MÉMOIRE PROFESSIONNEL

Prise en charge du projet de migration vers le nouvel hébergeur Cloud

Etudiant : BERNOIS Damien

Promotion : Administrateur Systèmes et Réseaux 2024-2025

Tuteur de l'entreprise :

Responsable pédagogique :

REMERCIEMENTS

Je tiens tout d'abord à exprimer ma profonde gratitude envers toute l'équipe du CNPF, et en particulier à M. XXX pour m'avoir offert l'opportunité d'effectuer ce contrat d'apprentissage au sein de leur structure, ainsi qu'à M. XXX dont les échanges ont contribué à la réussite de mes missions.

Mes remerciements s'entendent tout autant à M. XXX pour s'être porté garant d'être mon tuteur pédagogique, d'avoir supervisé mes missions tout au long de mon alternance grâce auxquelles j'ai pu approfondir mes compétences et réflexions.

De plus, je remercie M. XXX, ainsi que M. XXX pour m'avoir accompagné tout au long de ce projet, d'avoir été d'un soutien et d'une aide précieuse, avec qui j'ai pu collaborer afin de mener à bien ce dernier.

Sans oublier toute l'équipe du service du développement numérique, qui m'ont de même accompagné et intégré à l'environnement de l'entreprise durant cette année d'apprentissage, dont leur aide et conseil m'ont été d'un grand service.

Leur accueil chaleureux, leur encadrement attentif, leurs précieux conseils, ainsi que les missions qui m'ont été confiées ont grandement contribué à enrichir mon expérience professionnelle et mes connaissances en informatique.

Mes remerciements s'adressent également à toute l'équipe de l'école du CESI d'Orléans ainsi qu'aux intervenants externes, en particulier à Mme. XXX, la représentante et la responsable pédagogique de notre promotion, ainsi qu'à Mme. XXX, qui ont toutes deux su nous accompagner tout au long de cette année d'apprentissage et éclaircir nos points de doute.

Sans oublier les intervenants pédagogiques qui m'ont permis d'approfondir mes connaissances et d'assimiler de nouvelles notions afin de compléter et d'accompagner les savoir-faire de cette année d'apprentissage.

Enfin, je tiens aussi à exprimer ma reconnaissance envers ma famille et mes amis pour leur soutien tout au long de cette expérience professionnelle.

Cette alternance a été une véritable source d'enrichissement personnel et professionnel, et je suis reconnaissant envers toutes les personnes qui ont contribué à sa réussite.

Table des matières

OUTILS À DISPOSITION

Outils de correction écrite utilisé au cours de la rédaction du mémoire :

- https://www.reverso.net/orthographe/correcteur-francais/

Outils de console utilisés au cours du projet de fin d'étude :

- https://console.cloud.google.com/
- https://aws.amazon.com/fr/console/

Outils à disposition du Service du développement numérique :

- KEEPASS 2
- ZOOM WORKPLACE
- TALKSPIRIT
- NETSKOPE CLIENT
- DRAW.IO
- WORD OFFICE
- ZIMBRA MAIL
- GANTT PROJECT

SOURCES

Présentation de l'entreprise :

- https://www.cnpf.fr/

Documentation des hébergeurs cloud manipulés :

- https://cloud.google.com/architecture?hl=fr
- https://docs.aws.amazon.com/

Documentation des hébergeurs cloud analysés :

- https://cloud.google.com/architecture?hl=fr
- https://docs.aws.amazon.com/
- https://academy.cegedim.cloud/
- https://www.cloud-temple.com/

FIGURES

GLOSSAIRE

Les définitions ci-dessous sont rangées dans l'ordre alphabétique et non dans l'ordre chronologique de la lecture du mémoire, telles que :

- **APIs REST** : Interfaces de communication standardisées pour les applications web.
- **AWS** : Plateforme cloud d'Amazon proposant des services informatiques à la demande.
- **Bare-Metal** : Serveur physique dédié sans virtualisation.
- **Base cadastrale forestière** : Données foncières spécifiques aux parcelles forestières.
- **Base de données SQL** : Base structurée utilisant le langage SQL pour les requêtes.
- **BigQuery** : Service d'analyse de données massives de Google Cloud.
- **Business plans** : Documents présentant la stratégie financière d'un projet.
- **Cegedim** : Fournisseur français de services cloud souverain.
- **Celeste** : Fournisseur français d'accès internet et de services cloud.
- **Cloud Act** : Loi américaine obligeant les entreprises US à fournir des données sur demande.
- **Cloud C5** : Certification allemande de sécurité pour services cloud.
- **Cloud computing** : Fourniture de ressources IT (serveurs, stockage...) à la demande.
- **Cloud Hybride** : Combinaison de cloud privé et public pour plus de flexibilité.
- **Cloud souverain** : Infrastructure cloud contrôlée nationalement pour garantir la sécurité des données.
- **Cloud Temple** : Fournisseur français de services cloud souverain.
- **CloudFormation** : Outil AWS pour déployer des ressources via des modèles.
- **Compute** : Puissance de calcul fournie par des machines virtuelles ou physiques.
- **Contrôle locaux** : Mécanismes de surveillance et de conformité internes à l'organisation.
- **Cost Explorer** : Outil AWS de suivi et d'analyse des dépenses cloud.
- **Cryptage du transit** : Chiffrement des données lors de leur transmission.
- **Datacenters** : Centres physiques hébergeant serveurs, stockage et réseaux.
- **DevOps** : Méthodologie combinant développement et exploitation IT pour livrer plus vite.
- **Direct Connect** : Connexion réseau dédiée entre AWS et votre infrastructure.
- **DynamoDB** : Base de données NoSQL rapide et scalable d'AWS.
- **EventBridge** : Service d'événementiel AWS pour connecter applications et services.
- **FISA** : Loi Américaine autorisant la surveillance électronique à des fins de renseignement.
- **Forticlient VPN** : Client VPN de Fortinet pour sécuriser les connexions distantes.
- **Full cloud** : Infrastructure informatique entièrement hébergée dans le cloud.
- **GenAI** : Intelligence artificielle générative créant textes, images, code, etc.
- **Google Cloud** : Plateforme cloud de Google pour services IT à la demande.
- **HDS** : Certification française pour héberger des données de santé.
- **HIPAA/HITECH** : Lois américaines encadrant la sécurité des données médicales.
- **HSM** : Module matériel sécurisé pour la gestion de clés cryptographiques.
- **IaaS opensource** : Infrastructure cloud libre et modifiable par les utilisateurs.
- **Instances** : Machines virtuelles déployées dans le cloud.
- **ISAE 3402 type 2** : Norme d'audit des processus de contrôle interne sur la durée.
- **ISO 14001** : Norme internationale de gestion environnementale.
- **ISO 20000** : Norme de qualité pour la gestion des services informatiques.
- **ISO 27001/17/18** : Normes de sécurité de l'information et des services cloud.
- **ISO 50001** : Norme de management de l'énergie.
- **ISO 9001** : Norme de gestion de la qualité des processus.
- **KMS** : Service de gestion de clés cryptographiques dans le cloud.
- **Kubernetes** : Orchestrateur open source pour conteneurs (comme Docker).

- **Label Bas Carbone** : Certification française encourageant les projets réduisant les émissions.
- **Label Cloud de Confiance** : Label français garantissant la sécurité et souveraineté des services cloud.
- **Lambda** : Service AWS permettant d'exécuter du code sans gérer de serveur.
- **LinkT** : Fournisseur français d'accès internet et de services cloud.
- **Loi « Pisani »** : Loi française de 1963 encadrant la politique forestière.
- **l'UGAP – UGAP C3** : Centrale d'achat public française facilitant les marchés IT.
- **Microsoft Azure** : Plateforme cloud de Microsoft.
- **Multi-cloud** : Utilisation de plusieurs fournisseurs cloud simultanément.
- **Méthode PDCA** : Approche qualité basée sur Plan-Do-Check-Act.
- **Nitro** : Plateforme AWS de virtualisation sécurisée.
- **On premise** : Infrastructure informatique hébergée localement.
- **OpenShift (Red Hat)** : Plateforme Kubernetes pour applications conteneurisées.
- **PCI-DSS** : Norme de sécurité pour le traitement des données de cartes bancaires.
- **Portail d'authentification** : Interface sécurisée pour identifier les utilisateurs.
- **Programme for the Endorsement of Forest Certification** : Label mondial de gestion forestière durable.
- **Publisher Netskope** : Solution de sécurité cloud pour la gestion des accès et des données.
- **PUE** : Indicateur d'efficacité énergétique d'un datacenter.
- **RGPD (DPA, SLA, code CISPE)** : Réglementation européenne sur la protection des données.
- **Roue de Deming** : Autre nom de la méthode PDCA.
- **S3NS (Thales)** : Joint-venture entre Thales et Google pour un cloud de confiance.
- **Savings Plans** : Offres AWS pour optimiser les coûts à long terme.
- **Script** : Suite d'instructions exécutées automatiquement par un système.
- **SecNumCloud** : Référentiel de sécurité de l'ANSSI pour les services cloud.
- **SecOps** : Pratiques de sécurité intégrées aux opérations IT.
- **SentinelOne** : Solution de cybersécurité basée sur l'IA.
- **Service Desk** : Point de contact pour la gestion des incidents IT.
- **Souveraineté numérique** : Contrôle national sur les données et infrastructures numériques.
- **Sylvicole** : Relatif à la gestion et culture des forêts.
- **Systems d'informations** : Ensemble organisé de ressources pour traiter de l'information.
- **Terraform** : Outil d'infrastructure as code pour déployer du cloud.
- **Traçabilité ANSSI** : Suivi des événements de sécurité selon les règles de l'ANSSI.
- **VEEAM** : Logiciel de sauvegarde et de restauration pour environnements cloud/virtuels.
- **Vertex AI** : Plateforme Google Cloud pour construire et déployer des modèles IA.
- **WUE** : Indicateur d'efficacité d'utilisation de l'eau dans les datacenters.
- **Zero Trust Network Access** : Modèle de sécurité n'accordant aucun accès par défaut.
- **Zone de disponibilité** : Emplacement géographique redondant dans un cloud provider.

ABRÉVIATIONS

Les abréviations ci-dessous sont rangées dans l'ordre alphabétique et non dans l'ordre chronologique de la lecture du mémoire, telles que :

- **AI / IA** : Artificial Intelligence / Intelligence Artificielle
- **AMDEC** : Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité
- **ANSSI** : Agence Nationale de la Sécurité des Systèmes d'Information
- **API / API REST** : Application Programming Interface / Representational State Transfer
- **AWS** : Amazon Web Services
- **BSI** : Bundesamt für Sicherheit in der Informationstechnik
- **CaaS** : Container as a Service
- **CISPE** : Cloud Infrastructure Services Providers in Europe
- **Cloud Act** : Clarifying Lawful Overseas Use of Data Act
- **CNIL** : Commission Nationale de l'Informatique et des Libertés
- **CNPF** : Centre National de la Propriété Forestière
- **CNPPF :** Centre National Professionnel de la Propriété Forestière
- **CRPF :** Centre Régional de la Propriété Forestière
- **C5** : Cloud Computing Compliance Criteria Catalogue
- **DAF** : Directeur Administratif et Financier
- **DPA** : Data Processing Agreement
- **EC2** : Elastic Compute Cloud
- **EDR** : Endpoint Detection and Response
- **ESC :** European Sovereign Cloud
- **FISA** : Foreign Intelligence Surveillance Act
- **GCP** : Google Cloud Platform
- **HDS** : Hébergeur de Données de Santé
- **HIPAA** : Health Insurance Portability and Accountability Act
- **HITECH** : Health Information Technology for Economic and Clinical Health Act
- **HSM** : Hardware Security Module
- **IaaS** : Infrastructure as a Service
- **IaC** : Infrastructure as Code
- **IDF** : Institut pour le Développement Forestier
- **ISO / IEC** : International Organization for Standardization / International Electrotechnical Commission
- **IT** : Information Technology
- **KMS**: Key Management Service
- **KPI** : Key Performance Indicator
- **LAN** : Local Area Network
- **LDAP** : Lightweight Directory Access Protocol
- **ML** : Machine Learning
- **MSP** : Managed Service Provider
- **PaaS** : Platform as a Service
- **PCI-DSS** : Payment Card Industry Data Security Standard
- **PEFC** : Programme for the Endorsement of Forest Certification
- **PHT** : Prix Hors Taxes
- **PTHT** : Prix Total Hors Taxes
- **PUE** : Power Usage Effectiveness
- **RDS** : Relational Database Service

- **RGPD** : Règlement Général sur la Protection des Données
- **RH** : Ressources Humaines
- **ROI** : Retour sur Investissement
- **RSE** : Responsabilité Sociétale des Entreprises
- **R&D** : Recherche & Développement
- **SaaS** : Software as a Service
- **SDN** : Service du Développement Numérique
- **SI** : Système d'Information
- **SLA** : Service Level Agreement
- **SOC** : Security Operations Center
- **S3** : Simple Storage Service
- **TVA** : Taxe sur la Valeur Ajoutée
- **VPC** : Virtual Private Cloud
- **WBS** : Work Breakdown Structure
- **WUE** : Water Usage Effectiveness
- **ZTNA** : Zero Trust Network Access

1. Introduction

L'objectif de ce mémoire est de fournir une synthèse approfondie de ma période d'apprentissage au sein du CNPF. Cette immersion s'insère dans le contexte de ma formation ASR (Administrateur Systèmes et Réseaux) proposée par l'école CESI d'Orléans.

La finalité principale de cette alternance est de concrétiser et d'approfondir les connaissances théoriques acquises au cours de mes études, tout en découvrant de nouvelles notions et enrichir mon expérience professionnelle.

A. Ma mission

Au cours de mon apprentissage, j'ai eu l'opportunité d'avoir participé à divers projets, dont le principal et sujet de mon mémoire porte sur la **prise en charge du projet de la migration de l'hébergeur cloud actuel du CNPF (AWS) vers un nouvel hébergeur cloud**.

Comprenant **l'analyse de l'existant** et de la future mise en œuvre, la **prise de contact** avec les fournisseurs de solution cloud, **l'organisation du projet** dans les temps et coûts convenus, la **réflexion du choix de la solution** de migration avec l'équipe du SI (full cloud, hybride, quel hébergeur, etc) en fonction des besoins (en termes de réseau, système, données, stockage, sécurité, budget, support, etc.), la rédaction de procédures et de tests en amont et la mise en œuvre de la migration en elle-même (qui n'a pas pu être faite dans les temps due à divers facteurs externes développés dans le mémoire, mais a pu être simulée dans un contexte de mise en production de la migration sur l'hébergeur cloud GCP).

Ce projet m'a permis d'assimiler différentes compétences telles qu'approfondir mes connaissances en **cloud computing** et en réseaux, apprendre et me familiariser avec l'environnement cloud AWS et GCP, **étudier la faisabilité d'un projet** (risques de l'existant, risques de la migration, contraintes, contexte, coûts, délais, communication, etc.), adopter une démarche de mise en place d'un projet en entreprise, le savoir-être et savoir-vivre dans un environnement professionnel, la communication avec des fournisseurs et prestataires extérieurs.

B. Présentation des besoins

Ce projet a vu le jour à la suite d'un **besoin urgent de revoir l'infrastructure** de notre environnement cloud, en particulier pour des **raisons économiques** du fait que notre infrastructure cloud actuelle engendre des coûts non négligeables et pouvant être **optimisés**, voir évités.

Mais aussi pour des raisons **d'optimisation de la sécurité et de la gestion** de notre environnement cloud. Notre infrastructure cloud se vieillissant et n'étant plus conformément maintenue et documentée, cette dernière peut **entraîner des défaillances techniques** et un manquement de connaissance et de documentations pouvant **éterniser la reprise de l'activité** de ce dernier en cas de sinistre.

Il convient donc d'étudier les possibilités de migration de notre infrastructure cloud, ainsi que d'étudier les offres des différents hébergeurs cloud.

En vue des complications politiques actuelles et de **l'instabilité économique** (depuis février 2025) **impactant à grande échelle les systèmes d'information** des enseignes publiques françaises dues aux propos et actions du président américain actuel laissant sous-entendre la possibilité de l'isolation et/ou de l'arrêt de la communication avec les services cloud américain (engendrant la perte de notre infrastructure cloud et de toutes ces données).

Le CNPF se questionne aujourd'hui sur la **rationalisation et la faisabilité de ce projet**, ainsi que le **choix de l'hébergeur cloud** vers lequel nous allons basculer, en particulier en fonction de l'aspect de la **sécurité des données et de leur hébergement**, mais aussi du respect en vigueur du **RGPD française applicable aux données que notre enseigne détient**, étant donné que ces dernières avaient pour vocation d'être initialement hébergées sur les datacenters GCP basés à Paris, en France. Il est donc convenu de se demander vers quelle solution et quel hébergeur cette migration sera-t-elle faite.

Pour ce faire, la prise de contact avec différents hébergeurs cloud hébergés en France et étant **certifiés par les autorités françaises** est nécessaire afin d'étudier les différentes possibilités du futur hébergement.

2. Contexte de l'entreprise

A. Le Centre National de la Propriété Forestière

Le Centre National de la Propriété Forestière est l'**organisme public responsable de la gestion de la forêt privée en France**. Depuis janvier 2025, ce dernier est affilié au **ministère de la transition écologique**, anciennement lié au ministère de l'Agriculture et de l'Alimentation. Il représentant environ 75% des forêts du pays, son rôle majeur est d'accompagner les 3,5 millions de propriétaires privés dans la gestion durable de leurs 12,6 millions d'hectares de forêts, soit 23% du territoire métropolitain. Le CNPF a pour mission de **soutenir l'activité sylvicole des propriétaires forestiers privés** en les conseillant, en les formant et en regroupant leurs propriétés pour réaliser des projets forestiers.

Pour ce faire, il agrée les plans de gestion forestière, élabore des schémas régionaux et des codes de bonnes pratiques. Il conseille, informe et forme les propriétaires, notamment par des publications et des outils en ligne, pour promouvoir une gestion forestière efficace. Il encourage également le regroupement des petites parcelles forestières dispersées pour une **exploitation plus efficace et durable**, tout en contribuant à la **recherche et à l'innovation** dans des domaines tels que l'adaptation au changement climatique et l'amélioration génétique. Enfin, il sensibilise les propriétaires à l'**importance de la préservation de la biodiversité forestière**.

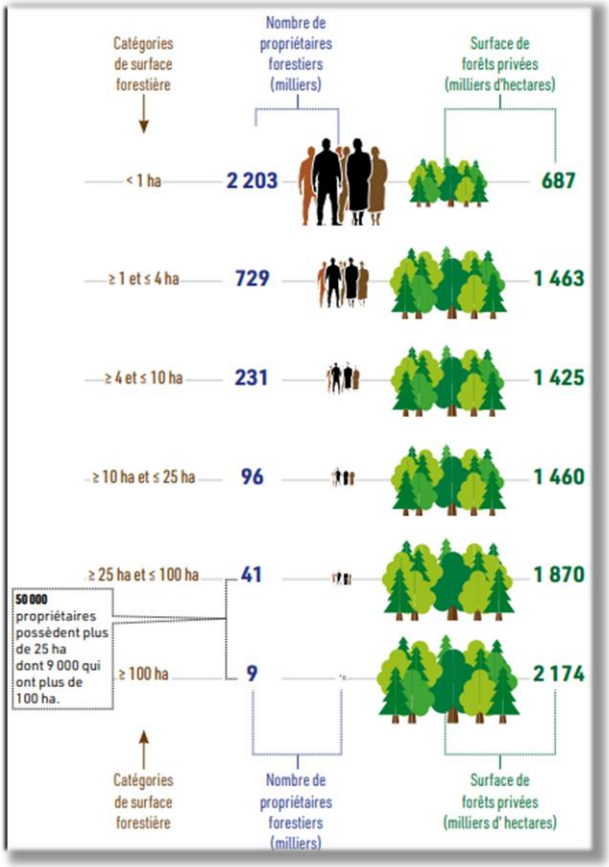


Figure 1 : Réseaux forestiers nationaux et européens

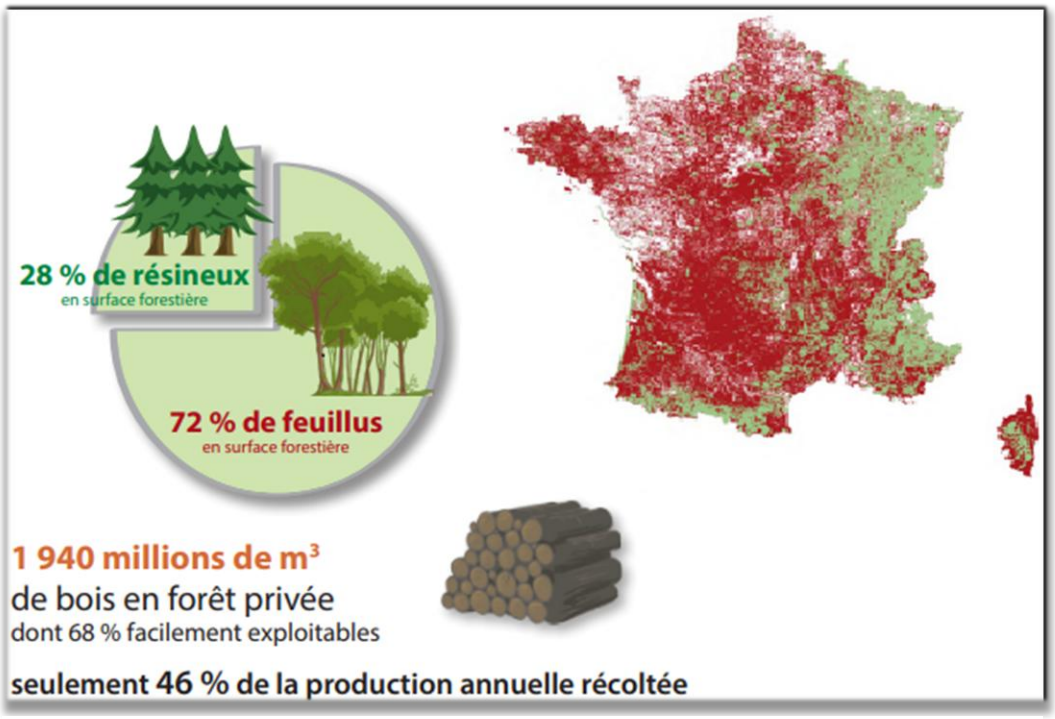


Figure 2 : Dispersion forestière

Le CNPF regroupe un total de **11 délégations régionales** appelées des Centres régionaux de la propriété forestière (CRPF), dont font partie **105 sites** parmi lesquels se retrouvent plus de **450 agents** répartis dans chacune de ces régions.

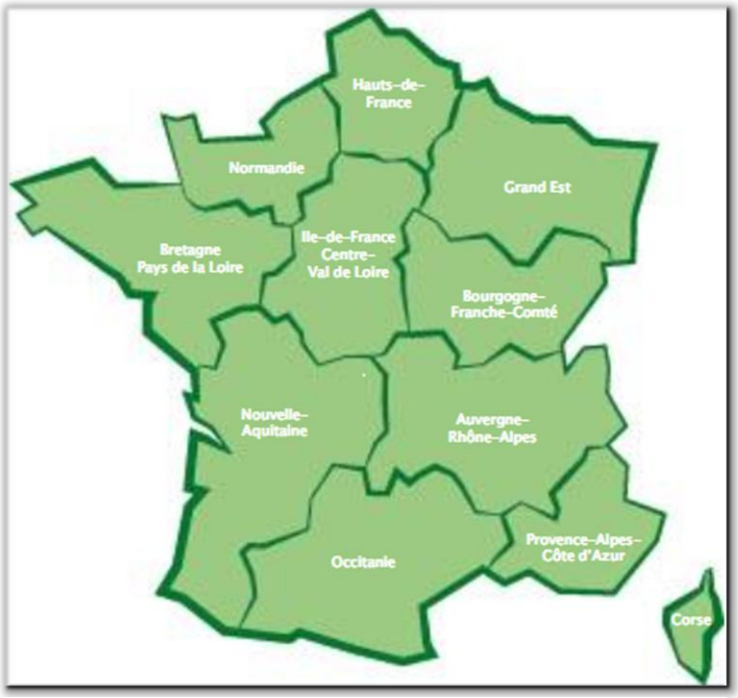


Figure 3 : Carte des régions

De plus, il possède un service de recherche et de développement appelé l'**Institut pour le développement forestier** (IDF) s'exprimant à travers des projets, de l'expérimentation, de l'édition et de la formation. L'équipe travaille en étroite collaboration avec les CRPF, avec un ancrage territorial proche des acteurs, notamment les sylviculteurs et les propriétaires forestiers afin d'assurer une **gestion durable des forêts privées**, mais aussi pour former et informer les forestiers privés.

Le centre innove en matière d'outils de diagnostic et d'aide à la décision dans les domaines de la biodiversité, de l'état sanitaire des forêts et de leur sensibilité aux changements climatiques. Il est également à l'origine du **Label Bas Carbone** grâce à son travail sur la séquestration du carbone en forêt.

B. Son histoire

Les Centres régionaux de la propriété forestière ont été créés en **1963 par la loi « Pisani »** instauré en août 1962, stipulant que la responsabilité de l'assainissement des marchés agricoles ne pouvait être prise en charge seulement par l'État et que les producteurs sont invités à se regrouper afin que la responsabilité soit aussi la leur.

À la suite de cela, en 2003, le Centre national de la propriété professionnel forestière (CNPPF) sera créé, l'IDF deviendra une entité du CNPPF en 2006.

Finalement, en 2010, l'**unification des 18 CRPF et du CNPPF** à des fins de simplifications juridiques et administratives deviendra le CNPF, une **entité publique de l'État** à caractère administratif.

Aujourd'hui, le CNPF comprend **11 CRPF** et est en étroite **collaboration avec 7 autres instituts**, a mis en place des programmes visant à certifier les forêts privées sous des labels comme le Programme for the Endorsement of Forest Certification (PEFC) et continue d'**accompagner les propriétaires de forêts privées en France** en faisant de la prévention des risques liés aux forêts, mettant en place des plans de gestion, ainsi que des projets liés à la biodiversité et à la lutte contre la déforestation et le réchauffement climatique.

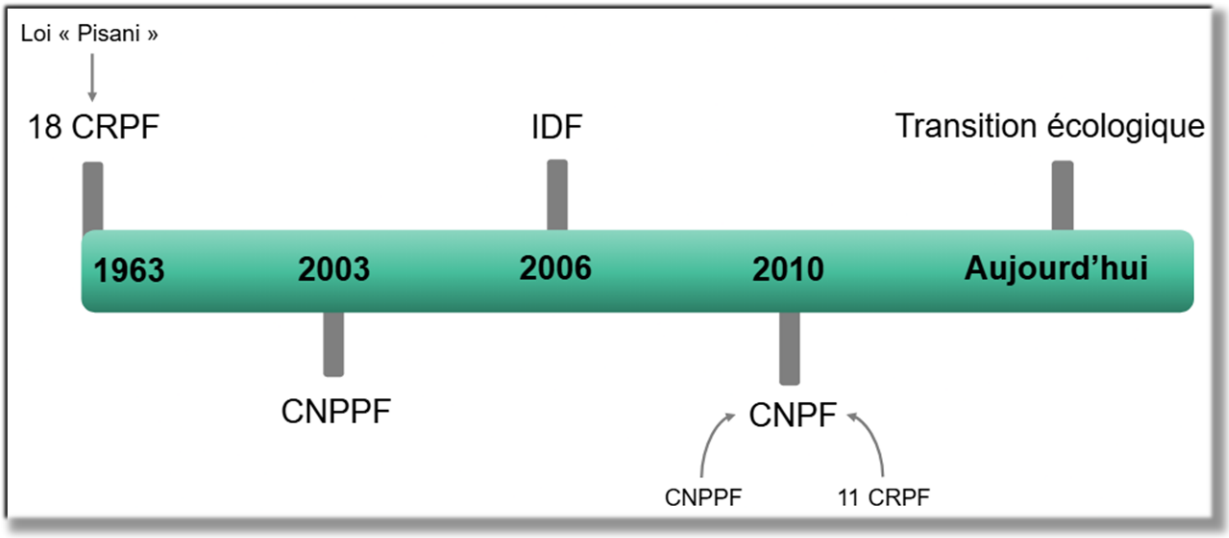


Figure 4 : Historique CNPF

C. Ses collaborateurs

Le Centre National de la Propriété Forestière **fait partie d'un large réseau forestier international et européen** et est donc en étroite **collaboration** avec différentes enseignes, parmi lesquels se retrouvent :

- **GIP ECOFOR** (Groupe d'intérêt public Ecosystèmes forestiers) : regroupe tous les organismes de recherche et de développement forestiers au niveau national.
- **EFI** (Institut forestier européen) : organisation internationale établie par les États européens qui mène des recherches et appuie les politiques sur les questions liées aux forêts.
- **FOREXT** (Réseau des organisations de vulgarisation forestière) : soutien ses organisations membres par le biais d'une collaboration internationale dans le renforcement de nouvelles capacités.

- **FRANSYLVA** (syndicat des propriétaires) : organisation représentant l'ensemble des propriétaires forestiers privés. Elle les informe, les défend et les représente.
- **CEPF** (Confédération européenne des propriétaires forestiers) : association regroupant toutes les organisations nationales de propriétaires forestiers en Europe.
- **FTP** (La plateforme technologique du secteur forestier) : plateforme technologique européenne dédiée au secteur forestier. C'est le lieu de rencontre pour l'industrie, les propriétaires forestiers et les pouvoirs publics.

- **AFORCE** (RMT) : réseau mixte technologique dédié à l'adaptation des forêts au changement climatiques.

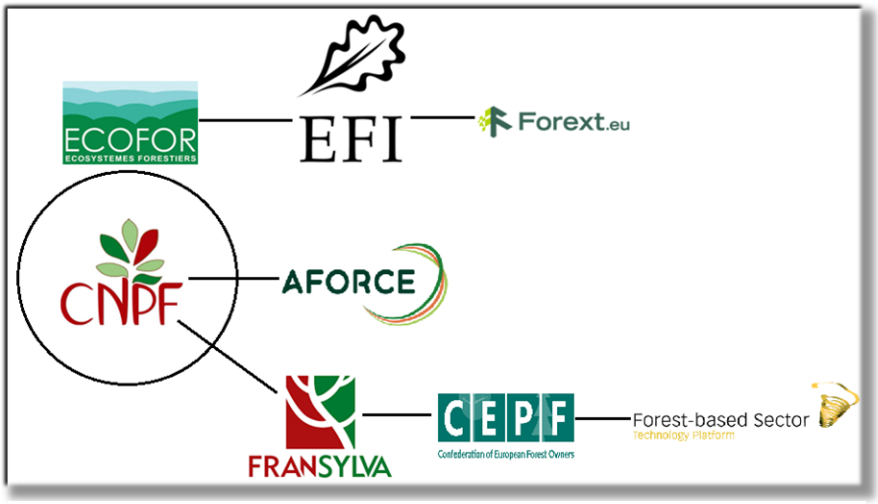


Figure 5 : Collaborateurs

D. Mon service

Le **Service du Développement Numérique** (SDN) du CNPF, principalement localisé sur le site d'Orléans, a pour mission d'assurer la **stabilité et la sécurité du système d'information**, tout en développant des solutions logicielles innovantes spécifiquement adaptées pour améliorer les opérations des forestiers à travers toute la France et leur fourni des outils permettant une gestion simplifier des terrains forestiers privées.

L'équipe du SDN est constituée de 16 personnes dont 3 prestataires et 4 alternants et se distingue par sa diversité de compétences, qui englobe notamment le développement logiciel ainsi que l'administration des systèmes et des réseaux. Cette variété de compétences permet au SDN de **répondre aux besoins et aux exigences des forestiers** de manière efficace.

Le SDN a pour mission principale de mettre en place et maintenir diverses solutions informatiques et techniques afin de **répondre aux besoins des quelques 450 agents** répartis sur les différents sites sur le territoire français. Par ce faire, le service reste à l'écoute des demandes et s'informe sur l'évolution du monde informatique en maintenant une infrastructure systèmes et réseaux à jour et en offrant des solutions toujours plus sécurisées.

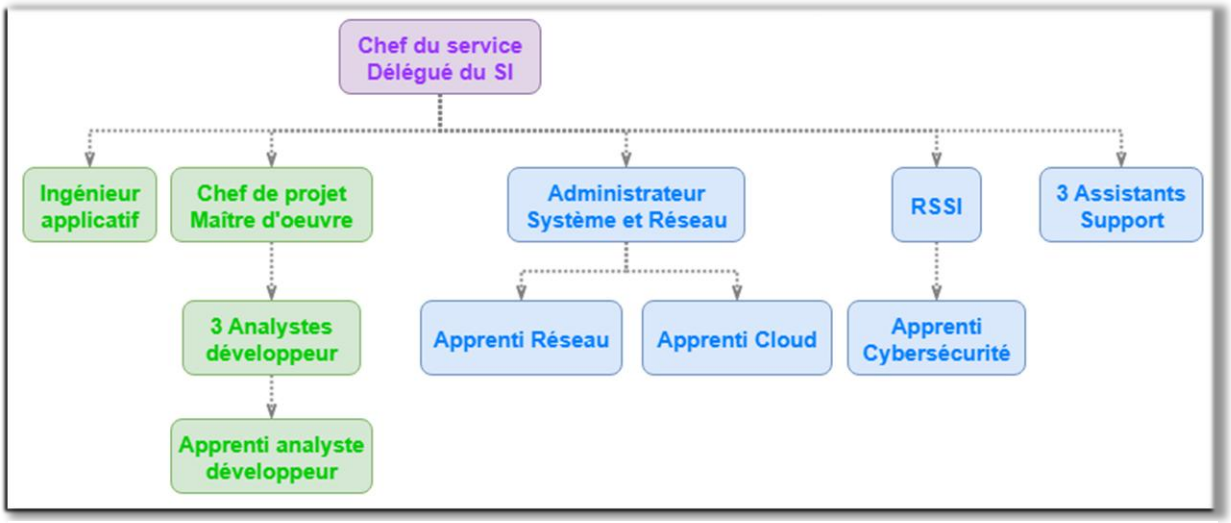


Figure 6 : Organigramme SDN

3. Projet

A. Contexte du projet

i. Problématique

La problématique majeure de notre contexte d'hébergement de notre environnement cloud actuel est d'ampleur **économique**, il vient s'ajouter à cela un besoin significatif de **mettre à niveau** ce dernier dû à un vieillissement et un manque de reconstitution de notre infrastructure cloud.

Du fait des circonstances de ces deux situations non négligeables par la Direction, il est impératif pour le SI de pallier ces problèmes en proposant à cette dernière une **solution fiable et économique**. Il est donc convenu de revoir l'entièreté de notre environnement cloud afin d'obtenir une plus-value en termes d'économie des coûts qu'engendre l'hébergement cloud au CNPF, mais aussi en termes de **structuration, d'optimisation et de sécurité** de ce dernier.

De ce fait, il convient donc de se demander « **Quelle(s) démarche(s) entreprendre afin d'optimiser l'hébergement de notre environnement cloud ?** » En cohérence avec le périmètre, les enjeux, ainsi que les besoins de notre contexte.

ii. Périmètre et enjeux

Au fur et à mesure que les solutions cloud se rapprochent toujours plus du **choix stratégique** au sein des systèmes d'information des organismes publics, leur déploiement ne se limite plus simplement qu'à des critères techniques ou économiques. Ce dernier s'inscrit désormais dans une forte **réflexion stratégique**, prenant en compte divers facteurs tels que la **souveraineté des données hébergées**, la conformité aux **exigences juridiques**, et la gestion des risques liés à une éventuelle **dépendance envers les fournisseurs** soumis à des législations étrangères.

L'adoption du **Cloud Act** (Clarifying Lawful Overseas Use of Data Act) aux États-Unis à partir de 2018 a profondément modifié la perception de la sécurité juridique des données hébergées sur des infrastructures cloud étrangères à la France. Cette législation permet aux autorités américaines de réclamer l'**accès à des données,** même lorsqu'elles sont stockées hors des États-Unis, dès lors qu'elles sont hébergées par une entreprise relevant du droit américain, telles que les grands leaders d'hébergement cloud des États-Unis comme AWS, Microsoft Azure ou Google Cloud.

Dans le cadre d'un organisme public tel que le CNPF, cette législation suscite des inquiétudes. L'établissement est responsable d'une **base cadastrale forestière** regroupant des **données personnelles sensibles** concernant plusieurs millions de propriétaires forestiers répartis sur le territoire France. Le simple risque que ces informations puissent, même simplement théoriquement, être accessibles par des autorités étrangères représente une **menace** importante pour la **souveraineté numérique** ainsi que la **protection des usagers** concernés.

Pour répondre à ces enjeux critiques, la notion de **cloud souverain** s'est progressivement imposée dans les stratégies des acteurs publics quant à l'hébergement de leurs données ainsi que de leur infrastructure cloud. Elle consiste à faire appel à des services d'hébergement capables de garantir une **protection de l'accès aux données** contre les législations

extraterritoriales, en assurant l'**hébergement des données sur le territoire européen**, par des entités bénéficiant du **droit local** et bénéficiant de **certifications reconnues** telles que SecNumCloud (ANSSI) ou le **label Cloud de Confiance**.

Des **alternatives françaises ou européennes**, telles que S3NS (Thales), Cloud Temple ou bien Cegedim, proposent aujourd'hui des **solutions compétitives**, bien qu'elles puissent être avancées sur les fonctionnalités proposées par leurs services que les offres des grands leaders du marché cloud, principalement américains. Le choix d'un fournisseur d'hébergement cloud ne doit donc pas se limiter à des critères techniques et fonctionnels, mais principalement s'inscrire dans la **gestion des risques juridiques et géopolitiques** quant au stockage et à l'accès aux données hébergées, tout en assurant une **conformité au RGPD**.

iii. Analyse du marché

En France, lorsqu'une **entité publique** (telle qu'une collectivité territoriale ou un établissement hospitalier) souhaite faire réaliser des travaux, obtenir des fournitures ou bénéficier de services (comme l'hébergement cloud), elle ne peut sélectionner librement la prestation d'une entreprise choisie. Elle est tenue de recourir à une procédure formalisée, le **marché public**.

Le marché public se définit comme un contrat conclu entre une entité publique et une entreprise privée, en vue de **répondre à un besoin précis** exprimé par le parti public. Ce contrat encadre la nature même de la prestation attendue (travaux, fournitures, services), les délais de cette dernière ainsi que les conditions budgétaires.

L'objectif premier du marché public est de garantir une **utilisation rigoureuse, transparente et équitable de l'argent public.** Cette utilisation implique la **mise en concurrence légitime** des différentes entreprises, de manière à permettre à l'entité publique une sélection basée sur des critères objectifs et dans le respect de l'**égalité de traitement**.

Dans le cas particulier des services numériques, et notamment dans notre contexte de type cloud computing (hébergement de données, hébergement de l'infrastructure réseau et système, virtualisation des serveurs, etc.), la **durée des marchés est généralement limitée à quatre ans**. Cette limitation permet de prendre en compte l'**évolution rapide des technologies** dans ce secteur, et de **favoriser une remise en concurrence** régulière.

iv. Services Cloud

Au fur et à mesure du développement des différentes technologies cloud, de **nouveaux modèles d'infrastructure hébergée** ont émergé, chacun d'entre eux répondant à des besoins et des exigences spécifiques exprimés par les entreprises demandeuses de prestations. Parmi ces modèles, on peut distinguer les suivants :

- **Le Cloud Public** s'appuie sur des infrastructures mutualisées, utilisées par plusieurs clients et gérées par les fournisseurs tiers. Ce modèle se distingue par sa flexibilité, sa capacité à évoluer rapidement et son mode de facturation basé sur la consommation, souvent avantageux pour les entreprises. Il est particulièrement utilisé pour des services standards, des environnements de test ou des outils collaboratifs. Toutefois, son mode de fonctionnement peut soulever des questions quant aux enjeux liés à la souveraineté des données hébergées, à la confidentialité et à la dépendance envers les fournisseurs.

- **Le Cloud Privé,** quant à lui, n'est réservé qu'à une seule organisation. Il offre un environnement isolé, mieux maîtrisé et généralement plus sécurisé que celui du cloud public. Il peut être hébergé sur site (on-premise) ou confié à un prestataire spécialisé. Ce type de cloud est conseillé d'être privilégié dans le cadre de traitement de données sensibles ou d'applications critiques, nécessitant une conformité aux politiques de sécurité internes à l'entreprise. Cependant, il implique des coûts plus élevés et une baisse de la flexibilité, en contrepartie d'un contrôle renforcé.

- **Le Cloud Hybride** combine les bénéfices des deux modèles précédents, public et privé. Il permet d'ajuster la répartition des charges de travail selon leur sensibilité ou leur criticité. Pour contextualiser, une organisation peut choisir d'héberger ses données sensibles dans un cloud privé, tout en exploitant le cloud public pour des services moins critiques et publics. Cette approche hybride offre une grande flexibilité, tout en assurant le respect des contraintes réglementaires et budgétaires. Néanmoins, cette dernière accroît considérablement le besoin de son infrastructure, accentuant la nécessité d'effectif et de fond afin d'assurer son maintien.

Dans le contexte des marchés publics, comme cité précédemment, les décisions en matière de cloud doivent se conformer au cadre réglementaire de ce dernier : **mise en concurrence équitable** via les appels d'offres, **limitation de la durée des contrats**, et **respect du RGPD**. L'adoption d'un **cloud de confiance**, **soutenu par l'État**, a pour objectif d'assurer un meilleur contrôle des données sensibles tout en limitant la dépendance des fournisseurs soumis à des législations étrangères et donc généralement non conformes au RGPD.

B. Organisation du projet

L'organisation est une composante nécessaire dans la **réflexion, l'étude et le développement** d'un projet, ici l'organisation de ce dernier nous permet de ne pas dériver de la ligne conductrice des besoins et des objectifs, d'assurer le **suivi** de ces derniers, de respecter les **dates limites** imposées, d'assurer la **communication** avec les parties prenantes et de respecter le **budget** mis en œuvre.

i. Pilotage

Les **indicateurs de suivi** sont un outil de gestion de projet qui permet de suivre l'avancement de différentes étapes clés du projet tout au long de ce dernier, tels que :

- **Suivi des coûts** des différentes ressources (matérielles/immatérielles et humaines) (pas de dépassement en fonction du budget établi en amont).
- **Suivi de l'avancement** des différentes étapes et respect des jalons (en fonction du planning Gantt établi en amont).
- **Contrôle des risques** (décharger l'avancement du projet des risques établis en amont).
- **Suivi de la disponibilité et de la communication** avec les acteurs clés du projet (disponibilité des acteurs clés, pas de prise de retard et mauvaises informations par manquement de communication).
- **Respect de la continuité et de la disponibilité des services et données** de l'environnement Cloud (continuité de la production, invisibilité de la migration pour les utilisateurs, etc).
- **Procédure de reprise** en cas d'incident(s)/problème(s) technique(s) (charge des responsabilités, contact avec le support des fournisseurs, etc).

