les inventaires, la classification)
- la sécurité des ressources humaines (sensibilisation du personnel et engagements)
- la sécurité physique sur place et dans l'environnement de travail.

ISO 27005: Gestion des risques liés à la sécurité de l'information

La norme ISO 27005 repose sur une structure de la gestion des risques en plusieurs étapes:



- Identification des risques
- Evaluation des risques (impact x la probabilité)
- Le traitement des risques (acceptations, transfert ou réduction de risques)
- Le suivi de la gestion de risque et la réévaluation régulière des risques encourus

ISO 270017-18: Sécurité du Cloud

Ces normes sont spécialisées pour comprendre la sécurité spécifique aux environnements cloud.

La norme 27017 est basé sur la norme ISO 27002 et recommande des contrôles de sécurité pour les utilisateurs et fournisseurs de services Cloud comme:

- rôles et responsabilités partagés dans un environnement de cloud computing
- retrait et restitution des biens des clients des services cloud à la fin du contrat
- protection et séparation de l'environnement virtuel d'un client des environnements d'autres clients
- durcissement des exigences des machines virtuelles pour répondre aux besoins des entreprises
- procédures pour les opérations administratives d'un environnement de cloud computing
- possibilité donnée aux clients de surveiller les activités pertinentes dans un environnement de cloud computing
- alignement de la gestion de la sécurité pour les réseaux virtuels et physiques

La norme ISO 27018 quand à elle cible la protection des données personnelles dans le Cloud, en lien direct avec les obligations du RGPD.

ISO 27701: PIMS (système de gestion des informations de confidentialité) : Gestion de la vie privée :

Cette norme étend la norme 27001/27002 pour intégrer les exigences relatives à la protection de la confidentialité, l'intégrité et la disponibilité des données sensibles et la protection des données personnelles. Elle décrit la gouvernance et les mesures de sécurité à mettre en place pour les traitements de données personnelles. Elle précise les particularités des traitements de données personnelles et le rôle de l'organisme comme responsable de traitement, sous-traitant, sous-traitant de sous-traitant. Elle cible aussi la conformité aux exigences du RGPD.

Ces normes permettent de gérer le contrôle d'accès, la gestion des actifs, de réduire les risques liés à la gestion humaine, de chiffrer les données, d'assurer la sécurité des communications et des opérations, la gestion d'incidents de sécurité, recenser et comprendre les menaces, déterminer l'impact et la probabilité de risque (gestion de risques), traiter les risques, fournir une gestion continu des risques et une surveillance accrue.

Nous avons donc ensuite implémenté ces normes dans des études de cas d'entreprises existantes et recommandé différentes mesures et outils afin de respecter et faciliter l'implémentation continue de ces normes dans les entreprises.

DOSSIER PROFESSIONNEL (DP)



2. Précisez les moyens utilisés :

Pour ce projet, j'ai utilisé un ordinateur avec une connexion Internet.

Nous nous sommes appuyés sur le site de la CNIL et de l'ANSSI (cyber.gouv.fr) en plus de recherches complémentaires sur Internet.

3. Avec qui avez-vous travaillé ?

Sur ce projet, j'ai travaillé en groupe avec deux camarades de ma classe

4. Contexte

Nom de l'entreprise, organisme ou association ▶ La Plateforme

Chantier, atelier, service ▶ Dans le cadre de la formation administrateur système et réseau

Période d'exercice Du 09/01/25 au 14/01/25

Activité-type 2 Mise en place et sécurisation d'un réseau simulé

Exemple n°1 - Cisco Packet Tracer

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

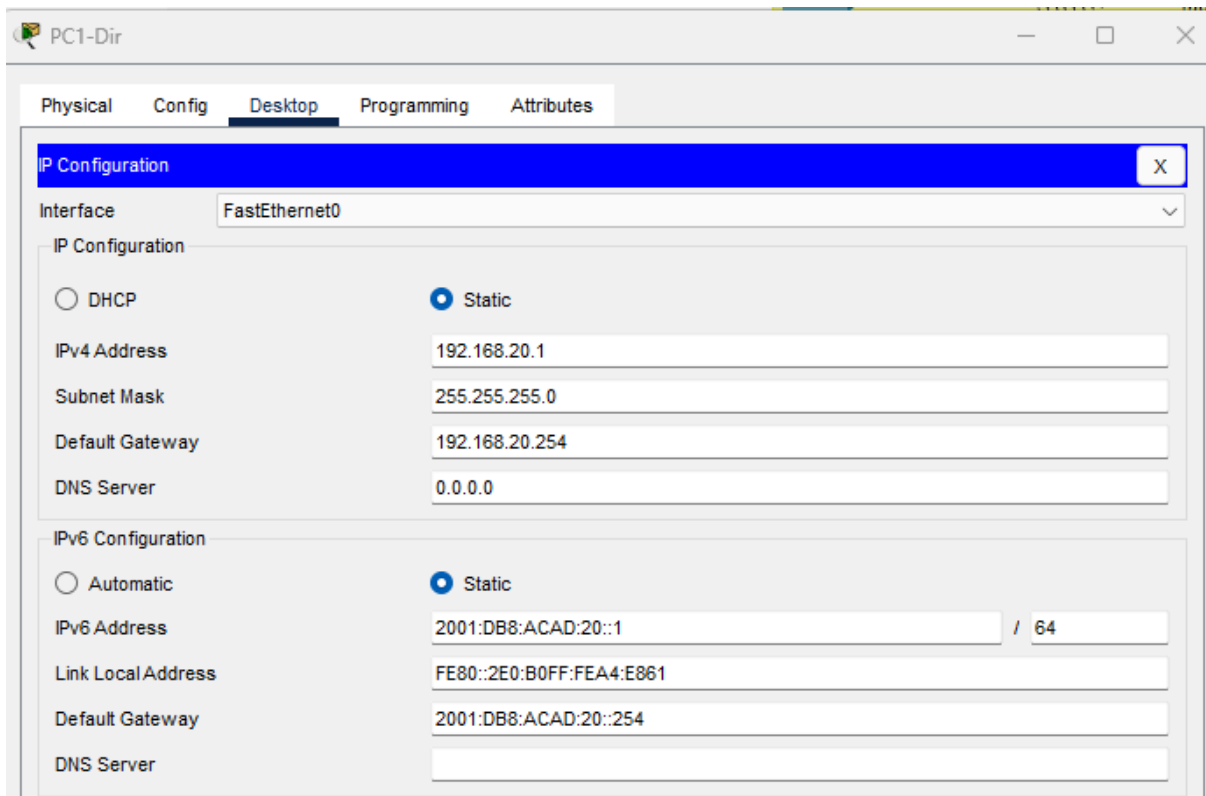
Durant mon apprentissage, j'ai appris à utiliser le logiciel Cisco Packet Tracer, un simulateur de réseau développé par Cisco Systems. Ce logiciel est principalement destiné à la modélisation et la simulation d'environnements réseau, sans nécessiter de matériel physique.