Les **indicateurs de réussite/performance (KPI)** sont aussi un outil de gestion de projet qui permet d'assurer l'atteinte des objectifs définis en amont lors de la préparation de ce dernier, tels que :

- **Recette de tests complétée** (procédure de tests définis en amont).
- **Intégrité des données** (aucune perte de données, possibilité de sauvegarde et de restauration en cas de besoin).
- **Efficacité du trafic** interne cloud, et avec l'extérieur (pas de fluctuation du trafic réseau, débit généralement linéaire).
- **Satisfaction des acteurs clés** concernés par le maintien et la mise à niveau du SI (satisfaction de l'équipe IT, et de la direction et des utilisateurs).
- **Retour sur investissement (ROI)** (apport de gain budgétaire au long terme (sur 5 ans) en fonction du coût de la solution initiale et du prix de la mise en œuvre du projet) (ROI de plus de 50%, économie de minimum 500 000€ sur 5 ans).
- **Plus-value technique** (meilleure sécurisation de l'infrastructure, trafic rapide et continu, supervision et management de l'infrastructure cloud améliorés).

ii. Acteurs clés

Les acteurs clés détaillés ci-dessous représentent les **ressources humaines** rentrant en compte dans ce projet, que ces dernières soient **internes ou externes** à l'entreprise. Il est important de définir ces derniers afin d'assurer la **continuité de la communication** avec ces différentes parties prenantes et donc la **prise de contact et d'information** quant à ces différentes solutions envisagées.

Fonction	Nom	Type
Directeur Général		Interne
Directeur de l'Administration Financière		
Chef du Service du Numérique		
Responsable de la Sécurité du SI		
Administrateur Système et Réseau		
Apprenti Administrateur Cloud	Damien BERNOIS	
Apprenti Cybersécurité		
Responsable Secteur Public		Externe
Contact GCP		
Contact S3NS		
Contact Devoteam		
Contact Cegedim		
Contact Cloud Temple		

Tableau 1 : Acteurs clés

iii. RACI

La matrice RACI est un outil de gestion de projet qui nous permet ici de **définir et de visualiser les différentes parties prenantes** du projet et leurs **responsabilités** qui leur sont attribuées.

Étapes du projet \ Acteurs	DG	DAF	Chef SDN	RSSI	ASR	Apprenti Admin Cloud	Apprenti Cyber	Resp Secteur Pub	Contacts GCP	Contacts S3NS	Contacts Devoteam	Contacts Cegedim	Contacts Temple
Cartographie de l'existant			I	C	A	R	R						
Analyse des contraintes		A	R	C	C	R	I						
Analyse des risques			C	A	C	R	R						
Comparatif des solutions	A	C	R	R	R	R	R	C	C	C	C	C	C
Aménagement de l'existant			A	C	C	R	R						
Étude de la nouvelle infrastructure Cloud			A	C	R	R	R						
Rédaction du rapport de migration (procédures, tests, études)			A	C	C	R	R						
Conception de la nouvelle infrastructure Cloud			A	C	C	R	R						
Copie/Sauvegarde de l'environnement cloud AWS actuel			A	C	R	R	R						
Recette de migration			A	C	C	R	R						
Migration de l'infrastructure			A	C	R	R	R						
Résiliation des contrats avec AWS	A	R	R	C	C	I	I						
Cartographie du nouvel environnement Cloud			A	C	C	R	R						

Figure 7 : Matrice RACI

- **R** : La ou les partie(s) prenante(s) qui réalise(nt) la tâche (« Responsible »).
- **A** : La partie prenante qui approuve la tâche (« Accountable »).
- **C** : La ou les partie(s) prenante(s) qui est/sont consulté(s) pour son savoir d'expert dans le domaine de la tâche (« Consulted »).
- **I** : La ou les partie(s) prenante(s) qui est/sont informé(s) dans l'avancement de la tâche (« Informed »).

iv. Organigrammes des tâches (WBS)

La modélisation d'un organigramme des différentes tâches du projet est un outil de gestion de projet permettant de **visualiser chacune des tâches** du projet dans un ordre **hiérarchique et chronologique** en énumérant ces derniers. Cela nous permet d'avoir une carte des **étapes à suivre** afin d'assurer la finalité du projet.

La schématisation de l'ORGANIGRAMME DES TÂCHES est jointe en annexe.

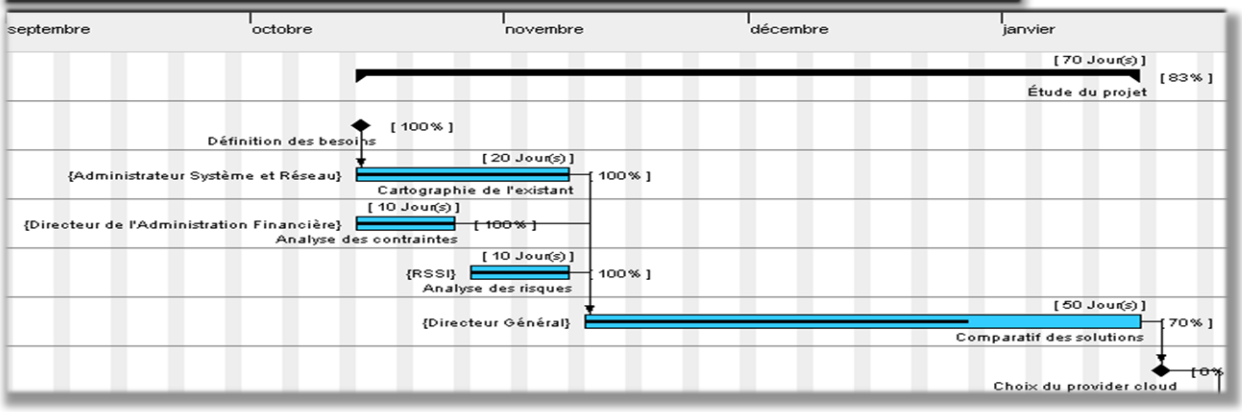
v. Plan organisationnel

L'**organisation et la structuration** des différentes étapes et jalons du projet est assurée à l'aide d'un plan organisationnel défini en amont du projet.

Un plan a initialement été mis en place, du fait des **changements décisifs soudains** quant à notre choix d'hébergement cloud comme détail précédemment dans la présentation des besoins, le plan ci-dessous s'est vu devenir **obsolète** et mis en pause étant donné que **l'étape du comparatif des solutions s'est éternisée**.

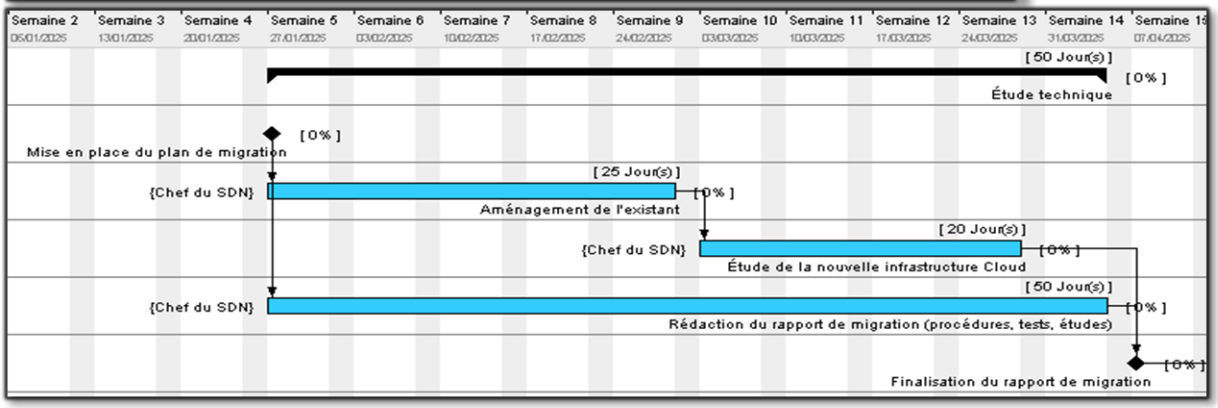
- Étude du projet :

Nom	Date de début	Date de fin
Étude du projet	14/10/2024	17/01/2025
Définition des besoins	14/10/2024	14/10/2024
Cartographie de l'existant	14/10/2024	08/11/2024
Analyse des contraintes	14/10/2024	25/10/2024
Analyse des risques	28/10/2024	08/11/2024
Comparatif des solutions	11/11/2024	17/01/2025
Choix du provider cloud	20/01/2025	20/01/2025



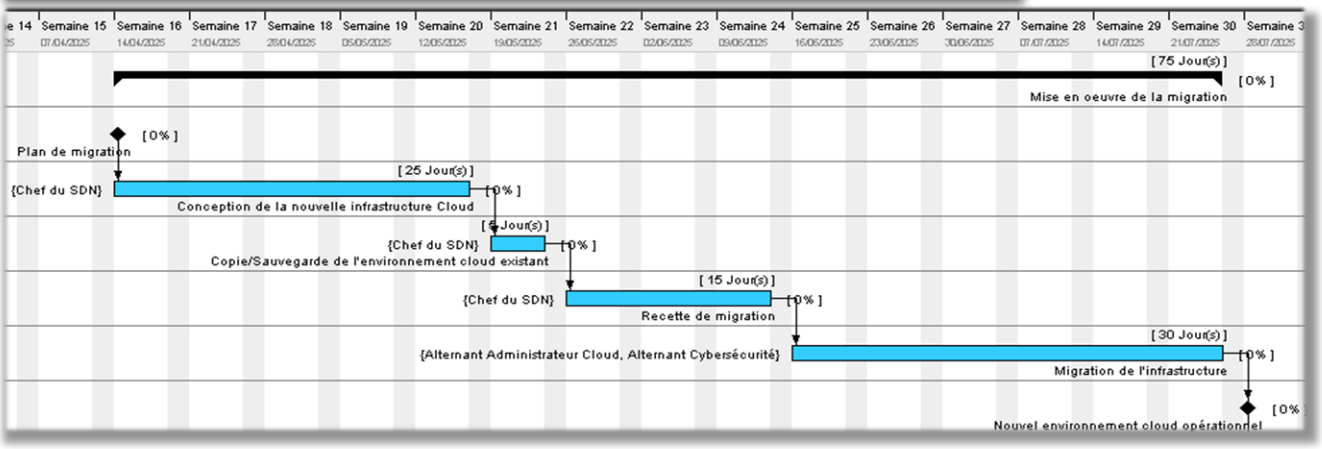
- Étude technique :

Nom	Date de début	Date de fin
Étude technique	27/01/2025	04/04/2025
Mise en place du plan de migration	27/01/2025	27/01/2025
Aménagement de l'existant	27/01/2025	28/02/2025
Étude de la nouvelle infrastructure Cloud	03/03/2025	28/03/2025
Rédaction du rapport de migration (procédures, tests, études)	27/01/2025	04/04/2025
Finalisation du rapport de migration	07/04/2025	07/04/2025



➢ Mise en œuvre de la migration :

Nom	Date de début	Date de fin
Mise en oeuvre de la migration	14/04/2025	25/07/2025
Plan de migration	14/04/2025	14/04/2025
Conception de la nouvelle infrastructure Cloud	14/04/2025	16/05/2025
Copie/Sauvegarde de l'environnement cloud existant	19/05/2025	23/05/2025
Recette de migration	26/05/2025	13/06/2025
Migration de l'infrastructure	16/06/2025	25/07/2025
Nouvel environnement cloud opérationnel	28/07/2025	28/07/2025



➢ Fin de projet :

Nom	Date de début	Date de fin
Fin du projet	28/07/2025	12/09/2025
Réunion avec la direction	28/07/2025	28/07/2025
Résiliation des contrats avec AWS	28/07/2025	12/09/2025
Cartographie du nouvel environnement Cloud	28/07/2025	29/08/2025
Finalisation du projet de migration cloud (technique et administratif)	15/09/2025	15/09/2025

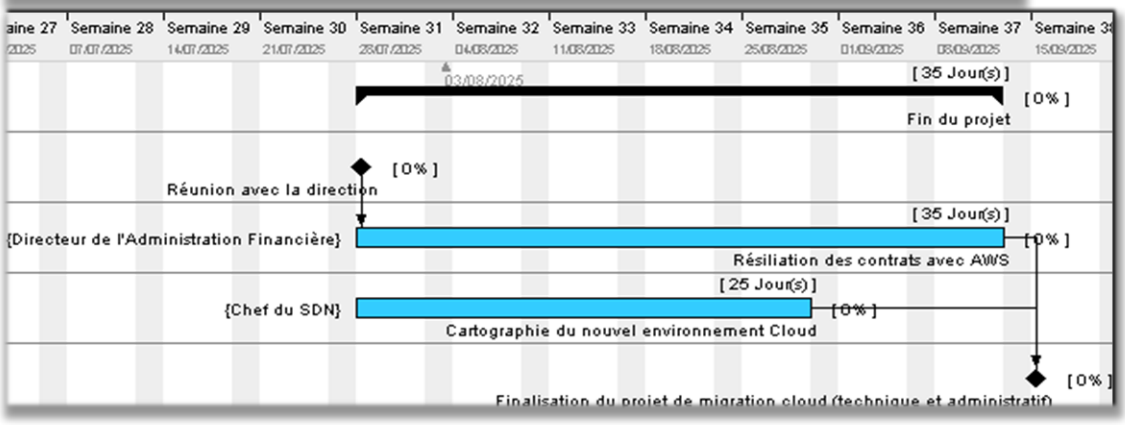


Figure 8 : Planning organisationnel

➢ Description du planning (modélisation des tâches) :

- Au-dessus : durée de la tâche (en jours).
- En-dessous : Nom de la tâche.
- À gauche : Responsable de la tâche (« Accountable » du RACI).
- À droite : Avancement de la tâche (en %).

vi. Communication

Les parties prenantes, qu'elles soient internes ou externes à l'entreprise, ont un **impact important** ou sont fortement **impactées** par ce projet, il est donc nécessaire de mettre en place une **stratégie de communication** afin d'assurer la **prise de contact, l'information** entre chacune des parties et l'**avancement** du projet.

Parties prenantes	Stratégie de communication	Support de communication	Personnes en charge de la communication	Délais
DG	Communication sur l'avancement	Rapport par mail	Chef du SDN, RSSI, ASR	1 semaine
DAF	Décision administrative	Rapport d'avancement		
Chef du SDN	Communication sur l'avancement Décision administrative Prise de contact avec les fournisseurs	Rapport par mail Rapport d'avancement Réunion avec l'équipe IT	RSSI, ASR, Apprentis	3 jours
RSSI	Questionnement technique		Chef du SDN, ASR, Apprentis	Quotidien
ASR	Communication sur l'avancement		Chef du SDN, RSSI, Apprentis	
Apprenti Admin Cloud	Prise de contact avec les fournisseurs		Chef du SDN, RSSI, ASR	
Apprenti Cybersécurité				
Responsable Secteur Public	Communication en cas de besoins	Prise de contact par mail Réunion avec l'équipe IT	Chef du SDN, RSSI, ASR, Apprentis	Sur demande
Contacts GCP				
Contacts S3NS				
Contacts Devoteam				
Contacts Cegedim				
Contacts Temple				

Figure 9 : Plan de communication

vii. Plan budgétaire

L'étude du budget quant à la mise en œuvre de ce projet comprend les **coûts de différentes ressources** telles que des **acteurs clés** (prestations, personnels internes, etc.), ainsi que des **coûts matériels ou immatériels**. De ce fait, il est nécessaire d'étudier le coût financier engendré par ce projet afin d'assurer un **suivi cohérent** et ne pas dépasser ce dernier.

- Coûts humains :

Personnel	PHT (€)	Durée	PTHT (€)
Chef du SDN	4 500	10	45 000
Direction de l'administration financière	6 500	10	65 000
Responsable de la sécurité du SI	4 000	10	40 000
Administrateur système et réseau	3 000	10	30 000
Apprenti administrateur cloud	1 000	10	10 000
Apprenti cybersécurité	1 000	10	10 000

Tableau 2 : Budget Humain

- Coûts des ressources :

Ressources (matérielles/immatérielles)	PHT (€)	Quantité	PTHT (€)
Crédit initial fourni par GCP pour la conception de l'infrastructure sur leur plateforme	5 000	1	5 000
Coût de l'hébergement Cloud sur AWS	~ 25 500	10	~ 255 000

Tableau 3 : Budget ressources

Le coût de l'hébergement Cloud sur AWS sera détaillé à la suite du mémoire dans l'analyse budgétaire.

Le coût total engendré sur par ce projet sur une durée de **10 mois**, comportant les coûts humains et les coûts de ressources, s'élève à environ **460 000 €.**

C. Étude de faisabilité

i. Analyse de l'existant

L'hébergement de notre environnement cloud actuel est assuré par la **plateforme d'AWS**. Cette dernière héberge aujourd'hui la majorité de notre infrastructure, dont la **totalité de nos serveurs et services** nécessaires au fonctionnement du CNPF (comprenant les applications métiers, les serveurs de fichiers, les serveurs d'administration, les environnements de production, de développement, de recette et de préproduction). Le choix de cette plateforme d'hébergement cloud est opéré par **l'UGAP – UGAP C3** à travers le marché public français.

Notre infrastructure était déployée sur l'ensemble du territoire français avec plus de 100 sites par l'intermédiaire de l'opérateur **CELESTE**. Toutefois, compte tenu de sa migration d'opérateur internet actuelle due à l'**appel d'offres** effectué par le **marché public UGAP** en **2022** (incluant l'opérateur **LINKT**), cette dernière se voit complexifiée temporairement.

Il est important de souligner que la **migration entre les 2 opérateurs** n'étant toujours pas finalisée, certains sites continuent de communiquer avec notre environnement cloud, de Céleste à LinkT, par **l'intermédiaire de notre pivot** sur le site Bourie (à Orléans). Il faut donc prendre en compte cette **contrainte technique** exceptionnelle et temporelle pour assurer la communication entre ces sites et le futur environnement Cloud.

- Schématisation de l'infrastructure globale de l'entité CNPF :

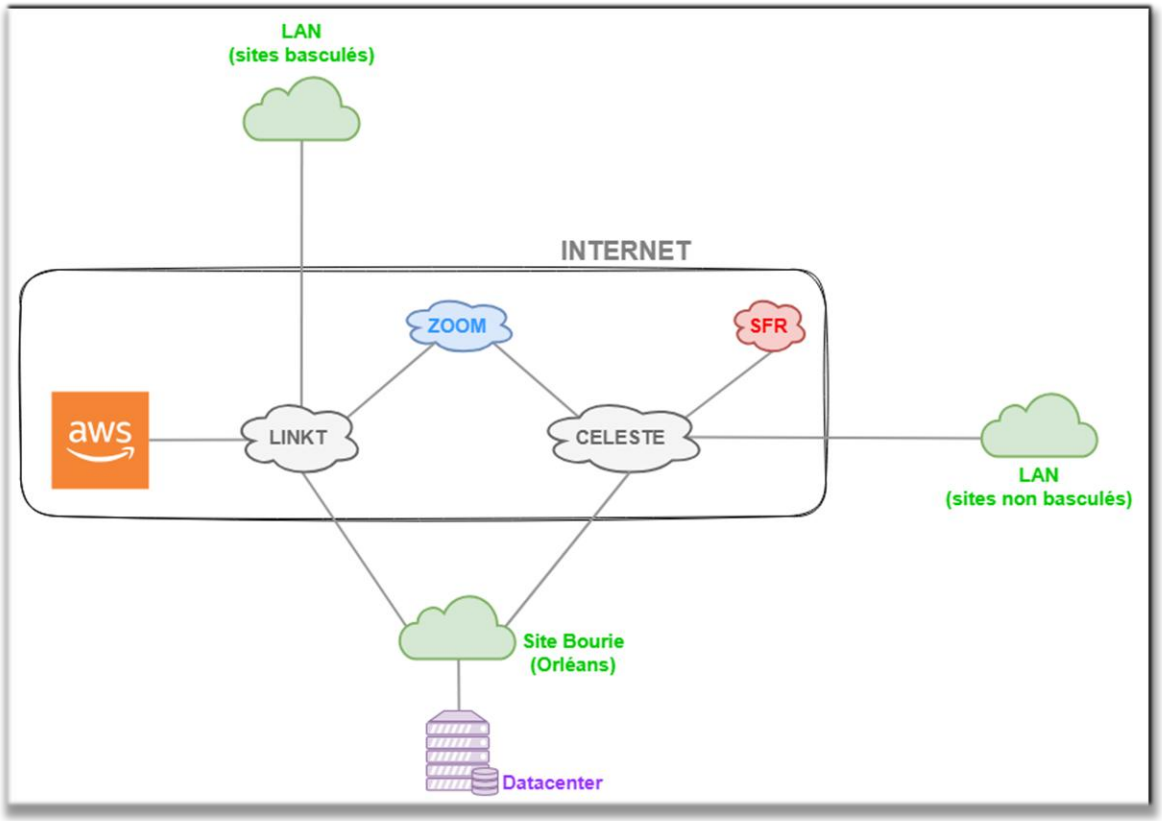


Figure 10 : Infrastructure globale CNPF

La totalité des serveurs de production sont virtualisés sur le modèle de la technologie **EC2** de l'opérateur et comptabilisent un total de 106 instances, parmi lesquelles se trouve 28 instances à l'arrêt (comprenant des instances pouvant être à nouveau relancées et d'autres n'étant que des instances temporaires qui ne seront plus exploitées par la suite) et 78 instances en cours d'exécution. Les agents du CNPF se connectent aux applications mis à disposition à travers le **portail d'authentification** ou en directe lors de service web dédié. La connexion entre le réseau privé s'effectue à travers une Fibre Optique qui se nomme **Direct Connect**, à travers l'**opérateur LinkT**, ce lien est configuré pour un débit de 100Mb/s.

- Schématisation de l'architecture de notre environnement cloud AWS :

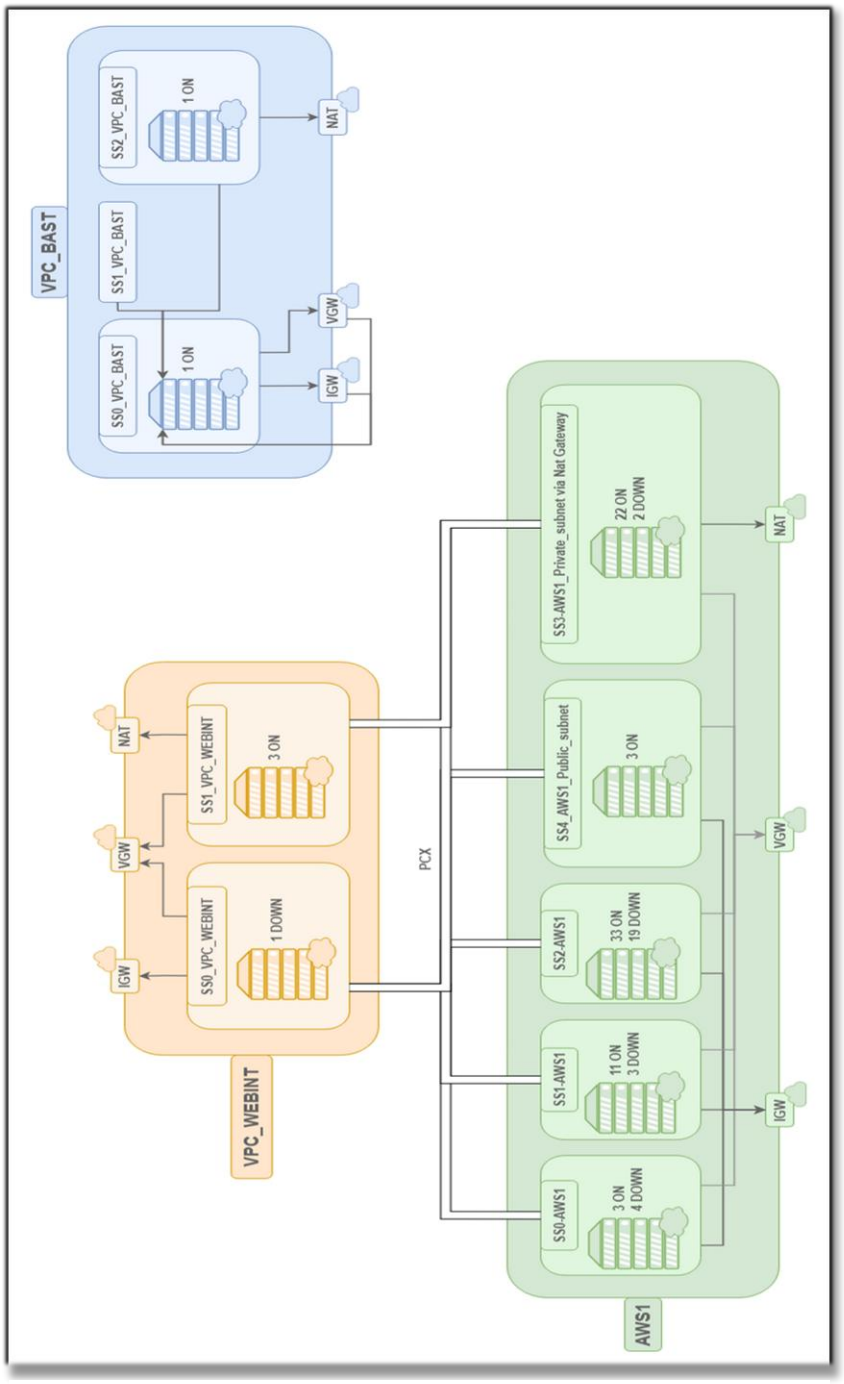


Figure 11 : Infrastructure AWS

Ces instances sont toutes hébergées sur le **datacenter de la région Europe/Paris**, eu-west-3. Chacune d'entre elles est hébergée sur le modèle de la technologie de stockage **S3** de l'opérateur, dans une des différentes **zones de disponibilité** suivantes, eu-west-3a, eu-west-3b et eu-west-3c. De plus, une sauvegarde des volumes de stockage rattachées à chacune de ces instances est effectuée sur la baie de sauvegarde **VEEAM** en local sur le site de la Bourie Rouge, à Orléans.

Le plan de sauvegarde actuel, défini entre l'**environnement Cloud AWS et notre baie de sauvegarde sur notre LAN**, sur le site de Bourie, n'étant **plus maintenu correctement**, étant peu optimal en termes d'**optimisation du trafic réseau** et ne sécurisant pas assez la disponibilité et l'intégrité des données, une analyse sur ce dernier sur le futur environnement Cloud est à étudier.

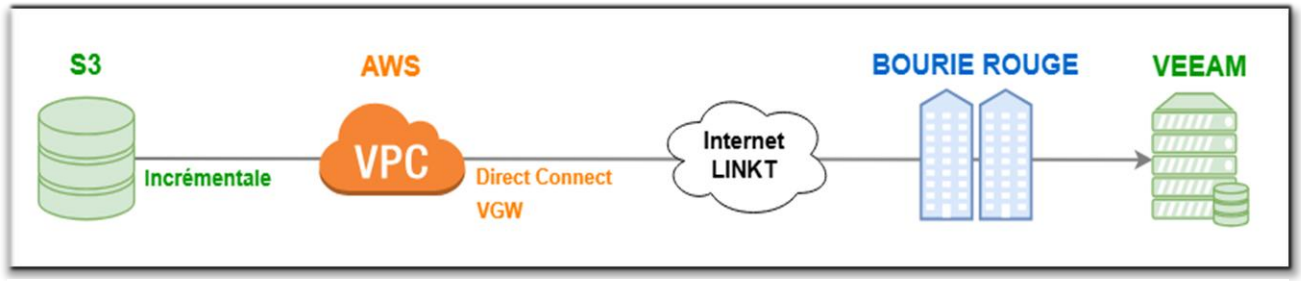


Figure 12 : Architecture de sauvegarde VEEAM

Notre infrastructure AWS héberge à ce jour **9 bases de données** à l'aide du service intégré d'AWS, RDS. Cette technologie permet le stockage des données de façon **rationnelle** (dans des tables) et est généralement exploitée avec des **bases de données SQL**. Ces dernières permettent la gestion rationnelle des données de différentes composantes de l'infrastructure telle que l'**application métier** « BioClimSol ».

La schématisation de la COMMUNICATION ET DEPENDANCE DES RDS est jointe en annexe à ce mémoire.

L'architecture sécurisée des serveurs, des applications et des données mise en place a pour vocation de suivre le **modèle ZTNA** (Zero Trust Network Access) proposé par le service Netskope mis en place sur l'infrastructure à l'aide du serveur **Publisher Netskope** se localisant sur AWS Cloud. Cette solution est une alternative au service **FortiClient VPN** mis en place pour le télétravail. FortiClient sera prochainement remplacé par Netskope à des fins de sécurité, et sera gardé comme solution de secours en cas de défaillance de la solution ZTNA futurement mise en place.

Il est donc nécessaire de **garder ce mode de fonctionnement** opératoire quant à la sécurisation des accès aux différentes ressources au sein de l'infrastructure, sur le nouvel environnement Cloud lors de la migration. La sécurité de cette dernière sera majoritairement construite autour de la **stratégie ZTNA**, sans pour autant en être **dépendante** et pouvant assurer une **reprise des services** en cas de dysfonctionnement de ce dernier ou bien en cas de **détachement** de ce mode de fonctionnement au sein de notre infrastructure.

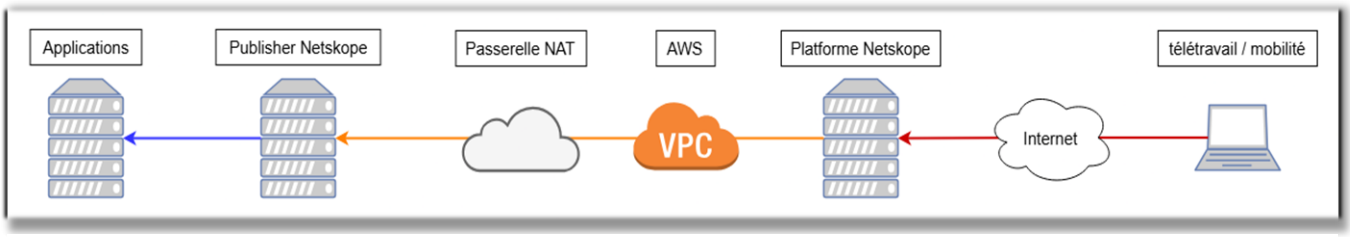


Figure 13 : Architecture de sécurité ZTNA

La rédaction d'une CARTOGRAPHIE des différentes ressources hébergées sur l'infrastructure cloud AWS est jointe en annexe.

ii. Analyse des risques du projet

L'étude des risques est une composante nécessaire à l'étude d'un projet afin de pouvoir identifier les points clés critiques de ce dernier.

Elle permet de définir en amont **les contraintes sur lesquelles le projet pourrait faiblir** lors de la mise en œuvre et pouvant éventuellement **engendrer des dérèglements dans l'organisation** du projet (délais, budgets, communication), ainsi que dans la disponibilité des informations mais aussi l'assurance de la mise en place conforme aux exigences de ce dernier.

- Énumération des risques :

Nom	Risque	Probabilité	Impact
R1	Perte de la continuité d'un ou plusieurs processus	Très Probable	Catastrophique
R2	Perte de données (mauvaise intégrité et disponibilité)	Très Probable	Catastrophique
R3	Discordance de processus dépendants entre eux (analyse AMDEC)	Très Probable	Catastrophique
R4	Manquement de sécurisation de la nouvelle infrastructure Cloud (cyberattaque)	Probable	Catastrophique
R5	Mauvaise communication avec le support du nouvel hébergeur Cloud (contrat, support, etc)	Possible	Majeur
R6	Mauvaise organisation du projet	Possible	Majeur
R7	Manquement de documentation, procédure et suivi manuscrit	Peu probable	Modéré

Tableau 4 : Définition des risques

- Matrice des risques :

Gravité / Probabilité	Improbable	Peu probable	Possible	Probable	Très probable
Négligeable					
Mineur					
Modéré		R7			
Majeur			R5 / R6		R3
Catastrophique				R4	R1 / R2

Tableau 5 : Matrice des risques

- Contrôle des risques :

Nom	Résolution
R1	Maintien de l'environnement Cloud initial (AWS) avant certitude de la bascule et vérification des mises en œuvre et recettes.
R2	Sauvegardes des instances et des volumes de stockage, image des instances, possibilité de backup toute perte de données ou défaillance importante.
R3	Schéma de flux réseau, étude de règles de communication, privatisation des réseaux, passerelles virtuelles privées, etc.
R4	Prise de contact régulière et rapide, contact technique et administratif, suivi du projet, possibilité d'accompagnement technique pour la mise en place, etc.
R5	Préparation du projet en amont avec la direction et l'équipe informatique (planning, budget, étape, recette, procédure, communication, etc.)
R6	Rédaction de procédure de déploiement et de tests, rédaction continue de mise en œuvre et des modifications.

Tableau 6 : Résolution des risques

iii. Analyse des risques des processus (AMDEC)

La méthode AMDEC (Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité) nous permet de **prévoir et de hiérarchiser** les éventuels risques d'un processus à l'aide d'une notation **d'échelles précises (fréquence, gravité, détection et criticité)**. En fonction des résultats obtenus et du contexte de chacun de ces risques, une **action corrective** peut être mise en place afin de corriger ces derniers en cas de sinistre.

Cette dernière assure la cartographie complète de l'entièreté de l'infrastructure cloud et est un élément essentiel à finaliser afin d'**assurer la migration** de chacun des processus cloud, mais aussi d'**assurer la continuité** de ces derniers post-migration.

Cette analyse n'étant pas finalisée pour la fin de ma période d'apprentissage, cette dernière devra être achevée avant la mise en œuvre de la migration. Cependant, certains processus ont déjà pu être définis comme ci-dessous :

- Descriptions :
  - Fréquence (1 à 10) : Probabilité d'apparition de la défaillance.
  - Gravité (1 à 10) : Impact de la défaillance sur le SI et ses utilisateurs.
  - Détection (1 à 10) : Taux de détection de la défaillance.
  - Criticité (1 à 30) : Somme des trois variantes précédentes définissant la criticité globale de ce risque.

- Référentiel :

Échelle de 1 à 10 (Fréquence / Gravité / Détection) :

1 à 2	3 à 4	5 à 6	7 à 8	9 à 10

- 1 à 2 : Minime et éventuellement négligeable.
- 3 à 4 : Léger et à surveiller régulièrement.
- 5 à 6 : Possible, à surveiller régulièrement et à maintenir.
- 7 à 8 : Très possible, à surveiller quotidiennement et à maintenir.
- 9 à 10 : Récurrent, à surveiller continuellement et à maintenir.

Échelle de 1 à 30 (Criticité) :

1 à 6	7 à 12	13 à 18	19 à 24	25 à 30

- 1 à 6 : Risque négligeable du processus.
- 7 à 12 : Risque mineur du processus.
- 13 à 18 : Risque modéré du processus.
- 19 à 24 : Risque majeur du processus.
- 25 à 30 : Risque critique du processus.

Description		Défaillance		
Élément	Fonction	Mode	Cause	Effet
CNPF-VIRTUALIA-APPLI	Serveur application "lourde" ERP + BDD	Surcharge de ressources	Non cohérence des ressources attribuées en fonction des besoins systèmes	Ralentissement des opérations
		Ralentissement de la communication avec le serveur	Ralentissement du trafic interne ou externe à l'hébergeur cloud	Lenteur de l'accessibilité au service et remontée des informations
		Obsolescence du système	Système non à jour	Risque potentiel de failles de cybersécurité / cyberattaques
		Indisponibilité des données	Défaillance de l'accès aux données	Services inutilisables et/ou non à jour

	Criticité				Résolution
Détection	Fréquence	Gravité	Détection	Criticité	Action corrective
Supervision et métrique / communication utilisateurs	4	3	3	10	Amélioration des ressources attribuées
Supervision et métrique / communication utilisateurs	2	4	3	9	Augmentation de la bande passante / révision du trafic avec les opérateurs
Supervision	3	9	8	20	Maintien à jour du système
Supervision et métrique / communication utilisateurs	1	9	2	12	Récupération des données à partir de VEEAM backup / réintégration des volumes

Figure 14 : AMDEC 1

Description		Défaillance		
Élément	Fonction	Mode	Cause	Effet
Portail-authentification-V2	Serveur d'authentification	Surcharge de ressources	Non cohérence des ressources attribuées en fonction des besoins systèmes	Ralentissement des opérations
		Ralentissement de la communication avec le serveur	Ralentissement du trafic interne ou externe à l'hébergeur cloud	Lenteur de l'accessibilité au service et remontée des informations
		Obsolescence du système	Système non à jour	Risque potentiel de failles de cybersécurité / cyberattaques
		Non communication avec un ou plusieurs services	Mauvaises règles de routage / mauvaise intégration réseau / mauvaises règles de filtrage	Non accès à un ou plusieurs services par le portail pour les utilisateurs

	Criticité				Résolution
Détection	Fréquence	Gravité	Détection	Criticité	Action corrective
Supervision et métrique / communication utilisateurs	4	3	3	10	Amélioration des ressources attribuées
Supervision et métrique / communication utilisateurs	2	4	3	9	Augmentation de la bande passante / révision du trafic avec les opérateurs
Supervision	3	9	8	20	Maintien à jour du système
Supervision et métrique / communication utilisateurs	2	9	7	18	Vérification individuelle de la communication avec le service non joignable

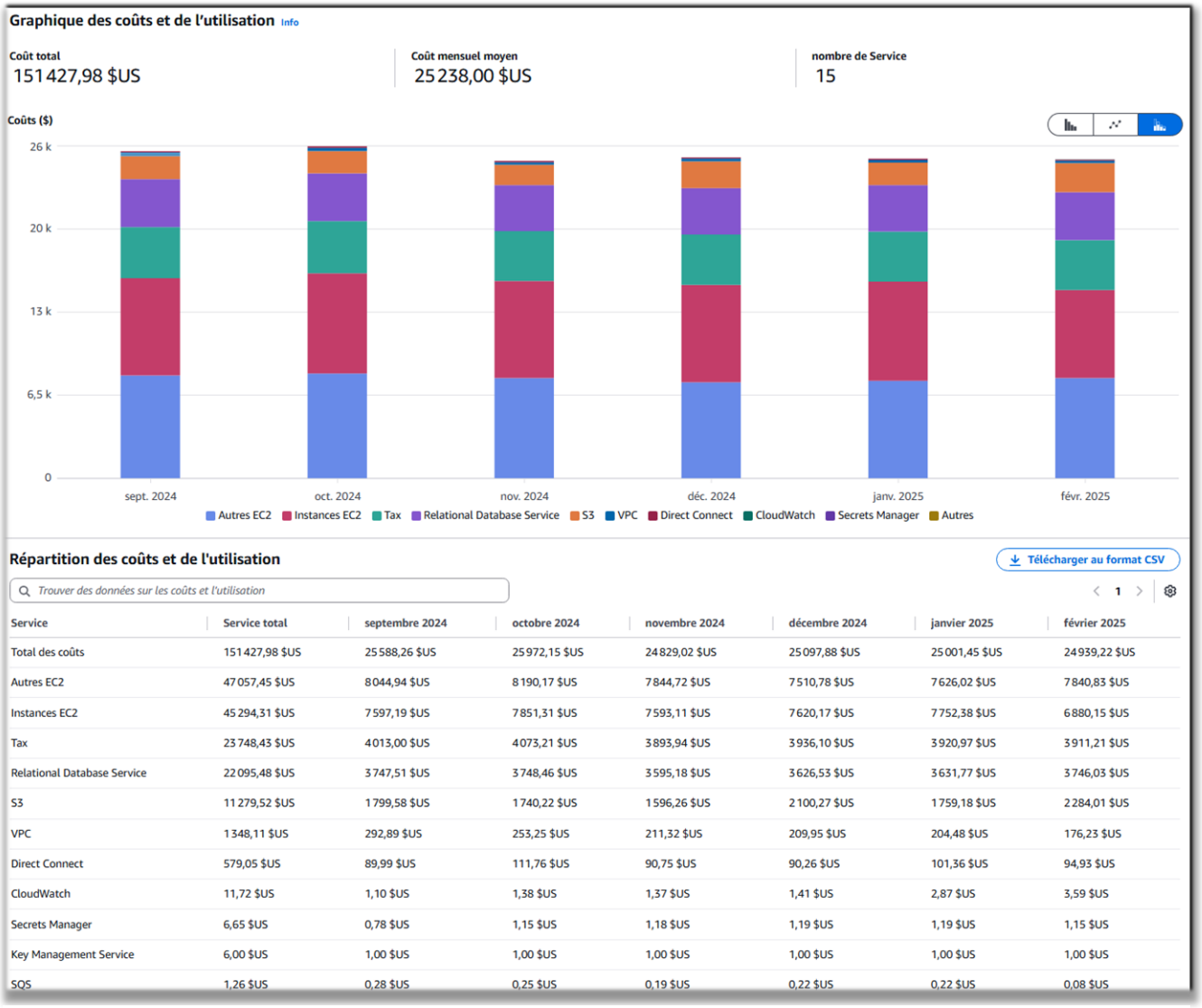
Figure 15 : AMDEC 2

iv. Analyse budgétaire

Du fait des coûts des différents **services utilisés**, de notre infrastructure réseau virtualisée au sein de cet hébergeur, du stockage stocker en interne, ainsi que du trafic sur le lien entre notre opérateur LinkT et notre environnement AWS, nous avons émis l'hypothèse d'une **future migration** de notre environnement cloud vers une autre plateforme virtuelle dans le but premier d'**assurer un environnement plus économique**, **plus clair et simple d'utilisation**, mais aussi en gardant un **suivi des coûts des services** ergonomique.

Dans ce cas, afin de pouvoir mettre en cohérence nos **besoins budgétaires, techniques et administratifs** auprès des différents opérateurs cloud retenus sur le **marché UGAP**, mais aussi afin de mettre en évidence les **points critiques** portant la **concordance** de ce projet, nous avons récupéré les coûts moyens engendrés par le maintien de notre infrastructure cloud AWS.

- Coût moyen de notre environnement cloud AWS :



Répartition des coûts et de l'utilisation

Télécharger au format CSV

Trouver des données sur les coûts et l'utilisation

Service	Service total	septembre 2024	octobre 2024	novembre 2024	décembre 2024	janvier 2025	février 2025
Total des coûts	151 427,98 $US	25 588,26 $US	25 972,15 $US	24 829,02 $US	25 097,88 $US	25 001,45 $US	24 939,22 $US
Autres EC2	47 057,45 $US	8 044,94 $US	8 190,17 $US	7 844,72 $US	7 510,78 $US	7 626,02 $US	7 840,83 $US
Instances EC2	45 294,31 $US	7 597,19 $US	7 851,31 $US	7 593,11 $US	7 620,17 $US	7 752,38 $US	6 880,15 $US
Tax	23 748,43 $US	4 013,00 $US	4 073,21 $US	3 893,94 $US	3 936,10 $US	3 920,97 $US	3 911,21 $US
Relational Database Service	22 095,48 $US	3 747,51 $US	3 748,46 $US	3 595,18 $US	3 626,53 $US	3 631,77 $US	3 746,03 $US
S3	11 279,52 $US	1 799,58 $US	1 740,22 $US	1 596,26 $US	2 100,27 $US	1 759,18 $US	2 284,01 $US
VPC	1 348,11 $US	292,89 $US	253,25 $US	211,32 $US	209,95 $US	204,48 $US	176,23 $US
Direct Connect	579,05 $US	89,99 $US	111,76 $US	90,75 $US	90,26 $US	101,36 $US	94,93 $US
CloudWatch	11,72 $US	1,10 $US	1,38 $US	1,37 $US	1,41 $US	2,87 $US	3,59 $US
Secrets Manager	6,65 $US	0,78 $US	1,15 $US	1,18 $US	1,19 $US	1,19 $US	1,15 $US
Key Management Service	6,00 $US	1,00 $US	1,00 $US	1,00 $US	1,00 $US	1,00 $US	1,00 $US
SQS	1,26 $US	0,28 $US	0,25 $US	0,19 $US	0,22 $US	0,22 $US	0,08 $US

Figure 16 : Coût moyen AWS

D'après la lecteur de ce graphique, les services majeurs qui engendrent, au CNPF, la majorité des coûts de son environnement cloud AWS sont celui de l'hébergement des **volumes de stockage (S3 et RDS)**, de l'hébergement de nos **instances (EC2),** ainsi que la **TAXE** financière (du fait de **l'emplacement géographique** des datacenters, ainsi que des règlements locaux (**TVA**)).

La rédaction d'un RÉCAPITULATIF DES COÛTS ENGENDRÉS par chacune des ressources AWS est jointe en annexe.

L'objectif majeur, à long terme, dans le cadre de notre besoin principal d'une **optimisation économique et d'un amoindrissement des coûts financiers** qu'engendre le maintien de notre environnement Cloud, serait comme l'indiquera le pilotage du projet à la suite de ce mémoire (Retour sur investissements du projet de migration), de tendre, à minima, vers un **gain de 50% du coût de l'hébergement de notre environnement cloud** comparé à l'actuel. Et cela tout en garantissant **l'intégrité, la sécurité et la confidentialité de nos données** hébergées sur un environnement Cloud strictement français, **certifié** par les autorités de la cybersécurité et de la protection des données (ANSSI, CNIL, etc.) et **ne faisant pas l'objet de la loi américaine du Cloud Act** applicable sur les services d'enseignes américaines hébergés sur d'autres continents.

v. Analyse des contraintes

L'analyse des contraintes est une composante tout aussi importante que celle des risques dans la **réflexion de la faisabilité** d'un projet. Ici notre analyse des contraintes se divisera en **6 domaines** (coûts, risques, ressources, portée, qualité et délais).

- Coûts : Objectifs de ROI ≥ 50% du coût de l'environnement cloud existant.
- Risques : Matrice de risques du projet défini précédemment.
- Ressources : Difficulté de la prise de contact avec les fournisseurs et le support cloud, acteurs clés, accès aux environnements cloud limité pour des démonstrations.
- Portée : Hébergement des données et de l'infrastructure sur un environnement nécessitant la certification en termes de protection des données (ANSSI et CNIL), pas d'obligation de transparence au Cloud Act.
- Qualité : Faible connaissance des nouveaux environnements cloud, nouvelles technologies et intitulés, étude d'une infrastructure cloud de zéro. Nécessité de la disponibilité, l'intégrité, l'efficacité, la sécurité, la documentation et la connaissance de la mise en place de la nouvelle infrastructure.
- Délais : Possibilité de décalage des dates clés, retard et non-respect de l'organisation du projet dû à un manque de communication.

➢ Triangle QCD :

Le triangle QCD permet d'analyser les **3 contraintes** primaires du projet (**Qualité, Coût, Délai**), ce dernier permet de trouver un juste **équilibre** entre ces 3 variables en fonction des besoins énoncés par l'entreprise quant à la mise en œuvre de ce projet.

En prenant en compte que le projet s'est vu être **retardé** dû à la variation des enjeux politiques et économiques avec les États-Unis, **2 solutions** sont définies ci-dessous.

La première étant celle initialement prévue, représentée par le plan organisationnel caractérisé précédemment dans la gestion de projet, cette dernière s'est vue **devenir obsolète** à la suite de cela et remplacer par un **second plan exhaustif** à la suite d'une décision de la direction quant à la transparence de la confidentialité de nos données due à la législation du Cloud Act, ainsi que de l'instabilité du marché des services américains avec le reste du monde.

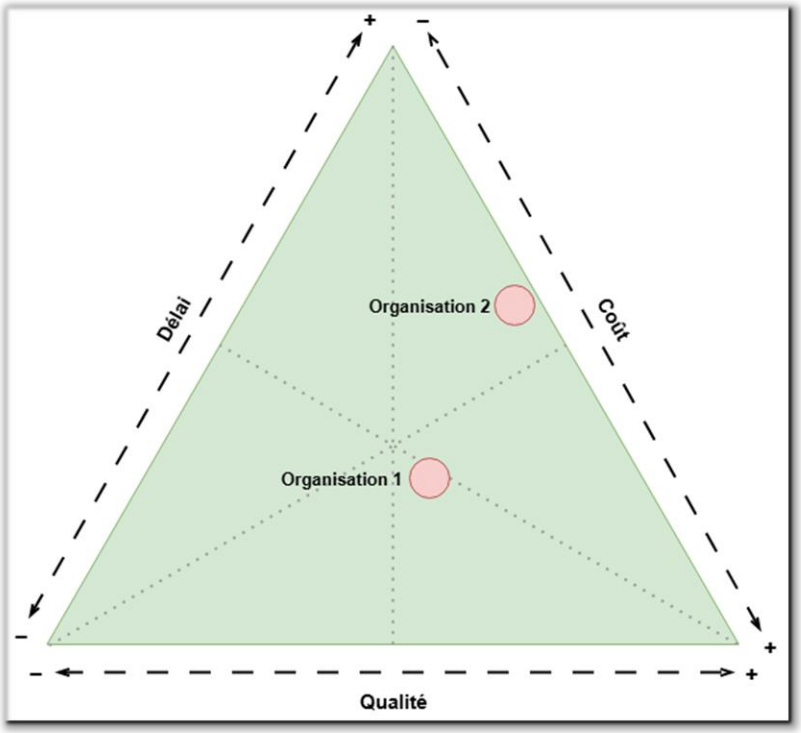


Figure 17 : Triangle QCD

➢ Organisation 1 :

Le point « Organisation 1» représente la solution initiale, c'est-à-dire la migration vers l'environnement cloud Google GCP en s'appuyant sur le planning organisationnel détaillé ci-dessus.

➢ Organisation 2 :

Le point « Organisation 2» quant à lui représente la solution actuelle, c'est-à-dire la possible migration vers l'environnement cloud Cegedim en s'appuyant sur le planning initial retardé.

Afin de pouvoir s'assurer de la **faisabilité du projet** et ne pas être pris au dépourvu par de potentielles contraintes qui engendreraient un dysfonctionnement de l'organisation du projet, il est nécessaire de s'assurer que le projet de migration est **S.M.A.R.T** (Spécifique, Mesurable, Atteignable, Relevant et Temporel) en se basant sur les différentes étapes du plan d'organisation du projet.

Objectifs	S.M.A.R.T
Étude du projet	Planifier, étudier et structurer les étapes et objectifs du projet, étudier les solutions cloud.
	Etudes de faisabilité, réunions, contact avec les fournisseurs.
	Mise en accord sur le choix du provider cloud.
	Outils de gestion, planning, budget, ressources, contact avec les fournisseurs disponibles.
	Du 14/10/2024 au 20/01/2025, 3 mois et 6 jours.
Étude technique	Étude, structure et rédaction post-migration.
	Analyse technique, missions intermédiaires afin d'assurer la migration.
	Missions intermédiaires finalisées, plan de procédure de la migration clair.
	Équipe informée, documentations, outils et accès disponibles.
	Du 27/01/2025 au 07/04/2025, 2 mois et 11 jours.
Déploiement de la migration	Migration de l'infrastructure, reprise possible en cas de dysfonctionnement.
	Étapes du plan de migration procédural, avancement %, plan de recette.
	Tests réalisés, communication, dépendance, trafic, intégrité fonctionnels, plan de migration finalisé.
	Accès à la plateforme, contact avec le support, suivi, environnement de test.
	Du 14/04/2025 au 28/07/2025, 3 mois et 14 jours.
Fin du projet	Clôture de la migration, environnement cloud fonctionnel, clôture des contrats avec AWS.
	Plan de migration finalisé, résiliation des contrats avec AWS, nouvel « abonnement » avec le nouveau provider cloud.
	Finalisation du projet, réunion avec la direction, plan de migration complet, nouvelle infrastructure cloud, nouveau contrat cloud, résiliation des contrats avec AWS.
	Accès à la plateforme, contact avec les fournisseurs.
	Du 28/07/2025 au 15/09/2025, 1 mois et 18 jours.

Tableau 7 : S.M.A.R.T

- S (Spécifique) : Définition pragmatique et précis des objectifs.
- M (Mesurable) : Avancement mesurable.
- A (Atteignable) : Objectifs réalisables.
- R (Réaliste) : Objectifs réalisables à l'aide des ressources à disposition.
- T (Temporel) : Situé et organisé dans le temps.

vi. Comparatif des solutions

Le **choix des solutions cloud** est l'étape clé principale à la mise en œuvre de ce projet, en effet, il est primordial d'**analyser** chacune des solutions à disposition sur le **marché public UGAP** sur lequel notre enseigne publique doit s'appuyer afin de souscrire à un contrat avec une entreprise fournissant un service bien précis pour précis précédemment dans l'analyse du marché public.

L'analyse de ces solutions sera fondée sur le **développement de 8 points** quant à l'hébergement d'une infrastructure telle que celle du CNPF sur un environnement Cloud. Le développement de ces points permettra **d'assurer le choix cohérent du nouvel hébergeur Cloud** en fonction des besoins exprimés précédemment.

Afin que le comparatif des solutions soit le plus **cohérent** possible en fonction des besoins et couvre le plus de points quant à **la sécurité, les certifications et la législation de l'hébergement des données, les coûts, les fonctionnalités et l'environnement, et le support** de l'environnement cloud cible. Pour ce faire, une étude structurée des différentes **documentations, forums**, etc. sur les différentes solutions cloud est nécessaire afin de s'assurer de couvrir tous les points précisés précédemment et ne pas négliger **l'importance de la migration** de notre infrastructure cloud.

La solution cloud actuelle (AWS) sera comparée avec les 3 solutions cloud du marché public UGAP envisagées, telles que :

Référence	AWS	GCP (S3NS)	Cloud Temple	Cegedim
Données	Accès API chiffrées (Nitro, HSM, KMS) Datacenter à Paris (3 zones de disponibilité)	Chiffrement HSM des clés par S3NS Thales, cryptage du transit Télémetrie partagée avec Google Séparées physiquement et logiquement des data centers GCP. Contrôle locaux Accès au code source non garanti (souveraineté potentiellement partielle)	Chiffrement HSM, traçabilité ANSSI Connectivité avec AWS et Azure Hébergement 100% français, Telehouse 3 à Magny-les-Hameaux	

Certifications	Certifié ISO 27001/17/18, PCI-DSS, SOC 1/2/3, HIPAA/HITECH, Cloud C5 (BSI) Conformes RGPD (DPA, SLA, code CISPE)	Cloud de confiance SecNumCloud 3.2 PCI-DSS, ISO 27001	SecnumCloud 3.2 cloud de confiance, RGPD (SLA) ISO 27001, ISO 9001, 14001, 50001, PCI-DSS	SecNumCloud 3.2 en IaaS, PaaS en cours 100% français, ISO 27001/17/18, 20000, 50000/1, ISAE 3402 type 2 Contrat orienter Cloud Souverain
Législation	Soumis Cloud Act/FISA Possibilité de ESC (European Sovereign Cloud)	Serveurs propriété de Thales, différenciation avec Cloud Act		
Coûts	A l'usage Suivi des coûts Outils d'optimisation et de support (Cost Explorer, Savings Plans, etc)	A l'usage Offre trop récente, pas de de grille tarifaire	A l'usage Suivi des coûts Engagement minimum de 1 mois	A l'usage, offre sur mesure Pas de grille tarifaire
Fonctionnalité et environnement	IaaS, PaaS, SaaS (EC2, S3, RDS, DynamoDB, Lambda, etc) IaC (Terraform, CloudFormation, etc) Marketplace mondial Hybride/multi-cloud possible (Terraform, MSP, etc) IA, ML, DevOps, R&D, intégration continue, etc	IaaS, PaaS (Compute, BigQuery, Vertex AI) Intégrateurs (SFEIR, agence du numérique en santé, etc)	IaaS, PaaS, Bare-Metal, IaaS opensource Hybride, multi-cloud Intégrateurs (Capgemini, Thales, CGI, etc) Marketplace Européen Datacenter ecoresponsable (PUE < 1,3 et WUE ~= 0, neutralité carbone pour 2026)	IaaS, Paas, CaaS (Container as a service) (Kubernetes, SentinelOne géré 24/7 via SOC) Orienté santé, finance, spatial, secteur public Engagement réduction consommation et émissions

	Initiative RSE (énergie renouvelable et efficace)			
Support	Support français 24/7 disponible pour les Business plans (différentes niveaux)	Support français 24/7 avec S3NS et Google Sécurisation gérée par Thales (SOC 1,2,3, supervision, contrôle cryptographique, validation mises à jour, etc)	Support français 24/7, SOC, EDR, patching bastion, scans de vulnéravilité, SecOps, service Desk, etc Support GenAI, APIs REST, Terraform, Openshift (Red Hat)	Support français 24/7 (SOC, EDR, patching, monitoring, scans de vulnérabilités) CaaS managés

Tableau 8 : Comparatif Cloud

D. Mission

La **roue de Deming** (méthode PDCA (Planifier, Déployer, Contrôler, Agir)) nous permet **d'assurer la faisabilité** des différentes missions internes à ce projet de façon **cyclique**, mais aussi de viser à **améliorer en continu la qualité et l'efficacité** des différentes étapes. Cette dernière s'intègre dans notre contexte de projet, étant donné que ce dernier est instable, puisqu'elle permet de créer des « **points de contrôles** » entre chaque étape afin de s'assurer que ce dernier ne puisse reculer.

Le projet ne pouvant être finalisé pour la date du rendu du mémoire et de la soutenance, ce dernier s'est vu être **partiellement compléter** sur ma période d'apprentissage. J'ai pu travailler majoritairement sur **l'analyse, l'étude, l'organisation et la phase de préparation de la migration**. De ce fait, les missions définis ci-après sont celles sur lesquels j'ai pu étudier, réaliser, documentation et présenter.

i. Unification de l'infrastructure Cloud

- Planifier :

À la suite d'une analyse et cartographie de l'entièreté de notre infrastructure Cloud et afin de préparer tous les éléments et mises en place nécessaires à la migration de cette dernière, il a premièrement été convenu de rationaliser et de centraliser notre infrastructure existante vers le réseau « AWS1 » afin de libérer le maximum de **plage d'adresses IP** pour la conception de la **nouvelle infrastructure**.

Plage d'adresses utilisées initialement :

Réseau	Réseau	CIDR	Plage
VPC_BAST	172.20.0.0	/20	172.20.0.1 - 172.20.15.254
VPC_WEBINT	172.20.16.0	/20	172.20.16.1 - 172.20.31.254
VPC_SHAREINT	172.20.32.0	/20	172.20.32.1 - 172.20.47.254
VPC_WAM	172.20.48.0	/20	172.20.48.1 - 172.20.63.254
AWS1	172.31.0.0	/16	172.31.0.1 - 172.31.254.254

Tableau 9 : Réseau IP AWS

Plage d'adresses utilisables :

- 172.16.0.0 /16 => 172.19.0.0 /16
- 172.21.0.0 /16 => 172.30.0.0 /16

Plage d'adresses non utilisables :

- 172.20.0.0 /16
- 172.31.0.0 /16 (« AWS1 »)

➢ Déployer :

- « VPC_SHAREINT » et « VPC_WAM » :

Ces deux VPC ne faisant plus l'objet d'un hébergement d'instances en cours d'exécution, ces derniers peuvent facilement être supprimés.

- « VPC_BAST » et « VPC_WEBINT » :

Ces deux autres VPC font l'objet d'un hébergement d'instances en cours d'exécution, **ne pouvant donc pas simplement supprimer** les VPC comme précédemment, il est nécessaire de mettre en place une **procédure de migration interne, entre les VPC**, sur notre compte d'hébergement AWS.

➢ Contrôler :

Une PROCÉDURE DE MIGRATION DES INSTANCES EN INTERNE a été mise en place afin d'assurer la migration des instances vers le réseau principal « AWS1 ».

Cette procédure a **premièrement été testée sur un réseau provisoire** avec une instance non critique provisoire afin de s'assurer de la conformité de cette dernière.

➢ Agir :

La procédure étant opérationnelle, il convient maintenant de mettre en œuvre cette dernière afin d'assurer la bonne migration des instances dans le contexte de nos réseaux « VPC_BAST » et « VPC_WEBINT ».

À la suite de la mise en œuvre de cette dernière, les plages d'adresses suivantes ont été libérées :

- 172.20.0.0 /20 (« VPC_BAST »)
- 172.20.16.0 /20 (« VPC_WEBINT »)
- 172.20.32.0 /20 (« VPC_SHAREINT »)
- 172.20.48.0 /20 (« VPC_WAM »)

Plage d'adresses utilisables :

- 172.16.0.0 /16 => 172.30.0.0 /16

Plage d'adresses non utilisables :

- 172.31.0.0 /16 (« AWS1 »)

Nouvelle infrastructure AWS avant la migration du provider Cloud :

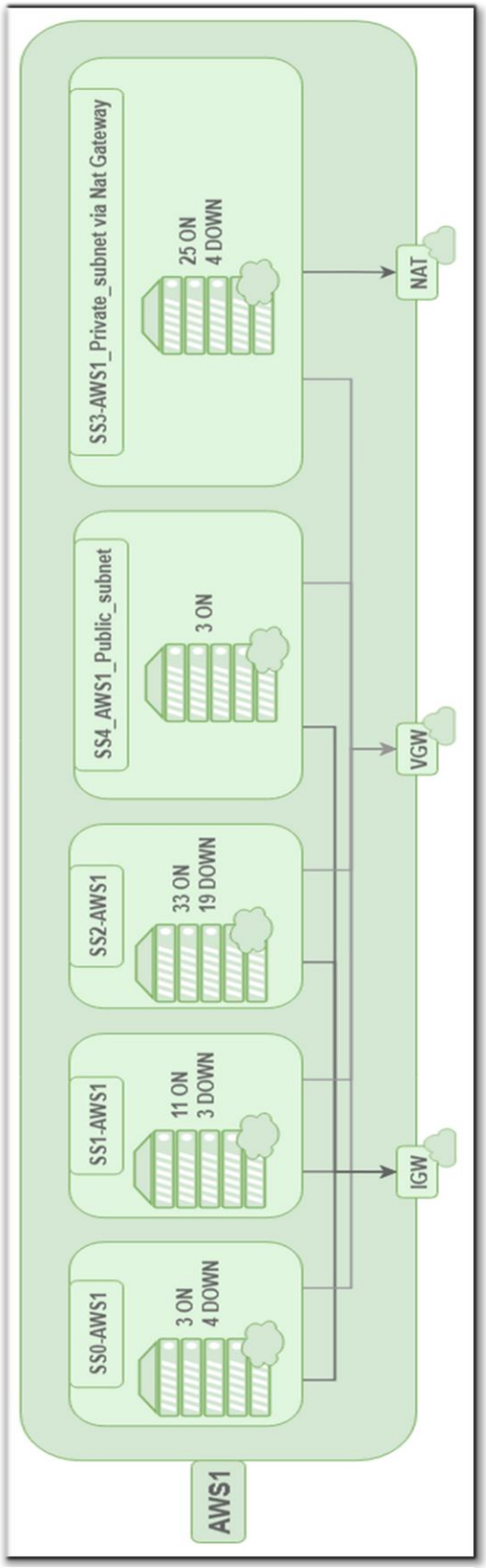


Figure 18 : Infrastructure AWS centralisée

ii. Optimisation de l'existant

- Planifier :

Ensuite, dû au retard engendré par **l'incertitude du nouvel hébergeur cloud cible**, afin d'assurer un **gain économique au plus tôt** sans pour autant avoir migré d'infrastructure, il a été convenu de mettre en place une **optimisation du coût de maintien des instance**s à l'aide d'un script de **gestion des horaires** de ces dernières à l'aide des services internes à l'environnement AWS.

- Déployer :

Pour ce faire, les fonctionnalités AWS « Lambda » et « EventBridge » à disposition des clients peuvent assurer la mise en place de ce script et l'application **récurrente** de ce dernier afin d'assurer une **gestion continue, autonome et dynamique** des instances à tout moment de la journée, sans la nécessité d'une intervention humaine. De plus, un **suivi des logs** avec une rétention de 14 jours est assuré en cas de sinistre ou de dysfonctionnement.

La rédaction d'une ÉTUDE DE L'OPTIMISATION DES COÛTS de notre infrastructure AWS actuelle est jointe en annexe.

- Contrôler :

Cette procédure a **premièrement été testée sur des instances provisoires** afin de s'assurer de la conformité de cette dernière.

Le suivi des logs obtenus après la mise en test du script Lambda, ainsi que du planificateur EventBridge, assure le bon fonctionnement de cette procédure, pouvant être mise en production sur l'entièreté de l'infrastructure cloud.

- Agir :

La mise en œuvre de ce script d'optimisation des coûts par la gestion des horaires des instances permet de réduire le coût mensuel du maintien des instances d'environ 2 586€.

Cela assure premièrement un **gain économique** sur la facture engendrée par l'environnement AWS (répondant principalement au besoin d'économie exprimé par l'entreprise), mais aussi un gain en termes de **gestion de l'infrastructure, des accès, ainsi que de la sécurité** (empêchant les cyberattaques sur des horaires nocturnes).

iii. Modélisation de la nouvelle infrastructure

- Planifier :

Afin d'assurer la faisabilité de la conception de la nouvelle infrastructure cloud sur le nouvel hébergeur, il est important de concevoir une **schématisation complète du plan de construction** de cette dernière afin de ne négliger aucun point réseau, **d'assurer le trafic et la sécurité** de l'environnement cloud.

Étant donné que notre première infrastructure a été conçue sans prendre en compte ces détails, elle s'est vite retrouvée obsolète, peu sécurisée, très coûteuse et peu structurée. Le CNPF voulant une infrastructure **robuste, ergonomique et optimisée**, la schématisation de cette dernière nous permettra de nous **délester de ces risques**.

- Déployer et Contrôler :

La schématisation de la nouvelle infrastructure s'appuiera essentiellement sur la cartographie effectuée précédemment afin de couvrir tous les **points sensibles** et résoudre chacune des contraintes et des risques de l'ancienne infrastructure.

- Agir :

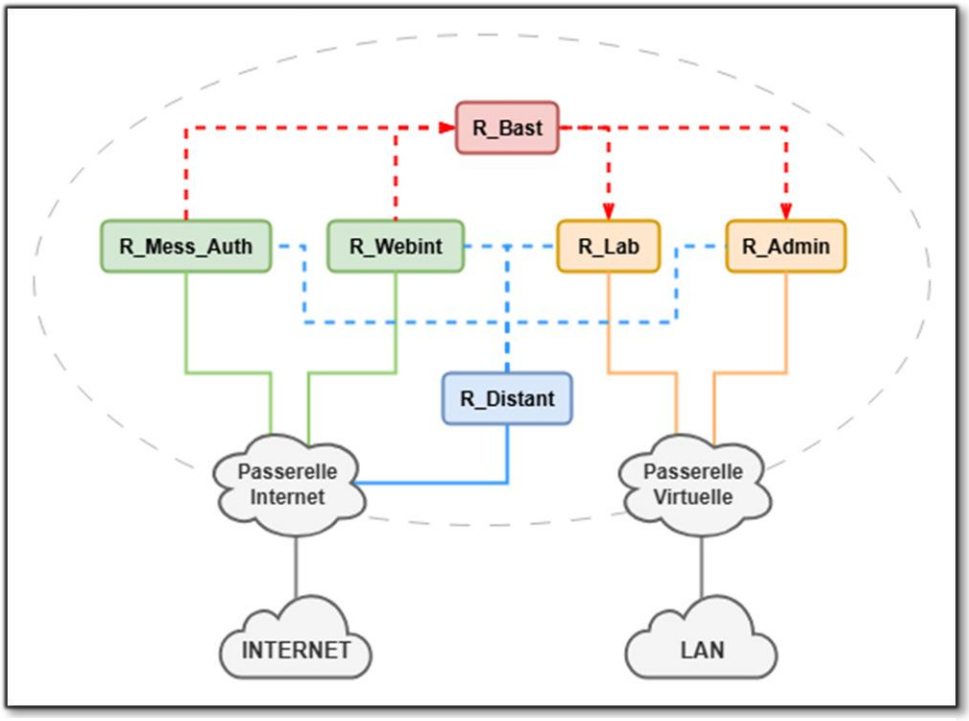


Figure 19 : Future infrastructure cloud

- R_Mess_Auth : Réseau hébergeant les serveurs de **communication** (Auth, mail, LDAP, etc).
- R_Webint : Réseau hébergeant les serveurs **Web et applicatifs** (Sylv'eclair, BioClimSol, Phototèque, etc).
- R_Admin : Réseau hébergeant les serveurs d'**administration** (RH, DAF, FORET, etc).
- R_Bast : Réseau hébergeant le **bastion** (sécurisation de la communication entre espace public (parvenant d'internet) et espace privé de l'environnement).
- R_Lab : Réseau hébergeant les serveurs de **test, de pré-production**, etc.
- R_Distant : Réseau hébergeant le serveur **ZTNA**, permettant de gérer les connexions aux ressources à distance.

La schématisation est un **support logique de la stratégie envisager** quant à la mise en œuvre de la nouvelle infrastructure sur le nouvel environnement cloud. Cette dernière est applicable sur la majorité des provider et fera l'objet de modifications pointilleuses en fonction de la solution de bascule afin de s'adapter à l'environnement cible.

iv. Procédure de migration (GCP)

- Planifier :

Dans un premier temps, nous avions potentiellement convenu de migrer notre infrastructure cloud au sein des **datacenters Google** avec la collaboration des **contrôleurs locaux de chez S3NS** Thales. De ce fait, la **prise de contact** avec l'équipe Google et S3NS a été initialisée et nous avons pu analyser les possibilités envisagées pour la migration, en réponse à nos besoins.

L'accès à un environnement GCP a été mis en œuvre et nous avons pu **maquetter une simulation de migration** entre notre infrastructure AWS et celle de GCP à l'aide des technologies internes à ces deux derniers.

Il a donc été important de mettre en œuvre un **plan de migration** afin de pouvoir tester et simuler ce dernier et d'assurer la faisabilité de cette migration entre ces deux environnements cloud.

Une **première solution** de migration a été envisagée, cette dernière était de basculer des images des instances, ainsi que des **copies des volumes de stockage sur notre baie de stockage local VEEAM** afin de pouvoir les **répliquer sur l'environnement GCP**. Cette solution révélait de **nombreux inconvénients** tels que la **saturation de la bande passante** de notre opérateur, le manque de place dans notre baie VEEAM, le **risque de perte de données et de disponibilité** de la baie en cas de surcharge.

Fort heureusement, une **fonctionnalité de migration** interne à AWS et GCP, grâce aux **APIs** de ces deux derniers, est déjà mis en œuvre et permet la bascule des ressources AWS vers l'environnement GCP de façon efficace et sécurisé.

- Déployer :

La migration par l'intermédiaire des fonctionnalités propres à AWS et GCP permet une **migration rapide** (connexion directe entre les deux environnements assurée par les fournisseurs), **sécurisée** (communication dans un tunnel VPN entre les environnements en HTTPS), **intègre et redondante** (réplication incrémentielle des données de AWS vers GCP).

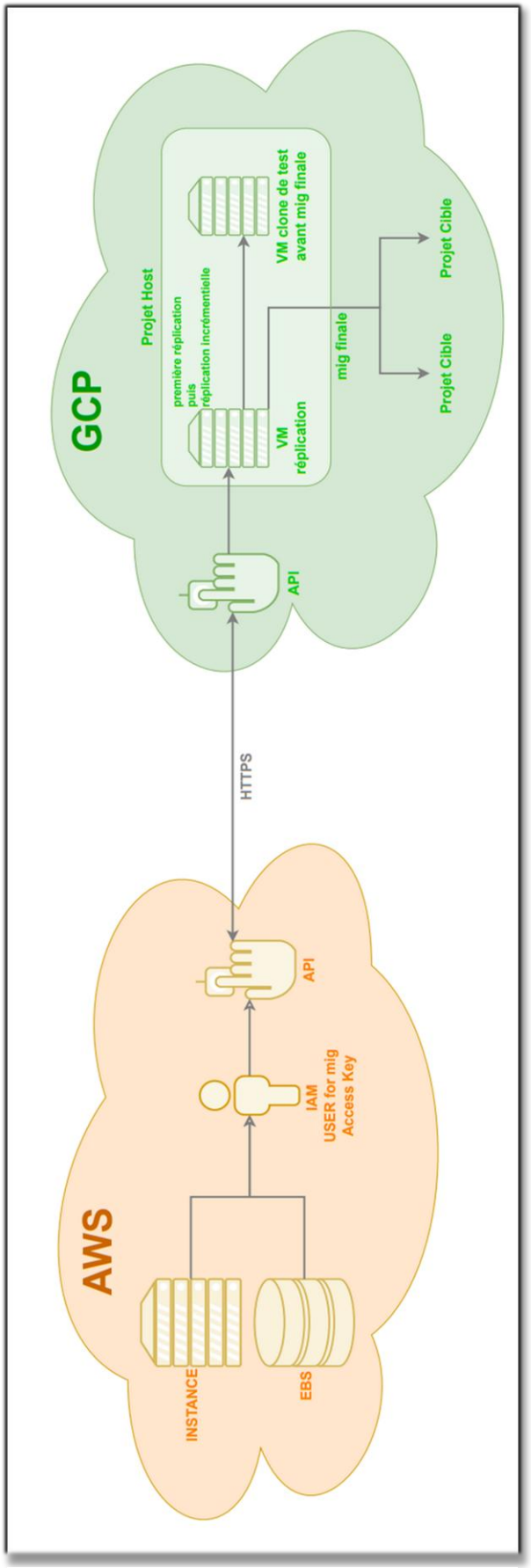


Figure 20 : Schématisation migration GCP

GCP assure qu'il assure l'intégrité des données réplications à l'aide d'un processus de **transfert progressif**, ce dernier premier de faire une **copie de la ressource source** sans impacter sa continuité.

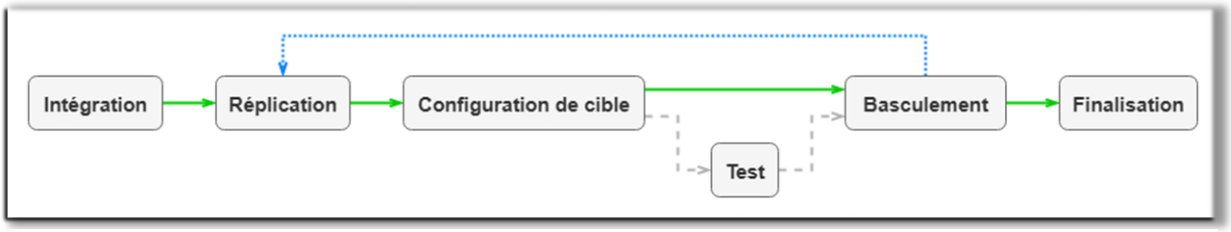


Figure 21 : Fonctionnement migration GCP

La rédaction d'un PLAN DE MIGRATION VERS GCP de notre infrastructure AWS actuelle est jointe en annexe.

- Contrôler :

Cette procédure a **premièrement été testée avec des instances provisoires** afin de s'assurer de la conformité de cette dernière, ainsi que de l'intégrité et la disponibilité des données migrées.

- Agir :

Étant donné le changement de décision quant à l'environnement cloud vers lequel nous allions migrer, ce plan de migration ne sera donc pas réellement mis en œuvre et appliqué dans un cadre de production. Malgré cela, ce dernier nous aura permis d'évoluer notre stratégie de migration afin d'assurer convenablement cette dernière vers notre futur hébergeur cloud.

E. Plan de continuité

Compte tenu de l'incertitude entourant le projet due aux enjeux politiques et économiques définis dans les besoins, des retards accumulés et de l'impossibilité de le finaliser dans la période de mon apprentissage, il est essentiel de mettre en place un **plan de continuité** afin de **garantir sa poursuite et sa mise en œuvre sur le long terme**.

Initialement orientée vers une migration vers GCP, cette **décision a été révisée** à la suite des récents événements politiques et économiques liés aux décisions de l'administration américaine, qui ont soulevé des inquiétudes quant à la souveraineté des données (Cloud Act, FISA) et la disponibilité des services (rupture des contrats, indisponibilité des services américains, surtaxes).

En réponse à ce changement d'orientation stratégique quant à la migration de notre environnement cloud, une **prise de contact** a été initiée avec plusieurs hébergeurs cloud souverains référencés sur le marché public UGAP, notamment **Cloud Temple et Cegedim**. À l'issue de cela et d'une **analyse comparative des offres en fonction de nos besoins**, le choix s'est finalement porté sur le provider Cegedim.

Il convient donc de conserver le **plan stratégique** initialement établi pour la migration vers GCP, en l'adaptant au nouveau fournisseur retenu. Ce plan se décompose donc en plusieurs étapes à suivre afin d'assurer la continuité et la finalisation du projet :

- **Estimation budgétaire** : Il convient donc en premier temps de solliciter **une évaluation précise des coûts** liés à l'hébergement de notre future infrastructure sur l'environnement Cegedim. Cette dernière permettra de valider la faisabilité financière du projet.
- **Finalisation contractuelle** : Une fois l'offre définie, la **signature des contrats** avec Cegedim initialisera la bascule vers ce nouvel hébergeur cloud. Ces contrats devront encadrer les aspects techniques, juridiques (notamment RGPD, SLA et souveraineté des données) et financiers.
- **Mise en œuvre de la nouvelle infrastructure** : L'étape suivante consistera à concevoir une nouvelle infrastructure cloud capable d'héberger et d'améliorer l'environnement actuellement hébergé sur AWS. Cette dernière s'appuiera sur la modélisation de la stratégie d'infrastructure envisagée afin de définir les ressources nécessaires.
- **Solutions de migration** : Il conviendra d'**analyser les différentes possibilités de migration** proposées par Cegedim ou bien par le biais de nos propres moyens afin de s'assurer de mettre en œuvre la **solution la plus fiable, à faible coût, sécurisée et assurant l'intégrité des données migrées**.
- **Mise en œuvre de la migration** : Finalement, une fois la stratégie de migration choisie, cette dernière pourra alors être appliquée de **façon progressive** (premièrement en phase de **test** afin de s'assurer de son fonctionnement), tout en assurant la **continuité et l'intégrité des services** hébergés sur l'infrastructure AWS.

Une fois la migration finalisée, l'environnement cloud pourra **officiellement basculer** sur la nouvelle infrastructure Cegedim, mettant ainsi fin à l'hébergement sur AWS. Il conviendra ensuite de procéder à la **résiliation des contrats avec AWS**, afin de clôturer définitivement l'hébergement de nos ressources sur ce dernier.

4. Conclusion

Cette année d'apprentissage a été principalement soutenue par ma participation à un projet de migration d'infrastructure cloud (initialement prévu vers GCP, puis redirigé vers Cegedim, un cloud souverain français). Ce **changement de décision**, porté par des tensions politiques et économiques liées aux décisions de l'administration américaine, a **influencé la trajectoire du projet**.

En vue de ce contexte instable, j'ai pu m'**impliquer dans toutes les phases critiques** de ce projet (audit de l'infrastructure existante, étude des nouvelles solutions de migration françaises, prise de contact avec les fournisseurs, réflexion contractuelle et planification technique).

Au cours de mon projet professionnel de fin d'études, j'ai été confronté à plusieurs difficultés, notamment en matière de **gestion du temps** (personnel et du projet), de **coordination** avec les différents acteurs impliqués (fournisseurs cloud, équipe IT), ainsi que dans le maintien de la **continuité des services hébergés** sur l'environnement AWS. Ces difficultés m'ont néanmoins permis de me dépasser, de mettre en œuvre une **approche plus structurée**, et de renforcer mes **compétences techniques et organisationnelles**.

Malgré le **retard** accumulé dans la mise en œuvre du projet, cette expérience a été formatrice. Elle m'a permis de développer des **compétences techniques** (infrastructure cloud, analyse de solutions, automatisation, sécurité des infrastructures et migration), mais aussi des **compétences en gestion de projet** (communication, prise de décision et adaptabilité face aux imprévus et organisation).

Finalement, afin de répondre à la problématique énoncée au début de ce mémoire, une **méthodologie rigoureuse** a été mise en œuvre, comprenant des outils d'analyse stratégique, technique et financière, tels que :

- La **roue de Deming** a été utilisée comme fil conducteur pour structurer les différentes missions intermédiaires à l'ensemble du projet.
- L'**analyse de l'existant**, à travers une **analyse des contraintes** (techniques, budgétaires, réglementaires, organisationnelles), nous a aidé à identifier les limites de la solution actuelle et les axes d'amélioration.
- L'**analyse budgétaire** a permis d'évaluer les coûts directs et indirects de l'hébergement cloud actuel.
- L'**analyse des risques** et l'analyse **AMDEC** ont permis d'anticiper les obstacles potentiels liés à la migration et de mettre en place des mesures adaptées.
- Le choix du nouvel hébergeur cloud a reposé sur un **comparatif détaillé des différentes solutions disponibles**, prenant en compte des critères techniques, économiques, organisationnels, juridiques et de sécurité.

La prise en charge de ce projet de migration ne s'est donc pas limitée à une opération technique, mais a été commandée comme un **projet stratégique**, structuré par une démarche d'**amélioration continue**, soutenue par des outils d'analyse. Cette approche permettra de garantir une migration maîtrisée, sécurisée et alignée avec les objectifs définis en amont.

5. Parcours professionnel

A. Parcours actuel

Depuis mon plus jeune âge, ma passion pour l'informatique s'est manifestée lorsque j'ai commencé à monter mes propres ordinateurs ainsi que ceux de mes amis à partir de l'âge de 12 ans. Cet intérêt m'a motivé par la suite à poursuivre dans la voie de l'informatique.

Après mes années de collège, entre 2018 et 2021, j'ai choisi de m'orienter vers les sciences au lycée (options Mathématiques, Physique-Chimie et Science de l'Ingénieur) car je voyais en elles la possibilité de construire mon avenir.

À la suite de l'obtention de mon baccalauréat, durant l'année scolaire 2021-22, j'ai entamé une première année en portail sciences à l'université La Source d'Orléans (options en Mathématiques, Physique et Informatique). Cependant, l'environnement et la formation ne m'ont pas convenu, ce qui m'a conduit à reconsidérer mon choix.

J'ai ensuite tenté l'expérience de la programmation en participant à la "Piscine" d'un mois à l'école 42 à Paris durant le mois d'Août 2022. Après trois semaines de programmation intensive, j'ai décidé d'arrêter car je ne me voyais pas poursuivre cette routine à long terme.

Finalement, j'ai intégré, entre 2022 et 2024, un BTS SIO (services informatiques aux organisations) (option SISR (solutions d'infrastructure, systèmes et réseaux) à Benjamin Franklin, à Orléans, où je me suis senti plus à ma place et ai ressenti un plus grand intérêt pour cette formation que durant mon année universitaire. Bien que je n'avais aucune connaissance en réseau, j'ai su rattraper ce retard et me suis découvert à apprécier ce domaine.

Aujourd'hui, j'ai rejoint la formation de Bachelor Administrateur Systèmes et réseaux en alternance proposée par l'école CESI sur le campus universitaire de La Source à Orléans durant cette année 2024-2025 et mon apprentissage se fait au sein du Centre National de la Propriété Forestière (CNPF) situé à Orléans.