Cisco Packet Tracer permet de concevoir, configurer et tester des topologies réseau virtuelles, comprenant des équipements tels que des commutateurs (switches), des routeurs, des PC, des serveurs, des pare-feux On peut également simuler des protocoles (DHCP, NAT, OSPF, VLAN, STP ...) et visualiser le cheminement des paquets.

J'ai tout d'abord mis en place plusieurs sous-réseaux reliés entre eux par des commutateurs de couche 2 et 3. Chaque sous-réseau comprend 2 PCs, 2 Phone VoIP, une Imprimante. J'ai ensuite mis en place une salle serveur comprenant un serveur AD, un serveur web et un serveur TFTP, une salle wifi avec un réseau sans fil wifi et une salle VPN.

Ensuite j'ai configuré les différentes adresses IPv4 et IPv6 de tous les composants:

DOSSIER PROFESSIONNEL (DP)



The screenshot shows the 'PC1-Dir' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is highlighted in blue. Below it, the 'Interface' dropdown is set to 'FastEthernet0'. The 'IP Configuration' section has two radio buttons: 'DHCP' (unselected) and 'Static' (selected). The 'Static' configuration includes the following fields:

Field	Value
IPv4 Address	192.168.20.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.20.254
DNS Server	0.0.0.0

The 'IPv6 Configuration' section also has two radio buttons: 'Automatic' (unselected) and 'Static' (selected). The 'Static' configuration includes the following fields:

Field	Value
IPv6 Address	2001:DB8:ACAD:20::1 / 64
Link Local Address	FE80::2E0:B0FF:FEA4:E861
Default Gateway	2001:DB8:ACAD:20::254
DNS Server	

Puis j'ai commencé la configuration des commutateurs de couche 2:

DOSSIER PROFESSIONNEL (DP)

Med/Assu

Physical Config **CLI** Attributes

IOS Command Line Interface

```
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

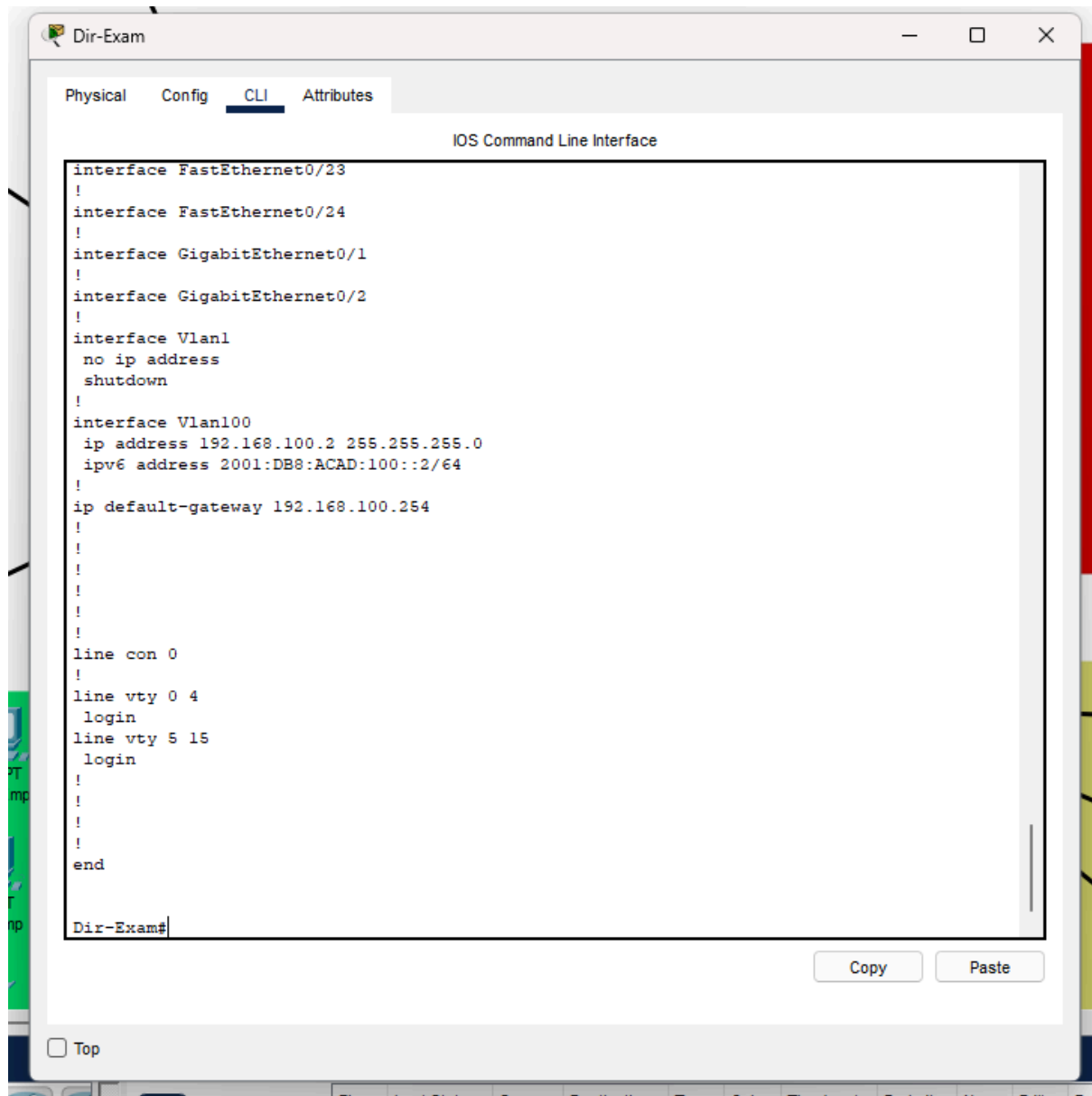
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Med-Assu
Med-Assu(config)#int vlan 100
Med-Assu(config-if)#ip address 192.168.100.4 255.255.255.0
Med-Assu(config-if)#exit
Med-Assu(config)#sdm prefer dual-ipv4
Med-Assu(config)#sdm prefer dual-ipv4-and-ipv6
% Incomplete command.
Med-Assu(config)#exit
Med-Assu#
%SYS-5-CONFIG_I: Configured from console by console

Med-Assu#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Med-Assu(config)#int vlan 100
Med-Assu(config-if)#exit
Med-Assu(config)#sdm prefer dual
Med-Assu(config)#sdm prefer dual-ipv4-and-ipv6 default
Changes to the running SDM preferences have been stored, but cannot take effect until
the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
Med-Assu(config)#exit
Med-Assu#
%SYS-5-CONFIG_I: Configured from console by console

Med-Assu#reload
System configuration has been modified. Save? [yes/no]:
% Please answer 'yes' or 'no'.
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
```