B. Compétences acquises

i. Hard Skills

Compétences	Niveau technique	Contexte
Administration	● ● ● ● ○	Administration système et réseau (serveurs AD et ses services, BDD SQL, commutateurs, pare-feu, routeurs)
Sécurisation du SI	● ● ● ● ○	ACL, IPS/IDS Stormshield, Opensense, gestion du flux
Continuité du SI	● ● ● ● ○	Redondance équipements (haute disponibilité stormshield, keepalived, réplication AD)
Maintenance du SI	● ● ● ● ○	Ticketing GLPI, gestion de parc, (dépannage, installation, configuration poste et logiciels)
Supervision	● ● ○ ○ ○	Zabbix (alerting, OID, journalisation, etc)
Sauvegarde et restauration	● ● ○ ○ ○	Plan sauvegarde Veeam BR, Veeam AWS
Automatisation	● ○ ○ ○ ○	Script python, powershell (Bash, Lambda AWS)
Virtualisation	● ● ● ● ○	Simulation Lab (VMware, Virtualbox, Nutanix)
Cloud	● ● ● ● ●	Migration d'un environnement cloud complet Conception d'une infrastructure cloud (AWS, GCP)

Tableau 10 : Hard skills

ii. Soft Skills

Compétences	Niveau technique	Contexte
Travail d'équipe	● ● ● ● ○	Travail en équipe projet (académique et professionnel)
Gestion de projet	● ● ● ● ○	Chef de projet académique, prise en charge de projet professionnel
Gestion de son temps	● ● ● ● ●	Planning, gestion des délais et jalons, respect des deadlines
Autonomie	● ● ● ● ○	Projet individuel académique et professionnel, (analyse, réflexion, mise en œuvre, documentation)
Rigueur	● ● ● ● ○	Structuration du travail, du temps, discipline, motivation
Contrôle de soi	● ● ● ○ ○	Gestion du stress et des responsabilités
Force de proposition	● ● ● ○ ○	Proposition, réflexion, analyse, rapport d'étude
Force de conviction	● ● ● ○ ○	Prise de position, argumentation
Curiosité	● ● ● ● ○	Passion, veille, évolution des compétences techniques et personnelles
Communication	● ● ● ○ ○	Communication en équipe, gestion de la parole, plan de communication
Savoir-être professionnel	● ● ● ● ○	Respect de la hiérarchie, des politiques et de l'environnement

Tableau 11 : Soft skills

C. Parcours futur envisagé

Aujourd'hui, j'envisage de continuer mes études au sein de l'école CESI à Orléans en tant que manager en Infrastructures et Cybersécurité des SI en alternance sur un cursus de 2 années afin de pouvoir approfondir et mettre en œuvre mes connaissances techniques, mais aussi de développer mes expériences professionnelles dans le monde du travail.

L'obtention de ce diplôme m'ouvrira diverses opportunités dans le domaine informatique et en particulier dans le domaine de la gestion des systèmes d'information.

Mon futur métier consistera à piloter les projets et équipes de l'environnement du SI, émettre un travail d'analyse et de réflexion sur la mise en place d'une solution dans l'objectif d'optimiser et d'évoluer ce dernier, faire de la veille informatique afin d'assurer le bon suivi du système d'information en rapport avec l'évolution des technologies et des risques de sécurité.

Mon métier cible à court terme sera ingénieur ou chef de projet infrastructures, cybersécurité ou cloud, pour finaliser au long terme le poste de responsable ou directeur du SI.

Afin de m'assurer ce futur, il sera aussi nécessaire d'effectuer des formations individuelles complémentaires à celles académiques afin de développer des compétences plus pointilleuses quant à la sécurisation et la gestion du SI, telles que les formations CFSSI de l'ANSSI.

D. Expérience professionnelle

Au cours de mes années d'études supérieures, en particulier durant mon BTS SIO, ainsi que mon Bachelor en alternance, j'ai pu avoir la chance d'accroître mes expériences professionnelles à travers des stages et de l'alternance.

Au cours de mes 2 années de BTS, j'ai exercé 2 périodes de stage qui sont les suivantes :

- Un premier stage d'une durée de 6 semaines au sein de la mairie de Fleury-les-Aubrais durant lequel j'ai pu être intégré et initié à une équipe informatique ainsi qu'à leur quotidien pour la première fois.
  J'ai eu comme missions de répondre aux incidents et aux demandes d'assistance sur un parc informatique (GLPI), la gestion et configurations de la structure d'un Active Directory, ainsi que de rédiger des documentations diverses sur l'installation de services fournis aux utilisateurs par la Mairie.

- Un second stage d'une durée de 7 semaines au sein du Centre National de la Propriété Forestière à Orléans durant lequel il m'a été confié une courte mission sur la réflexion d'une nouvelle stratégie d'infrastructure de leur environnement cloud.
  J'ai eu comme missions d'étudier et d'apprendre l'environnement cloud AWS de l'entreprise, faire une proposition de solutions d'infrastructures réseaux AWS, ainsi que de rédiger les procédures et documentations diverses sur la mise en place d'un environnement AWS et ses technologies.

Afin, au cours de ma Bachelor en alternance, j'ai travaillé au sein du Centre National de la Propriété Forestière sur une amplitude de 34 semaines durant lesquelles j'ai été intégré à diverse projets dont le principal est la prise en charge du projet de migration de notre hébergeur cloud. Mes missions ont été les suivantes :

- Étude de faisabilité et prise en charge du projet de migration vers le nouvel hébergeur cloud GCP.
- Étude et apprentissage de l'environnement cloud GCP.
- Étude de l'optimisation de la sécurité, des flux et des coûts de l'environnement cloud AWS de l'entreprise.
- Documentation et cartographie (schématique et manuscrite) de l'infrastructure cloud AWS.
- Mise en place d'une solution de gestion des instances (scripting Python 3.12) sur l'environnement AWS.
- Étude d'optimisation et révision de la solution de sauvegarde interne à l'environnement cloud et du backup en LAN sur un environnement VEEAM.
- Mise en place et configurations d'un service ZTNA, Netskope.
- Procédures, documentations, guide d'emploi et rapport sur la mise en place de ce service ZTNA.
- Travaille en équipe et communication avec les collaborateurs et les fournisseurs.

En somme, la totalité de ces projets, ainsi que de ces expériences professionnelles m'ont permis de développer le travail, la communication et le savoir-être en équipe, ainsi que la gestion du temps, du stress, mais aussi la prise de parole, de position et de réflexion.

E. Expérience académique

Ma formation en BTS SIO à Benjamin Franklin m'a apporté des connaissances en administration des réseaux et des systèmes, ainsi qu'en supervision et gestion des services informatiques. Les compétences durant ce dernier sont les suivantes :

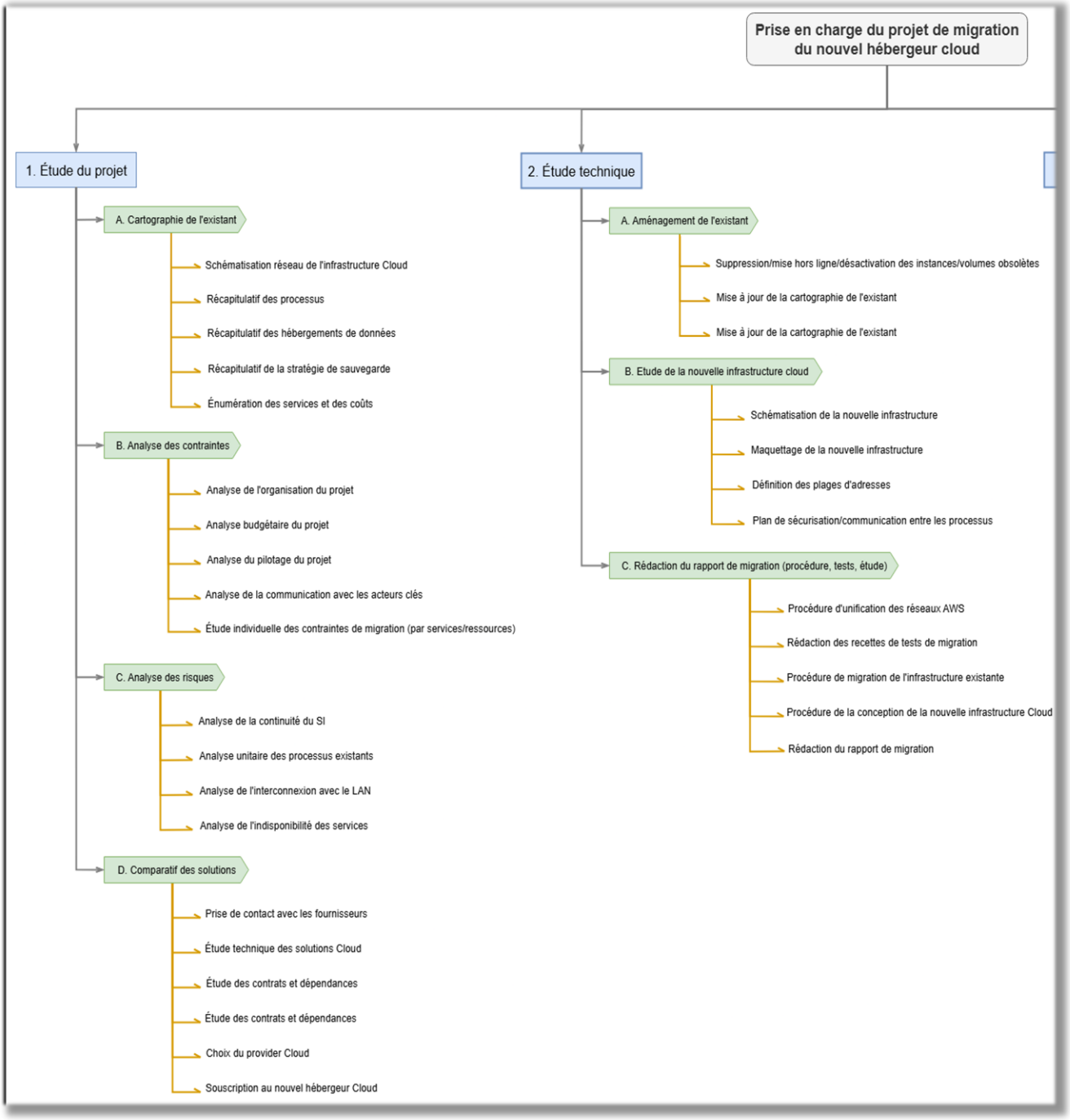
- Mise en place d'une infrastructure réseau et segmentation des VLAN.
- Configuration avancée des switchs (VLAN) et routeurs (WAN, LAN, DMZ).
- Segmentation et sécurisation des infrastructures réseau.
- Configuration avancée d'un routeur pour gérer les accès WAN/LAN.
- Mise en place des règles de filtrages (ACL).
- Déploiement des services AD, DNS et DHCP avec redondance.
- Déploiement d'Active Directory (AD) avec DNS et DHCP en haute disponibilité.
- Mise en place de solution garantissant la disponibilité des services critiques :
- Mise en place de solution de redondance avec Keepalived (VIP) et GlusterFS (synchronisation de serveurs web).
- Installation et administration des solutions de supervision Zabbix et PRTG.
- Gestion du parc informatique avec GLPI et Fusion Inventory (GLPI inventory).
- Mise en place d'un serveur de messagerie Postfix.

Quant à ma formation en Bachelor ASR (Administrateur système et réseau) au CESI, cette dernière m'a permis de développer des compétences en gestion et en sécurisation des infrastructures informatiques, en mettant le point sur le réseau, le système, la virtualisation, ainsi que sur la gestion de projet.

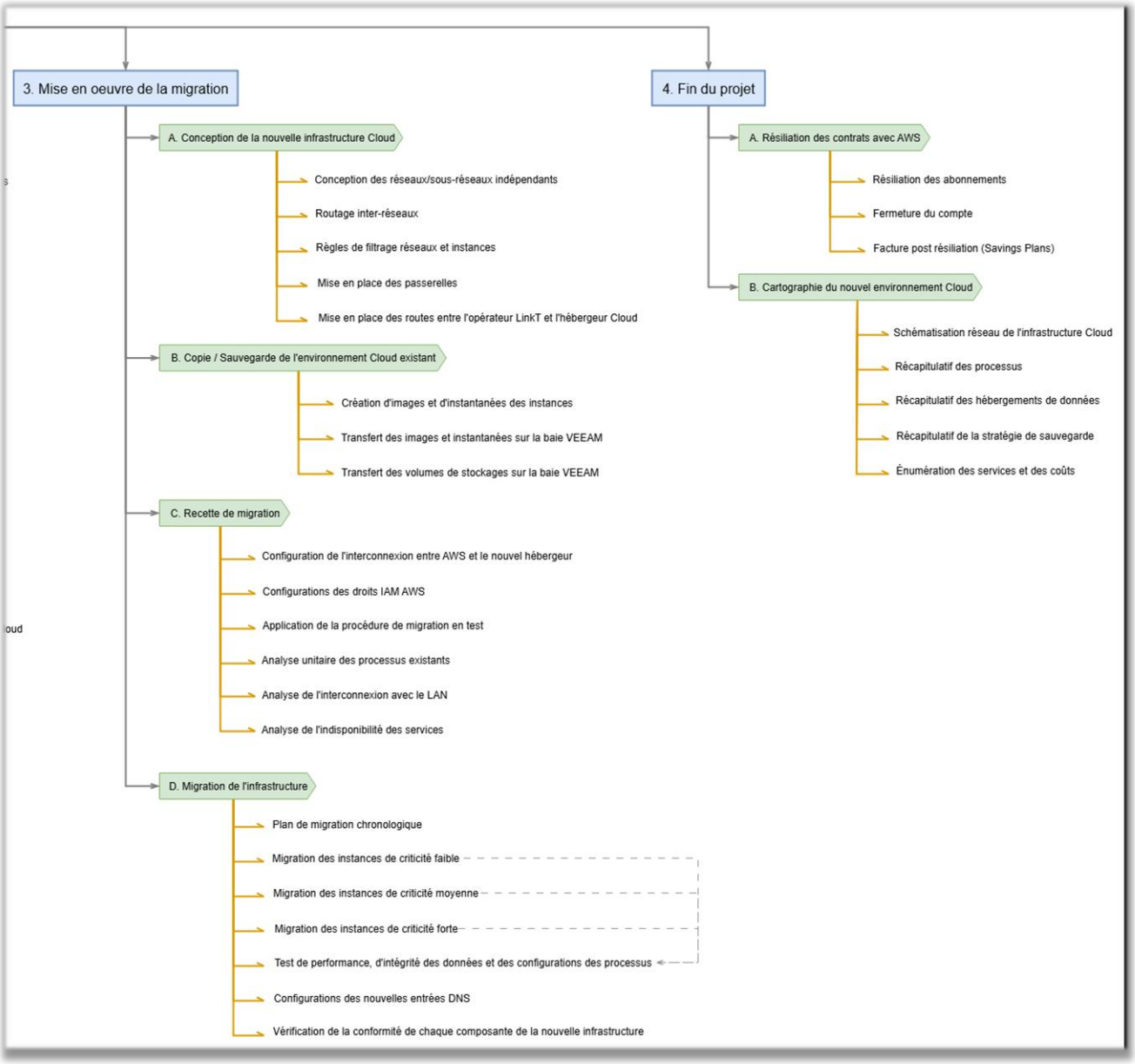
- Modélisation des infrastructures systèmes et réseaux : Gestion de projet avec une analyse des besoins tout en proposant des solutions.
- Déploiement des infrastructures systèmes et réseaux : Déploiement d'un environnement virtualisé avec VMWare.
- Mise en place des machines virtuelles avec les services suivants : AD, DNS, DHCP. GPO
- Maintenir et sécuriser les infrastructures et réseaux : Conception, sécurisation et administration des infrastructures et réseaux locaux et étendus.
- Manager les équipes et les projets informatiques : Gestion de projet sur l'élaboration et le suivi de projet avec WBS, RACI, Gantt, REX, Budget, analyse des risques, pilotage (KPI).

ANNEXES

A. Organigramme des tâches (WBS)

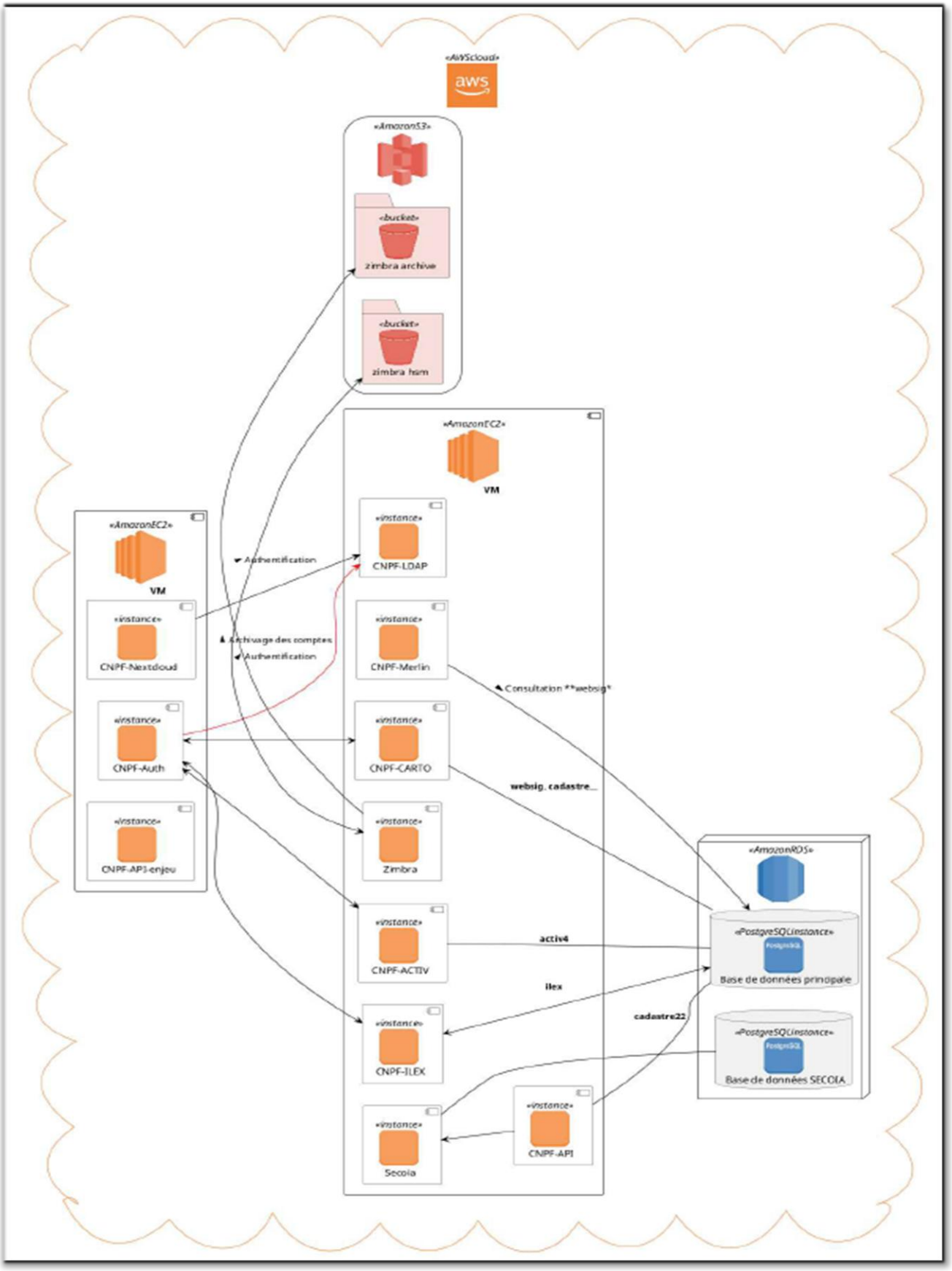


Retour au chapitre *Retour à la table des matières*

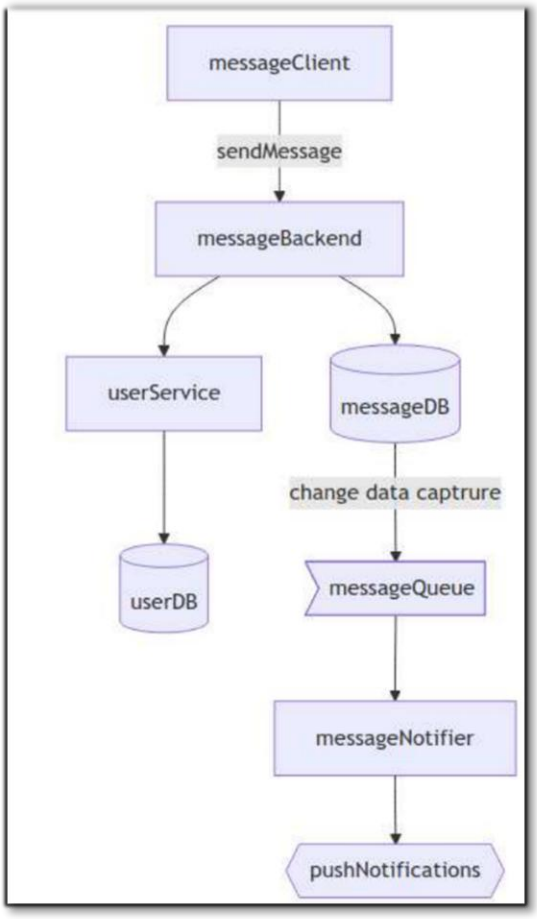


Retour au chapitre *Retour à la table des matières*

B. Communication et dépendance des RDS



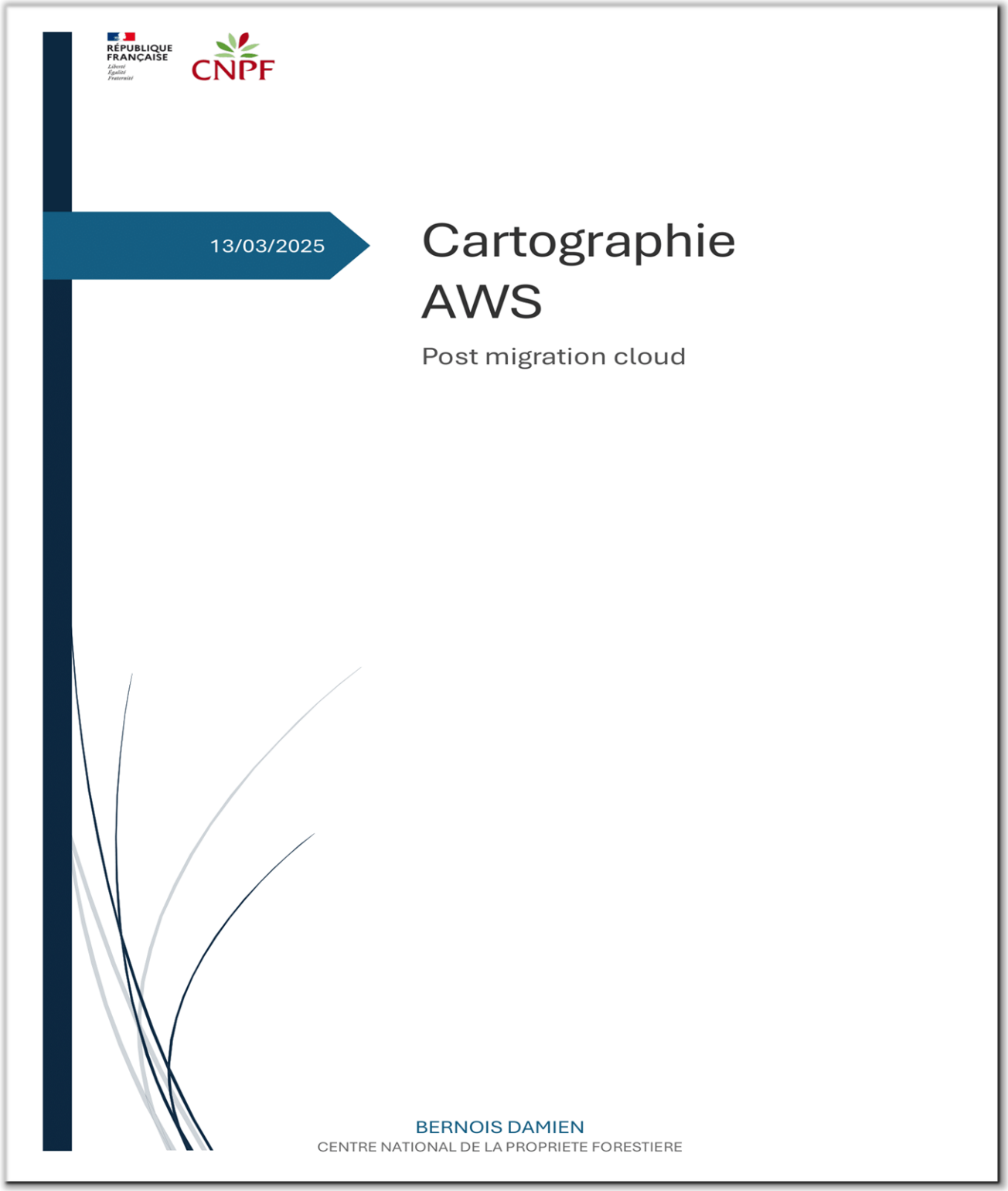
Retour au chapitre Retour à la table des matières



Retour au chapitre *Retour à la table des matières*

C. Cartographie de l'infrastructure cloud existante

Pour des raisons évidentes de confidentialité et de risques de diffusions de données sensibles relatives à l'infrastructure du CNPF, les adresses IP privées et publiques seront masquées ci-dessous par des rectangles noirs.



Retour au chapitre *Retour à la table des matières*

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CNPF

Table des matières

Retour au chapitre Retour à la table des matières

GLOSSAIRE

- **AWS (Amazon Web Services)** : AWS est la plateforme cloud d'Amazon qui fournit des services comme la virtualisation, le calcul et le stockage.
- **GCP (Google Cloud Platform)** : GCP est la plateforme cloud de Google qui fournit des services comme la virtualisation, le calcul et le stockage.
- **Instance EC2 (Elastic Compute Cloud)** : Une instance EC2 est une VM exécutée sur des serveurs physiques du datacenter AWS pouvant accueillir différentes configurations de matériel telles que la puissance du processeur (CPU), de la mémoire (RAM) et de l'espace de disque dur (EBS), ainsi que leur type.
- **Datacenter (Centre de Données)** : Un datacenter est une très grande infrastructure située dans une zone géographique précise permettant de stocker, traiter, distribuer des données à l'aide de puissants serveurs, systèmes de stockage et autres.
- **EBS (Elastic Block Store)** : Un EBS est un volume de stockage permettant de stocker des données de manière persistante afin de pouvoir, par la suite, rattacher ces derniers à des instances. Ces différents EBS sont stockés dans le service S3 d'AWS. Il existe une variété de types de stockage adaptés à différents cas d'usage, changeant les coûts de ces derniers.
- **RDS (Relational Database Service) :** Le RDS est un service qui permet d'effectuer la plupart des tâches de gestion des bases de données sur AWS, tels que les sauvegardes, la détection de défaillance, les correctifs logiciels, et d'autres.
- **S3 (Simple Storage Service)** : S3 est un service de stockage cloud qui permet de stocker et récupérer facilement des données à grande échelle et avec une haute disponibilité.
- **S3 Glacier Deep Archive** : Les types de stockage S3 Glacier sont conçus pour l'archivage de données offrant une disponibilité de 99,99% de ces dernières. Cet archivage permet une plus grande flexibilité de récupération et un accès rapide.
- **VPC (Virtual Private Cloud)** : Un VPC est un réseau virtuel privé qui permet de lancer des ressources AWS, tels que des instances EC2, dans un environnement réseau isolé défini. Il est possible de rendre de façonner ce réseau à l'aide de diverses fonctionnalités à disposition sur AWS.
- **Direct Connect :** Un Direct Connect est un service réseau permettant d'établir une connexion privée entre leur infrastructure LAN sur site et leur infrastructure cloud
- **LAN (Local Area Network)** : Un LAN est un réseau local privé restreint interconnectant différents appareils, il est souvent situé dans des zones géographiques minimes telles qu'un bâtiment, un campus. Il est similaire au réseau VPC d'AWS, mais n'est pas virtualisé sur un datacenter.
- **CloudWatch :** Le CloudWatch collecte des données sur l'ensemble des ressources AWS utilisées dans l'environnement cloud. Cela permet de pouvoir définir des alertes sur des variations des données systèmes collectées.

Retour au chapitre Retour à la table des matières

- **Secrets Manager :** Le Secrets Manager permet de gérer de façon centralisée les secrets, informations d'identification de base de données, les clés API et autres. Cela évite de stocker les informations d'identification codées en dur dans le code source des applications. Il est aussi possible de mettre en place des politiques aidant à contrôler les accès à ces secrets.
- **KMS (Key Management Service) :** Le KMS est un outil permettant de gérer et de contrôler de façon simplifiée les différentes clés de chiffrement utilisées sur l'environnement cloud AWS.
- **SQS (Simple Queue Service) :** Le SQS permet de créer des files d'attente de messages entre deux destinataires de l'environnement AWS, en particulier des applications n'ayant pas de serveurs. Cela peut aider à récolter des données afin de mettre en place des métriques.
- **Zone de disponibilité :** Une zone de disponibilité est un emplacement physique isolé des autres, au sein d'une même région géographique. Cette isolation apporte de nombreuses plus-values telles qu'une continuité des services d'une zone fonctionnelle en cas de défaillance d'une autre.
- **NAT (Network Address Translation)** : Une passerelle NAT est un dispositif réseau permettant de traduire une adresse IP privée d'un réseau en une adresse IP publique, et vice versa. Cela peut permettre à des instances dans un réseau privé d'accéder à Internet tout en masquant leurs adresses IP privées.
- **ENI (Elastic Network Interface)** : Une ENI est une interface réseau virtuelle attachée aux instances permettant d'attribuer des adresses IP et configurer les connexions réseau.
- **AMI (Amazon Machine Image)** : Une AMI est une image qui comporte un système d'exploitation, des applications et des configurations spécifiques. Ces dernières permettent, lors de la création d'une instance, d'avoir une copie conforme à l'AMI sélectionnée, fournissant un gain de temps lors de sa création. Ces différentes AMI sont stockées dans le service S3 d'AWS.
- **EIP (Elastic IP)** : Une EIP est une IP publique statique pouvant être allouée et rattaché à une ENI, qu'elle soit celle d'une instance EC2, ou bien celle d'une passerelle NAT.
- **VGW (Virtual Gateway)** : Une VGW est une passerelle permettant de créer un point d'accès vers un réseau externe comme notre réseau LAN. Cette passerelle assure un échange sécurisé avec le destinataire.
- **IGW (Internet Gateway)** : Une IGW est une passerelle permettant de créer un point d'accès vers Internet depuis un VPC.
- **PCX (VPC Peering Connexion)** : Un PCX est une connexion entre deux VPC permettant de router le trafic entre ces derniers.
- **Endpoint (Point de terminaison)** : Un Endpoint est une passerelle permettant à un VPC de communiquer avec un autre service AWS sans passer par une IP publique. Elle assure un point d'accès privé vers ce service depuis les instances de ce VPC.

- **Jeux d'options DHCP** : Un jeu d'options DHCP permet de contrôler les paramètres DNS, de domaine et NTP au sein des VPC. Il permet de personnaliser les VPC avec nos propres serveurs DNS, nom de domaine, etc. Cependant, il n'est possible d'associer qu'un seul jeu d'options DHCP à la fois à un VPC.
- **Instantanées EBS** : Les instantanées EBS sont des sauvegardes incrémentielles des volumes de stockage EBS. Ces dernières peuvent être réutilisées à la suite d'une perte de données ou bien pour la migration de données entre régions et comptes AWS.
- **Sauvegarde incrémentielle** : Une sauvegarde incrémentielle est un type de sauvegarde qui consiste à uniquement conserver les modifications apportées depuis la précédente sauvegarde. Cela apporte un gain de volume car nous conservons que les modifications apportées et non la sauvegarde dans sa globalité.
- **SNS (Simple Notification Service)**: Un SNS est un service Web permettant de faciliter la configuration, l'exploitation et l'envoi de notifications ou messages depuis le cloud. Il permet de donner l'accès aux ressources informatiques à l'échelle du Web et est utilisé majoritairement sur les points de terminaisons.
- **Systems Manager** : Le System Manager est un service permettant de visualiser et de gérer de façon centralisée des différentes ressources telles que les instances EC2. Il peut vous permettre d'automatiser des tâches, de faire des correctifs et bien d'autres.
- **ACL (Access Control List)**: Une ACL est une liste de contrôle d'accès qui permet de gérer les accès à un réseau en fournissant des instructions aux commutateurs ou aux routeurs sur les réseaux de trafic qui sont autorisées.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CNPF

CONTEXTE

L'hébergement de notre environnement cloud actuel est assuré par la plateforme d'AWS. Cette dernière héberge aujourd'hui la majorité de notre infrastructure (comprenant les applications métiers, les serveurs de fichiers, les serveurs d'administration, les environnements de production, de développement, de recette et de préproduction).

Du fait des coûts des différents services utilisés, ainsi que de notre infrastructure réseau virtualisée au sein de cet hébergeur, nous avons émis l'hypothèse d'une future migration de notre environnement cloud vers une autre plateforme d'hébergement cloud dans le but premier d'assurer un environnement plus économique, plus clair et simple d'utilisation, mais aussi avec un suivi des coûts de services plus ergonomique.

Ce document fait acte de cartographie manuscrite de notre environnement cloud AWS. De plus, une cartographie schématique complète et une plus simpliste sont jointes à ce document afin d'avoir une vue plus globale et concrète de notre infrastructure cloud.

Tous deux serviront, par la suite, de point d'appui pour argumenter et comparer les plus-values que pourrait nous offrir un futur autre environnement d'hébergement cloud relativement à celui d'AWS, ainsi qu'assurer la faisabilité de cette migration.

Ce document répertorie toute notre infrastructure, ainsi que nos ressources cloud sur AWS. Il est donc important de souligner que ce dernier, ainsi que les informations rédigées ci-dessous, sont de caractère sensible. Ils ne doivent donc aucunement être partagés au grand public et doivent rester privés et internes au CNPF.

Retour au chapitre Retour à la table des matières

AWS met à disposition de ces utilisateurs de nombreux services afin de maintenir l'environnement cloud, parmi ces derniers, seulement **13 sont utilisés** sur notre infrastructure cloud actuelle. Ces services sont les suivants :

- Elastic Compute Cloud (EC2)
- Relational Database Service (RDS)
- Simple Storage Service (S3)
- Data Transfer
- Virtual Private Cloud (VPC)
- Direct Connect
- Secrets Manager
- Key Management Service (KMS)
- S3 Glacier Deep Archive
- CloudWatch
- Simple Notification Service (SNS)
- Simple Queue Service (SQS)
- Systems Manager

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CNPF

1. Services de virtualisation

1.1. Instances EC2

Notre infrastructure Cloud héberge actuellement **106 instances**, parmi lesquelles se trouve **29 instances à l'arrêt** (comprenant des instances pouvant être à nouveau relancées et d'autres n'étant que des instances temporaires qui ne seront plus exploitées par la suite) et **77 instances en cours d'exécution**.

Ces instances sont toutes hébergées sur le datacenter de la région de Paris, eu-west-3. Chacune d'entre elles est hébergée dans une des différentes zones de disponibilité suivantes, eu-west-3a, eu-west-3b et eu-west-3c.

Chacune des 106 instances ont leur propre type de machine répondant aux besoins de performances des services hébergés sur ces dernières, parmi ces instances, il existe les types suivants :

Instance EC2 EN COURS D'EXECTION (77)	
Type	**Quantité**
t2.micro	7
t2.medium	3
t2.large	6
t2.xlarge	13
t2.2xlarge	2
t3.nano	1
t3.micro	6
t3.small	2
t3.medium	9
t3.large	16
t3.xlarge	9
t3.2xlarge	1
m5.xlarge	1
m5.2xlarge	1

Instance EC2 HORS LIGNE (29)	
Type	**Quantité**
t2.micro	6
t2.small	2
t2.medium	2
t2.large	5
t2.xlarge	4
t2.2xlarge	1
t3.medium	2
t3.large	2
t3.xlarge	3
t3.2xlarge	2

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CNPF

Voici le détail des instances hébergées sur notre cloud AWS :

INSTANCES EC2 EN COURS D'EXECUTION				
Nom	**Type**	**Plateforme**	**VPC**	**Sous-réseau**
APO-JAR-teltransmission-PHU-BPE	t2.xlarge	Linux/UNIX Debian	AWS1	SS1-AWS1
FPF-prod_bo	t2.xlarge	Linux/UNIX Debian [redacted]	AWS1	SS2-AWS1
LFB-V1-prod	t2.xlarge	Linux/UNIX Debian[redacted]	AWS1	SS2-AWS1
FRCT-prod	t2.micro	Linux/UNIX Debian[redacted]	AWS1	SS2-AWS1
LFB-MongoDB	t2.medium	Linux/UNIX Debian	AWS1	SS2-AWS1
CNPF-Nextcloud ([redacted])	t3.xlarge	Linux/UNIX Debian [redacted]	AWS1	SS2-AWS1
Climessences-prod_v1.0.0	t2.xlarge	Linux/UNIX Debian [redacted]	AWS1	SS2-AWS1
CNPF-ACTIV	t3.micro	Linux/UNIX Debian [redacted]	AWS1	SS1-AWS1
CNPF-ILEX	t3.micro	Linux/UNIX Debian [redacted]	AWS1	SS1-AWS1
CNPF-RDP-Gateway & acs.fr DC	t2.xlarge	Windows, Server[redacted]	AWS1	SS1-AWS1
CNPF-DNS1 (PROD)	t3.micro	Linux/UNIX Debian [redacted]	AWS1	SS1-AWS1
CNPF-CARTO	t3.xlarge	Linux/UNIX	AWS1	SS1-AWS1
LDAP Server (ldap Old)	t2.medium	Linux/UNIX	AWS1	SS1-AWS1
CNPF_DVF_foncier	t2.micro	Linux/UNIX Debian [redacted]	AWS1	SS2-AWS1
CNPF-Merlin	t2.xlarge	Windows, Server[redacted]	AWS1	SS2-AWS1
CNPF-GFIpep	t2.2xlarge	Windows, Server[redacted]	AWS1	SS2-AWS1
LFB-V2-recette-drupal9	t2.xlarge	Linux/UNIX Debian [redacted]	AWS1	SS2-AWS1
WALLIX_Access_Manager_PROD_v[redacted]	t3.small	Linux/UNIX Debian [redacted]	AWS1	SS2-AWS1
CNPF_McAfee_1	t2.large	Windows, Server[redacted]	AWS1	SS2-AWS1
Mailcatcher	t3.micro	Linux/UNIX Debian [redacted]	AWS1	SS0-AWS1
Recette-Teletrans-Serveur	t2.micro	Linux/UNIX Debian	AWS1	SS2-AWS1
Climessences-recette_v1.0.0	t2.xlarge	Linux/UNIX Debian [redacted]	AWS1	SS2-AWS1
LFB-V1-recette	t2.xlarge	Linux/UNIX	AWS1	SS2-AWS1
CNPF-API	t3.micro	Linux/UNIX Debian [redacted]	AWS1	SS2-AWS1
CNPF-LDAP (ldap New)	t2.micro	Linux/UNIX Debian [redacted]	AWS1	SS1-AWS1

4

Retour au chapitre Retour à la table des matières

Graylog	t3.medium	Linux/UNIX Debian [redacted]	AWS1	SS1-AWS1
Matomo	t3.large	Linux/UNIX Debian [redacted]	AWS1	SS2-AWS1
CNPF-VIRTUALIA-APPLI	t3.2xlarge	Windows, Server[redacted]	AWS1	SS2-AWS1
CNPF-VIRTUALIA-IIS	t3.xlarge	Windows, Server[redacted]	AWS1	SS2-AWS1
GFI-CAB	t2.micro	Linux/UNIX	AWS1	SS2-AWS1
StreamGoomer Manager	t3.xlarge	Linux/UNIX	AWS1	SS1-AWS1
MyMetricks Server	t2.xlarge	Linux/UNIX	AWS1	SS2-AWS1
Portail-authentification-V2 (lemon [redacted]	t3.medium	Linux/UNIX Debian [redacted]	AWS1	SS2-AWS1
WALLIX_Bastion_PROD_[redacted]	t3.medium	Linux/UNIX	AWS1	SS2-AWS1
VPC_BAST_FIREWALL (prod)	t2.xlarge	Linux/UNIX	VPC_BAST	SS0_VPC_BAST
foret-gibier	t3.small	Linux/UNIX Debian [redacted]	AWS1	SS2-AWS1
BioClim_Test	t2.large	Linux/UNIX Debian [redacted]	AWS1	SS1-AWS1
StormShield_SMC_Server_[redacted]	t3.xlarge	Linux/UNIX	VPC_BAST	SS2_VPC_BAST
CNPF-web-prod	t3.xlarge	Linux/UNIX Debian [redacted]	AWS1	SS2-AWS1
sftp	t3.nano	Linux/UNIX Debian [redacted]	AWS1	SS2-AWS1
SonarQube Server	t2.large	Linux/UNIX Debian [redacted]	AWS1	SS4_AWS1_Public_subnet
Gitlab Server	t2.xlarge	Linux/UNIX Debian [redacted]	AWS1	SS4_AWS1_Public_subnet
Gitlab Runner	t3.medium	Linux/UNIX Debian [redacted]	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
Zimbra Server PROD [redacted]	m5.2xlarge	Linux/UNIX	AWS1	SS2-AWS1
Bioclimsol_Auth_Server_TEST	t2.micro	Linux/UNIX Debian [redacted]	AWS1	SS2-AWS1
Merlin-Tdata	t3.large	Windows, Server[redacted]	VPC_WEBINT	SS1_VPC_WEBINT
secoia_v2 server (2nd installation) - (VPC Webint - ss1)	m5.xlarge	Linux/UNIX Debian [redacted]	VPC_WEBINT	SS1_VPC_WEBINT
API_Carto_enjeux (Recette)	t2.large	Linux/UNIX	AWS1	SS2-AWS1
DG_FILESERVER	t3.large	Windows, Server[redacted]	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
Veeam Console	t3.medium	Linux/UNIX	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
BioClimSol-Dev-Test	t2.medium	Linux/UNIX Debian [redacted]	AWS1	SS2-AWS1
CIDF_FILESERVER	t3.large	Windows, Server[redacted]	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
PACA_FILESERVER	t3.large	Windows, Server[redacted]	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
AURA_FILESERVER	t3.large	Windows, Server[redacted]	AWS1	SS3-AWS1_Private_subnet via Nat Gateway

GEST_FILESERVER	t3.large	Windows, Server [redacted]	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
HDFN_FILESERVER	t3.large	Windows, Server [redacted]	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
BPDL_FILESERVER	t3.large	Windows, Server [redacted]	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
BFC_FILESERVER	t3.large	Windows, Server [redacted]	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
OCCI_FILESERVER	t3.large	Windows, Server [redacted]	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
Cryhod Share Server	t2.micro	Linux/UNIX Debian [redacted]	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
Windows_[redacted]_TSE_Server_(PROD)	t2.large	Windows, Server [redacted]	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
antispam	t2.xlarge	Linux/UNIX	AWS1	SS0-AWS1
CNPF_ADSERVER	t2.2xlarge	Windows, Server [redacted]	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
NAQUI_FILESERVER	t3.large	Windows, Server [redacted]	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
IDF_FILESERVER	t3.large	Windows, Server [redacted]	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
Wapt Server	t2.large	Ubuntu [redacted]	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
CNPF-web-preprod_Cloned	t3.large	Linux/UNIX Debian [redacted]	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
New_Photofor	t3.medium	Linux/UNIX [redacted]	AWS1	SS4_AWS1_Public_subnet
NetsKope Publisher	t3.medium	Linux/UNIX	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
secoia preprod	t3.xlarge	Linux/UNIX	VPC_WEBINT	SS1_VPC_WEBINT
CNPF-ocsinventory PROD (v2.8.1)	t3.medium	Linux/UNIX Ubuntu Focal [redacted]	AWS1	SS2-AWS1
Virtualia v5 - Form	t3.large	Linux/UNIX	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
VirtualiaV5 - Test	t3.large	Linux/UNIX	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
VirtualiaV5 - Prod	t3.xlarge	Linux/UNIX Debian [redacted]	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
Climessences V1 Recette Drupal10	t3.xlarge	Linux/UNIX	AWS1	SS0-AWS1
Gophish_Server	t3.micro	Linux/UNIX Debian [redacted]	AWS1	SS2-AWS1
BioClimSol_V2_prod	t3.medium	Linux/UNIX Debian [redacted]	AWS1	SS2-AWS1

INSTANCES EC2 HORS LIGNE				
Nom	**Type**	**Plateforme**	**VPC**	**Sous-réseau**
FRCT-dev	t2.micro	Linux/Unix Debian	AWS1	SS2-AWS1
SFT_POC_Carto_Cadastre	t2.micro	Linux/Unix Debian	AWS1	SS0-AWS1
RLT_Catalogue_2	t2.small	Linux/Unix	AWS1	SS2-AWS1
cnpf-SG	t3.large	Linux/Unix	AWS1	SS0-AWS1
Pentest Server	t2.large	Linux/Unix Debian [redacted]	AWS1	SS2-AWS1
Connecteur-SW2-Prod	t2.micro	Linux/Unix Debian	AWS1	SS2-AWS1
Virtual Room Connector	t2.large	Linux/Unix	AWS1	SS0-AWS1
StreamGoomer Collector	t3.large	Linux/Unix	AWS1	SS1-AWS1
TheGreenBow TAS Server	t2.small	Linux/Unix	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
Windows_Server_rescue_Sylvain	t2.large	Windows	AWS1	SS3-AWS1_Private_subnet via Nat Gateway
(RDP_CNPF)	t2.medium	Windows	AWS1	SS2-AWS1
CNPF-VIRTUALIA-APPLI_RESTORED	t3.2xlarge	Windows, Server [redacted]	AWS1	SS2-AWS1
Redmine-[redacted]	t2.medium	Linux/Unix	AWS1	SS2-AWS1
SUADEO_Serveur_application	t2.2xlarge	Windows	AWS1	SS2-AWS1
srvobm.cnpf.fr	t2.xlarge	Linux/Unix	AWS1	SS2-AWS1
FPF-prod_fo	t2.xlarge	Linux/Unix Debian [redacted]	AWS1	SS2-AWS1
Zimbra Docs PROD	t2.large	Linux/Unix	AWS1	SS2-AWS1
Climessences-preprod_v1.0.0)	t3.xlarge	Linux/Unix Debian [redacted]	AWS1	SS2-AWS1
LFB-V1-preprod	t2.xlarge	Linux/Unix Debian [redacted]	AWS1	SS2-AWS1
FPF-dev	t2.xlarge	Linux/Unix	AWS1	SS2-AWS1
sylvi-par	t2.micro	Linux/Unix Debian [redacted]	AWS1	SS1-AWS1
FRCT-recette	t2.micro	Linux/Unix Debian [redacted]	AWS1	SS2-AWS1
SUADEO_Recette	t3.2xlarge	Windows	AWS1	SS2-AWS1
Recette-Merlin	t3.xlarge	Windows	AWS1	SS0-AWS1
mig-CNPF-DNS2	t2.micro	Linux/Unix	AWS1	SS1-AWS1
Client2_Zimbra_MIG	t3.medium	Linux/Unix, Ubuntu [redacted]	AWS1	SS2-AWS1
Client1_Zimbra_MIG	t3.medium	Linux/Unix, Ubuntu [redacted]	AWS1	SS2-AWS1
TEST_API_POC_Carto	t2.large	Linux/Unix Debian [redacted]	AWS1	SS2-AWS1
Zimbra Server TEST [redacted]	t3.xlarge	Linux/Unix	VPC_WEBINT	SS0_VPC_WEBINT

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CNPF

1.2. Volumes de stockage (EBS)

Notre infrastructure Cloud AWS héberge actuellement **143** volumes de stockage EBS, chacun réparti sur différentes zones de disponibilité. Parmi ces volumes, 3 ne sont attachées à aucune instance EC2 et sont donc simplement stockés sur l'environnement cloud, mais pas exploités.