Copy Paste

☐ Top



J'ai créer et configurer des interfaces virtuelles (SVI):

interface vlan 20

description Passerelle SVI Direction

ip address 192.168.20.254 255.255.255.0

ipv6 address 2001:db8:acad:20::254/64

no shutdown



exit

Puis, j'ai utilisé ces commandes pour la configuration de mon routeur en extrémité:

en

conf t

int g0/0

ip address 192.168.110.254 255.255.255.0

ipv6 address 2001:db8:acad:110::254/64

no shut

exit

int s0/1/1

ip address 10.0.0.2 255.255.255.0

ipv6 address 2001:db8:acad:1001::2/64

no shutdown

adresse bouclage routeur

interface loopback 0

ip address

exit

ip route 0.0.0.0 0.0.0.0 10.0.0.1

ipv6 unicast-routing

ipv6 route ::/0 2001:db8:acad:1001::1

Puis ces commandes pour mon routeur central:

en

conf t



```
hostname RouteurVPN
enable secret 1234-Metropole:1234
ip ssh version 2
ip domain-name metropolecg.com
username admin secret 1234-Metropole:1234
crypto key generate rsa
line console 0
password 1234-Metropole:1234
line vty 0 15
transport input ssh
login local
exit
service password-encryption
banner motd #Acces aux Personnes Autorisees seulement!#
exit
copy run start
```

```
ip route 192.168.110.0 255.255.255.0 10.0.0.2
ip route 0.0.0.0 0.0.0.0 192.168.10.2
ipv6 unicast-routing
ipv6 route 2001:db8:acad:110::0/64 2001:db8:acad:1001::2
ipv6 route ::/0 2001:db8:acad:10::2
```

Après j'ai configuré mon commutateur de couche 3:

```
en
conf t
hostname SwitchL3
interface g1/0/1
no switchport
ip address 192.168.10.2 255.255.255.0
```



```
ipv6 address 2001:db8:acad:10::2/64
```

```
exit
```

```
ip route 0.0.0.0 0.0.0.0 192.168.10.1
```

```
ipv6 unicast-routing
```

J'ai ensuite configuré les différents VLAN dont j'avais besoin via cette commande: (j'ai répété l'opération pour tous les VLANs que je souhaitais mettre en place.

```
configure terminal
```

```
vlan 20
```

```
name Direction
```

```
end
```

attribution vlan:

```
configure terminal
```

```
int f0/1
```

```
switchport mode access
```

```
switchport access vlan 20
```

```
end
```

Ensuite, j'ai mis en place un trunk de vlan pour la téléphonie:

```
int g0/1
```

```
switchport mode trunk
```

```
switchport trunk native vlan 100
```

```
switchport trunk allowed vlan 20,21,40,50,100
```

```
end
```

Puis j'ai routé mes VLAN entre eux afin qu'ils puissent communiquer ou non via mon commutateur de couche 3.

```
SwitchL3(config)# vlan 20
```

name Direction

exit

interface g1/0/2

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk native vlan 100

switchport trunk allowed vlan

20,21,40,50,100

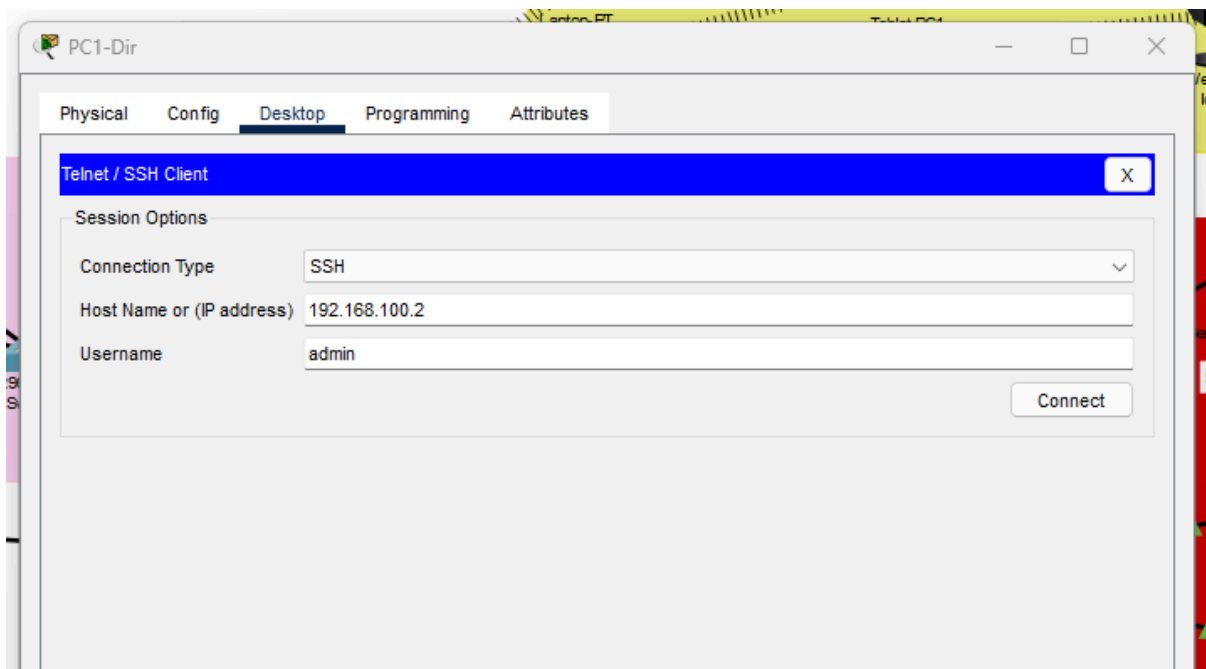
int g1/0/6

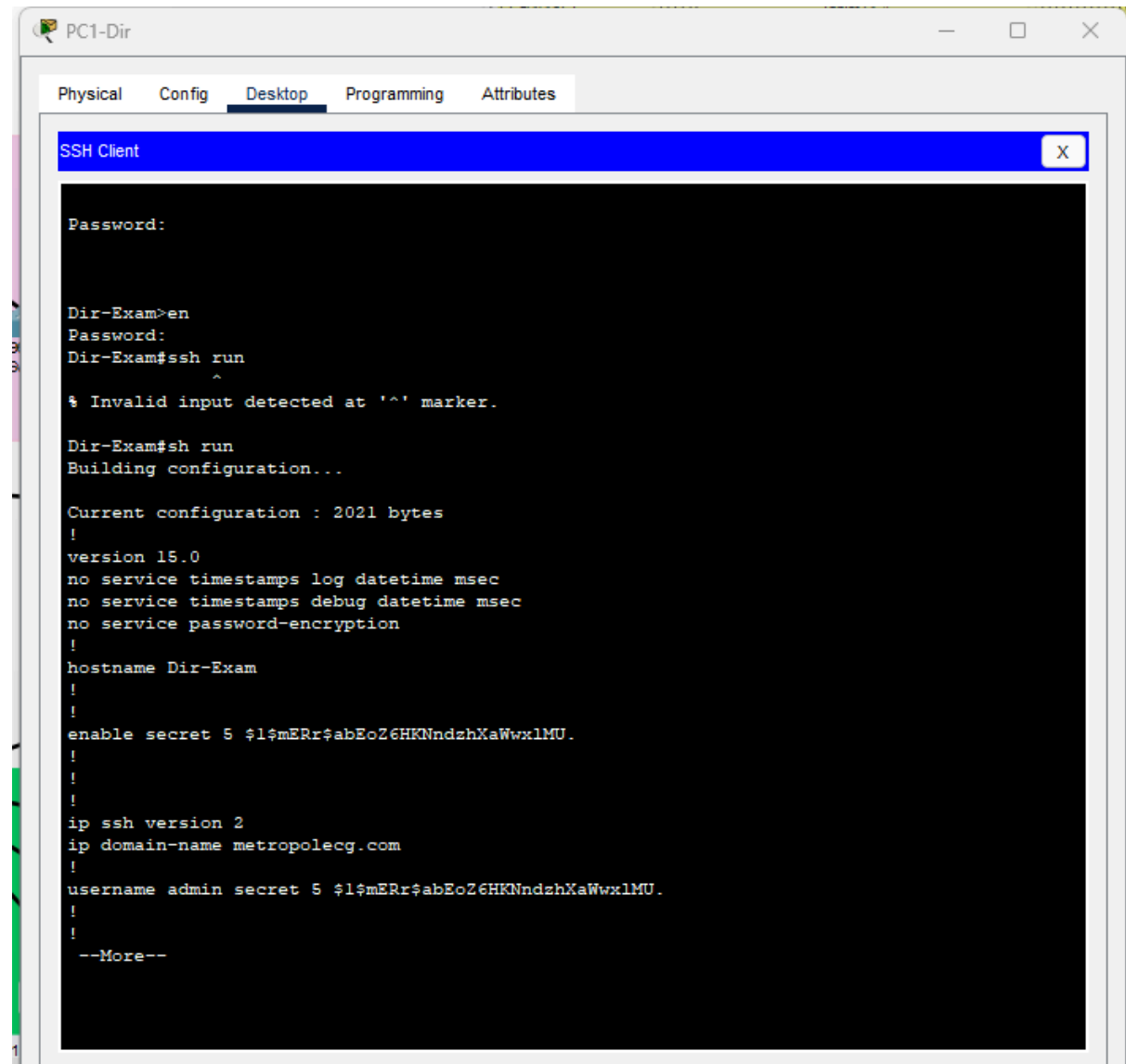
switchport mode access

switchport access vlan 30

exit

J'ai sécurisé l'accès à mes VLANs via SSH





J'ai utilisé ses commandes pour sauvegarder des documents sur un serveur TFTP

DOSSIER PROFESSIONNEL (DP)

```
RouteurVPN#copy running-config tftp
Address or name of remote host []? 192.168.30.3
Destination filename [RouteurVPN-config]?

Writing running-config.....!!
[OK - 1412 bytes]

1412 bytes copied in 7.036 secs (200 bytes/sec)
RouteurVPN#
```

Copy

Paste

Serveur-Fichiers

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP**
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

TFTP

Service ☒ On ☐ Off

File

RouteurVPN-config

asa842-k8.bin

asa923-k8.bin

c1841-advipservicesk9-mz.124-15.T1.bin

c1841-ipbase-mz.123-14.T7.bin

c1841-ipbasek9-mz.124-12.bin

c1900-universalk9-mz.SPA.155-3.M4a.bin

c2600-advipservicesk9-mz.124-15.T1.bin

c2600-i-mz.122-28.bin

c2600-ipbasek9-mz.124-8.bin

c2800nm-advipservicesk9-mz.124-15.T1.bin

c2800nm-advipservicesk9-mz.151-4.M4a.bin

c2800nm-ipbase-mz.123-14.T7.bin

c2800nm-ipbasek9-mz.124-8.bin

c2900-universalk9-mz.SPA.155-3.M4a.bin

c2950-i6q4l2-mz.121-22.EA4.bin

c2950-i6q4l2-mz.121-22.EA8.bin

c2960-lanbase-mz.122-25.FX.bin

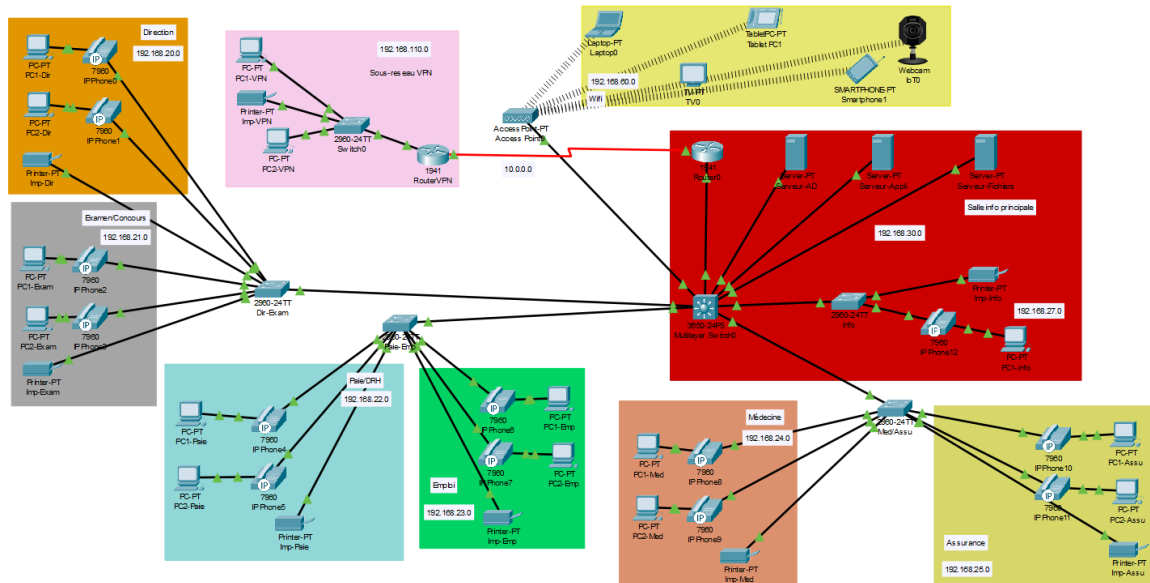
c2960-lanbase-mz.122-25.SEE1.bin

c2960-lanbasek9-mz.150-2.SE4.bin

Remove File

☐ Top

Architecture finale de mon réseau:



2. Précisez les moyens utilisés :

Pour ce projet, j'ai utilisé un ordinateur avec une connexion Internet.