De plus, nous disposons de **767** instantanées EBS servant de sauvegarde/back-up à ces volumes de stockage en cas de perte de ces derniers.

Voici le détail des volumes de stockage hébergées sur notre cloud AWS :

Nom du volume	ID du volume	type	Capacité (en GiB)	ID de l'instantanée	Ressources attachées
	vol-0b76999a5774de530	gp2	150	snap-0fd4d561c9fda0504	i-05278444474ccb152 (TEST_API_POC_Carto)
IDF_FILESERVER	vol-085936458bfee54c2	gp2	60	snap-0ddcbcd66ed3c615f	i-0f300100525fec48b (IDF_FILESERVER)
	vol-0370b968d13cd1356	gp2	30	snap-0ddcbcd66ed3c615f	i-03b28a6add802ea68 (Windows_Server_rescue_Sylvain)
	vol-0b74b3879396c57c1	gp2	20	snap-0890254dc106db76b	i-076165f3720d8f36a (Client2_Zimbra_MIG)
WALLIX_Bastion_System_disk	vol-0cf2df930f033fb4d	gp2	200	snap-04dee1d57287e60e8	i-0441332ada949fa1f (WALLIX_Bastion_PROD_[redacted])
	vol-0ec8caa3661be81ad	gp2	200	snap-00c9871693b2c35ec	i-056fc393e7f948dc8 (StormShield_SMC_Server_[redacted])
	vol-0602b0b5da618d60a	gp2	20	snap-0e084fa48f252ce38	i-0104157e6c6e333bf (Client1_Zimbra_MIG)
	vol-0dc4f7e39ba22d816	gp2	20	snap-0d4bcd0678f2ced59	i-03d7c6477d0e6c755 (VPC_BAST_FIREWALL (prod))
	vol-04fd26d7907a47f80	gp2	250	snap-070760b7737d26b0b	i-0a31d02e3f14f9557 (Merlin-Tdata)
CNPF-VIRTUALIA-IIS	vol-02f0c5d709b313059	gp2	200	snap-0e02b0f90e0343d33	i-03a1d3bf3595e4e23 (CNPF-VIRTUALIA-IIS)
Connecteur-SW2-Prod	vol-03531b0da5cd0338a	gp2	30	snap-0fd4d561c9fda0504	i-02cbeb797c8563bde (Connecteur-SW2-Prod)
GFI-CAB	vol-0e01a0f7f0d6ccdf9	gp2	20	snap-0aa29922b0227713d	i-05894ffeaed803354 (GFI-CAB)
	vol-05f4d1195b3a8abc6	gp2	40	snap-0fd4d561c9fda0504	i-0d54a06012d780c97 (Pentest Server)
CIDF_FILESERVER	vol-05ce4d3adb8148720	gp2	60	snap-0d9519affada539b0	i-0702be67a3bc721c2 (CIDF_FILESERVER)
ZIMBRA-DOCS	vol-076443f09288d311b	gp2	20	snap-05d59b825a631ad53	i-0bf413ccd7378a16e (Zimbra Docs PROD)
	vol-0ec5d9f45d1ffa0fa	gp2	500	snap-0c5b9bd7cb750baae	i-0a78ea43b44b0553f (MyMetricks Server)
	vol-053d05ce55d3edf89	gp2	8	snap-0fd4d561c9fda0504	i-0d3f4d7ca2c9e13a3 (sftp)
NAQUI_FILESERVER	vol-051103e049f92b0fe	gp2	60	snap-0ddcbcd66ed3c615f	i-0bd189e3b5baa4e57 (NAQUI_FILESERVER)
	vol-0f77ec935cd298abd	gp2	30	snap-070f5d1ca7c6e9571	i-056fc393e7f948dc8 (StormShield_SMC_Server_[redacted])
	vol-0cc1bc7907f4f0359	gp2	8	snap-0b47dd0d62c132448	i-07f0881ed89d60180 (Cryhod Share Server)
	vol-0eb30fb10a7b13661	gp2	100	snap-0d732619c92957be3	i-0ed62fa2f927be456 (Virtual Room Connector)
	vol-01b5aa0bcc3841da4	gp2	8	snap-0a9b835bbd9a8ebef	i-0fe9fb8b9cb133d11 (Bioclimsol_Auth_Server_TEST)

Retour au chapitre Retour à la table des matières

	vol-01202ee91ab5d69ff	gp3	100	snap-0fd4d561c9fda0504	i-0db611651c98e8677 (BioClim_Test)
	vol-061d80f429197ef0e	gp3	30	snap-02c8e52e20773ea3f	i-022a87ab89f348492 (CNPF-ILEX)
	vol-00963bd603d47333b	gp3	250	snap-0e92d9802bb36eeb7	i-0b75d571d399a936b (API_Carto_enjeux (Recette))
Climessences-v2	vol-043a66963cef87042	gp3	300	snap-02c8e52e20773ea3f	i-0f9bdcb6bad85d550 (Climessences-recette_v1.0.0)
CNPF-nextCloud	vol-07cd6f1ef83a90b22	gp3	500	snap-0519c238f55e58aef	i-0c82987b761e666be (CNPF-Nextcloud[redacted]
veeam console	vol-043b9c871468bbc00	gp3	20	snap-031b30c6fafa44df2	i-06177bc1ef5077dd8 (Veeam Console)
mig-CNPF-carto	vol-0513b0ba176440aa8	gp3	50	snap-027f710833c1831b1	i-0a79d7d9b85d17f7b (CNPF-CARTO)
Testaugapo	vol-0a409abd399be7ffc	gp3	300		i-0ab4fd28975f98178 (CNPF_McAfee_1)
Wallix AM	vol-0f98f270014269856	gp3	14	snap-02db18c02192bc2ca	i-0aaaf8529c21b5ce8 (WALLIX_Access_Manager_PROD_[redacted]
	vol-052831644b9460543	gp3	200	snap-0bfcac98461fffb57	i-0825ce02ed72d68ec (LFB-V1-preprod)
rect-merlin	vol-0eb3fe40b9a6dc3fa	gp3	1 000	snap-045c848921dc88949	i-066bd7997b4bedafc (Recette-Merlin)
mig-CNPF-ACTIV	vol-05e89baed45c6bd15	gp3	30	snap-02c8e52e20773ea3f	i-04a12babed9c6d6fe (CNPF-ACTIV)
CNPF-VIRTUALIA-APPLI	vol-061b581c35de6be06	gp3	500	snap-01a88b213666e96f8	i-09dcf239575356b9b (CNPF-VIRTUALIA-APPLI_RESTORED)
APO-JAR-teltransmission-PHU-BPE	vol-05e0ccc531553f87c	gp3	30	snap-050a30497679237f7	i-0b42a20ea1fc56b5a (APO-JAR-teltransmission-PHU-BPE)
PACA_FILESERVER	vol-02cf7d812cd4532dc	gp3	60	snap-0d9519affada539b0	i-0fa783fe484e6e83b (PACA_FILESERVER)
	vol-0b59bf1fb9c53156d	gp3	20	snap-0d4c7fe6f7036eee1	i-0e6dfbe6cab443307 (NetsKope Publisher)
FPF-preprod	vol-0e4272dfe3151a6f4	gp3	100	snap-0519c3c3d5aa016d4	i-054af68e633d50f97 (FPF-prod_bo)
CNPF-VIRTUALIA-APPLI	vol-0203a843a200b3ff4	gp3	500	snap-0e02b0f90e0343d33	i-0ad3b635801c8889c (CNPF-VIRTUALIA-APPLI)
BioClimSol_V2_prod	vol-05517837891b48ec7	gp3	8	snap-03b199492b0572b61	i-05ed399c73337757c (BioClimSol_V2_prod)
	vol-015ef53f482e94c5c	gp3	60	snap-093292eb484470f74	i-00b49ff4751c5958e (Virtualia v5 - Form)
FPF-prod	vol-061530b5563c59d41	gp3	100	snap-06455b2f31764fdc6	i-0f4f3883b4b4f05d1 (FPF-prod_fo)
	vol-01e44c3220793d62e	gp3	30	snap-0a4ea7d387cdca4da	i-0ebfbba3170f5421e (Zimbra Server PROD [redacted])
	vol-08e2f16507041036a	gp3	100	snap-023e7eb417b08a13a	
CNPF-SGM	vol-04b029ba27059870f	gp3	100	snap-0de00c0b6127adef9	i-0cf2311f09cac456c (StreamGoomer Manager)
Climessences	vol-01853e727825768f0	gp3	1 200	snap-07b29d06dfb31e0a8	i-014dce4c3324003a3 (Climessences-prod_v1.0.0)
chasse	vol-09956ebd48f1364d0	gp3	8	snap-0e0ae5d0f6f76b560	i-03d2452c55fe57125 (foret-gibier)
	vol-047e467921d1f3c5e	gp3	50	snap-0b33635813ceafa8c	i-031a25934b7ecb1b2 (secoia preprod)
	vol-0160ecb12bb9e277c	gp3	100		i-061a72926ef8c9fa5 (CNPF_ADSERVER)
	vol-0a6a150b05ea8ccca	gp3	200	snap-01e1059e33a7d0e2d	i-0a1fc61801ad023a9 (CNPF-web-preprod_Cloned)
FRCT-recette	vol-051b4854c2504a217	gp3	250	snap-0ad0e34a42898db0e	i-030c0be689086ff48 (FRCT-recette)
	vol-0d7d1883d6bfebaab	gp3	200	snap-05159589c1960cefb	i-09cfafd5638d8e6e7 (SUADEO_Recette)

	vol-04395955063dd9d28	gp3	20	snap-091ed6b03f0e44fe7	i-00b49ff4751c5958e (Virtualia v5 - Form)
	vol-0cae6db1415a2dd04	gp3	60	snap-0bfa8d4318ebd046a	i-0bb2e8e2d84547401 (RDP_CNPF_Voir_Balises)
	vol-0957b333b6bcc3806	gp3	60		i-0db090a410cb4f1db (VirtualiaV5 - Prod)
	vol-038cdb71fc8e31fa6	gp3	30	snap-029a7cff5bff609ac	i-0150f2d3d31a00b2f (New_Photofor)
	vol-0abfb900081587a56	gp3	300	snap-0ac3be67383fef271	i-07d9b09084a427984 (CNPF-RDP-Gateway & acs.fr DC)
AURA_FILESERVER	vol-0280b941b10b7d3a7	gp3	60	snap-0d9519affada539b0	i-01f04524ee740ef2a (AURA_FILESERVER)
	vol-0ef7c7e95d6896015	gp3	200	snap-0cb5541f233863316	i-0c0a9fb2ff85b09ba (Zimbra Server TEST [redacted])
	vol-026350035535fbc2e	gp3	100	snap-05f86fc3e6233bed4	i-093c60fe94e3fdca1 (CNPF-GFIpep)
	vol-019409ae227b0c040	gp3	800	snap-0d777ec9dfc032750	i-086c6a24f363ffd23 (srvobm.cnpf.fr)
	vol-091e49e0efaa8313e	gp3	50	snap-0cad5739a8003a469	i-07bdb7b8be8d82b4f (Wapt Server)
SonarQube	vol-052737e14fbb74018	gp3	1000	snap-0a9b835bbd9a8ebef	i-01ce916d98337949f (SonarQube Server)
FRCT-dev	vol-0695eb29201555e07	gp3	30	snap-050a30497679237f7	i-02d368fe77a1f7142 (FRCT-dev)
GFIPep - Data Disk	vol-0d80cf9ce1ead0f9e	gp3	1 000		i-093c60fe94e3fdca1 (CNPF-GFIpep)
SUADEO_Serveur_application	vol-048762334d94522cd	gp3	200	snap-0986ce6d1df6990f1	i-0aa2b0d958a5c82fa (SUADEO_Serveur_application)
AD_CENTRAL_Disk_system	vol-021e55d3ff5e6692e	gp3	100	snap-0d9519affada539b0	
	vol-00482476bda4b3bd5	gp3	500	snap-0dbf6ea966781b5ca	i-01246656413ce8e9f (StreamGoomer Collector)
	vol-0abae1a96f40610cc	gp3	230	snap-0a6c154aa2b7beca3	i-0ebfbba3170f5421e (Zimbra Server PROD [redacted])
Dev_softeam_Portail_carto	vol-0448f94e4442af35d	gp3	100	snap-050a30497679237f7	i-0c76f653e25f400b8 (SFT_POC_Carto_Cadastre)
	vol-03e9e6d22ba9e4215	gp3	30	snap-0fd4d561c9fda0504	i-039c2b75783701ce5 (Matomo)
OCCI_FILESERVER	vol-04f81e243d5970b15	gp3	60	snap-0d9519affada539b0	i-09623837b31ea7f3f (OCCI_FILESERVER)
BFC_FILESERVER	vol-0695c90daf6e630b9	gp3	60	snap-0d9519affada539b0	i-022e6747119565f4 (BFC_FILESERVER)
CNPF-API	vol-04ca7ebcacf167324	gp3	20	snap-0fd4d561c9fda0504	i-0cea583a26e80bed3 (CNPF-API)
FRCT-recette	vol-008e6d7a7932243f1	gp3	500	snap-050a30497679237f7	i-04f25f919638e34d3 (FRCT-prod)
	vol-04bee680013460e28	gp3	100	snap-023e7eb417b08a13a	
BPDL_FILESERVER	vol-0601225c861591c02	gp3	60	snap-0d9519affada539b0	i-0a7f4b7c9b2773b19 (BPDL_FILESERVER)
Graylog	vol-06ceabe403a0e5a76	gp3	60	snap-07554d529170adbff	i-0093041badac5910a (Graylog)
mig-merlin-a	vol-0b875925109a4d74f	gp3	500	snap-037690fd9c3135de7	i-08b412f096091ce59 (CNPF-Merlin)
mig-CNPF-ocsinventory	vol-0ee20078deae4f187	gp3	20	snap-07eadafdd43698e38	i-0e4478bc260c27899 (CNPF-ocsinventory PROD [redacted])
	vol-0af9e0d955fb01a4a	gp3	100	snap-0d57ef2ab200bff3d	i-0d06d97def251d1f4 (BioClimSol-Dev-Test)
	vol-0f9cc7bbecf22d65d	gp3	20	snap-091ed6b03f0e44fe7	i-03a346fa53dd48471 (VirtualiaV5 - Test)
Gitlab	vol-0296549b6ddb9bd67	gp3	1 000	snap-0a9b835bbd9a8ebef	i-00ed7f75a76832bb2 (Gitlab Server)
LFB-MongoDB	vol-0cf496cac4bf78f8c	gp3	30	snap-050a30497679237f7	i-01121aeb9f4132c97 (LFB-MongoDB)

Retour au chapitre Retour à la table des matières

Redmine-4.1.0	vol-082316d5e713223fa	gp3	100	snap-08c69965927f8344c	i-02a72cbb3e8ceca27 (Redmine-[redacted]
	vol-02edf965630b5a21d	gp3	100	snap-0a9b835bbd9a8ebef	i-084e466885263652f (Gitlab Runner)
	vol-0b016ebe4e57e6eec	gp3	50	snap-06dfd5f2ccf4f0923	i-0012342a7248e6ee9 (secoia_v2 server (2nd installation) - (VPC Webint - ss1))
RTL Catalogue	vol-01a95a2ff9200516c	gp3	120	snap-077c1706e27ac0cbd	i-0ad4476b41003b653 (RLT_Catalogue_2)
	vol-07dbff07923c3c4c8	gp3	200	snap-0fd4d561c9fda0504	i-04cf242eb5d4e0742 (CNPF-web-prod)
	vol-077ff8a08be02f4c9	gp3	8	snap-03b199492b0572b61	i-0a7d3d9fa64809e0b (Gophish_Server)
	vol-00291b2ec99bc4d13	gp3	60	snap-093292eb484470f74	i-03a346fa53dd48471 (VirtualiaV5 - Test)
	vol-042c96ace391c0d90	gp3	200	snap-0bfcac98461fffb57	i-059a5928072dd405f (LFB-V1-recette)
lldap02	vol-0301ae64c07a00c99	gp3	50	snap-098a0f3e1be7df9b9	i-090ab342ceca42675 (LDAP Server (ldap Old))
LFB-prod	vol-06caf859916cd476d	gp3	200	snap-0ba2f88d3b886dc11	i-0bafc04048ddc9054 (LFB-V1-prod)
	vol-03766912d84a8eb18	gp3	10	snap-03b199492b0572b61	i-0db090a410cb4f1db (VirtualiaV5 - Prod)
LFB-drupal9	vol-00183635db2051481	gp3	200	snap-046837f7c2a57ea3d	i-00f55ac6c94e7c718 (LFB-V2-recette-drupal9)
sylvi-par	vol-04e492a25740b375b	gp3	100	snap-07b29d06dfb31e0a8	i-0ecf982146a6fa556 (sylvi-par)
	vol-0ba4ee013ed35bb74	gp3	60	snap-0d08fe72ea55e1e24	i-053072ff7ee9b44cc (antispam)
FPF-dev	vol-07e76372adca470df	gp3	100	snap-0519c3c3d5aa016d4	i-097b9c1f49cede2c3 (FPF-dev)
Climessence-preprod_v1.0.0	vol-026d8e21a5802f9e8	gp3	300	snap-0fd4d561c9fda0504	i-0b3dcb4ebecc02c44 (Climessences-preprod_v1.0.0)
CNPF-VIRTUALIA-IIS1	vol-0038706a9030a238e	gp3	200		i-03a1d3bf3595e4e23 (CNPF-VIRTUALIA-IIS)
Portail-authentification	vol-059c657a924560a40	gp3	20	snap-005a07055e027b5bc	i-0534e5b0ed88e8e56 (Portail-authentification-V2 ([redacted]))
Recette-Teletrans-Serveur	vol-0386d0310dda170b4	gp3	30	snap-050a30497679237f7	i-04681d6d6f9b87b4f (Recette-Teletrans-Serveur)
mig-merlin-b	vol-00c4039d257914330	gp3	1 000		i-08b412f096091ce59 (CNPF-Merlin)
CNPF-VIRTUALIA-APPLI1	vol-05ec0317adc745dba	gp3	500	snap-07576a48598510516	i-09dcf239575356b9b (CNPF-VIRTUALIA-APPLI_RESTORED)
	vol-08c05d9e61e3a357a	gp3	150	snap-0a2c80e151b6c6c8b	i-0ab4fd28975f98178 (CNPF_McAfee_1)
rect-merlin	vol-0f9904d3219c4f45d	gp3	500	snap-0b25090e2559ee9e1	i-066bd7997b4bedafc (Recette-Merlin)
CNPF-VIRTUALIA-APPLI1	vol-0542a1f4a1aad3c58	gp3	500		i-0ad3b635801c8889c (CNPF-VIRTUALIA-APPLI)
	vol-0db46ab98a7bffffd	gp3	500		i-0012342a7248e6ee9 (secoia_v2 server (2nd installation) - (VPC Webint - ss1))
mig-CNPF-DNS2	vol-0527b8edd4bcd7072	gp3	8	snap-02c8e52e20773ea3f	i-02f5c3d4ea31a49ad (mig-CNPF-DNS2)
	vol-03a81daf349492f70	gp3	10	snap-039e1cb625872a504	i-0400a0529479e625a (TheGreenBow TAS Server)
mig-CNPF-DNS1	vol-0590d4020d65d8119	gp3	8	snap-02c8e52e20773ea3f	i-0509b896288e73fbe (CNPF-DNS1 (PROD))
	vol-0dd5e979ea720d187	gp3	8	snap-0829453c21ec783a0	i-0e6d4854b1da6d874 (cnpf-SG)
GEST_FILESERVER	vol-06e3fb027de9ce4da	gp3	60	snap-0d9519affada539b0	i-01cf3cf239150aff9 (GEST_FILESERVER)
testaugapo1	vol-0eccda4f72f12184c	gp3	100		i-0ab4fd28975f98178 (CNPF_McAfee_1)

11

Retour au chapitre Retour à la table des matières

HDFN_FILESERVER	vol-069087f300fe982d2	gp3	60	snap-0d9519affada539b0	i-08fad5eb92cbde14f (HDFN_FILESERVER)
Central_File_Serveur_DisqueDur_01	vol-0ce78137ebfe65ec7	gp3	4 000		
	vol-0d58469e5692bd3a3	gp3	300	snap-054d7263422afd9d6	i-0014f2b9e861ee110 (Climessences V1 Recette Drupal10)
	vol-06da8d9eb8fea41fe	gp3	30	snap-0257f3099d23a15fc	i-0c0a9fb2ff85b09ba (Zimbra Server TEST ([redacted]))
RLE-DVF	vol-00be968cccd664b1b	gp3	30	snap-07b29d06dfb31e0a8	i-03dfffae96e4ef119 (CNPF_DVF_foncier)
CNPF-LDAP	vol-07c9559147019e840	gp3	8	snap-0fd4d561c9fda0504	i-09468b02d2d6bab39 (CNPF-LDAP (ldap New))
TSE_ACS_SERVER_RESTORED	vol-0908b32574d99c6c0	gp3	200		i-04c5593fe32f8e8d6 (Windows_[redacted]_TSE_Server _(PROD))
DG_FILESERVER	vol-0a052569f22fc230a	gp3	100	snap-0d9519affada539b0	i-022748bec937a416b (DG_FILESERVER)
	vol-0702a6935aec82c78	gp3	16	snap-0675087ee1c2db4c2	i-06177bc1ef5077dd8 (Veeam Console)
Mailcatcher	vol-07f35583679b95993	gp3	8	snap-02c8e52e20773ea3f	i-03e50c40a7cd8fca3 (Mailcatcher)
BPDL_FILESERVER	vol-0a1ca45c951b4a682	sc1	10 000		i-0a7f4b7c9b2773b19 (BPDL_FILESERVER)
GEST_FILESERVER	vol-0364ac4ef401c0382	sc1	10 000		i-01cf3cf239150aff9 (GEST_FILESERVER)
OCCI_FILESERVER	vol-0f7f40b99dc502622	sc1	10 000		i-09623837b31ea7f3f (OCCI_FILESERVER)
IDF_FILESERVER	vol-07e2fa48118249177	sc1	10 000		i-0f300100525fec48b (IDF_FILESERVER)
	vol-03c2ac2e9cae83e2f	sc1	1 000		i-0150f2d3d31a00b2f (New_Photofor)
AURA_FILESERVER	vol-0be0ac072a05431af	sc1	10 000		i-01f04524ee740ef2a (AURA_FILESERVER)
PACA_FILESERVER	vol-0a37e91ad405f857f	sc1	10 000		i-0fa783fe484e6e83b (PACA_FILESERVER)
DG_FILESERVER	vol-09e518d54461d308c	sc1	10 000		i-022748bec937a416b (DG_FILESERVER)
Cloud Extension	vol-004de3879354e72c9	sc1	1 500		i-0c82987b761e666be (CNPF-Nextcloud ([redacted]))
BFC_FILESERVER	vol-0609742bbcf2ee9af	sc1	10 000		i-022e6747119565f4 (BFC_FILESERVER)
BioClimSol_V2_prod	vol-086574e9ac0c60fab	sc1	125		i-05ed399c73337757c (BioClimSol_V2_prod)
	vol-0dea77dbcca6cd942	sc1	1 000	snap-085662adad3455ebe	i-0c0a9fb2ff85b09ba (Zimbra Server TEST ([redacted]))
ZIMBRA HSM	vol-0531bdff07a9529cc	sc1	1 300	snap-0a5d152333602c254	i-0ebfbba3170f5421e (Zimbra Server PROD ([redacted]))
CIDF_FILESERVER	vol-087d1bd428d0d0fcd	sc1	10 000		i-0702be67a3bc721c2 (CIDF_FILESERVER)
HDFN_FILESERVER	vol-0367627b5c0f18d19	sc1	10 000		i-08fad5eb92cbde14f (HDFN_FILESERVER)
NAQUI_FILESERVER	vol-0cd603ef7281f5b31	sc1	10 000		i-0bd189e3b5baa4e57 (NAQUI_FILESERVER)
	vol-0079b83f8eb9e0529	st1	500	snap-02bf3ec4eadc56a03	i-031a25934b7ecb1b2 (secoia preprod)

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CNPF

1.3. AMI

Notre infrastructure Cloud héberge **38** AMI, dont 37 AMI fonctionnelles et 1 AMI désactivée, qui sont les suivantes :

Nom de l'AMI	ID de l'AMI	Type	Volume	Platforme
stormshield_eva_firewall_backup_26_01_2022	ami-084563700dfa7690e	gp2	11 Gio	Linux/UNIX
CNPF-web-prod-avant-MEP-Aforce	ami-01dc9738640b2da75	gp3	200 Gio	Linux/UNIX
climessences-preprod-1	ami-0eaeb5e73e445964b	gp2	900 Gio	Linux/UNIX
Redmine_4.1.0	ami-07fd04c8a57c02b20	gp3	100 Gio	Linux/UNIX
AD_Central_AMI	ami-0bb6a3f93c1bfa43a	gp3	100 Gio	Windows
portailcarto_svg	ami-0cc60f1510431242d	gp3	50 Gio	Linux/UNIX
climessences recette	ami-0cab206e80f47d042	gp3	300 Gio	Linux/UNIX
LFB-prod_5.1.5	ami-052dde359ec92366d	gp2	200 Gio	Linux/UNIX
lfb-psg_test	ami-09147a1c5cc898606	gp2	200 Gio	Linux/UNIX
climessences-preprod-2	ami-014fdb278402ff906	gp2	900 Gio	Linux/UNIX
Serveur_API_Carto_enjeux_Recette	ami-0e45ddb43e37c0b2b	gp3	250 Gio	Linux/UNIX
frct-mise-en-production	ami-014ee99bfd15342b6	gp2	250 Gio	Linux/UNIX
windows_client_VPC_BAST_26_01_2022	ami-0619294d13ced90d5	gp2	30 Gio	Windows
import-ami-0613722d65add7c41	ami-0ed77564dfa60fd8e	gp2	20 Gio	Linux/UNIX
img_merlin_c	ami-096dc1a84caa8217b	gp3	500 Gio	Windows
Veeam_appliance_backup_16_11_2024	ami-0f9ce92142bcb62f5	gp3 gp3	16 Gio 20 Gio	Linux/UNIX
LFB-Prod 5.1.10	ami-0002a461b6f9d5bfc	gp3	200 Gio	Linux/UNIX
AMI Climessences V1 Recette	ami-0bca77bc66a17fdbf	gp3	300 Gio	Linux/UNIX
Backup_Climessence_prod_avant test migration	ami-08a73a64720928992	gp3	1200 Gio	Linux/UNIX
import-ami-0e23ba81617a8c473	ami-0facba9242c492104	gp2	500 Gio	Linux/UNIX
LFB-psg_deploy	ami-035e74a0b69287a90	gp2	200 Gio	Linux/UNIX
cloud_image	ami-0c5b0e7a71454d8f1	gp3	500 Gio	Linux/UNIX
Climessences-recette_v1.1.0	ami-00481010ed390352f	gp3	300 Gio	Linux/UNIX
virtualia_v5	ami-0dd077f4973880b9a	gp3 gp3	10 Gio 60 Gio	Linux/UNIX
CNPF-SECU-STORMSHIELD	ami-0dcc4647c2930b001	gp3	30 Gio	Linux/UNIX
LFB_prod_V2.0	ami-078736d4b7519d3df	gp2	200 Gio	Linux/UNIX
LFB-prod_5.1.6	ami-09593ab30cf897faa	gp2	200 Gio	Linux/UNIX
CNPF_DVF_foncier	ami-0b29befd0cf9bf05f	gp2	30 Gio	Linux/UNIX
AWSSupport-CopyEC2Instance Source for i-08b94548cb46afa18_2024-08-13_16.08.24	ami-05804954f1bf0b0cf	gp3 st1	50 Gio 500 Gio	Linux/UNIX
preprop_to_prod	ami-0bc98d645a1febe00	gp3	200 Gio	Linux/UNIX
srvobm2020-12-01	ami-04b61d4d5b38f8801	io1	640 Gio	Linux/UNIX
linux_client_VPC_BAST_26_01_2022	ami-04f1b17dab1e8e86c	gp2	8 Gio	Linux/UNIX
secoia_backup_02_09_2022	ami-0e5146b2b049393a1	gp3 st1	50 Gio 500 Gio	Linux/UNIX
import-ami-00db1aa850267016a	ami-0eb172b920090c1cd	gp2	100 Gio	Linux/UNIX
aws-FW image	ami-0f608c1f780230798	gp3	30 Gio	Linux/UNIX
image_secoia_prod	ami-062bb1184fb48e4a3	gp3 gp3	50 Gio 500 Gio	Linux/UNIX
backup_OCS_inventory_prod_avant_MAJ_2023_02_10	ami-0221e42836499c198	gp3	20 Gio	Linux/UNIX
shinken_20191123 **(désactivée)**	ami-098adf968225af654	gp2	30 Gio	Linux/UNIX

Retour au chapitre Retour à la table des matières

2. Services réseaux

2.1. Arborescence des réseaux

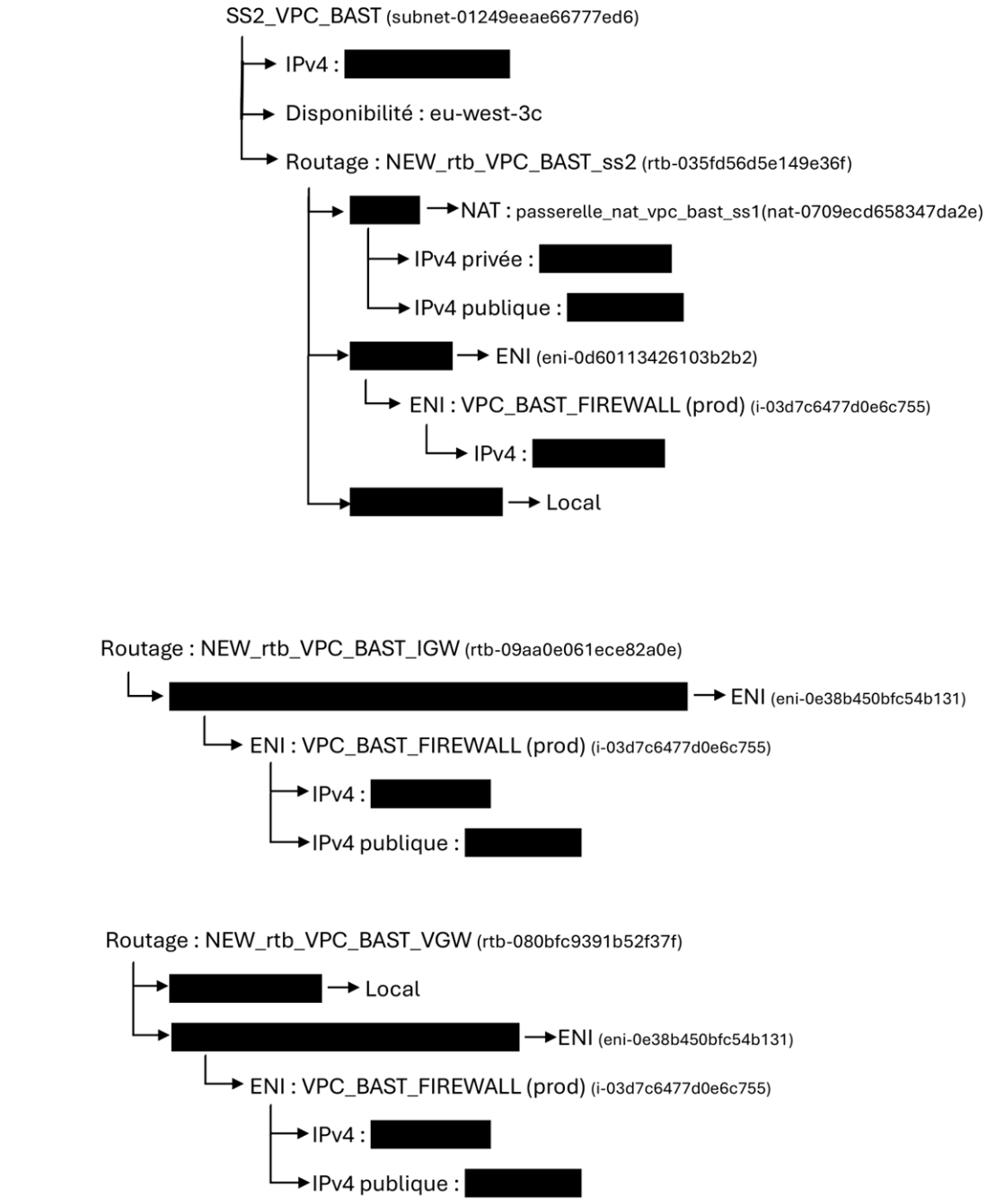
2.1.1. VPC « BAST »

Le VPC « BAST » héberge le Stormshield Management Center (SMC), le point central de gestion des différents pare-feu installés sur chacun des plus de 100 sites CNPF en France. Afin que l'accès à cette instance sensible soit sécurisé, un pare-feu virtuel a été mis en place, servant de point de passage entre la passerelle d'entrée au VPC BAST et la SMC hébergée sur un autre sous-réseau que le pare-feu virtuel.

Le réseau est construit à l'aide de différents services réseaux AWS de la façon décrite ci-dessous :

VPC : VPC_BAST (vpc-02f86d740e1197b70)
- ACL réseau : acl-0c30f096894b35ef8
  - Jeux d'options DHCP : option_amazon_DNS (dopt-b1efb4d8)
- Sous-réseaux :
  - SS0_VPC_BAST (subnet-03b8c4f9e063cc945)
    - IPv4 : [redacted]
    - Disponibilité : eu-west-3c
    - Routage : NEW_rtb_VPC_BAST_ss0 (rtb-0b2aa06d606924c05)
      - [redacted] → IGW_VPC_BAST (igw-075c63f316f7e0474)
      - [redacted] → AWS_VPC_BAST (vgw-0bfa1f6cb05b4830b)
      - [redacted] → Local
  - SS1_VPC_BAST (subnet-0bcdf7c4b0e9527ef)
    - IPv4 : [redacted]
    - Disponibilité : eu-west-3c
    - Routage : NEW_rtb_VPC_BAST_ss1 (rtb-0720098d3bf4dadb1)
      - [redacted] → ENI (eni-0d60113426103b2b2)
        - ENI : VPC_BAST_FIREWALL (prod) (i-03d7c6477d0e6c755)
          - IPv4 : [redacted]

14



15

Retour au chapitre Retour à la table des matières

2.1.2. VPC « WEBINT »

Le VPC « WEBINT » héberge des instances d'applications métiers, mais aussi des instances de test. Ce réseau est minime dans notre environnement cloud et n'a pas de but particulier d'hébergement.