J'ai utilisé le logiciel Cisco Packet Tracer

DOSSIER PROFESSIONNEL ^(DP)



3. Avec qui avez-vous travaillé ?

Sur ce projet, j'ai travaillé seul.

4. Contexte

Nom de l'entreprise, organisme ou association ➤ La Plateforme

Chantier, atelier, service ➤ Dans le cadre de la formation administrateur système et réseau

Période d'exercice ➤ Du 13/03/24 au 18/03/24

5. Informations complémentaires (facultatif)

Activité-type 3

Administrer et sécuriser les infrastructures systèmes et virtualisés

Exemple n°1 ➤ Conteneurisation et déploiement de services avec Docker

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :



Dans le cadre de mon apprentissage, j'ai réalisé une série de travaux pratiques portant sur l'installation, l'utilisation et l'automatisation de Docker, une technologie de conteneurisation largement utilisée dans les environnements DevOps et cloud.

Pour cet exemple, j'ai commencé par installer docker. Après m'être assuré que Docker fonctionne correctement, j'ai recréé le conteneur helloworld avec un dockerfile.

```
FROM debian:bullseye-slim
```

```
RUN apt-get update
```

```
CMD ["echo","hello world"]
```

J'ai ensuite utilisé Dockerfile pour créer une image SSH avec un autre port que le port 22. Puis je me suis renseigné sur l'utilisation et la gestion des volumes de docker.

```
FROM debian:bullseye

RUN apt-get update && \
    apt-get install -y openssh-server && \
    mkdir /var/run/sshd

#création user
RUN echo 'root:root123' | chpasswd

#autoriser root login
RUN sed -i 's/^#PermitRootLogin prohibit-password/PermitRootLogin yes/' /etc/ssh/sshd_config

#changer le port SSH
RUN sed -i 's/^#Port 22/Port 2222/' /etc/ssh/sshd_config

EXPOSE 2222

CMD ["echo","hello world"]
```

Après ça, j'ai créé deux conteneurs nginx et FTP liés entre eux à l'aide de docker compose et d'un fichier yml et j'ai créé un volume commun pour accéder au dossier web.



```
services:
  nginx:
    image: nginx:latest
    ports:
      - "8080:8080"
    volumes:
      - shared_data:/usr/share/nginx.html

  ftp:
    image: stilliard/pure-ftpd
    ports:
      - "2100:21"
    environment:
      - PUBLICHOST=localhost
      - FTP_USER_NAME=user
      - FTP_USER_PASS=pass123
      - FTP_USER_HOME=/home/user
    volumes:
      - shared_data:/home/user

volumes:
  shared_data:
```

Pour tester la fonctionnalité du conteneur FTP, j'ai créé un simple fichier index.html avec mon nom et prénom sur mon ordinateur pour pouvoir l'envoyer sur mon conteneur FTP grâce au logiciel de FileZilla.

Pour le conteneur nginx, je l'ai créé sans utiliser une image existante avec dockerfile. J'ai ensuite créé une registry local et ajouté une UI afin de pouvoir le gérer facilement depuis une interface web.

Ensuite, j'ai fait un script bash pour effacer docker et un autre script pour automatiser l'installation de Docker.

DOSSIER PROFESSIONNEL (DP)



```
GNU nano 7.2                                dockerInstall
#uninstall all conflicting packages

for pkg in docker.io docker-doc docker-compose podman-docker containerd runc; d>

# Add Docker's official GPG key:
sudo apt-get update
sudo apt-get install ca-certificates curl
sudo install -m 0755 -d /etc/apt/keyrings
sudo curl -fsSL https://download.docker.com/linux/debian/gpg -o /etc/apt/keyrin>
sudo chmod a+r /etc/apt/keyrings/docker.asc

# Add the repository to Apt sources:
echo \
  "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.as>
  $(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \
  sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt-get update

#install the latest version

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace  ^U Paste     ^J Justifv   ^_ Go To Line

#install the latest version

sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin

#test

sudo docker run hello-world

#add group

sudo groupadd docker

#add user

sudo usermod -aG docker $nerds

#Add docker system boot

sudo systemctl enable docker.service
sudo systemctl enable containerd.service

[ Wrote 37 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo     M-A Set Mark  M-] To
^X Exit      ^R Read File ^\ Replace  ^U Paste     ^J Justify   ^_ Go To Line M-F Redo     M-G Copy      M-^ Paste
```

2. Précisez les moyens utilisés :

DOSSIER PROFESSIONNEL ^(DP)

J'ai utilisé un ordinateur avec une connexion Internet sur lequel j'ai configuré une VM debian 12 (8Go, 1Go, 1 CPU)

J'ai utilisé docker

3. Avec qui avez-vous travaillé ?

Sur ce projet, j'ai seul

4. Contexte

Nom de l'entreprise, organisme ou association ▶ La Plateforme

Chantier, atelier, service ▶ Dans le cadre de la formation administrateur système et réseau

Période d'exercice ▶ Du 13/05/24 au 20/05/24

Activité-type 3

Administrer et sécuriser les infrastructures systèmes et virtualisés

Exemple n°2 - Docker Swarm

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Dans le cadre d'un projet orienté vers la mise en place de solutions de Continuité d'Activité (PCA) et de Reprise d'Activité (PRA), un cluster Docker Swarm a été déployé sur une infrastructure Debian. L'objectif était de garantir une architecture résiliente, capable de maintenir les services critiques même en cas de défaillance partielle du système.

Docker Swarm est une fonctionnalité d'orchestration de conteneurs intégrée à Docker. Elle permet de regrouper plusieurs machines (nœuds) en un cluster, appelé Swarm, afin de gérer et répartir automatiquement l'exécution des conteneurs entre elles.

Nous avons devons mettre en place 3 VMs, une VM Master qui a pour adresse IP 192.168.220.195, une VM Slave qui a pour adresse IP 192.168.220.196 et une VM NFS où l'on installera le serveur qui a pour adresse IP 192.168.220.197.

Le token généré:

**SWMTKN-1-5y9pj8kug3dr0xjcv1duljd46ssfzbhx1b4zsr9fhotrycfw87-ck9df076d9po4kyljionka7p6
192.168.220.195:2377**

Étape 1 : Préparation des Machines Virtuelles (VM)

1. Créer les VM Debian
 - Une VM pour le **Maître de la Survie (Master)**.
 - Plusieurs VM pour les **Esclaves de Secours (Slaves)**.
 - Une VM pour la **Station de Résilience (NFS)**.
2. Configurer les Machines Virtuelles
 - Installer Debian sur chaque VM.
 - Mettre à jour les systèmes avec les dernières mises à jour de sécurité et paquets logiciels (`apt update && apt upgrade`).
 - Configurer les adresses IP statiques pour chaque VM.