Le réseau est construit à l'aide de différents services réseaux AWS de la façon décrite ci-dessous :

VPC : VPC_WEBINT (vpc-0eae2b28e5df119dc)
- ACL réseau : acl-0c7aafebde6a126d6
  - Jeux d'options DHCP : option private DNS (dopt-0f62795a9becbafc4)
- Sous-réseaux :
  - SS0_VPC_WEBINT (subnet-08bebb0d4be8e6f3f)
    - IPv4 : [redacted]
    - Disponibilité : eu-west-3c
    - Routage : rtb_VPC_WEBINT_ss0 (rtb-089ffe478364b628d)
      - [redacted] → IGW_VPC_BAST (igw-075c63f316f7e0474)
      - [redacted] → VGW : AWS_VPC_BAST (vgw-0bfa1f6cb05b4830b)
      - [redacted] → Local
      - [redacted] → PCX-VPC_Webint-VPC_aws1 (pcx-0494af28db4bfdb6b)
  - SS1_VPC_WEBINT (subnet-0e8c4a813bde8da4c)
    - IPv4 : [redacted]
    - Disponibilité : eu-west-3c
    - Routage : rtb_VPC_WEBINT_ss1 (rtb-06bade2455c196c7c)
      - [redacted] → Local
      - [redacted] → PCX-VPC_Webint-VPC_aws1 (pcx-0494af28db4bfdb6b)
      - [redacted] → VGW : AWS_VPC_BAST (vgw-0bfa1f6cb05b4830b)
      - [redacted] → IGW_VPC_BAST (igw-075c63f316f7e0474)

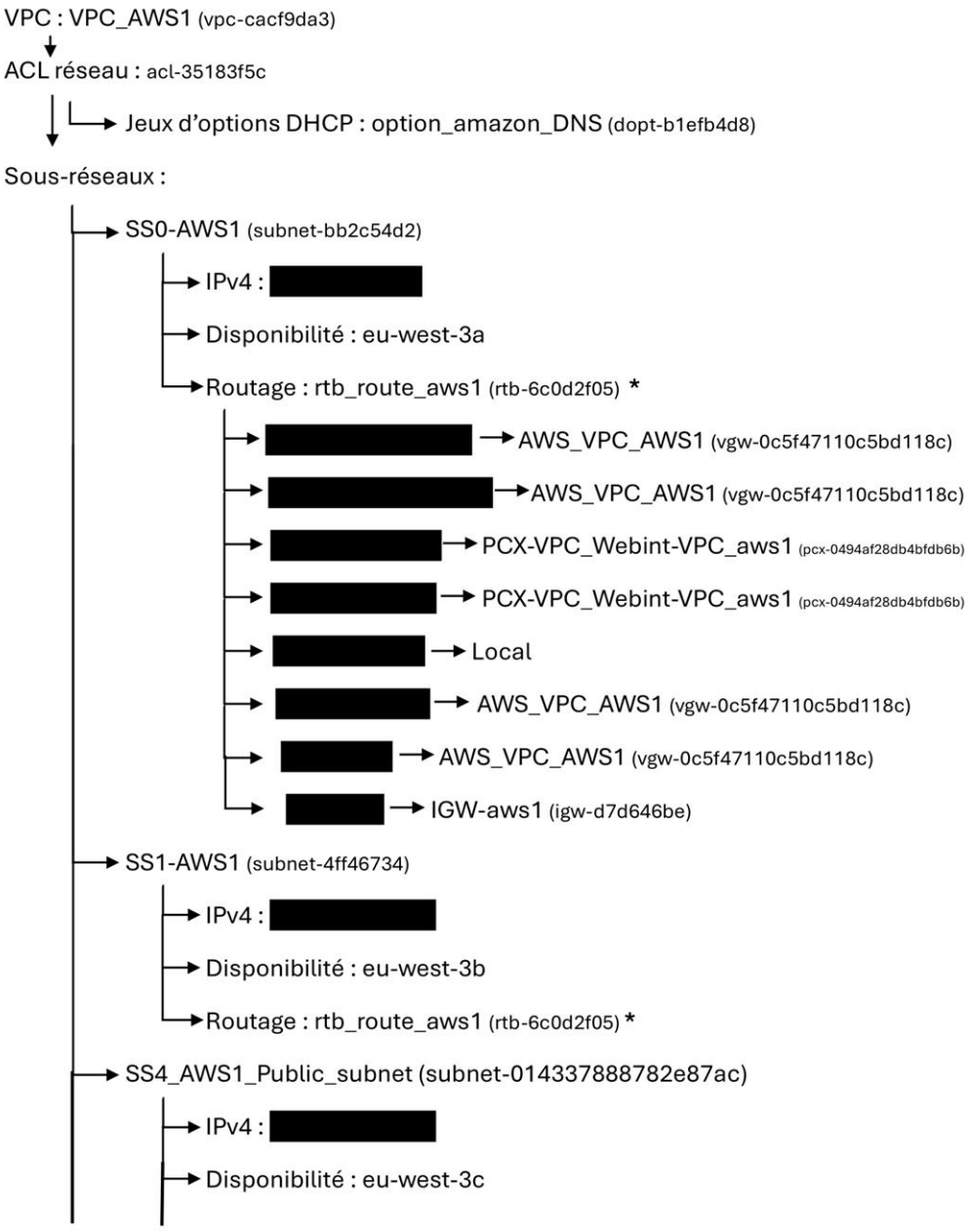
16

Retour au chapitre Retour à la table des matières

2.1.3. VPC « AWS1 »

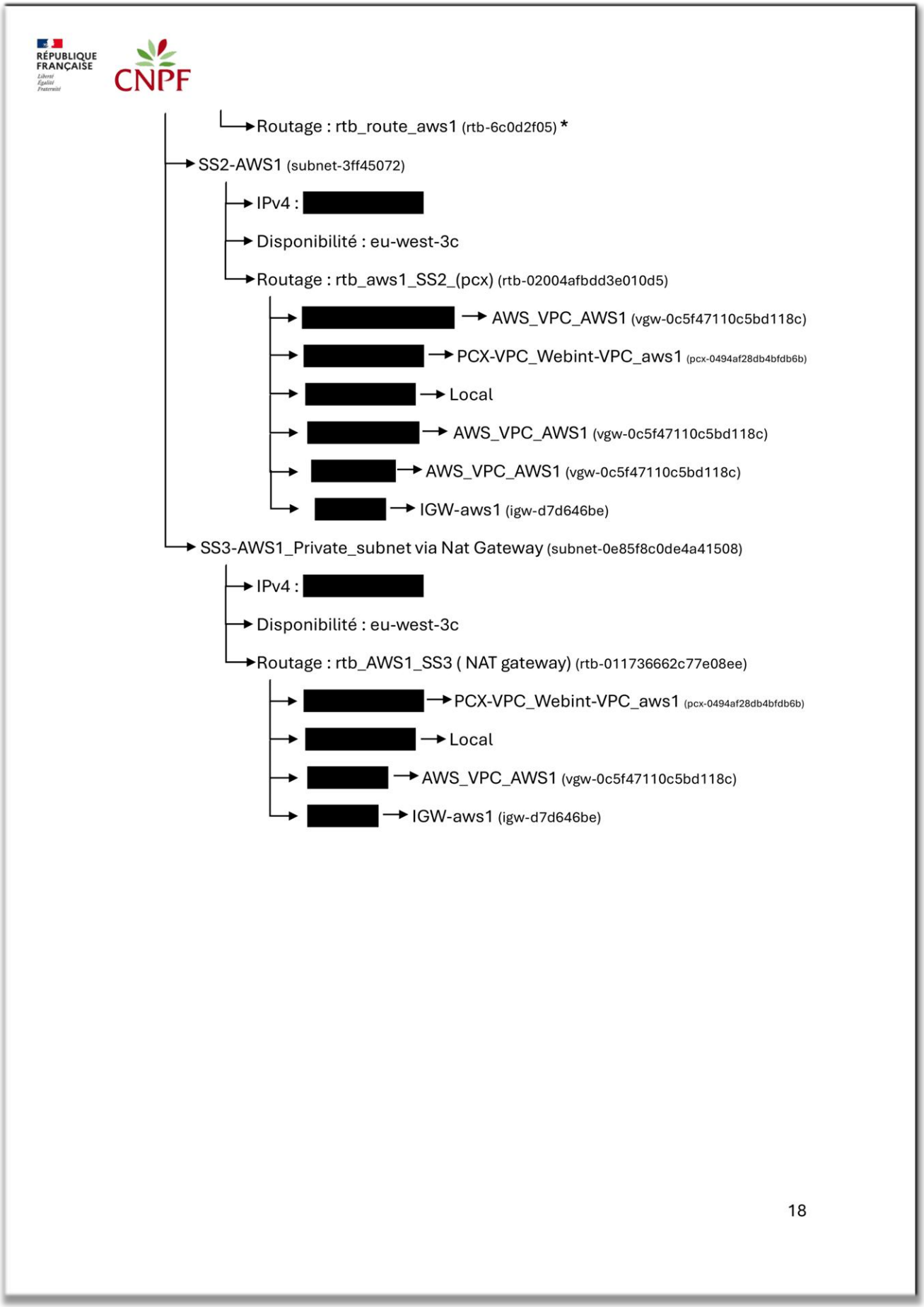
Le VPC « AWS1 » joue le rôle du réseau privé central. Il héberge la grande majorité de notre infrastructure cloud.

Le réseau est construit à l'aide de différents services réseaux AWS de la façon décrite ci-dessous :



17

Retour au chapitre Retour à la table des matières



Retour au chapitre Retour à la table des matières

2.2. Détails des composantes réseaux

2.2.1. Elastic IP (EIP)

Notre infrastructure Cloud AWS héberge **5** EIP, parmi lesquelles 2 sont rattachées à des instances EC2 et 3 autres à des passerelles NAT.

En voici les détails :

IP privée	ID interface réseau	ID allocation	ID association
[redacted]	eni-0a42d8d96c3d270ad	eipalloc-0e92aa086a92b45d1	eipassoc-019ce6851561392f2
	eni-0d28158b02599d2d0	eipalloc-0fe19be682ef7c4b9	eipassoc-0ee2dbe61253b15e5
	eni-086d054925326c05e	eipalloc-067aa372b7502cd28	eipassoc-0cbe277109138193c
	eni-0276d2ed7fd0b17c7	eipalloc-040915388a95454eb	eipassoc-0aa34696f1d29cf85
	eni-0627291de404ef117	eipalloc-0de17cfb2cab3a52	eipassoc-047f6ac8fdb57e70d

ID instance associée	ID passerelle NAT associée	DNS inverse
	nat-00bbd9202c75dac06 (passerelle NAT - VPC AWS1)	
	nat-0709ecd658347da2e (passerelle_nat_vpc_bast_ss1)	
i-0509b896288e73fbe		[redacted]
	nat-0cf2784f089ce1bef (passerelle NAT - VPC WEBINT SS0)	
i-053072ff7ee9b44cc		[redacted]

2.2.2. Passerelle NAT

Notre infrastructure Cloud AWS héberge actuellement **3** passerelles NAT, dont chacune d'entre elles est rattachées à une ENI.

En voici les détails :

Références	PASSERELLES NAT		
Nom	passerelle NAT - VPC AWS1	passerelle_nat_vpc_bast_ss1	passerelle NAT - VPC WEBINT SS0
ID NAT	nat-00bbd9202c75dac06	nat-0709ecd658347da2e	nat-0cf2784f089ce1bef
ID ENI	eni-0a42d8d96c3d270ad	eni-0d28158b02599d2d0	eni-0276d2ed7fd0b17c7
type	publique	publique	publique
IP publique	[redacted]		
IP privée			
VPC	AWS1	VPC_BAST	VPC_WEBINT
Sous-réseau	SS2-AWS1	SS1_VPC_BAST	SS0_VPC_WEBINT

2.2.3. Passerelle privée virtuelle (VGW)

Notre infrastructure Cloud AWS héberge **3** VGW, chacune d'entre elles est rattachées à un VPC.

En voici les détails :

Nom VGW	ID VGW	type	VPC attaché
AWS_VPC_WEBINT	vgw-03b6ed00e950ff49b	[redacted]	vpc-0eae2b28e5df119dc | VPC_WEBINT
AWS_VPC_AWS1	vgw-0c5f47110c5bd118c		vpc-cacf9da3 | AWS1
AWS_VPC_BAST	vgw-0bfa1f6cb05b4830b		vpc-02f86d740e1197b70 | VPC_BAST

2.2.4. Passerelle Internet (IGW)

Notre infrastructure Cloud AWS héberge **3** IGW, chacune d'entre elles est rattachées à un VPC.

En voici les détails :

Nom IGW	ID IGW	VPC attaché
IGW_VPC_BAST	igw-075c63f316f7e0474	vpc-02f86d740e1197b70 | VPC_BAST
IGW_VPC_WEBINT_internet_gateway	igw-0b13e937e20ce694d	vpc-0eae2b28e5df119dc | VPC_WEBINT
IGW-aws1	igw-d7d646be	vpc-cacf9da3 | AWS1

2.2.5. Connexion d'appairage (PCX, VPC peering)

Notre infrastructure Cloud AWS héberge **1 unique** PCX. Ce dernier sert de passerelle pour le trafic entre le VPC AWS1 et le VPC WEBINT uniquement.

En voici les détails :

Nom du PCX	ID du PCX
PCX-VPC_Webint-VPC_aws1	pcx-0494af28db4bfdb6b

VPC du demandeur	Réseau du demandeur	Disponibilité	Résolution DNS
vpc-0eae2b28e5df119dc / VPC_WEBINT	[redacted]	eu-west-3	Désactivée
VPC de l'accepteur	**Réseau de l'accepteur**	**Disponibilité**	**Résolution DNS**
vpc-cacf9da3 / AWS1	[redacted]	eu-west-3	Activée

ID de la table de routage	VPC	Principal	Association de sous-réseaux
rtb-06bade2455c196c7c	VPC_WEBINT	Non	SS1_VPC_WEBINT
rtb-011736662c77e08ee	AWS1	Non	SS3-AWS1_Private_subnet via Nat Gateway
rtb-02004afbdd3e010d5	AWS1	Non	SS2-AWS1
rtb-089ffe478364b628d	VPC_WEBINT	Oui	SS0_VPC_WEBINT
rtb-6c0d2f05	AWS1	Oui	Aucun sous-réseaux

2.2.6. Point de terminaison (Endpoint)

Notre infrastructure Cloud AWS héberge **1 unique** Endpoint, permettant aux deux sous-réseaux SS0-AWS1 et SS1-AWS1 du VPC AWS1 d'accéder aux ressources du service « com.amazonaws.vpce.eu-west-3.vpce-svc-09542670dacfa661b ».

En voici les détails :

ID Endpoint	ID de VPC	Sous-réseaux	Disponibilité	IP privée	ID de l'ENI
vpce-04ecc7007a245498f	vpc-cacf9da3 (AWS1)	subnet-4ff46734 (SS1-AWS1)	eu-west-3b	[redacted]	eni-02d78baadc65e3747
		subnet-bb2c54d2 (SS0-AWS1)	eu-west-3a	[redacted]	eni-07512ecb3ca3e1175

2.2.7. Jeux d'options DHCP

Notre infrastructure Cloud AWS héberge **2** jeux d'options DHCP.

En voici les détails :

Nom	ID	Nom de domaine	Serveur DNS
option private DNS	dopt-0f62795a9becbafc4		[redacted]
option_amazon_DNS	dopt-b1efb4d8	eu-west-3.compute.internal	(AmazonProvidedDNS)

D. Récapitulatif des coûts de ressources (janvier 2025)

Détails du chiffrage des services AWS
(Janvier 2025)

Le chiffrement des différents services AWS trouvables dans ce document se base sur les données de consommation du mois de février 2025. Les données de consommations pouvant varier d'un mois à l'autre, ces prix ne sont pas à prendre au pied de la lettre et représentent une estimation de l'utilisation et du coût de chacun des services de notre environnement cloud AWS.

Les 10 services utilisés au sein de notre infrastructure cloud AWS sont les suivants :

- **EC2**
- **VPC**
- **Direct Connect**
- **S3**
- **KMS**
- **RDS**
- **Data Transfer**
- **SQS**
- **Secrets Manager**
- **CloudWatch**

Page | 1

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CNPF

Retour au chapitre Retour à la table des matières

Table des matières

Retour au chapitre Retour à la table des matières

1. EC2 (Elastic Compute Cloud)

Elastic Compute Cloud		**14601,22 USD**
EU (Paris)		14601,22 USD
Amazon Elastic Compute Cloud NatGateway		169,90 USD
$0.05 per GB Data Processed by NAT Gateways	1381,908 GB	69,10 USD
$0.05 per NAT Gateway Hour	2016 Hrs	100,80 USD
Amazon Elastic Compute Cloud running Linux/UNIX		4089,45 USD
$0.0059 per On Demand Linux t3.nano Instance Hour	670 Hrs	3,95 USD
$0.0118 per On Demand Linux t3.micro Instance Hour	3537,164 Hrs	41,74 USD
$0.0132 per On Demand Linux t2.micro Instance Hour	4701 Hrs	62,05 USD
$0.0236 per On Demand Linux t3.small Instance Hour	1343 Hrs	31,69 USD
$0.0472 per On Demand Linux t3.medium Instance Hour	5036,493 Hrs	237,72 USD
$0.0528 per On Demand Linux t2.medium Instance Hour	2428,984 Hrs	128,25 USD
$0.0944 per On Demand Linux t3.large Instance Hour	2685 Hrs	253,46 USD
$0.101 per On Demand Linux c5.large Instance Hour	35,432 Hrs	3,58 USD
$0.1056 per On Demand Linux t2.large Instance Hour	2682,548 Hrs	283,28 USD
$0.1888 per On Demand Linux t3.xlarge Instance Hour	5372,046 Hrs	1014,24 USD
$0.202 per On Demand Linux c5.xlarge Instance Hour	2,858 Hrs	0,58 USD
$0.2112 per On Demand Linux t2.xlarge Instance Hour	7380 Hrs	1558,66 USD
$0.224 per On Demand Linux m5.xlarge Instance Hour	672 Hrs	150,53 USD
$0.404 per On Demand Linux c5.2xlarge Instance Hour	47,303 Hrs	19,11 USD
$0.448 per On Demand Linux m5.2xlarge Instance Hour	671 Hrs	300,61 USD
Amazon Elastic Compute Cloud running Windows		2680,95 USD
$0.122 per On Demand Windows t3.large Instance Hour	8060 Hrs	983,32 USD
$0.1336 per On Demand Windows t2.large Instance Hour	1343 Hrs	179,42 USD
$0.2522 per On Demand Windows t2.xlarge Instance Hour	1344 Hrs	338,96 USD
$0.2624 per On Demand Windows t3.xlarge Instance Hour	669 Hrs	175,55 USD
$0.4844 per On Demand Windows t2.2xlarge Instance Hour	1344 Hrs	651,03 USD
$0.5248 per On Demand Windows t3.2xlarge Instance Hour	672 Hrs	352,67 USD
Amazon Elastic Compute Cloud T3CPUCredits		2,98 USD
$0.05 per vCPU-Hour of T3 CPU Credits	59,576 vCPU-Hours	2,98 USD

Retour au chapitre Retour à la table des matières

EBS		7657,95 USD
$0.00 for 1700 Mbps per m5.2xlarge instance-hour (or partial hour)	671 Hrs	0,00 USD
$0.00 for 174 Mbps per t3.small instance-hour (or partial hour)	1343 Hrs	0,00 USD
$0.00 for 347 Mbps per t3.medium instance-hour (or partial hour)	3692 Hrs	0,00 USD
$0.00 for 43 Mbps per t3.nano instance-hour (or partial hour)	670 Hrs	0,00 USD
$0.00 for 695 Mbps per t3.2xlarge instance-hour (or partial hour)	672 Hrs	0,00 USD
$0.00 for 695 Mbps per t3.large instance-hour (or partial hour)	10073 Hrs	0,00 USD
$0.00 for 695 Mbps per t3.xlarge instance-hour (or partial hour)	4697 Hrs	0,00 USD
$0.00 for 850 Mbps per m5.xlarge instance-hour (or partial hour)	672 Hrs	0,00 USD
$0.00 for 87 Mbps per t3.micro instance-hour (or partial hour)	3537,164 Hrs	0,00 USD
$0.0007 per 1000 Requests of EBS direct APIs (List) - EU (Paris)	35509 Requests	0,02 USD
$0.0058 per provisioned IOPS-month of gp3 - EU (Paris)	1000 IOPS-Mo	5,80 USD
$0.0174 per GB-month of Cold HDD (sc1) provisioned storage	115707,894 GB-Mo	2013,32 USD
$0.0464 per provisioned MiBps-month of gp3 - EU (Paris)	0,164 GiBps-mo	7,79 USD
$0.053 per GB-Month of snapshot data stored	58515,26 GB-Mo	3101,31 USD
$0.053 per GB-month of Throughput Optimized HDD (st1) provisioned storage	816,175 GB-Mo	43,26 USD
$0.0928 per GB-month of General Purpose (gp3) provisioned storage - EU (Paris)	23351,04 GB-Mo	2166,98 USD
$0.116 per GB-month of General Purpose SSD (gp2) provisioned storage	2754,089 GB-Mo	319,47 USD

2. VPC (Virtual Private Cloud)

Virtual Private Cloud		**176,23 USD**
EU (Paris)		176,23 USD
Amazon Virtual Private Cloud Public IPv4 Addresses		176,23 USD
$0.005 per In-use public IPv4 address per hour	35245,534 Hrs	176,23 USD

3. Direct Connect

Direct Connect		**94,93 USD**
EU (Paris)		94,93 USD
AWS Direct Connect CreateDirectConnectPort		60,48 USD
$0.0300 per connected 50M hosted connection port-hour (or partial hour) (EU (Paris), Equinix PA3, Paris, FR	672 hours	20,16 USD
$0.0600 per connected 100M hosted connection port-hour (or partial hour) (EU (Paris), Equinix PA3, Paris, F	672 hours	40,32 USD
AWS Direct Connect EUW3-EQPA3-DataXfer-In:dc.3		0,00 USD
$0.0000 per GB - AWS Direct Connect to AWS Private Cloud data transfer Inbound per GB EU (Paris)	17665,262 GB	0,00 USD
AWS Direct Connect EUW3-EQPA3-DataXfer-Out:dc.3		34,45 USD
$0.0200 per GB - AWS Direct Connect to AWS Private Cloud data transfer Outbound per GB EU (Paris)	1722,631 GB	34,45 USD

Retour au chapitre Retour à la table des matières

4. S3 (Simple Storage Service)

Simple Storage Service		**1 529,21 USD**
Any		0,00 USD
EU (Paris)		1 529,21 USD
Amazon Simple Storage Service EUW3-Requests-Tier1		390,02 USD
$0.0053 per 1,000 PUT, COPY, POST, or LIST requests	73 589 504 Requests	390,02 USD
Amazon Simple Storage Service EUW3-Requests-Tier2		5,54 USD
$0.0042 per 10,000 GET and all other requests	13 193 377 Requests	5,54 USD
Amazon Simple Storage Service EUW3-TimedStorage-ByteHrs		1 133,58 USD
$0.023 per GB - next 450 TB / month of storage used	23 088,469 GB-Mo	531,03 USD
$0.024 per GB - first 50 TB / month of storage used	25 106,075 GB-Mo	602,55 USD
Amazon Simple Storage Service EUW3-TimedStorage-GlacierByteHrs		0,06 USD
$0.00405 per GB / month of storage used - Amazon Glacier	15,342 GB-Mo	0,06 USD
Amazon Simple Storage Service GetAG		0,00 USD
$0.03 per 1,000 GetAG requests for S3 Access Grants	3 Requests	0,00 USD
S3 Glacier Deep Archive		**0,21 USD**
EU (Paris)		0,21 USD
Amazon S3 Glacier Deep Archive EUW3-TimedStorage-GDA-ByteHrs		0,21 USD
$0.0018 per GB-Month for storage used in Glacier Deep Archive in EU (Paris)	116,829 GB-Mo	0,21 USD

5. KMS (Key Management Service)

Key Management Service		**1,00 USD**
EU (Paris)		1,00 USD
AWS Key Management Service eu-west-3-KMS-Keys		1,00 USD
$1 per customer managed KMS key version in EU (Paris)	1 Keys	1,00 USD
AWS Key Management Service eu-west-3-KMS-Requests		0,00 USD
$0.00 per request - Monthly Global Free Tier for KMS requests	45 Requests	0,00 USD
$0.03 per 10000 KMS requests in EU (Paris)	1 082 Requests	0,00 USD

Retour au chapitre Retour à la table des matières

6. RDS (Rational Database Service)

Relational Database Service		3735,83 USD
EU (Frankfurt)		146,62 USD
Amazon Relational Database Service Backup Storage		146,62 USD
$0.103 per additional GB-month of backup storage exceeding free allocation	1423,473 GB-Mo	146,62 USD
EU (Paris)		3589,21 USD
Amazon RDS Proxy		59,14 USD
$0.022 per hour per vCPU of DB instance running RDS Proxy	2687,998 Hrs	59,14 USD
Amazon Relational Database Service Backup Storage		15,64 USD
$0.1 per additional GB-month of backup storage exceeding free allocation running PostgreSQL	27,396 GB-Mo	2,74 USD
$0.100 per additional GB-month of backup storage exceeding free allocation	128,967 GB-Mo	12,90 USD
Amazon Relational Database Service for MariaDB		367,58 USD
$ 0.176 per RDS db.m6g.large Single-AZ instance hour (or partial hour) running MariaDB	672 Hrs	118,27 USD
$ 0.352 per RDS db.m6g.large Multi-AZ instance hour (or partial hour) running MariaDB	672 Hrs	236,54 USD
USD 0.019 per db.t3.micro Single-AZ instance hour (or partial hour) running MariaDB	672 Hrs	12,77 USD
Amazon Relational Database Service for MySQL Community Edition		12,20 USD
USD 0.019 per db.t3.micro Single-AZ instance hour (or partial hour) running MySQL	642,176 Hrs	12,20 USD
Amazon Relational Database Service for PostgreSQL		726,99 USD
$ 0.184 per RDS db.m6g.large Single-AZ instance hour (or partial hour) running PostgreSQL	672 Hrs	123,65 USD
$ 0.368 per RDS db.m6g.xlarge Single-AZ instance hour (or partial hour) running PostgreSQL	370,36 Hrs	136,29 USD
$ 0.412 per RDS db.m6i.xlarge Single-AZ instance hour (or partial hour) running PostgreSQL	301,639 Hrs	124,28 USD
$0.412 per RDS db.m5.xlarge Single-AZ instance hour (or partial hour) running PostgreSQL	765,112 Hrs	315,23 USD
USD 0.041 per db.t3.small Single-AZ instance hour (or partial hour) running PostgreSQL	672 Hrs	27,55 USD
Amazon Relational Database Service Provisioned Storage		2407,66 USD
$0.116 per IOPS-month of provisioned io1 IOPS running PostgreSQL	6415,676 IOPS-Mo	744,22 USD
$0.133 per GB-month of provisioned gp2 storage running MariaDB	120 GB-Mo	15,96 USD
$0.133 per GB-month of provisioned gp2 storage running MySQL	20 GB-Mo	2,66 USD
$0.133 per GB-month of provisioned gp2 storage running PostgreSQL	100 GB-Mo	13,30 USD
$0.133 per GB-month of provisioned GP3 storage running PostgreSQL	20 GB-Mo	2,66 USD
$0.145 per GB-month of provisioned io1 storage running PostgreSQL	6054,235 GB-Mo	877,86 USD
$0.231 per IOPS-month of provisioned io1 IOPS for Multi-AZ deployments running MariaDB	3000 IOPS-Mo	693,00 USD
$0.29 per GB-month of provisioned io1 storage for Multi-AZ deployments running MariaDB	200 GB-Mo	58,00 USD

Retour au chapitre Retour à la table des matières

7. Data Transfer

AWS Data Transfer EUW3-APS1-AWS-Out-Bytes		0,01 USD
$0.02 per GB - EU (Paris) data transfer to Asia Pacific (Singapore)	0,293 GB	0,01 USD
AWS Data Transfer EUW3-EUC1-AWS-Out-Bytes		10,39 USD
$0.02 per GB - EU (Paris) data transfer to EU (Germany)	519,278 GB	10,39 USD
AWS Data Transfer EUW3-USE2-AWS-Out-Bytes		0,07 USD
$0.02 per GB - EU (Paris) data transfer to US East (Ohio)	3,584 GB	0,07 USD
Bandwidth		873,78 USD
$0.00 per GB - regional data transfer - in/out/between EC2 Azs or using elastic IPs or ELB	0,005 GB	0,00 USD
$0.00 per GB - regional data transfer - in/out/between EC2 Azs or using elastic IPs or ELB	0,007 GB	0,00 USD
$0.000 per GB - data transfer in per month	998,362 GB	0,00 USD
$0.000 per GB - data transfer out under the monthly global free tier	32,649 GB	0,00 USD
$0.000 per GB - regional data transfer under the monthly global free tier	0,951 GB	0,00 USD
$0.010 per GB - regional data transfer - in/out/between EC2 AZs or using elastic IPs or ELB	944,654 GB	9,45 USD
$0.085 per GB - next 40 TB / month data transfer out	1 549,448 GB	131,70 USD
$0.090 per GB - first 10 TB / month data transfer out beyond the global free tier	8 140,357 GB	732,63 USD
USD0.0 per GB for EUW3-DataTransfer-AZ-In-Bytes	266,183 GB	0,00 USD
USD0.0 per GB for EUW3-DataTransfer-AZ-Out-Bytes	145,827 GB	0,00 USD

8. SQS (Simple Queue Service)

Simple Queue Service		**0,08 USD**
Asia Pacific (Mumbai)		0,00 USD
Asia Pacific (Osaka)		0,00 USD
Asia Pacific (Seoul)		0,00 USD
Asia Pacific (Singapore)		0,00 USD
Asia Pacific (Sydney)		0,00 USD
Asia Pacific (Tokyo)		0,00 USD
Canada (Central)		0,00 USD
EU (Frankfurt)		0,00 USD
EU (Ireland)		0,00 USD
EU (London)		0,00 USD
EU (Paris)		0,08 USD
Amazon Simple Queue Service EUW3-Requests-FIFO-Tier1		0,00 USD
First 1,000,000 Amazon SQS Requests per month are free	296 975 Requests	0,00 USD
Amazon Simple Queue Service EUW3-Requests-Tier1		0,08 USD
$0.40 per million Amazon SQS standard requests in Tier1 in EU (Paris)	210 125 Requests	0,08 USD
First 1,000,000 Amazon SQS Requests per month are free	86 503 Requests	0,00 USD

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CNPF

Retour au chapitre Retour à la table des matières

9. Secrets Manager

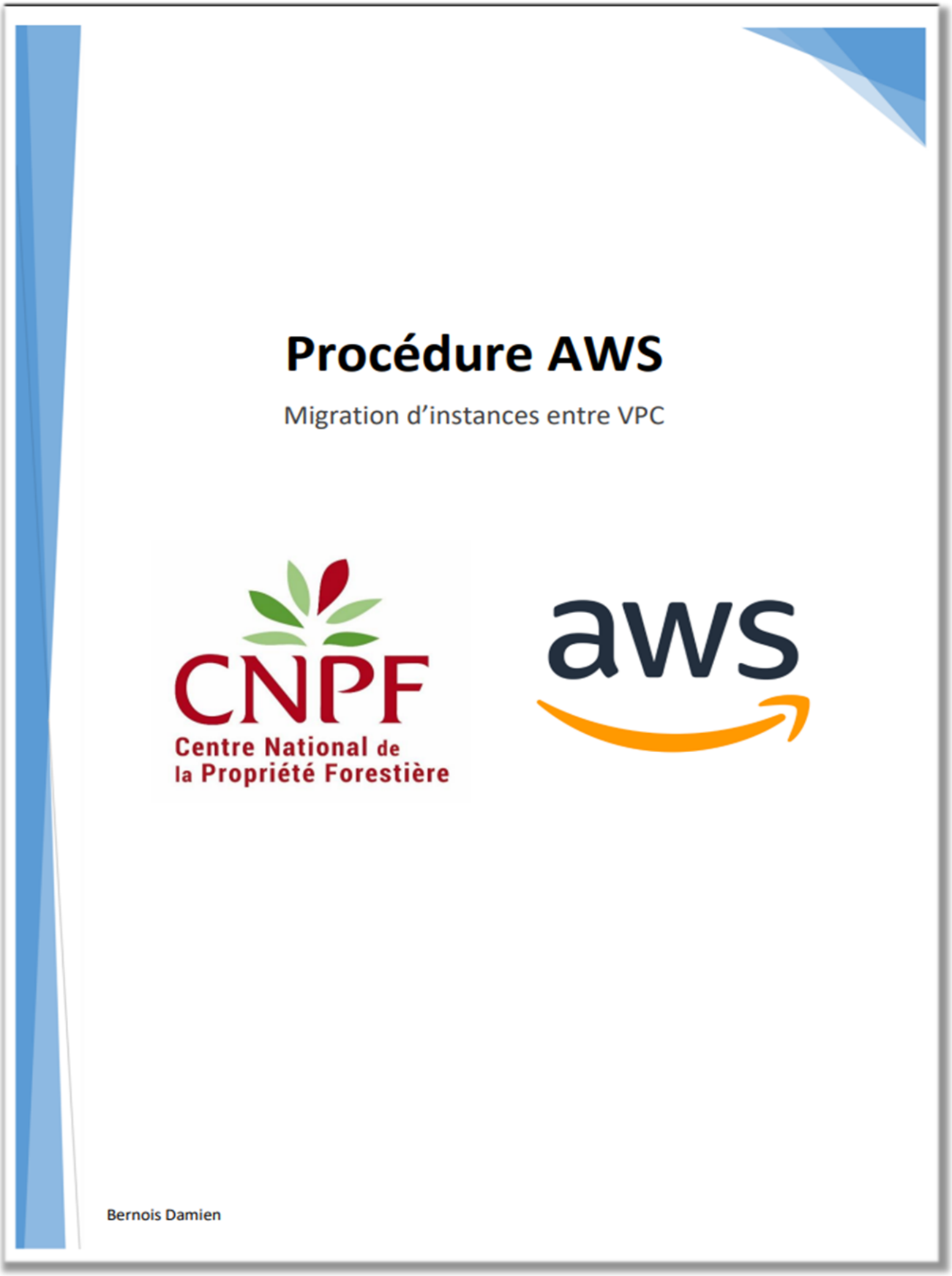
Secrets Manager		**1,15 USD**
Asia Pacific (Mumbai)		0,00 USD
Asia Pacific (Osaka)		0,00 USD
Asia Pacific (Seoul)		0,00 USD
Asia Pacific (Singapore)		0,00 USD
Asia Pacific (Sydney)		0,00 USD
Asia Pacific (Tokyo)		0,00 USD
Canada (Central)		0,00 USD
EU (Frankfurt)		0,00 USD
EU (Ireland)		0,00 USD
EU (London)		0,00 USD
EU (Paris)		1,15 USD
AWS Secrets Manager EUW3-AWSSecretsManager-Secrets		0,80 USD
$0.40 per Secret	1,991 Secrets	0,80 USD
AWS Secrets Manager EUW3-AWSSecretsManagerAPIRequest		0,36 USD
$0.05 per 10000 API Requests	71 316 API Requests	0,36 USD

10. Cloud Watch

CloudWatch		**3,59 USD**
Any		2,25 USD
AmazonCloudWatch DashboardHour		2,25 USD
$3.00 per Dashboard per Month	0,75 Dashboards	2,25 USD
First 3 Dashboards per month are free.	0,25 Dashboards	0,00 USD
EU (Paris)		1,34 USD
Amazon CloudWatch		0,30 USD
$0.00 per request - first 1,000,000 requests	32 Requests	0,00 USD
$0.10 per alarm metric month (standard resolution) - EU (Paris)	3 Alarms	0,30 USD
AmazonCloudWatch PutLogEvents		1,04 USD
$0.5985 per GB custom log data ingested in Standard log class - EU (Paris)	1,741 GB	1,04 USD

Retour au chapitre Retour à la table des matières

E. Procédure de migration interne



Procédure AWS

Migration d'instances entre VPC

CNPF
Centre National de la Propriété Forestière

aws

Bernois Damien

Retour au chapitre *Retour à la table des matières*

Table des matières

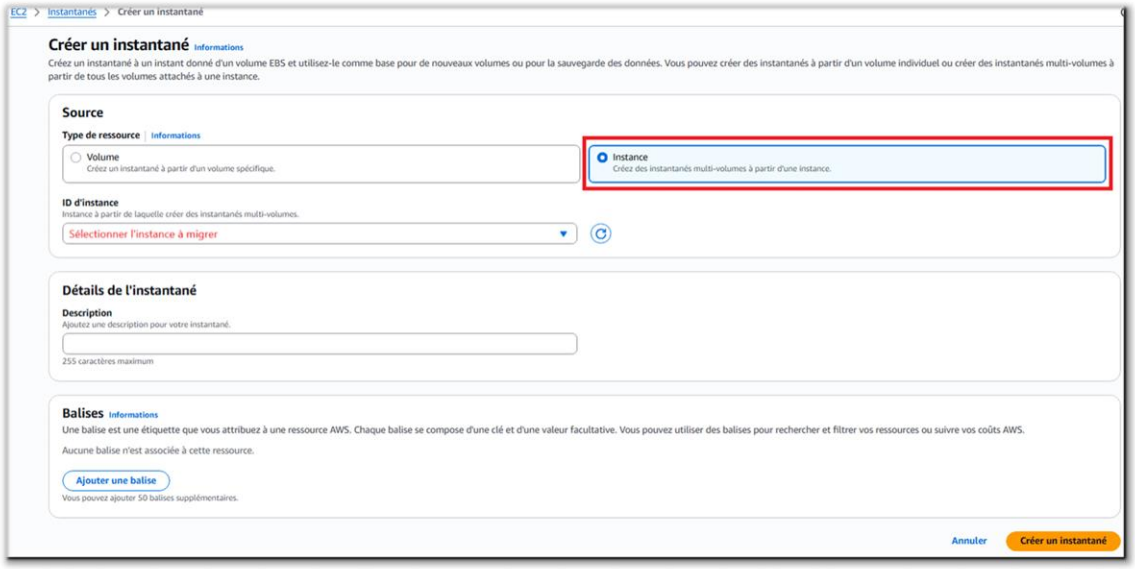
Bernois Damien

1. Sauvegarde des données

A. Création d'une instantanée

La création d'une instantanée de l'instance cible avant sa migration permet, en cas de dysfonctionnement ou bien de perte de données, d'assurer l'intégrité et la récupération des données initiales.

- Console AWS > EC2 > Instantanés > Créer un instantané:

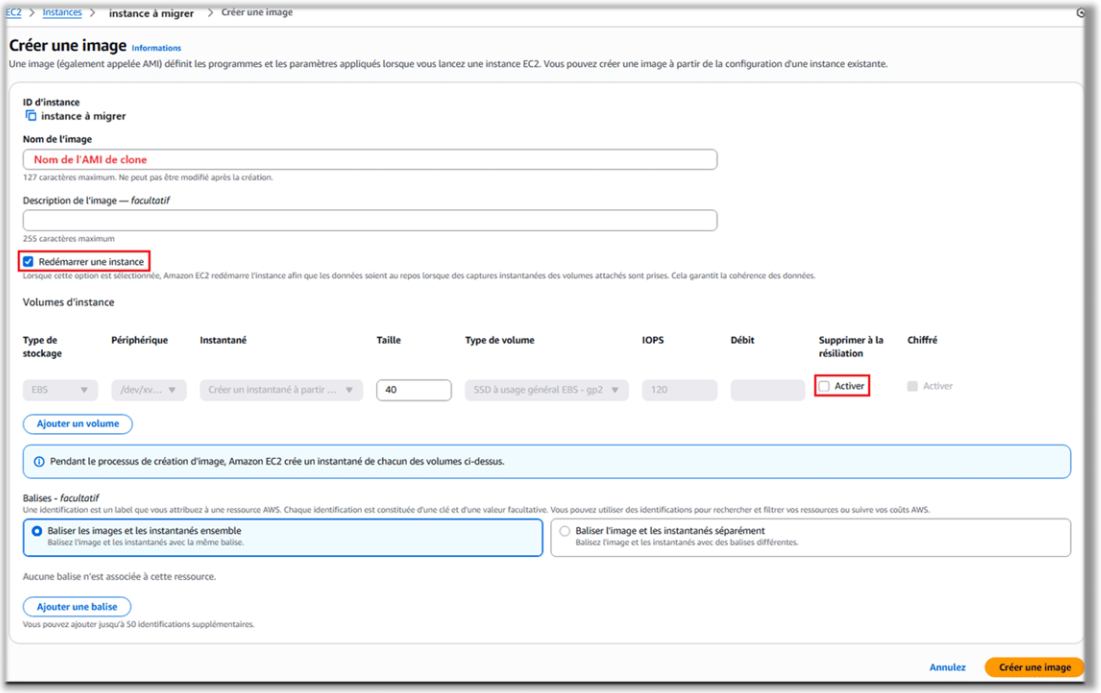


B. Création d'une image

La création d'une image (AMI AWS) à partir de l'instance cible permet aussi, en cas de dysfonctionnement ou bien de perte de données, d'assurer l'intégrité et la récupération des données initiales.

De plus, cette dernière aidera à faire le basculement de l'instance sur un autre réseau VPC à travers un simple clonage.

- Console AWS > EC2 > Instances > « sélectionner l'instance à migrer » > Créer une image:



Retour au chapitre Retour à la table des matières

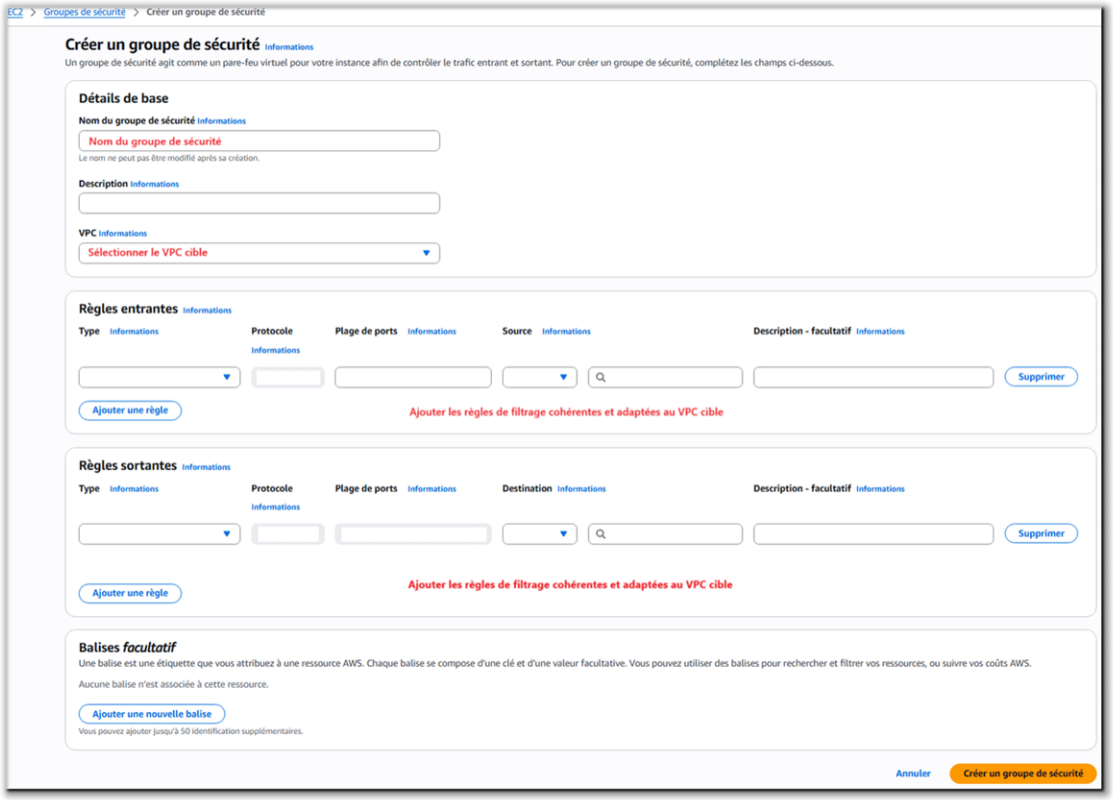
2. Intégration et configuration réseau

A. Création du groupe de sécurité (si nécessaire)

La création du groupe de sécurité (ACL machine) adapté aux nouvelles exigences réseau assure la bonne intégration du clone de l'instance au sein du futur VPC cible.

Il est très important de prendre en compte chacune des règles de filtrage du groupe de sécurité initial, et de les adapter en changeant les plages réseaux/IP réseau. Les protocoles et ports restant théoriquement les mêmes, ces dernières ne font pas l'objet d'un besoin de modification.