Étape 2 : Installer Docker et Docker Swarm

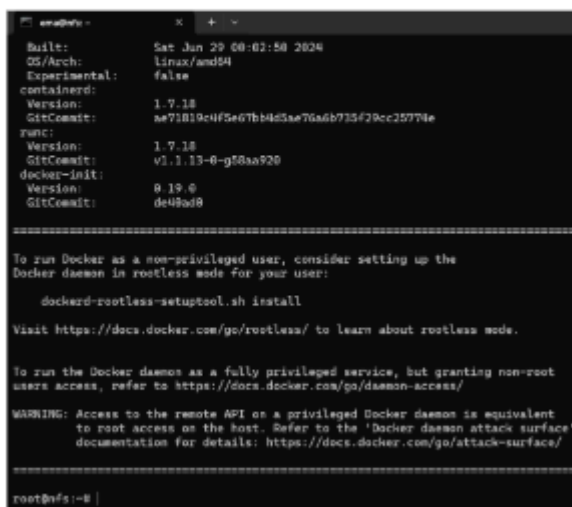
1. Installer Docker sur chaque VM

Utiliser le script officiel de Docker pour une installation simplifiée :

sh

Copier le code

```
curl -fsSL https://get.docker.com -o get-docker.sh
sudo sh get-docker.sh
```



```
ama@nfs:~$ sudo sh get-docker.sh
Built: Sat Jan 29 00:02:50 2024
OS/Arch: linux/amd64
Experimental: false
containerd:
  Version: 1.7.18
  GitCommit: ae71819c4f5e67bb4d5ae76a6b735f29cc2577de
runc:
  Version: 1.7.18
  GitCommit: v1.1.13-0-g58aa920
docker-init:
  Version: 0.19.0
  GitCommit: de48ad9

=====
To run Docker as a non-privileged user, consider setting up the
Docker daemon in rootless mode for your user:

  dockerd-rootless-setuptool.sh install

Visit https://docs.docker.com/go/rootless/ to learn about rootless mode.

To run the Docker daemon as a fully privileged service, but granting non-root
users access, refer to https://docs.docker.com/go/daemon-access/

WARNING: Access to the remote API on a privileged Docker daemon is equivalent
to root access on the host. Refer to the 'Docker daemon attack surface'
documentation for details: https://docs.docker.com/go/attack-surface/

=====
root@nfs:~#
```

2. Initialiser Docker Swarm

Sur le **Maître de la Survie** (Master):

sh

Copier le code

```
docker swarm init --advertise-addr <Master-IP>
```

○

○ Joindre les **Esclaves de Secours** (Slaves) au Swarm :

Récupérer le token de join sur le Master :

sh

Copier le code

```
docker swarm join-token worker
```

■

Sur chaque Slave, exécuter la commande join avec le token obtenu :

sh

Copier le code

```
docker swarm join --token <token> <Master-IP>:2377
```

■

Puis nous installons et configurons la Station de Résilience NFS et nous montons nos volumes NFS sur chaque VM:

Installer le serveur NFS :

sh

Copier le code

```
sudo apt install nfs-kernel-server
```

○

○ Configurer les répertoires à partager :

Ajouter dans `/etc/exports` les répertoires à partager, par exemple :

bash

Copier le code

```
/srv/nfs/kubedata *(rw,sync,no_subtree_check)
```

■

Démarrer et activer NFS :

sh

Copier le code

```
sudo systemctl start nfs-kernel-server
```

```
sudo systemctl enable nfs-kernel-server
```

Installer le client NFS sur chaque VM :

sh

Copier le code

```
sudo apt install nfs-common
```

○

Monter les volumes :

sh

Copier le code

```
sudo mount <NFS-Server-IP>:/srv/nfs/kubedata /mnt/kubedata
```

○

- Ajouter dans `/etc/fstab` pour un montage automatique au démarrage.

⚡ - - - - - ⚡

Puis, nous nous attaquons aux déploiements des conteneurs résilients: le repository local, MariaDB et PHP, nginx et vscode.

Utiliser Docker Compose ou un stack file pour déployer un registry local :

yaml

Copier le code

```
version: '3.3'
```

```
services:
```

```
registry:
  image: registry:2
  ports:
    - "5000:5000"
  volumes:
    - /mnt/kubedata/registry:/var/lib/registry
```

2. Déployer MariaDB (Bastion de la Base de Données)

Utiliser Docker Compose ou un stack file :

yaml

Copier le code

```
version: '3.3'
services:
  mariadb:
    image: mariadb
    environment:
      MYSQL_ROOT_PASSWORD: example
    volumes:
      - /mnt/kubedata/mariadb:/var/lib/mysql
```

3. Déployer PHP (Ravitaillement Rapide)

Exemple de service PHP-FPM :

yaml

Copier le code

```
version: '3.3'
services:
  php:
    image: php:fpm
```

4. Déployer Nginx (Sentinelle Web)

Utiliser Docker Compose ou un stack file :

yaml

Copier le code

```
version: '3.3'
services:
  nginx:
    image: nginx
    ports:
      - "80:80"
```

```
- "443:443"
volumes:
  - /mnt/kubedata/nginx:/etc/nginx/conf.d
```

o

5. Déployer VSCode Server (QG de Commandement)

Utiliser Docker Compose ou un stack file :

yaml

Copier le code

```
version: '3.3'
```

```
services:
```

```
  code-server:
```

```
    image: codercom/code-server
```

```
    environment:
```

```
      PASSWORD: "yourpassword"
```

```
    ports:
```

```
      - "8443:8443"
```

```
    volumes:
```

```
      - /mnt/kubedata/code-server:/home/coder/project
```

Étape 1 : Mettre à jour le système

```
sh
Copier le code
sudo apt update
sudo apt upgrade -y
```

Étape 2 : Installer les dépendances nécessaires

```
sh
Copier le code
sudo apt install apt-transport-https ca-certificates curl gnupg
lsb-release -y
```

Étape 3 : Ajouter la clé GPG officielle de Docker

```
sh
Copier le code
curl -fsSL https://download.docker.com/linux/debian/gpg | sudo gpg
--dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg
```

Étape 4 : Ajouter le dépôt Docker

```
sh
Copier le code
echo "deb [arch=amd64
signed-by=/usr/share/keyrings/docker-archive-keyring.gpg]
https://download.docker.com/linux/debian $(lsb_release -cs) stable"
| sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
```

Étape 5 : Installer Docker Engine

```
sh
Copier le code
sudo apt update
```

```
sudo apt install docker-ce docker-ce-cli containerd.io -y
```

Étape 6 : Vérifier l'installation de Docker

sh

Copier le code

```
sudo docker version
```

Étape 7 : Initialiser Docker Swarm sur le Master

sh

Copier le code

```
sudo docker swarm init --advertise-addr <Master-IP>
```

Étape 8 : Joindre les Slaves au Swarm

Sur le Master, obtenir le token de join :

sh

Copier le code

```
sudo docker swarm join-token worker
```

1.

Sur chaque Slave, exécuter la commande join avec le token obtenu :

sh

Copier le code

```
sudo docker swarm join --token <token> <Master-IP>:2377
```

2.

En suivant ces étapes, vous devriez être en mesure d'installer Docker et de configurer Docker Swarm manuellement sur Debian. Assurez-vous de remplacer **<Master-IP>** et **<token>** par les valeurs appropriées pour votre environnement.

DOSSIER PROFESSIONNEL (DP)

```
ema@nfs: ~  
ema@debian: ~  
mount.nfs: access denied by server while mounting 192.168.220.198:/srv/nfs  
^Cot@debian:/mnt/nfs# sudo mount 192.168.220.0:/srv/nfs /mnt/nfs  
root@debian:/mnt/nfs# cd  
root@debian:~# apt-get install-y nfs-common  
E: L'opération install-y n'est pas valable  
root@debian:~# apt-get install -y nfs-common  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances... Fait  
Lecture des informations d'état... Fait  
nfs-common est déjà la version la plus récente (1:2.6.2-4).  
Le paquet suivant a été installé automatiquement et n'est plus nécessaire :  
  linux-image-6.1.0-18-amd64  
Veuillez utiliser « apt autoremove » pour le supprimer.  
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.  
root@debian:~# cd /mnt/nfs  
root@debian:/mnt/nfs# sudo mount 192.168.220.198:/srv/nfs /mnt/nfs  
mount.nfs: access denied by server while mounting 192.168.220.198:/srv/nfs  
root@debian:/mnt/nfs# sudo mount 192.168.220.198:/srv/nfs /mnt/nfs  
root@debian:/mnt/nfs# echo "192.168.220.198:/srv/nfs /mnt/nfs nfs defaults 0 0" | sudo tee -a /etc/fstab  
sudo: tee -a : commande introuvable  
root@debian:/mnt/nfs# echo "192.168.220.198:/srv/nfs /mnt/nfs nfs defaults 0 0" | sudo tee -a /etc/fstab  
192.168.220.198:/srv/nfs /mnt/nfs nfs defaults 0 0  
root@debian:/mnt/nfs# sudo docker network create--driver overlay rzo_overlay
```

```
ema@nfs: ~  
ema@debian: ~  
root@debian:/mnt/nfs# sudo mount 192.168.220.198:/srv/nfs /mnt/nfs  
mount.nfs: access denied by server while mounting 192.168.220.198:/srv/nfs  
root@debian:/mnt/nfs# sudo mount 192.168.220.198:/srv/nfs /mnt/nfs  
root@debian:/mnt/nfs# echo "192.168.220.198:/srv/nfs /mnt/nfs nfs defaults 0 0" | sudo tee -a /etc/fstab  
sudo: tee -a : commande introuvable  
root@debian:/mnt/nfs# echo "192.168.220.198:/srv/nfs /mnt/nfs nfs defaults 0 0" | sudo tee -a /etc/fstab  
192.168.220.198:/srv/nfs /mnt/nfs nfs defaults 0 0  
root@debian:/mnt/nfs# sudo docker network create--driver overlay rzo_overlay  
  
Usage:  docker network COMMAND  
  
Manage networks  
  
Commands:  
  connect    Connect a container to a network  
  create     Create a network  
  disconnect Disconnect a container from a network  
  inspect    Display detailed information on one or more networks  
  ls         List networks  
  prune     Remove all unused networks  
  rm         Remove one or more networks
```

```
ema@nfs: ~  
disconnect Disconnect a container from a network  
inspect Display detailed information on one or more networks  
ls List networks  
prune Remove all unused networks  
rm Remove one or more networks  
  
Run 'docker network COMMAND --help' for more information on a command.  
root@debian:/mnt/nfs#  
root@debian:/mnt/nfs#  
root@debian:/mnt/nfs# sudo docker service create --name nexus --network rzo_overlay --publish 8081:8081 --mount type=bind,source=/mnt/nfs/nexus-data,target=/nexus-data --sonatype/nexus3  
Error response from daemon: network rzo_overlay not found  
root@debian:/mnt/nfs# cd  
root@debian:~# /home/  
bash: /home/: est un dossier  
root@debian:~# udo docker service create --name nexus --network rzo_overlay --publish 8081:8081 --mount type=bind,source=/mnt/nfs/nexus-data,target=/nexus-data --sonatype/nexus3  
bash: udo : commande introuvable  
root@debian:~# sudo docker service create --name nexus --network rzo_overlay --publish 8081:8081 --mount type=bind,source=/mnt/nfs/nexus-data,target=/nexus-data --sonatype/nexus3  
Error response from daemon: network rzo_overlay not found  
root@debian:~# sudo docker network create --driver overlay rzo_overlay  
hzy8wr9edsbalk5gp0l7ypc9o  
root@debian:~#
```

Nexus créé :

```
ema@nfs: ~  
bash: udo : commande introuvable  
root@debian:~# sudo docker service create --name nexus --network rzo_overlay --publish 8081:8081 --mount type=bind,source=/mnt/nfs/nexus-data,target=/nexus-data --sonatype/nexus3  
Error response from daemon: network rzo_overlay not found  
root@debian:~# sudo docker network create --driver overlay rzo_overlay  
hzy8wr9edsbalk5gp0l7ypc9o  
root@debian:~# sudo docker service create --name nexus --network rzo_overlay --publish 8081:8081 --mount type=bind,source=/mnt/nfs/nexus-data,target=/nexus-data --sonatype/nexus3  
5nd3wox2hkuk1vwlkqj50zc9  
overall progress: 0 out of 1 tasks  
1/1: invalid mount config for type "bind": bind source path does not exist: /mnt/nfs/nexus-data  
Use 'docker service ps 5nd3wox2hkuk1vwlkqj50zc9' to check progress.  
root@debian:~# sudo docker service create --name nexus --network rzo_overlay --publish 8081:8081 --mount type=bind,source=/mnt/nfs/nexus-data,target=/nexus-data --sonatype/nexus3  
Error response from daemon: rpc error: code = InvalidArgument desc = port '8081' is already in use by service 'nexus' (5nd3wox2hkuk1vwlkqj50zc9) as an ingress port  
root@debian:~# cd /mnt/nfs  
root@debian:/mnt/nfs# ls  
root@debian:/mnt/nfs# docker service ls  
ID NAME MODE REPLICAS IMAGE  
5nd3wox2hkuk1vwlkqj50zc9 nexus replicated 0/1 sonatype/nexus3:latest  
root@debian:/mnt/nfs#
```


DOSSIER PROFESSIONNEL ^(DP)



2. Précisez les moyens utilisés :

Pour ce projet, nous avons utilisé un ordinateur avec une connexion Internet

3. Avec qui avez-vous travaillé ?

Sur ce projet, j'ai travaillé avec deux de mes camarades de classe.