- Console AWS > EC2 > Groupes de sécurité > Créer un groupe de sécurité :



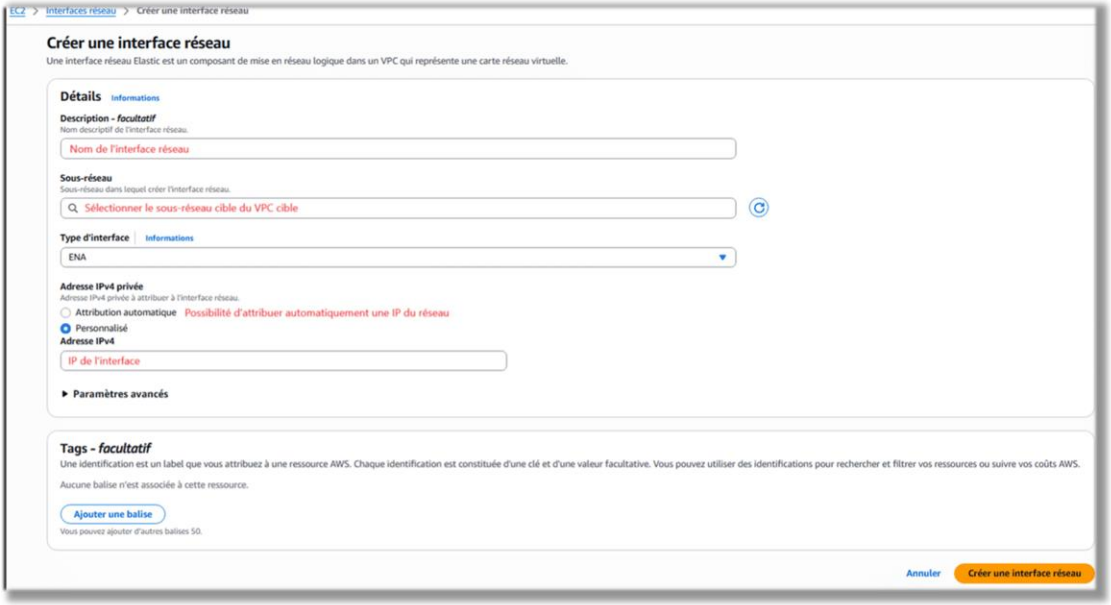
Retour au chapitre Retour à la table des matières

B. Création d'une interface réseau

La création d'une interface réseau (ENI AWS) qui sera, par la suite, rattachée à l'instance clone assurera l'intégration au futur VPC cible.

De plus, il est nécessaire, lors de cette création, de rattacher le groupe de sécurité créé en amont afin d'appliquer les règles de filtrage machine à cette interface réseau, et donc à l'instance clone.

- Console AWS > EC2 > Interface réseau > Créer une interface réseau :



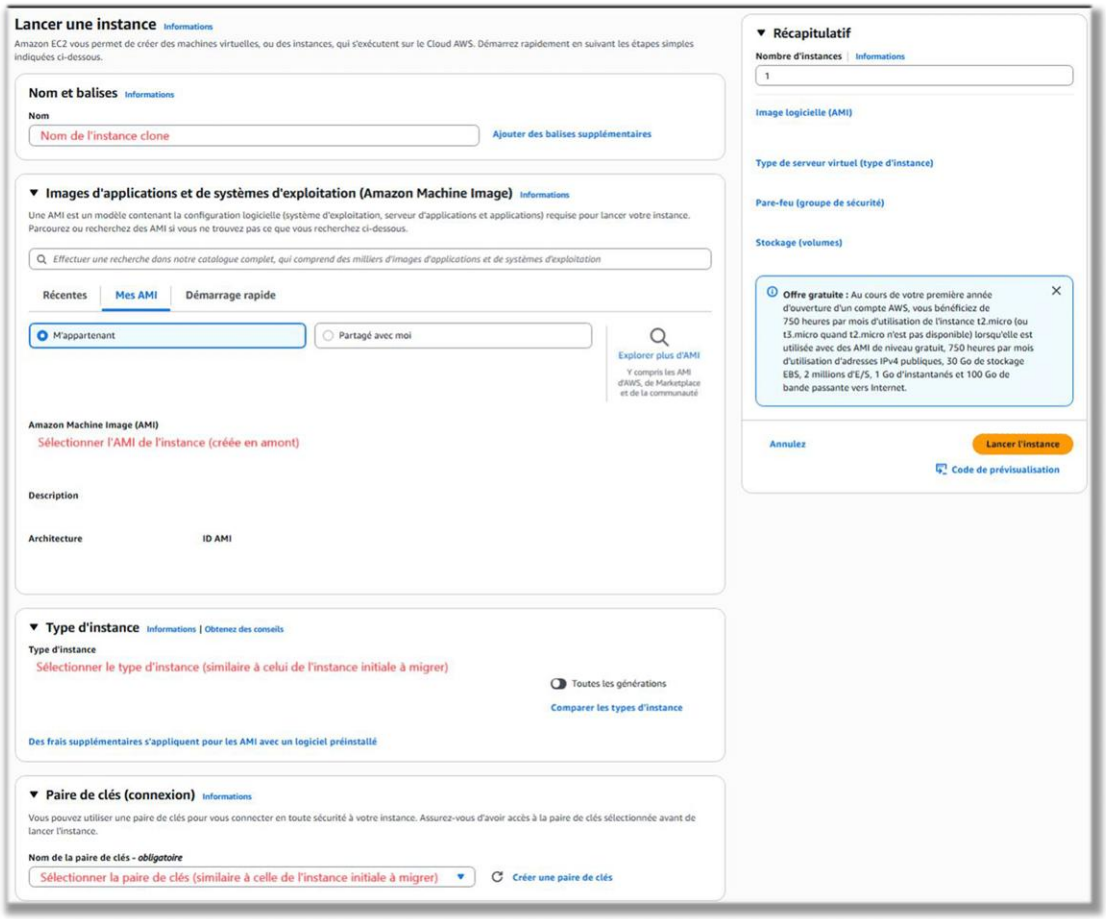
Retour au chapitre Retour à la table des matières

3. Création de l'instance clone

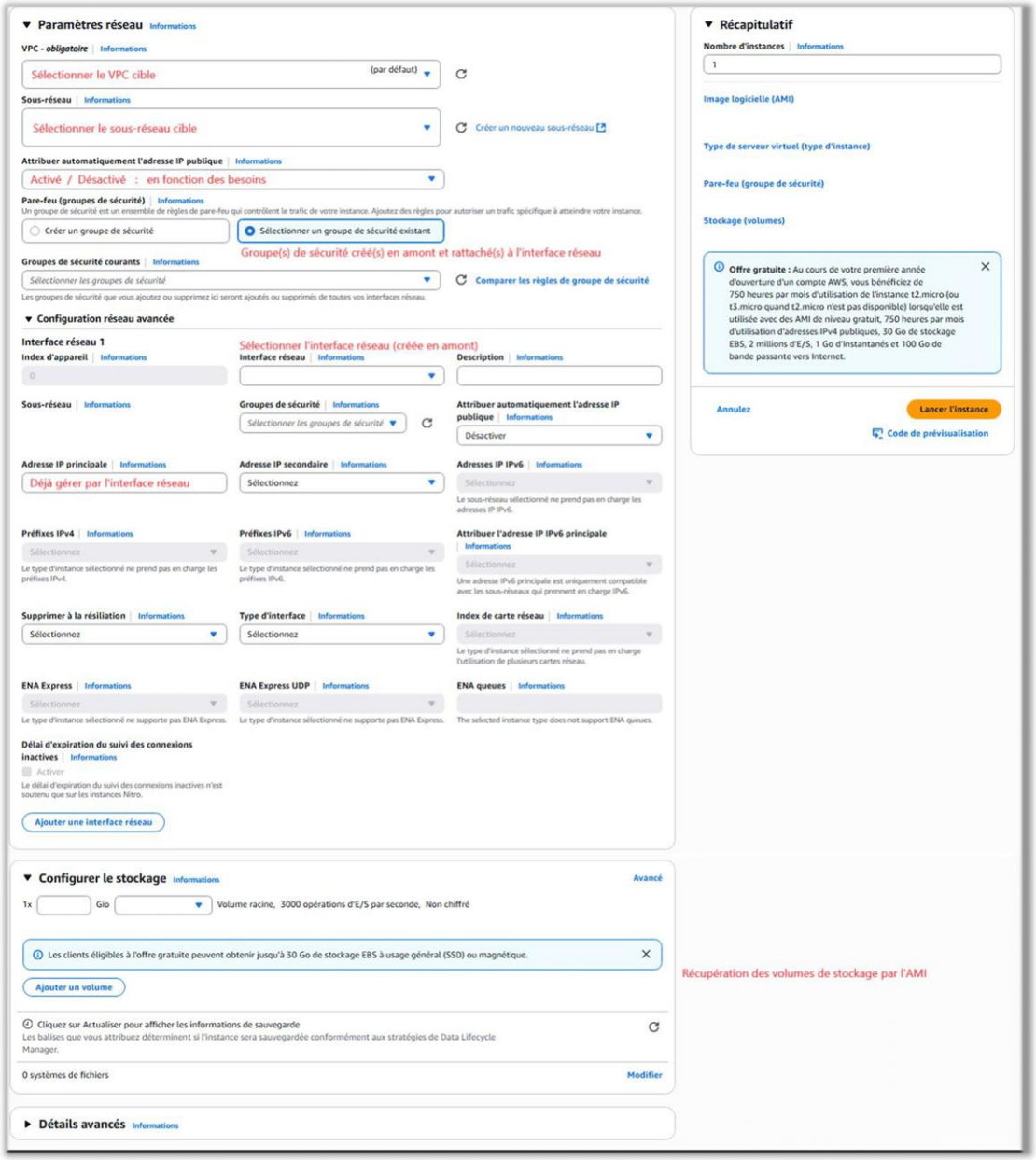
A. Création de l'instance

Afin d'assurer la bonne intégration et la symétrie de l'instance clone, il est important de prendre en compte les points suivants :

- Reprendre la même architecture (type) d'instance que celle initiale.
- Choisir l'AMI créé en amont comme modèle de système.
- Choisir l'ENI créé en amont comme carte réseau.



Retour au chapitre Retour à la table des matières



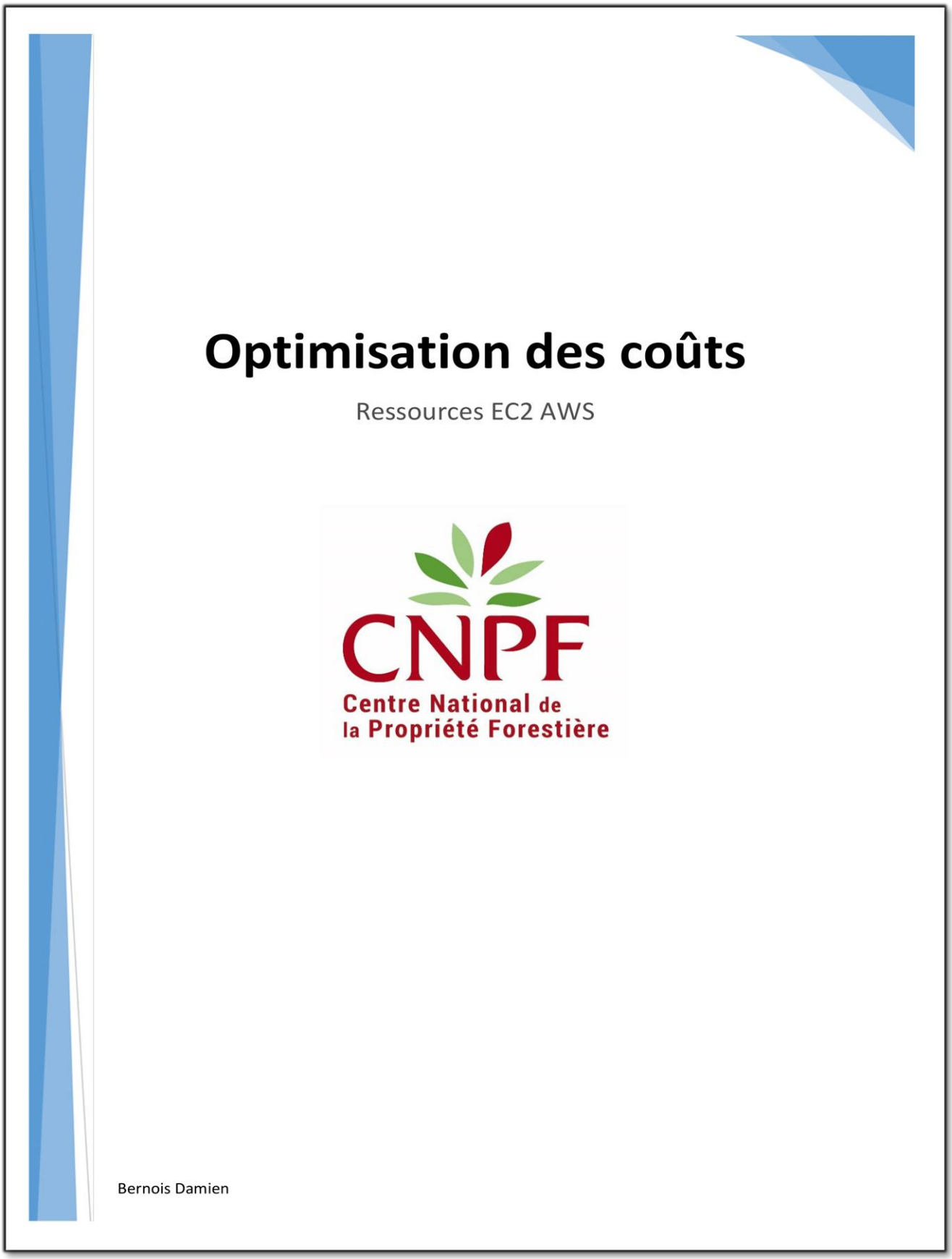
Retour au chapitre Retour à la table des matières

B. Points clés post migration

Afin de finaliser la migration d'une instance, les 4 points clés primordiaux suivants sont à respecter et à effectuer :

- Revérifier la logique de chacun des paramètres de l'instance clone, ainsi que la cohérence du système et des données.
- Changement de l'entrée DNS par la nouvelle IP de la nouvelle interface réseau rattachée à l'instance clone.
- Éteindre l'instance initiale afin de ne pas engendrer de surcoûts de maintien et la résilier (suppression de l'instance, ainsi que des anciens volumes de stockages EBS) seulement 24h à 48h après la migration effectuée en cas d'effets de bord non prévus.

F. Optimisation des coûts EC2 AWS



Retour au chapitre *Retour à la table des matières*

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CNPF

Table des matières

Bernois Damien

CESI
ÉCOLE D'INGÉNIEURS

CNPF Centre National de la Propriété Forestière

Bernois Damien

CONTEXTE

L'hébergement de notre environnement cloud actuel est assuré par la **plateforme d'AWS**. Cette dernière héberge aujourd'hui la **majorité de notre infrastructure** (comprenant les applications métiers, les serveurs de fichiers, les serveurs d'administration, les environnements de production, de développement, de recette et de préproduction).

À la suite d'une **étude des coûts engendrés** par les différentes ressources hébergées sur notre environnement cloud, en particulier celle des quelques 109 instances EC2, la direction générale du CNPF a pris la décision de réduire le budget alloué au maintien de ce dernier.

Afin de répondre à ce changement de **stratégie budgétaire**, l'étude de la mise en place d'une solution pouvant **optimiser et réduire les coûts** de ces instances a été soutenue.

La solution retenue pour ce projet est la suivante : **gestion des horaires d'exécution des instances.**

La mise en place de ce projet d'optimisation de l'infrastructure cloud s'effectuera en 4 temps :

- Le premier ; remettre à l'ordre du jour toutes les instances hébergées, **opérer un triage** nécessaire, ainsi qu'effectuer le **calcul des coûts**.
- Le deuxième ; **étudier les différentes solutions** envisageables, ainsi que leurs coûts de mise en œuvre.
- Le troisième, **étudier la priorité et l'utilisation** des instances afin d'estimer quel type de gestion d'horaires appliquer sur ces dernières.
- Le dernier ; la mise en place de la **configuration de la gestion** à l'aide des fonctionnalités AWS (IAM, Lambda, Planificateur EventBridge et CloudWatch).

Bernois Damien

1. Etude de l'existant

A. Recensement des ressources

i. Instances hors ligne

Notre infrastructure Cloud héberge actuellement **109 instances**, parmi lesquelles se trouve **28 instances à l'arrêt** (comprenant des instances pouvant être à nouveau relancées et d'autres n'étant que des instances temporaires qui ne seront plus exploitées par la suite).

Nom	ID	Type
FRCT-dev	i-02d368fe77a1f7142	t2.micro
SFT_POC_Carto_Cadastre	i-0c76f653e25f400b8	t2.micro
RLT_Catalogue_2	i-0ad4476b41003b653	t2.small
cnpf-SG	i-0e6d4854b1da6d874	t3.large
Pentest Server	i-0d54a06012d780c97	t2.large
Connecteur-SW2-Prod	i-02cbeb797c8563bde	t2.micro
Virtual Room Connector	i-0ed62fa2f927be456	t2.large
StreamGoomer Collector	i-01246656413ce8e9f	t3.large
TheGreenBow TAS Server	i-0400a0529479e625a	t2.small
Windows_Server_rescue_Sylvain	i-03b28a6add802ea68	t2.large
RDP_CNPF_Voir_Balises	i-0bb2e8e2d84547401	t2.medium
CNPF-VIRTUALIA-APPLI_RESTORED	i-09dcf239575356b9b	t3.2xlarge
Redmine-4.1.0	i-02a72cbb3e8ceca27	t2.medium
SUADEO_Serveur_application	i-0aa2b0d958a5c82fa	t2.2xlarge
srvobm.cnpf.fr	i-086c6a24f363ffd23	t2.xlarge
FPF-prod_fo	i-0f4f3883b4b4f05d1	t2.xlarge
Climessences-preprod_v1.0.0)	i-0b3dcb4ebecc02c44	t3.xlarge
LFB-V1-preprod	i-0825ce02ed72d68ec	t2.xlarge
FPF-dev	i-097b9c1f49cede2c3	t2.xlarge
sylvi-par	i-0ecf982146a6fa556	t2.micro
FRCT-recette	i-030c0be689086ff48	t2.micro
SUADEO_Recette	i-09cfafd5638d8e6e7	t3.2xlarge
Recette-Merlin	i-066bd7997b4bedafc	t3.xlarge
mig-CNPF-DNS2	i-02f5c3d4ea31a49ad	t2.micro
Client2_Zimbra_MIG	i-076165f3720d8f36a	t3.medium
Client1_Zimbra_MIG	i-0104157e6c6e333bf	t3.medium
TEST_API_POC_Carto	i-05278444474ccb152	t2.large
Zimbra Server TEST (patch44)	i-02cbeb797c8563bde	t3.xlarge

Type	Quantité
t2.micro	6
t2.small	2
t2.medium	2
t2.large	4
t2.xlarge	4
t2.2xlarge	1
t3.medium	2
t3.large	2
t3.xlarge	3
t3.2xlarge	2

Bernois Damien

ii. Instances en cours d'exécution

Notre infrastructure Cloud héberge actuellement **109 instances**, parmi lesquelles se trouve **81 instances en cours d'exécution**.

Nom	ID	Type
APO-JAR-teltransmission-PHU-BPE	i-0b42a20ea1fc56b5a	t2.xlarge
FPF-prod_bo	i-054af68e633d50f97	t2.xlarge
LFB-V1-prod	i-0bafc04048ddc9054	t2.xlarge
FRCT-prod	i-04f25f919638e34d3	t2.micro
LFB-MongoDB	i-01121aeb9f4132c97	t2.medium
CNPF-Nextcloud (29.0.11)	i-0c82987b761e666be	t3.xlarge
Climessences-prod_v1.0.0	i-014dce4c3324003a3	t2.xlarge
CNPF-ACTIV	i-04a12babed9c6d6fe	t3.micro
CNPF-ILEX	i-022a87ab89f348492	t3.micro
CNPF-RDP-Gateway & acs.fr DC	i-07d9b09084a427984	t2.xlarge
CNPF-DNS1 (PROD)	i-0509b896288e73fbe	t3.micro
CNPF-CARTO	i-0a79d7d9b85d17f7b	t3.xlarge
LDAP Server (ldap Old)	i-090ab342ceca42675	t2.medium
CNPF_DVF_foncier	i-03dfffae96e4ef119	t2.micro
CNPF-Merlin	i-08b412f096091ce59	t2.xlarge
CNPF-GFIpep	i-093c60fe94e3fdca1	t2.2xlarge
LFB-V2-recette-drupal9	i-00f55ac6c94e7c718	t2.xlarge
WALLIX_Access_Manager_PROD_v4.0.6	i-0aaaf8529c21b5ce8	t3.small
CNPF_McAfee_1	i-0ab4fd28975f98178	t2.large
Mailcatcher	i-03e50c40a7cd8fca3	t3.micro
Recette-Teletrans-Serveur	i-04681d6d6f9b87b4f	t2.micro
Climessences-recette_v1.0.0	i-0f9bdcb6bad85d550	t2.xlarge
LFB-V1-recette	i-059a5928072dd405f	t2.xlarge
CNPF-API	i-0cea583a26e80bed3	t3.micro
CNPF-LDAP (ldap New)	i-09468b02d2d6bab39	t2.micro
Graylog	i-0093041badac5910a	t3.medium
Matomo	i-039c2b75783701ce5	t3.large
CNPF-VIRTUALIA-APPLI	i-0ad3b635801c8889c	t3.2xlarge
CNPF-VIRTUALIA-IIS	i-03a1d3bf3595e4e23	t3.xlarge
GFI-CAB	i-05894ffeaed803354	t2.micro
StreamGoomer Manager	i-0cf2311f09cac456c	t3.xlarge
MyMetricks Server	i-0a78ea43b44b0553f	t2.xlarge
Portail-authentification-V2 (lemon v2.0x)	i-0534e5b0ed88e8e56	t3.medium
WALLIX_Bastion_PROD_v10.0.7	i-0441332ada949fa1f	t3.medium
VPC_BAST_FIREWALL (prod)	i-03d7c6477d0e6c755	t2.xlarge
foret-gibier	i-03d2452c55fe57125	t3.small
BioClim_Test	i-0db611651c98e8677	t2.large
StormShield_SMC_Server_v3.6.0	i-056fc393e7f948dc8	t3.xlarge
CNPF-web-prod	i-04cf242eb5d4e0742	t3.xlarge
sftp	i-0d3f4d7ca2c9e13a3	t3.nano
SonarQube Server	i-01ce916d98337949f	t2.large
Gitlab Server	i-00ed7f75a76832bb2	t2.xlarge
Gitlab Runner	i-084e466885263652f	t3.medium
Zimbra Server PROD (patch 44)	i-0ebfbba3170f5421e	m5.2xlarge
Bioclimsol_Auth_Server_TEST	i-0fe9fb8b9cb133d11	t2.micro

Bernois Damien

Merlin-Tdata	i-0a31d02e3f14f9557	t3.large
secoia_v2 server (2nd installation) - (VPC Webint - ss1)	i-0012342a7248e6ee9	m5.xlarge
API_Carto_enjeux (Recette)	i-0b75d571d399a936b	t2.large
DG_FILESERVER	i-022748bec937a416b	t3.large
Veeam Console	i-06177bc1ef5077dd8	t3.medium
BioClimSol-Dev-Test	i-0d06d97def251d1f4	t2.medium
CIDF_FILESERVER	i-0702be67a3bc721c2	t3.large
PACA_FILESERVER	i-0fa783fe484e6e83b	t3.large
AURA_FILESERVER	i-01f04524ee740ef2a	t3.large
GEST_FILESERVER	i-01cf3cf239150aff9	t3.large
HDFN_FILESERVER	i-08fad5eb92cbde14f	t3.large
BPDL_FILESERVER	i-0a7f4b7c9b2773b19	t3.large
BFC_FILESERVER	i-022e67471119565f4	t3.large
OCCI_FILESERVER	i-09623837b31ea7f3f	t3.large
Cryhod Share Server	i-07f0881ed89d60180	t2.micro
Windows_2016_TSE_Server_(PROD)	i-04c5593fe32f8e8d6	t2.large
antispam	i-053072ff7ee9b44cc	t2.xlarge
CNPF_ADSERVER	i-061a72926ef8c9fa5	t2.2xlarge
NAQUI_FILESERVER	i-0bd189e3b5baa4e57	t3.large
IDF_FILESERVER	i-0f300100525fec48b	t3.large
Wapt Server	i-07bdb7b8be8d82b4f	t2.large
CNPF-web-preprod_Cloned	i-0a1fc61801ad023a9	t3.large
New_Photofor	i-0150f2d3d31a00b2f	t3.medium
NetsKope Publisher	i-0e6dfbe6cab443307	t3.medium
secoia preprod	i-031a25934b7ecb1b2	t3.xlarge
CNPF-ocsinventory PROD (v2.8.1)	i-0e4478bc260c27899	t3.medium
Virtualia v5 - Form	i-00b49ff4751c5958e	t3.large
VirtualiaV5 - Test	i-03a346fa53dd48471	t3.large
VirtualiaV5 - Prod	i-0db090a410cb4f1db	t3.xlarge
Climessences V1 Recette Drupal10	i-0014f2b9e861ee110	t3.xlarge
Gophish_Server	i-0a7d3d9fa64809e0b	t3.micro
BioClimSol_V2_prod	i-05ed399c73337757c	t3.medium
Zimbra Docs PROD	i-0bf413ccd7378a16e	t2.large
GLPI Server	i-0d2a7da31ec0b411c	t2.micro
sylveclair_preprod	i-062ce8df32720ecd6	t3.small
New_Photofor	i-0150f2d3d31a00b2f	t3.medium

Type	Quantité	Type	Quantité
t2.micro	8	t3.small	3
t2.medium	3	t3.medium	10
t2.large	7	t3.large	16
t2.xlarge	13	t3.xlarge	9
t2.2xlarge	2	t3.2xlarge	1
t3.nano	1	m5.xlarge	1
t3.micro	6	m5.2xlarge	1

Bernois Damien

Retour au chapitre Retour à la table des matières

B. Triage des ressources

i. Tri des instances hors ligne

➢ Recensement des instances :

Nom	ID	Action
FRCT-dev	i-02d368fe77a1f7142	SUPPRIMER
SFT_POC_Carto_Cadastre	i-0c76f653e25f400b8	
RLT_Catalogue_2	i-0ad4476b41003b653	
cnpf-SG	i-0e6d4854b1da6d874	A GARDER
Pentest Server	i-0d54a06012d780c97	
Connecteur-SW2-Prod	i-02cbeb797c8563bde	
StreamGoomer Collector	i-01246656413ce8e9f	SUPPRIMER
Windows_Server_rescue_Sylvain	i-03b28a6add802ea68	
CNPF-VIRTUALIA-APPLI_RESTORED	i-09dcf239575356b9b	
Redmine-4.1.0	i-02a72cbb3e8ceca27	
SUADEO_Serveur_application	i-0aa2b0d958a5c82fa	A GARDER
srvobm.cnpf.fr	i-086c6a24f363ffd23	SUPPRIMER
FPF-prod_fo	i-0f4f3883b4b4f05d1	A GARDER
Climessences-preprod_v1.0.0)	i-0b3dcb4ebecc02c44	
LFB-V1-preprod	i-0825ce02ed72d68ec	
FPF-dev	i-097b9c1f49cede2c3	SUPPRIMER
sylvi-par	i-0ecf982146a6fa556	
FRCT-recette	i-030c0be689086ff48	
SUADEO_Recette	i-09cfafd5638d8e6e7	A GARDER
Recette-Merlin	i-066bd7997b4bedafc	
mig-CNPF-DNS2	i-02f5c3d4ea31a49ad	SUPPRIMER
TEST_API_POC_Carto	i-05278444474ccb152	
Client2_Zimbra_MIG	i-076165f3720d8f36a	
Client1_Zimbra_MIG	i-0104157e6c6e333bf	
Virtual Room Connector	i-0ed62fa2f927be456	
TheGreenBow TAS Server	i-0400a0529479e625a	
RDP_CNPF_Voir_Balises	i-0bb2e8e2d84547401	
Zimbra Server TEST (patch 44)	i-0c0a9fb2ff85b09ba	A GARDER

Bernois Damien

ii. Tri des instances en cours d'exécution

Nom	ID	Sauvegardée
APO-JAR-teltransmission-PHU-BPE	i-0b42a20ea1fc56b5a	
FPF-prod_bo	i-054af68e633d50f97	
LFB-V1-prod	i-0bafc04048ddc9054	OUI
FRCT-prod	i-04f25f919638e34d3	
LFB-MongoDB	i-01121aeb9f4132c97	
CNPF-Nextcloud (29.0.11)	i-0c82987b761e666be	OUI
Climessences-prod_v1.0.0	i-014dce4c3324003a3	
CNPF-ACTIV	i-04a12babed9c6d6fe	
CNPF-ILEX	i-022a87ab89f348492	
CNPF-RDP-Gateway & acs.fr DC	i-07d9b09084a427984	
CNPF-DNS1 (PROD)	i-0509b896288e73fbe	
CNPF-CARTO	i-0a79d7d9b85d17f7b	
LDAP Server (ldap Old)	i-090ab342ceca42675	
CNPF_DVF_foncier	i-03dfffae96e4ef119	OUI
CNPF-Merlin	i-08b412f096091ce59	
CNPF-GFIpep	i-093c60fe94e3fdca1	
LFB-V2-recette-drupal9	i-00f55ac6c94e7c718	
WALLIX_Access_Manager_PROD_v4.0.6	i-0aaaf8529c21b5ce8	
CNPF_McAfee_1	i-0ab4fd28975f98178	
Mailcatcher	i-03e50c40a7cd8fca3	
Recette-Teletrans-Serveur	i-04681d6d6f9b87b4f	
Climessences-recette_v1.0.0	i-0f9bdcb6bad85d550	
LFB-V1-recette	i-059a5928072dd405f	
CNPF-API	i-0cea583a26e80bed3	OUI
CNPF-LDAP (ldap New)	i-09468b02d2d6bab39	
Graylog	i-0093041badac5910a	
Matomo	i-039c2b75783701ce5	
CNPF-VIRTUALIA-APPLI	i-0ad3b635801c8889c	
CNPF-VIRTUALIA-IIS	i-03a1d3bf3595e4e23	
GFI-CAB	i-05894ffeaed803354	OUI
StreamGoomer Manager	i-0cf2311f09cac456c	
MyMetricks Server	i-0a78ea43b44b0553f	
Portail-authentification-V2 (lemon v2.0x)	i-0534e5b0ed88e8e56	
WALLIX_Bastion_PROD_v10.0.7	i-0441332ada949fa1f	
VPC_BAST_FIREWALL (prod)	i-03d7c6477d0e6c755	
foret-gibier	i-03d2452c55fe57125	OUI
BioClim_Test	i-0db611651c98e8677	
StormShield_SMC_Server_v3.6.0	i-056fc393e7f948dc8	OUI
CNPF-web-prod	i-04cf242eb5d4e0742	
sftp	i-0d3f4d7ca2c9e13a3	
SonarQube Server	i-01ce916d98337949f	
Gitlab Server	i-00ed7f75a76832bb2	OUI
Gitlab Runner	i-084e466885263652f	
Zimbra Server PROD (patch 44)	i-0ebfbba3170f5421e	
Bioclimsol_Auth_Server_TEST	i-0fe9fb8b9cb133d11	
Merlin-Tdata	i-0a31d02e3f14f9557	OUI
secoia_v2 server (2nd installation) - (VPC Webint - ss1)	i-0012342a7248e6ee9	

Bernois Damien

API_Carto_enjeux (Recette)	i-0b75d571d399a936b	
DG_FILESERVER	i-022748bec937a416b	OUI
Veeam Console	i-06177bc1ef5077dd8	
BioClimSol-Dev-Test	i-0d06d97def251d1f4	
CIDF_FILESERVER	i-0702be67a3bc721c2	OUI
PACA_FILESERVER	i-0fa783fe484e6e83b	
AURA_FILESERVER	i-01f04524ee740ef2a	OUI
GEST_FILESERVER	i-01cf3cf239150aff9	
HDFN_FILESERVER	i-08fad5eb92cbde14f	
BPDL_FILESERVER	i-0a7f4b7c9b2773b19	OUI
BFC_FILESERVER	i-022e67471119565f4	
OCCI_FILESERVER	i-09623837b31ea7f3f	
Cryhod Share Server	i-07f0881ed89d60180	OUI
Windows_2016_TSE_Server_(PROD)	i-04c5593fe32f8e8d6	
antispam	i-053072ff7ee9b44cc	
CNPF_ADSERVER	i-061a72926ef8c9fa5	OUI
NAQUI_FILESERVER	i-0bd189e3b5baa4e57	
IDF_FILESERVER	i-0f300100525fec48b	
Wapt Server	i-07bdb7b8be8d82b4f	
CNPF-web-preprod_Cloned	i-0a1fc61801ad023a9	
New_Photofor	i-0150f2d3d31a00b2f	
NetsKope Publisher	i-0e6dfbe6cab443307	OUI
secoia preprod	i-031a25934b7ecb1b2	
CNPF-ocsinventory PROD (v2.8.1)	i-0e4478bc260c27899	OUI
Virtualia v5 - Form	i-00b49ff4751c5958e	
VirtualiaV5 - Test	i-03a346fa53dd48471	
VirtualiaV5 - Prod	i-0db090a410cb4f1db	
Climessences V1 Recette Drupal10	i-0014f2b9e861ee110	
Gophish_Server	i-0a7d3d9fa64809e0b	
BioClimSol_V2_prod	i-05ed399c73337757c	
Zimbra Docs PROD	i-0bf413ccd7378a16e	

- Stratégie de sauvegarde actuelle :

Type	Fréquence	Horaire	Rétention
Incrémentielle	Quotidienne (lundi au samedi)	01 : 00	10 jours
Complète	Dimanche	01 : 00	1 mois

Bernois Damien

2. Etude de la solution

A. Fonctionnalités des services retenus

i. Solution de planificateur évènementiel

La solution retenue afin de pouvoir appliquer la gestion des horaires de façon **récurrente et automatisée** est le service intégré à AWS, **EventBridge**.

Ce dernier nous permet **d'automatiser l'appel d'un script**, assurant l'application de ce dernier en temps et en heure et ce de façon répétée. Cette solution permettra à l'administrateur de changer, en cas de besoin et à tout moment, les horaires de planification d'appel au script.

ii. Solution de Scripting

La solution retenue afin de pouvoir héberger les scripts, en faire l'appel et qui fera office de gestion des horaires des instances est le service intégré à AWS, **Lambda**.

Ce dernier nous permet de **configurer des codes** sans pour autant avoir la nécessité de provisionner un serveur à l'appui. Ces codes peuvent donc être appliqués sur des instances EC2 (comme dans notre cas) à l'aide d'un **service événementiel** (ici le planificateur EventBridge) et d'une description des **rôles IAM** pour les script Lambda.

iii. Solution de log

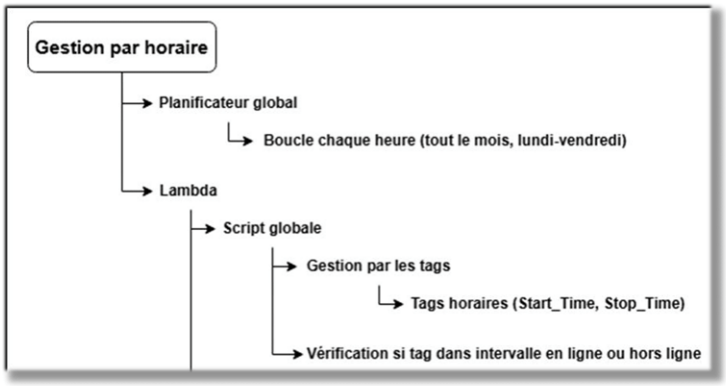
La solution retenue afin de pouvoir **sauvegarder les logs** des résultats retournés par la fonction du script Lambda à chaque planification est le service intégré à AWS, **CloudWatch**.

Ce dernier nous permet de **récupérer les informations** des logs de chacune des planifications du script Lambda, permettant, au long, et en cas de besoin, de pouvoir retrouver des données en cas de dysfonctionnement de ce dernier, afin d'aider au débogage.

Bernois Damien

B. Solutions envisageables

i. Gestion par horaire

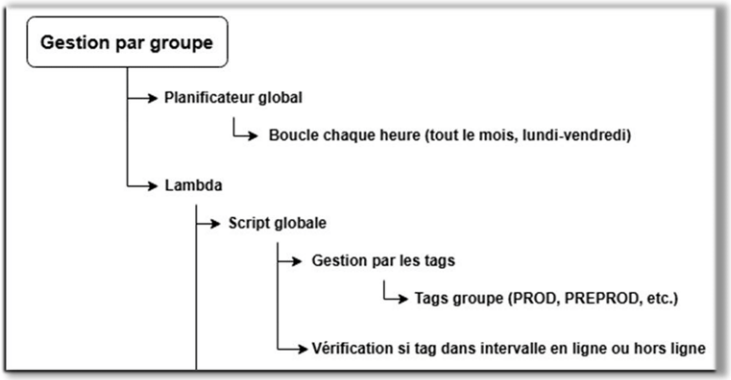


- Avantages :
  - Gestion des planificateurs amoindrie
  - Gestion à l'heure près
  - Récupération des instances par 2 tags (« Start_time » et « Stop_time »)

- Inconvénients :
  - Récurrence des requêtes
  - Récurrence des évènements
  - Script plus complexe
  - Consommation du trafic

Retour au chapitre Retour à la table des matières

ii. Gestion par groupe



- Avantages :
  - Gestion des planificateurs amoindrie
  - Gestion à l'heure près
  - Récupération des instances par seulement 1 tag (« Groupe »)
  - Gestion général plus souple et simple (plus apte à évoluer)

- Inconvénients :
  - Récurrence des requêtes
  - Récurrence des évènements
  - Script plus complexe
  - Consommation du trafic

Bernois Damien

3. Etude de la gestion des horaires

Afin d'assurer la **gestion des horaires** des différentes instances concernées, il est nécessaire de rattacher chacune d'elles à des **tags « groupe »** afin de pouvoir **regrouper et simplifier** la gestion des horaires à travers la mise en place des différents services et scripts de gestion.

Pour ce faire, il faut en amont étudier les différentes **priorités et nécessités de mise en fonctionnement** des différentes instances, que cela soit pour l'exploitation de la ressource par les utilisations, tout comme la sauvegarde de cette dernière vers notre baie de stockage VEEAM.

A. Regroupement des instances

Instances	ID	Groupe
APO-JAR-teltransmission-PHU-BPE	i-0b42a20ea1fc56b5a	PRODUCTION
FPF-prod_bo	i-054af68e633d50f97	
LFB-V1-prod	i-0bafc04048ddc9054	
FRCT-prod	i-04f25f919638e34d3	
Climessences-prod_v1.0.0	i-014dce4c3324003a3	
CNPF-ACTIV	i-04a12babed9c6d6fe	
CNPF-ILEX	i-022a87ab89f348492	
CNPF-RDP-Gateway & acs.fr DC	i-07d9b09084a427984	
CNPF-DNS1 (PROD)	i-0509b896288e73fbe	
CNPF-CARTO	i-0a79d7d9b85d17f7b	
LDAP Server (ldap Old)	i-090ab342ceca42675	
CNPF_DVF_foncier	i-03dfffae96e4ef119	
CNPF-Merlin	i-08b412f096091ce59	
CNPF-GFIpep	i-093c60fe94e3fdca1	
WALLIX_Access_Manager_PROD_v4.0.6	i-0aaaf8529c21b5ce8	
CNPF_McAfee_1	i-0ab4fd28975f98178	
Mailcatcher	i-03e50c40a7cd8fca3	
CNPF-LDAP (ldap New)	i-09468b02d2d6bab39	
Graylog	i-0093041badac5910a	
Matomo	i-039c2b75783701ce5	
CNPF-VIRTUALIA-APPLI	i-0ad3b635801c8889c	
CNPF-VIRTUALIA-IIS	i-03a1d3bf3595e4e23	
GFI-CAB	i-05894ffeaed803354	
StreamGoomer Manager	i-0cf2311f09cac456c	
MyMetricks Server	i-0a78ea43b44b0553f	
Portail-authentification-V2 (lemon v2.0x)	i-0534e5b0ed88e8e56	
WALLIX_Bastion_PROD_v10.0.7	i-0441332ada949fa1f	
VPC_BAST_FIREWALL (prod)	i-03d7c6477d0e6c755	
foret-gibier	i-03d2452c55fe57125	
StormShield_SMC_Server_v3.6.0	i-056fc393e7f948dc8	
CNPF-web-prod	i-04cf242eb5d4e0742	
SonarQube Server	i-01ce916d98337949f	
Gitlab Server	i-00ed7f75a76832bb2	
Gitlab Runner	i-084e466885263652f	
Zimbra Server PROD (patch 44)	i-0ebfbba3170f5421e	
secoia_v2 server (2nd installation) - (VPC Webint - ss1)	i-0012342a7248e6ee9	
Cryhod Share Server	i-07f0881ed89d60180	
Windows_2016_TSE_Server_(PROD)	i-04c5593fe32f8e8d6	
antispam	i-053072ff7ee9b44cc	

Bernois Damien

Wapt Server	i-07bdb7b8be8d82b4f	
New_Photofor	i-0150f2d3d31a00b2f	
NetsKope Publisher	i-0e6dfbe6cab443307	
CNPF-ocsinventory PROD (v2.8.1)	i-0e4478bc260c27899	
Virtualia v5 - Form	i-00b49ff4751c5958e	
VirtualiaV5 - Prod	i-0db090a410cb4f1db	
Gophish_Server	i-0a7d3d9fa64809e0b	
BioClimSol_V2_prod	i-05ed399c73337757c	
Zimbra Docs PROD	i-0bf413ccd7378a16e	
New_Photofor	i-0150f2d3d31a00b2f	
LFB-MongoDB	i-01121aeb9f4132c97	
CNPF-Nextcloud (v30)	i-0c82987b761e666be	
sftp	i-0d3f4d7ca2c9e13a3	
DG_FILESERVER	i-022748bec937a416b	
Veeam Console	i-06177bc1ef5077dd8	
CIDF_FILESERVER	i-0702be67a3bc721c2	
PACA_FILESERVER	i-0fa783fe484e6e83b	
AURA_FILESERVER	i-01f04524ee740ef2a	
GEST_FILESERVER	i-01cf3cf239150aff9	
HDFN_FILESERVER	i-08fad5eb92cbde14f	
BPDL_FILESERVER	i-0a7f4b7c9b2773b19	
BFC_FILESERVER	i-022e67471119565f4	
OCCI_FILESERVER	i-09623837b31ea7f3f	
CNPF_ADSERVER	i-061a72926ef8c9fa5	
NAQUI_FILESERVER	i-0bd189e3b5baa4e57	
IDF_FILESERVER	i-0f300100525fec48b	
CNPF-web-preprod_Cloned	i-0a1fc61801ad023a9	PREPRODUCTION
secoia preprod	i-031a25934b7ecb1b2	
GLPI Server	i-0d2a7da31ec0b411c	
sylveclair_preprod	i-062ce8df32720ecd6	
LFB-V2-recette-drupal9	i-00f55ac6c94e7c718	RECETTE
Recette-Teletrans-Serveur	i-04681d6d6f9b87b4f	
Climessences-recette_v1.0.0	i-0f9bdcb6bad85d550	
LFB-V1-recette	i-059a5928072dd405f	
BioClim_Test	i-0db611651c98e8677	
Bioclimsol_Auth_Server_TEST	i-0fe9fb8b9cb133d11	
API_Carto_enjeux (Recette)	i-0b75d571d399a936b	
BioClimSol-Dev-Test	i-0d06d97def251d1f4	
VirtualiaV5 - Test	i-03a346fa53dd48471	
Climessences V1 Recette Drupal10	i-0014f2b9e861ee110	
LFB-V1-prod	i-0bafc04048ddc9054	SAUVEGARDE
CNPF-Nextcloud (29.0.11)	i-0c82987b761e666be	
Climessences-prod_v1.0.0	i-014dce4c3324003a3	
CNPF-ACTIV	i-04a12babed9c6d6fe	
CNPF-ILEX	i-022a87ab89f348492	
CNPF-RDP-Gateway & acs.fr DC	i-07d9b09084a427984	
CNPF-DNS1 (PROD)	i-0509b896288e73fbe	
CNPF-CARTO	i-0a79d7d9b85d17f7b	
CNPF_DVF_foncier	i-03dfffae96e4ef119	
CNPF-Merlin	i-08b412f096091ce59	
CNPF-GFIpep	i-093c60fe94e3fdca1	
CNPF-API	i-0cea583a26e80bed3	

Bernois Damien

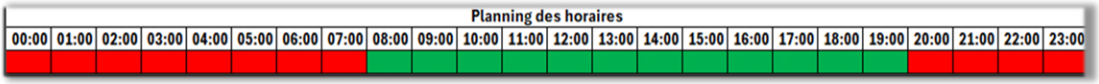
CNPF-LDAP (ldap New)	i-09468b02d2d6bab39	
GFI-CAB	i-05894ffeaed803354	
StreamGoomer Manager	i-0cf2311f09cac456c	
foret-gibier	i-03d2452c55fe57125	
StormShield_SMC_Server_v3.6.0	i-056fc393e7f948dc8	
CNPF-web-prod	i-04cf242eb5d4e0742	
Gitlab Server	i-00ed7f75a76832bb2	
Gitlab Runner	i-084e466885263652f	
Merlin-Tdata	i-0a31d02e3f14f9557	
DG_FILESERVER	i-022748bec937a416b	
CIDF_FILESERVER	i-0702be67a3bc721c2	
AURA_FILESERVER	i-01f04524ee740ef2a	
BPDL_FILESERVER	i-0a7f4b7c9b2773b19	
BFC_FILESERVER	i-022e67471119565f4	
Cryhod Share Server	i-07f0881ed89d60180	
Windows_2016_TSE_Server_(PROD)	i-04c5593fe32f8e8d6	
CNPF_ADSERVER	i-061a72926ef8c9fa5	
NAQUI_FILESERVER	i-0bd189e3b5baa4e57	
NetsKope Publisher	i-0e6dfbe6cab443307	
CNPF-ocsinventory PROD (v2.8.1)	i-0e4478bc260c27899	

Bernois Damien

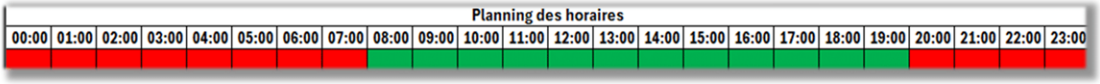
B. Classement des politiques de gestion

Groupe	Stratégie	Horaire fonctionnel	Horaire non-fonctionnel
Production	Horaire de mise en ligne large, prévois des horaires plus étendues en cas d'heures supplémentaires.	07 : 00 à 21 : 00	21 : 00 à 07 : 00

Groupe	Stratégie	Horaire fonctionnel	Horaire non-fonctionnel
Préproduction	Horaire de mise en ligne légèrement large, prévois des horaires légèrement plus étendues en cas d'heures supplémentaires.	08 : 00 à 19 : 00	19 : 00 à 08 : 00



Groupe	Stratégie	Horaire fonctionnel	Horaire non-fonctionnel
Recette	Horaire de mise en ligne légèrement large, prévois des horaires légèrement plus étendues en cas d'heures supplémentaires.	08 : 00 à 19 : 00	19 : 00 à 08 : 00



Groupe	Stratégie	Horaire fonctionnel	Horaire non-fonctionnel
Sauvegarde	Horaire de mise en ligne très légère durant la nuit afin de prévoir les sauvegardes.	01 : 00 à 06 : 00	03 : 00 à 06 : 00

Bernois Damien

4. Configuration de la gestion des horaires

A. Solution retenue

La solution retenue, pour des raisons de simplification de la gestion des planificateurs, d'une possibilité d'évolution du script, de la précision de l'application de ce dernier ainsi que son coût (gratuite), est celle de la gestion des horaires du fait d'un unique planificateur et un script complet à l'aide de tags de groupe (précisant les horaires d'exécution au sein du script).