4. Contexte

Nom de l'entreprise, organisme ou association ▶ La Plateforme

Chantier, atelier, service ▶ Dans le cadre de la formation administrateur système et réseau

Période d'exercice ▶ Du 24/06/24 au 01/07/24

Activité-type 4

Déploiement d'une solution de supervision centralisée

Exemple n°1 - SIEM ELK

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

ELK (ElasticSearch, Logstash, Kibana) est une solution open source utilisée pour la collecte, l'analyse et la visualisation centralisée de logs. Elle est largement déployée dans les environnements de production pour assurer une supervision efficace, une détection rapide d'incidents et un diagnostic précis des infrastructures informatiques.

ElasticSearch permet de stocker, indexer et interroger rapidement de grandes quantités de données comme: des logs systèmes, des journaux applicatifs et des métriques réseaux.

Logstash permet de collecter, filtrer, transformer et enrichir les logs. Il facilite également l'uniformisation des formats de logs avant de les transmettre à Elasticsearch pour indexation.

Kibana est une interface web de visualisation des données stockées dans Elasticsearch. Elle permet de créer des tableaux de bord dynamiques, des graphes en temps réel et des alertes visuelles et est très utile pour l'analyse d'événements de sécurité et le suivi de performances systèmes.

Nous avons donc déployé un ELK pour centraliser les logs d'un système et pouvoir les analyser

Nous avons suivis ce tutoriel afin de monter et déployer un ELK:

https://gitlab.com/xavki/presentations-elk/-/blob/master/2-installation-elasticsearch/install_elk.sh

```
#!/bin/bash
```

```
## Variables #####
```

```
VERSION="7.6.1"
```

```
#VERSION="7.4.1"
```

```
IP=$(hostname -I | cut -d " " -f 2)
```

```
## Check root #####
```

```
sudo -n true
```

```
if [ $? -ne 0 ]
```

```
then
```

```
    echo "This script requires user to have passwordless sudo access"
```

```
    exit
```

```
fi
```

```
## Functions #####
```

```
dependency_check_deb() {
```

```
java -version
```

```
if [ $? -ne 0 ]
```

```
then
```

```
    sudo apt-get install openjdk-7-jre-headless -y
```

```
    elif [ "$(java -version 2> /tmp/version && awk '/version/ { gsub("/", "", $NF); print ( $NF < 1.7 ) ? "YES" : "NO" }' /tmp/version)" == "YES" ]
```

```
    then
```

```
        sudo apt-get install openjdk-7-jre-headless -y
```

```
fi
```

```
}
```

```
dependency_check_rpm() {  
    java -version  
    if [ $? -ne 0 ]  
    then  
        sudo yum install java-11-openjdk-headless.x86_64 -y  
    fi  
}  
  
debian_elk() {  
    sudo apt-get update
```

```
    sudo wget --directory-prefix=/opt/  
https://artifacts.elastic.co/downloads/logstash/logstash-${VERSION}.deb  
    sudo dpkg -i /opt/logstash*.deb  
    sudo wget --directory-prefix=/opt/  
https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-${VERSION}-amd64.deb  
    sudo dpkg -i /opt/elasticsearch*.deb  
    sudo wget --directory-prefix=/opt/  
https://artifacts.elastic.co/downloads/kibana/kibana-${VERSION}-amd64.deb  
    sudo dpkg -i /opt/kibana*.deb  
    sudo service logstash start  
    sudo service elasticsearch start  
    sudo service kibana start  
}
```

```
rpm_elk() {
    sudo yum install wget -y
    sudo wget --directory-prefix=/opt/
https://artifacts.elastic.co/downloads/logstash/logstash-${VERSION}.rpm
    sudo rpm -ivh /opt/logstash*.rpm
    sudo wget --directory-prefix=/opt/
https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-${VERSION}-x86_64.rpm
    sudo rpm -ivh /opt/elasticsearch*.rpm
    sudo wget --directory-prefix=/opt/
https://artifacts.elastic.co/downloads/kibana/kibana-${VERSION}-x86_64.rpm
    sudo rpm -ivh /opt/kibana*.rpm
    sudo systemctl enable logstash
    sudo systemctl start logstash
    sudo systemctl enable elasticsearch
    sudo systemctl start elasticsearch
    sudo systemctl enable kibana
    sudo systemctl start kibana
}

vagrant_steps() {
    sudo systemctl stop firewalld
    sudo systemctl disable firewalld
    sed -i s/"#server.host: \"localhost\""/"server.host: \"0.0.0.0\""/g /etc/kibana/kibana.yml
    sudo systemctl restart kibana
    sed -i s/"#discovery.seed_hosts: \".\""/"discovery.seed_hosts: [\"${IP}\", \"127.0.0.1\"]"/g
    /etc/elasticsearch/elasticsearch.yml
    sed -i s/"#network.host: \".\""/"network.host: 0.0.0.0"/g /etc/elasticsearch/elasticsearch.yml
    sudo systemctl restart elasticsearch
}

## Exec #####

if [ "$(grep -Ei 'debian|buntu|mint' /etc/*release)" ]
```

```
then
    echo " It's a Debian based system"
    dependency_check_deb
    debian_elk
elif [ "$(grep -Ei 'fedora|redhat|centos' /etc/*release)" ]
then
    echo "It's a RedHat based system."
    dependency_check_rpm
    rpm_elk
                                vagrant_steps
else
    echo "This script doesn't support ELK installation on this OS."
fi
```

2. Précisez les moyens utilisés :

DOSSIER PROFESSIONNEL ^(DP)

Pour ce projet, nous avons utilisé un ordinateur avec une connexion Internet

3. Avec qui avez-vous travaillé ?

Sur ce projet, j'ai travaillé avec deux de mes camarades de classe.

4. Contexte

Nom de l'entreprise, organisme ou association	La Plateforme
---	---------------

Chantier, atelier, service	➤ Dans le cadre de la formation administrateur système et réseau
----------------------------	--

Période d'exercice	➤ Du 26/08/24 au 05/09/24
--------------------	---------------------------

Titres, diplômes, CQP, attestations de formation

DOSSIER PROFESSIONNEL ^(DP)

(facultatif)

Intitulé	Autorité ou organisme	Date
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.

DOSSIER PROFESSIONNEL ^(DP)

Déclaration sur l'honneur

Je soussigné(e) [prénom et nom] , **Mylène RODRIGUES DOS SANTOS**

déclare sur l'honneur que les renseignements fournis dans ce dossier sont exacts et que je
suis l'auteur(e) des réalisations jointes.

Cliquez ici pour taper du texte.

Fait à **La Ciotat**

le **21/07/2025**

pour faire valoir ce que de droit.

Cliquez ici pour taper du texte.

Signature : RODRIGUES DOS SANTOS Mylène

DOSSIER PROFESSIONNEL ^(DP)

Documents illustrant la pratique professionnelle

(facultatif)

Intitulé
Cliquez ici pour taper du texte.

DOSSIER PROFESSIONNEL ^(DP)

ANNEXES

(Si le RC le prévoit)