B. Scripting des actions et tests

Afin d'assurer la **gestion des horaires** des différentes instances concernées, il est nécessaire de configurer un **script** permettant de gérer le démarrage ou l'arrêt des instances concernées à l'aide de la fonctionnalité des « balises » (**tag**) sur AWS.

```python
import boto3
from datetime import datetime, timedelta

ec2 = boto3.client('ec2')

#définit de plage d'horaire par groupe
tag_metiers = {
    'PRODUCTION':    ('07:00', '21:00'),
    'PREPRODUCTION': ('08:00', '18:00'),
    'RECETTE':       ('08:00', '18:00'),
    'SAUVEGARDE':    ('00:00', '06:00'),
}

#première fonction récupérant les données d'horaires
def is_in_list(current, start, stop):
    current_datetime = datetime.strptime(current, '%H:%M')
    start_datetime = datetime.strptime(start, '%H:%M')
    stop_datetime = datetime.strptime(stop, '%H:%M')
    #compare les heures d'horaires de du groupe de l'instance avec l'heure actuelle
    if start_datetime <= stop_datetime:
        return start_datetime <= current_datetime < stop_datetime
    else :
        return current_datetime >= start_datetime or current_datetime < stop_datetime
```

Bernois Damien

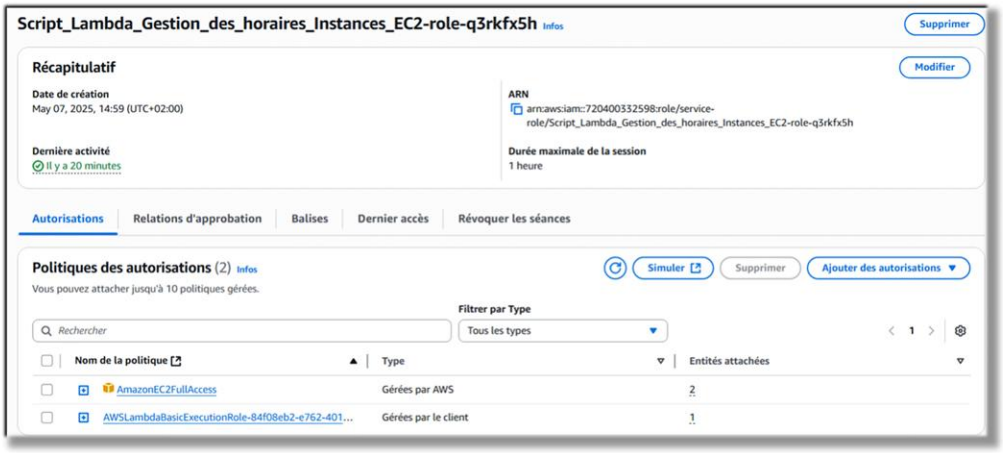
```python

#deuxième fonction de vérification et d'application
def lambda_handler(event, context):
    #récupère l'heure actuelle en format HH:MM en UTC
    current_time = (datetime.utcnow() + timedelta(hours=+2)).strftime('%H:%M')
    print(f"Heure actuelle (UTC Europe/Paris) : ", current_time)

    #créer la liste des instances à démarrer ou arrêter
    to_start = []
    to_stop = []

    #récupère toutes les instances EC2 avec le filtre "gestion_des_horaires"
    response = ec2.describe_instances(
        Filters = [
            {'Name': 'tag-key', 'Values': ['gestion_des_horaires']},
            {'Name': 'tag-key', 'Values': list(tag_metiers.keys())},
            {'Name': 'instance-state-name', 'Values': ['running', 'stopped']}
        ]
    )

    for reservation in response ['Reservations']:
        for instance in reservation['Instances']:

            #récupère les informations de l'instance
            instance_name = instance['KeyName']
            instance_id = instance['InstanceId']
            state = instance['State']['Name']

            #récupère les tags
            tags = {tag['Key']: tag['Value'] for tag in instance.get('Tags', [])}

            #récupère le tag_metiers de l'instance
            tag_found = None
            start_time = stop_time = None
            for tag in tag_metiers:
                if tag in tags:
                    tag_found = tag
                    start_time, stop_time = tag_metiers[tag]
                    break

            #vérifie sur l'horaire actuel est cohérent avec l'heure défini par le tag_metiers
            if tag_found :
                if is_in_list(current_time, start_time, stop_time):
                    if state == 'stopped':
                        to_start.append(instance_id)
                else :
                    if state == 'running':
                        to_stop.append(instance_id)

            #Affiche toutes les informations de l'instance
            print(f"\nInstance :  \n- Nom : ", instance_name,
                  f"\n- ID : ", instance_id,
                  f"\n- Etat : ", state,
                  f"\n- Groupe : ", tag_found,
                  f"\n- Horaire de démarrage : ", start_time,
                  f"\n- Horaire d'arrêt : ", stop_time)

    #Démarre ou éteins l'instance en fonction du résultat obtenu précédemment
    if to_start:
        ec2.start_instances(InstanceIds=to_start)
        print(f"Démarrage des instances suivantes : ", to_start)
    if to_stop:
        ec2.stop_instances(InstanceIds=to_stop)
        print(f"Arrêt des instances suivantes : ", to_stop)
```

Bernois Damien

[Retour au chapitre](#) [Retour à la table des matières](#)

Afin de pouvoir tester le fonctionnement du script mis en place, il est nécessaire, en amont, de créer un « **Test Events** ». Ici la création de l'événement de test « Script_Lambda_TEST », ainsi que la création du **rôle IAM** permet au script **d'accéder aux ressources EC2** afin de pouvoir exécuter ses fonctions.

- Création du rôle IAM :



- Création et application de l'évènement de test :

Dans notre contexte de test actuel, 3 instances de Test sont mises en place, chacune d'entre elles est attribuée à un groupe différent (PRODUCTION, PREPRODUCTION et RECETTE) et sont en état « hors ligne ».

```
Function Logs:
START RequestId: 320d140e-6b73-415a-a1ab-ae6b016b59aa Version: $LATEST
Heure actuelle (UTC Europe/Paris) :  11:16
Instance :
- Nom :  test
- ID :  i-0b4066dea0dffd111
- État :  stopped
- Groupe :  PRODUCTION
- Horaire de démarrage :  07:00
- Horaire d'arrêt :  21:00
Instance :
- Nom :  instances test gestion des horaires 2
- ID :  i-09c185016dda02220
- État :  stopped
- Groupe :  PREPRODUCTION
- Horaire de démarrage :  08:00
- Horaire d'arrêt :  18:00
Instance :
- Nom :  gestion des horaires instances EC2 TEST 3
- ID :  i-0e232674be75d0208
- État :  stopped
- Groupe :  RECETTE
- Horaire de démarrage :  08:00
- Horaire d'arrêt :  18:00
Démarrage des instances suivantes :  ['i-0b4066dea0dffd111', 'i-09c185016dda02220', 'i-0e232674be75d0208']
END RequestId: 320d140e-6b73-415a-a1ab-ae6b016b59aa
REPORT RequestId: 320d140e-6b73-415a-a1ab-ae6b016b59aa  Duration: 1314.11 ms    Billed Duration: 1315 ms    Memory Size: 128 MB Max Memory Used: 95 MB  Init
Duration: 542.30 ms
```

Les 3 instances de test concernées sont reconnues comme « hors ligne ». Étant donné l'état actuel de ces instances, ainsi que le fait qu'elles devraient être « en ligne » dû à l'heure actuelle comprise dans l'intervalle des horaires d'exécution de chacun des 3 groupes, le script met en ligne ces dernières.

Bernois Damien

Retour au chapitre Retour à la table des matières

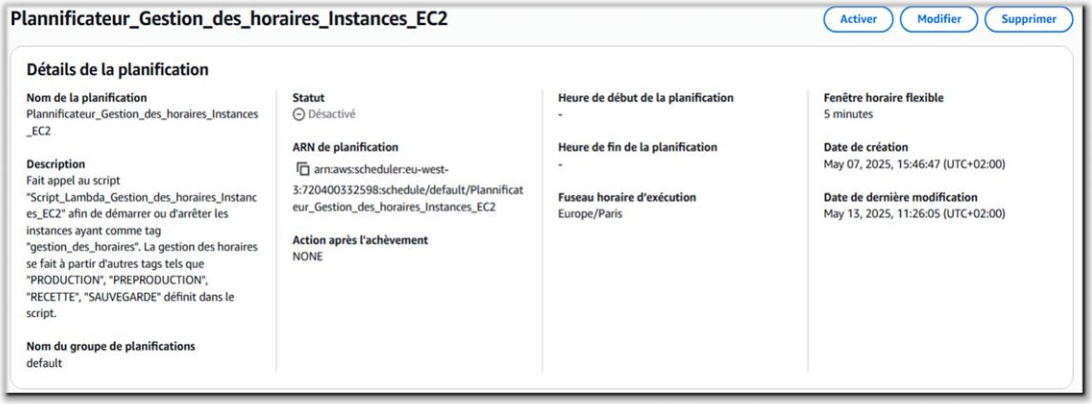
```
Function Logs:
START RequestId: 349145ca-a640-415a-96fe-5be9cb3f39fc Version: $LATEST
Heure actuelle (UTC Europe/Paris) :  11:20
Instance :
- Nom :  test
- ID :  i-0b4066dea0dffd111
- État :  running
- Groupe :  PRODUCTION
- Horaire de démarrage :  07:00
- Horaire d'arrêt :  21:00
Instance :
- Nom :  instances test gestion des horaires 2
- ID :  i-09c185016dda02220
- État :  running
- Groupe :  PREPRODUCTION
- Horaire de démarrage :  08:00
- Horaire d'arrêt :  18:00
Instance :
- Nom :  gestion des horaires instances EC2 TEST 3
- ID :  i-0e232674be75d0208
- État :  running
- Groupe :  RECETTE
- Horaire de démarrage :  08:00
- Horaire d'arrêt :  18:00
END RequestId: 349145ca-a640-415a-96fe-5be9cb3f39fc
REPORT RequestId: 349145ca-a640-415a-96fe-5be9cb3f39fc  Duration: 684.03 ms Billed Duration: 685 ms Memory Size: 128 MB Max Memory Used: 95 MB
```

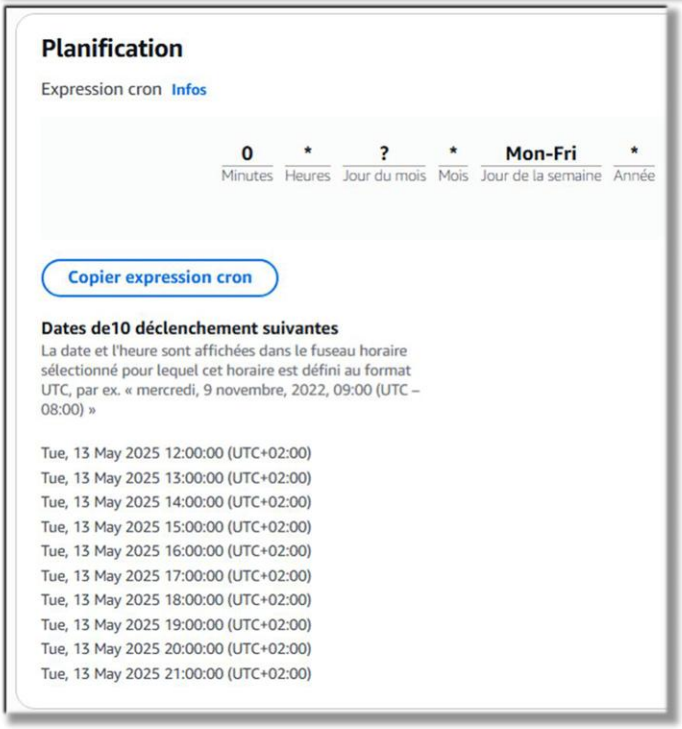
Les 3 instances de test concernées sont bien reconnues comme en ligne. Étant donné que l'heure actuelle est comprise dans l'intervalle des horaires d'exécution de chacun des 3 groupes, aucune modification de leur état n'est effectuée.

Bernois Damien

C. Planification de la d'activation du script

Afin d'assurer la **gestion des horaires** des différentes instances concernées, il est aussi nécessaire de configurer un **planificateur** permettant d'exécuter le script de gestion des horaires en fonction d'une stratégie d'**expression CRON**.





L'expression CRON permet au planificateur de s'exécuter chaque heure, du lundi au vendredi.

De plus, une fenêtre d'horaire flexible de l'exécution du planificateur de 5 minutes est définie afin d'assurer sa planification en cas de ralentissement du réseau.

Bernois Damien

Retour au chapitre Retour à la table des matières

Ici le script de gestion des horaires est la cible de ce planificateur, à chaque itération de l'expression CRON, le planificateur va exécuter ce dernier.

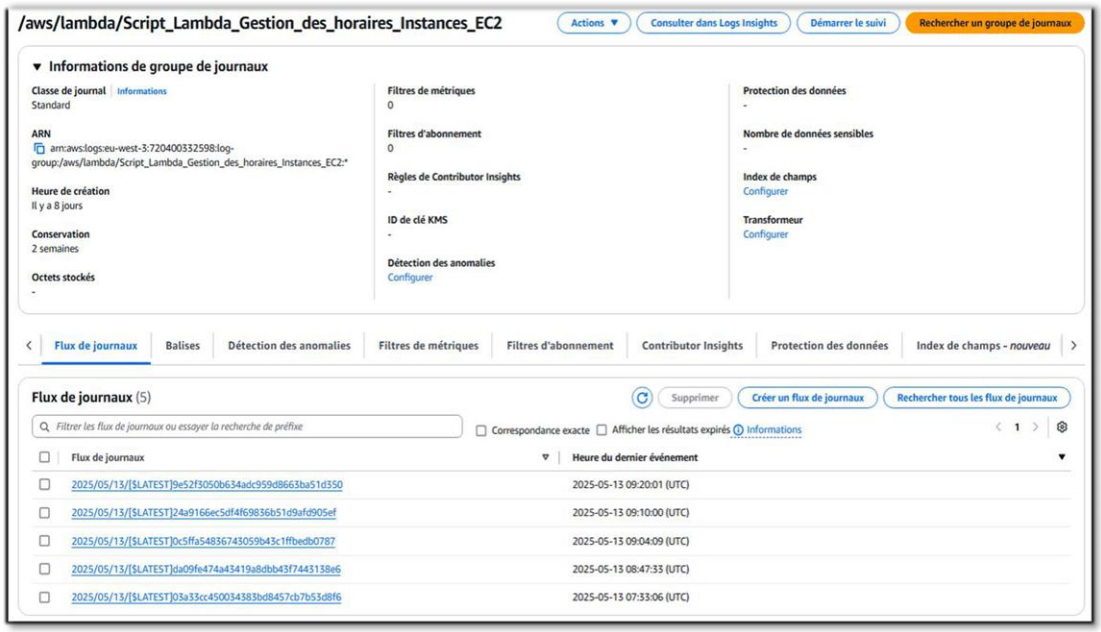
Pour ce faire, ce dernier a aussi besoin d'accéder aux ressources EC2 afin de pouvoir récupérer leurs données, ainsi que pouvoir changer l'état de ces dernières.

Bernois Damien

Retour au chapitre Retour à la table des matières

D. Récupération des logs

Afin d'assurer la **récupération et la sauvegarde des logs** de chaque itération de la mise en œuvre du script Lambda par le planificateur EventBridge, la mise en place d'un dossier de log sur le service CloudWatch est nécessaire. La création de ce dernier se fait automatiquement lors de la création de la première application du script.



Une rétention de 2 semaines (14 jours) est mise en place, afin de pouvoir remonter les informations en cas d'incidents. À partir de 14 jours, le log sera supprimé. Un total de 336 logs est maintenu sauvegardé au sein de ce groupe de logs CloudWatch.

Bernois Damien

Retour au chapitre Retour à la table des matières

5. Ressources économisées

A. Instances obsolètes

i. Référentiel des coûts

Ce référentiel des coûts des instances concernées se base sur le service de calcul des coûts des services proposé par AWS répertoriant les **coûts de chaque ressource** en **temps réel**, par **zone géographique**.

Ressources	Type	Prix
Volume de stockage EBS	gp2	0.10 $/Go/Mois
	gp3	0.08 $/Go/Mois
Instance EC2	t2.nano	0.0066 $/Heure
	t2.micro	0.0132 $/Heure
	t2.small	0.0264 $/Heure
	t2.medium	0.0528 $/Heure
	t2.large	0.1056 $/Heure
	t2.xlarge	0.2112 $/Heure
	t2.2xlarge	0.4224 $/Heure
	t3.nano	0.0059 $/Heure
	t3.micro	0.0118 $/Heure
	t3.small	0,0236 $/Heure
	t3.medium	0.0472 $/Heure
	t3.large	0,0944 $/Heure
	t3.xlarge	0.1888 $/Heure
	t3.2xlarge	0.3776 $/Heure
	m5.large	0,112 $/Heure
	m5.xlarge	0,224 $/Heure
	m5.2xlarge	0,448 $/Heure

Bernois Damien

ii. Suppression

Ici, la suppression des instances obsolètes permet de s'affranchir des possibles coûts qui auraient été engendrés en cas de mise en ligne de ces dernières et d'hébergement de leurs données.

La nécessité de mettre hors ligne les instances ne faisant plus l'objet d'une utilité dans un temps imparti permet à cette dernière de ne plus engendrer des coûts de maintien de ses ressources.

Cependant, dès lors qu'une instance ne fera plus l'objet d'une utilisation, mettre hors ligne cette dernière ne réduira pas à 0 les coûts qu'elle engendre. Effectivement, cette dernière fera toujours l'objet de l'hébergement de ces volumes de stockage qui engendrent à leur tour un coût de maintien.

Nom	ID	Type	Volume EBS
FRCT-dev	i-02d368fe77a1f7142	t2.micro	30 GB gp3
SFT_POC_Carto_Cadastre	i-0c76f653e25f400b8	t2.micro	100 GB gp3
RLT_Catalogue_2	i-0ad4476b41003b653	t2.small	120 GB gp3
StreamGoomer Collector	i-01246656413ce8e9f	t3.large	500 GB gp3
Windows_Server_rescue_Sylvain	i-03b28a6add802ea68	t2.large	30 GB gp2
CNPF-VIRTUALIA-APPLI_RESTORED	i-09dcf239575356b9b	t3.2xlarge	2 * 500 GB gp3
Redmine-4.1.0	i-02a72cbb3e8ceca27	t2.medium	100 GB gp3
srvobm.cnpf.fr	i-086c6a24f363ffd23	t2.xlarge	800 GB gp3
FPF-dev	i-097b9c1f49cede2c3	t2.xlarge	100 GB gp3
sylvi-par	i-0ecf982146a6fa556	t2.micro	100 GB gp3
FRCT-recette	i-030c0be689086ff48	t2.micro	250 GB gp3
mig-CNPF-DNS2	i-02f5c3d4ea31a49ad	t2.micro	8 GB gp3
TEST_API_POC_Carto	i-05278444474ccb152	t2.large	150 GB gp2
Client2_Zimbra_MIG	i-076165f3720d8f36a	t3.medium	20 GB gp2
Client1_Zimbra_MIG	i-0104157e6c6e333bf	t3.medium	20 GB gp2
Virtual Room Connector	i-0ed62fa2f927be456	t2.large	100 GB gp2
TheGreenBow TAS Server	i-0400a0529479e625a	t2.small	10 GB gp3
RDP_CNPF_Voir_Balises	i-0bb2e8e2d84547401	t2.medium	60 GB gp3

Ressources	Quantité	Calcul	Coût économisé	Total
gp2	320 GB	320 * 0.10 $	32$	286.24 $ / 251,81 €
gp3	3 178 GB	3 178 * 0.08 $	254.24 $	
t2.micro	5 instances	5 * 744 * 0.0132 $	49.104 $	1 138.32 $ / 1 001,40 €
t2.small	2 instances	2 * 744 * 0.0264 $	39.2832 $	
t2.medium	2 instances	2 * 744 * 0.0528 $	78.5664 $	
t2.large	3 instances	3 * 744 * 0.1056 $	235.6992 $	
t2.xlarge	2 instances	2 * 744 * 0.2112 $	314.2656 $	
t3.medium	2 instances	2 * 744 * 0.0472 $	70.2336 $	
t3.large	1 instance	744 * 0.0944 $	70.2336 $	
t3.2xlarge	1 instance	744 * 0.3776 $	280.9344 $	
				1 424.56 $ / 1 253,21 €

La mise hors ligne étant déjà effectuée, l'économie du maintien des instances de 1 001,40 € était déjà opérationnelle. Dans notre cas, la **résiliation** (suppression) de ces instances ne faisant plus l'objet d'une nécessité de maintien au sein de notre infrastructure, nous a permis de **supprimer les volumes de stockage** EBS leur étant rattachés. De ce fait, cela a engendré une réduction des coûts totaux de **251,81 €** par mois.

Bernois Damien

iii. Mise hors ligne

Nom	ID	Type
cnpf-SG	i-0e6d4854b1da6d874	t3.large
Pentest Server	i-0d54a06012d780c97	t2.large
Connecteur-SW2-Prod	i-02cbeb797c8563bde	t2.micro
SUADEO_Serveur_application	i-0aa2b0d958a5c82fa	t2.2xlarge
FPF-prod_fo	i-0f4f3883b4b4f05d1	t2.xlarge
Climessences-preprod_v1.0.0)	i-0b3dcb4ebecc02c44	t3.xlarge
LFB-V1-preprod	i-0825ce02ed72d68ec	t2.xlarge
SUADEO_Recette	i-09cfafd5638d8e6e7	t3.2xlarge
Recette-Merlin	i-066bd7997b4bedafc	t3.xlarge
Zimbra Server TEST (patch 44)	i-0c0a9fb2ff85b09ba	t3.xlarge

Ressources	Quantité	Calcul	Coût économisé	Total
t2.micro	1 instance	744 * 0.0132 $	9.8208 $	1 278.79 $ / 1141,01 €
t2.large	1 instance	744 * 0.1056 $	78.5664 $	
t2.xlarge	2 instances	2 * 744 * 0.2112 $	314.2656 $	
t2.2xlarge	1 instance	744 * 0.4224 $	314.2656 $	
t3.large	1 instance	744 * 0.0944 $	70.2336 $	
t3.xlarge	3 instances	3 * 744 * 0.0944 $	210.7008 $	
t3.2xlarge	1 instance	744 * 0.3776 $	280.9344 $	

La mise hors ligne étant déjà effectuée, l'économie du maintien des instances de 1141,01 € était déjà opérationnelle.

Bernois Damien

B. Coûts des services et solutions retenus

i. EventBridge

D'après la tarification de la calculatrice AWS du service EventBridge :

Forfait gratuit (par mois)	Coûts
1M premiers évènements	0.2 $ par requête

Consommation des ressources estimée	Coûts
744 évènements max /mois	0

ii. Lambda

D'après la tarification de la calculatrice AWS du service Lambda :

Forfait gratuit (par mois)	Coûts
1M premières requêtes	0.2 $ par requête
400K premiers GB-sec	0.0000167$ par Go-sec

Consommation des ressources estimée	Coûts
744 requêtes / mois	0
Environ 5 500 Go /mois	0

iii. CloudWatch

D'après la tarification de la calculatrice AWS du service CloudWatch :

Forfait gratuit (par mois)	Coûts
5 premiers GB	0.5 $ par Go données ingérées
	0.03 $ par Go de données stockées

Consommation des ressources estimée	Coûts	Total
Environ 60 Go de données ingérées	27.5 $ / 24,53 €	26.18 €
Environ 60 Go de données stockées	1.65 $ / 1,47 €	

Bernois Damien

C. Coûts de la gestion des horaires

i. Production

➢ Instances concernées :

Instances	ID	Type
FPF-prod_bo	i-054af68e633d50f97	t2.xlarge
LFB-V1-prod	i-0bafc04048ddc9054	t2.xlarge
FRCT-prod	i-04f25f919638e34d3	t2.micro
Climessences-prod_v1.0.0	i-014dce4c3324003a3	t2.xlarge
CNPF-ACTIV	i-04a12babed9c6d6fe	t3.micro
CNPF-ILEX	i-022a87ab89f348492	t3.micro
CNPF-RDP-Gateway & acs.fr DC	i-07d9b09084a427984	t2.xlarge
CNPF-DNS1 (PROD)	i-0509b896288e73fbe	t3.micro
CNPF-CARTO	i-0a79d7d9b85d17f7b	t3.xlarge
LDAP Server (ldap Old)	i-090ab342ceca42675	t2.medium
CNPF_DVF_foncier	i-03dfffae96e4ef119	t2.micro
CNPF-Merlin	i-08b412f096091ce59	t2.xlarge
CNPF-GFIpep	i-093c60fe94e3fdca1	t2.2xlarge
WALLIX_Access_Manager_PROD_v4.0.6	i-0aaaf8529c21b5ce8	t3.small
CNPF_McAfee_1	i-0ab4fd28975f98178	t2.large
Mailcatcher	i-03e50c40a7cd8fca3	t3.micro
CNPF-LDAP (ldap New)	i-09468b02d2d6bab39	t2.micro
Graylog	i-0093041badac5910a	t3.medium
Matomo	i-039c2b75783701ce5	t3.large
CNPF-VIRTUALIA-APPLI	i-0ad3b635801c8889c	t3.2xlarge
CNPF-VIRTUALIA-IIS	i-03a1d3bf3595e4e23	t3.xlarge
GFI-CAB	i-05894ffeaed803354	t2.micro
StreamGoomer Manager	i-0cf2311f09cac456c	t3.xlarge
MyMetricks Server	i-0a78ea43b44b0553f	t2.xlarge
Portail-authentification-V2 (lemon v2.0x)	i-0534e5b0ed88e8e56	t3.medium
WALLIX_Bastion_PROD_v10.0.7	i-0441332ada949fa1f	t3.medium
VPC_BAST_FIREWALL (prod)	i-03d7c6477d0e6c755	t2.xlarge
foret-gibier	i-03d2452c55fe57125	t3.small
StormShield_SMC_Server_v3.6.0	i-056fc393e7f948dc8	t3.xlarge
CNPF-web-prod	i-04cf242eb5d4e0742	t3.xlarge
SonarQube Server	i-01ce916d98337949f	t2.large
Gitlab Server	i-00ed7f75a76832bb2	t2.xlarge
Gitlab Runner	i-084e466885263652f	t3.medium
Zimbra Server PROD (patch 44)	i-0ebfbba3170f5421e	m5.2xlarge
secoia_v2 server (2nd installation) - (VPC Webint - ss1)	i-0012342a7248e6ee9	m5.xlarge
Cryhod Share Server	i-07f0881ed89d60180	t2.micro
Windows_2016_TSE_Server_(PROD)	i-04c5593fe32f8e8d6	t2.large
antispam	i-053072ff7ee9b44cc	t2.xlarge
Wapt Server	i-07bdb7b8be8d82b4f	t2.large
New_Photofor	i-0150f2d3d31a00b2f	t3.medium
NetsKope Publisher	i-0e6dfbe6cab443307	t3.medium
CNPF-ocsinventory PROD (v2.8.1)	i-0e4478bc260c27899	t3.medium
Virtualia v5 - Form	i-00b49ff4751c5958e	t3.large
VirtualiaV5 - Prod	i-0db090a410cb4f1db	t3.large
Gophish_Server	i-0a7d3d9fa64809e0b	t3.micro

Bernois Damien

BioClimSol_V2_prod	i-05ed399c73337757c	t3.medium
Zimbra Docs PROD	i-0bf413ccd7378a16e	t2.large
New_Photofor	i-0150f2d3d31a00b2f	t3.medium
LFB-MongoDB	LFB-MongoDB	t2.medium
CNPF-Nextcloud (v30)	CNPF-Nextcloud (v30)	t3.xlarge
sftp	sftp	t3.nano
DG_FILESERVER	DG_FILESERVER	t3.large
Veeam Console	Veeam Console	t3.medium
CIDF_FILESERVER	CIDF_FILESERVER	t3.large
PACA_FILESERVER	PACA_FILESERVER	t3.large
AURA_FILESERVER	AURA_FILESERVER	t3.large
GEST_FILESERVER	GEST_FILESERVER	t3.large
HDFN_FILESERVER	HDFN_FILESERVER	t3.large
BPDL_FILESERVER	BPDL_FILESERVER	t3.large
BFC_FILESERVER	BFC_FILESERVER	t3.large
OCCI_FILESERVER	OCCI_FILESERVER	t3.large
CNPF_ADSERVER	CNPF_ADSERVER	t3.large
NAQUI_FILESERVER	NAQUI_FILESERVER	t3.large
IDF_FILESERVER	IDF_FILESERVER	t3.large

- Coût moyen mensuel engendré (mise en ligne) :

Ressources	Quantité	Calcul	Coût engendré	Total
t2.micro	5	434 * 5 * 0.0132	28.644	3 218.3 $ / 2 876,9 €
t2.medium	2	434 * 2 * 0.0528	45.8304	
t2.large	5	434 * 5 * 0.1056	229.152	
t2.xlarge	10	434 * 10 * 0.2112	916.152	
t2.2xlarge	1	434 * 0.4224	183.3216	
t3.nano		434 * 0.0059	2.5606	
t3.micro	5	434 * 5 * 0.0118	25.606	
t3.small	2	434 * 2 * 0,0236	20.4848	
t3.medium	10	434 * 10 * 0.0472	204.848	
t3.large	15	434 * 15 * 0.0944	614.544	
t3.xlarge	6	434 * 6 * 0.1888	491.6352	
t3.2xlarge	1	434 * 0.3776	163.8784	
m5.xlarge		434 * 0,224	97.216	
m5.2xlarge		434 * 0,448	194.432	

434 = 14 (nb heure ne ligne /j) * 31 (nb jour /mois)

- Coût moyen mensuel économisé (mise en hors ligne) :

Ressources	Quantité	Calcul	Coût économisé	Total
t2.micro	5	310 * 5 * 0.0132	20.46	2 332.32 $ / 2084,92 €
t2.medium	2	310 * 2 * 0.0528	32.736	
t2.large	5	310 * 5 * 0.1056	163.68	
t2.xlarge	10	310 * 10 * 0.2112	654.72	
t2.2xlarge	1	310 * 0.4224	137.144	
t3.nano		310 * 0.0059	1.829	
t3.micro	5	310 * 5 * 0.0118	18.29	
t3.small	2	310 * 2 * 0,0236	14.632	
t3.medium	10	310 * 10 * 0.0472	146.32	
t3.large	15	310 * 15 * 0.0944	438.96	

Bernois Damien

Retour au chapitre Retour à la table des matières

t3.xlarge	6	310 * 6 * 0.1888	351.168	
t3.2xlarge	1	310 * 0.3776	117.056	
m5.xlarge		310 * 0,224	69.44	
m5.2xlarge		310 * 0,448	138.88	

310 = 10 (nb heure ne ligne /j) * 31 (nb jour /mois)

- Coût total des instances :

Type	Total
En ligne	3 218.3 $ / 2 876,9 €
Hors ligne	2 332.32 $ / 2084,92 €

Bernois Damien

ii. Préproduction

- Instances concernées :

Instances	ID	Type
CNPF-web-preprod_Cloned	i-0a1fc61801ad023a9	t3.large
secoia preprod	i-031a25934b7ecb1b2	t3.xlarge
GLPI Server	i-0d2a7da31ec0b411c	t2.micro
sylveclair_preprod	i-062ce8df32720ecd6	t3.small

- Coûts :

Le coût moyen mensuel engendré (mise en ligne) et économisé (mise en hors ligne) sont **identiques** car la stratégie de gestion d'horaires indique 12h hors ligne et 12 autres en ligne.

Ressources	Quantité	Calcul	Coût	Total
t2.micro	1	372 * 0.0132	4.9104	119.04 $ / 106,41 €
t3.small		372 * 0,0236	8.7792	
t3.large		372 * 0.0944	35.1168	
t3.xlarge		372 * 0.1888	70.2336	

372 = 12 (nb heure ne ligne /j) * 31 (nb jour /mois)

- Coût total des instances :

Type	Total
Coût engendré	119.04 $ / 106,41 €
Coût économisé	119.04 / 106,41 €

Bernois Damien

iii. Recette

- Instances concernées :

Instances	ID	Type
LFB-V2-recette-drupal9	i-00f55ac6c94e7c718	t2.xlarge
Recette-Teletrans-Serveur	i-04681d6d6f9b87b4f	t2.micro
Climessences-recette_v1.0.0	i-0f9bdcb6bad85d550	t2.xlarge
LFB-V1-recette	i-059a5928072dd405f	t2.xlarge
BioClim_Test	i-0db611651c98e8677	t2.large
Bioclimsol_Auth_Server_TEST	i-0fe9fb8b9cb133d11	t2.micro
API_Carto_enjeux (Recette)	i-0b75d571d399a936b	t2.large
BioClimSol-Dev-Test	i-0d06d97def251d1f4	t2.medium
VirtualiaV5 - Test	i-03a346fa53dd48471	t3.large
Climessences V1 Recette Drupal10	i-0014f2b9e861ee110	t3.xlarge

- Coûts :

Le coût moyen mensuel engendré (mise en ligne) et économisé (mise en hors ligne) sont **identiques** car la stratégie de gestion d'horaires indique 12h hors ligne et 12 autres en ligne.

Ressources	Quantité	Calcul	Coût	Total
t2.micro	2	372 * 2 * 0.0132	9.8208	449.08 $ / 401,44 €
t2.medium	1	372 * 0.0528	19.6416	
t2.large	2	372 * 2 * 0.1056	78.5664	
t2.xlarge	3	372 * 3 * 0.2112	235.6992	
t3.large	1	372 * 0.0944	35.1168	
t3.xlarge		372 * 0.1888	70.2336	

372 = 12 (nb heure ne ligne /j) * 31 (nb jour /mois)

- Coût total des instances :

Type	Total
Coût engendré	449.08 $ / 401,44 €
Coût économisé	449.08 / 401,44 €

Bernois Damien

iv. Sauvegarde

Ici, la subtilité des instances du groupe « **SAUVEGARDE** » est qu'elles **appartiennent aussi** au groupe « **PRODUCTION** ». Cela veut dire que lors du calcul du coût total engendré et économisé par les instances EC2 à la suite de la mise en place du système de gestion des horaires par scripting, il faudra **ajouter** au prix de mise en ligne, celui engendré par les horaires de maintien des instances de sauvegarde.

- Instances concernées :

Instances	ID	Type
LFB-V1-prod	i-0bafc04048ddc9054	t2.xlarge
CNPF-Nextcloud (v30)	i-0c82987b761e666be	t3.xlarge
Climessences-prod_v1.0.0	i-014dce4c3324003a3	t2.xlarge
CNPF-ACTIV	i-04a12babed9c6d6fe	t3.micro
CNPF-ILEX	i-022a87ab89f348492	t3.micro
CNPF-RDP-Gateway & acs.fr DC	i-07d9b09084a427984	t2.xlarge
CNPF-DNS1 (PROD)	i-0509b896288e73fbe	t3.micro
CNPF-CARTO	i-0a79d7d9b85d17f7b	t3.xlarge
CNPF_DVF_foncier	i-03dfffae96e4ef119	t2.micro
CNPF-Merlin	i-08b412f096091ce59	t2.xlarge
CNPF-GFIpep	i-093c60fe94e3fdca1	t2.2xlarge
CNPF-API	i-0cea583a26e80bed3	t3.micro
CNPF-LDAP (ldap New)	i-09468b02d2d6bab39	t2.micro
GFI-CAB	i-05894ffeaed803354	t2.micro
StreamGoomer Manager	i-0cf2311f09cac456c	t3.xlarge
foret-gibier	i-03d2452c55fe57125	t3.small
StormShield_SMC_Server_v3.6.0	i-056fc393e7f948dc8	t3.xlarge
CNPF-web-prod	i-04cf242eb5d4e0742	t3.xlarge
Gitlab Server	i-00ed7f75a76832bb2	t2.xlarge
Gitlab Runner	i-084e466885263652f	t3.medium
Merlin-Tdata	i-0a31d02e3f14f9557	t3.large
DG_FILESERVER	i-022748bec937a416b	t3.large
CIDF_FILESERVER	i-0702be67a3bc721c2	t3.large
AURA_FILESERVER	i-01f04524ee740ef2a	t3.large
BPDL_FILESERVER	i-0a7f4b7c9b2773b19	t3.large
BFC_FILESERVER	i-022e67471119565f4	t3.large
Cryhod Share Server	i-07f0881ed89d60180	t2.micro
Windows_2016_TSE_Server_(PROD)	i-04c5593fe32f8e8d6	t2.large
CNPF_ADSERVER	i-061a72926ef8c9fa5	t2.2xlarge
NAQUI_FILESERVER	i-0bd189e3b5baa4e57	t3.large
NetsKope Publisher	i-0e6dfbe6cab443307	t3.medium
CNPF-ocsinventory PROD (v2.8.1)	i-0e4478bc260c27899	t3.medium

Bernois Damien

- Coût moyen mensuel engendré (mise en ligne) :

Ressources	Quantité	Calcul	Coût engendré	Total
t2.micro	4	186 * 4 * 0.0132	9.8208	721.01 $ / 643,12 €
t2.large	1	186 * 0.1056	19.6416	
t2.xlarge	5	186 * 5 * 0.2112	196.416	
t2.2xlarge	2	186 * 2 * 0.4224	157.1328	
t3.micro	4	186 * 4 * 0.0118	8.7792	
t3.small	1	186 * 0,0236	4.3896	
t3.medium	3	186 * 3 * 0.0472	26.3376	
t3.large	7	186 * 7 * 0.0944	122.9088	
t3.xlarge	5	186 * 5 * 0.1888	175.584	

186 = 6 (nb heure ne ligne /j) * 31 (nb jour /mois)

- Coût total des instances :

Type	Total
Coût engendré	721.01 $ / 643,12 €

Bernois Damien

6. Plus-values du projet

A. Bénéfice de sécurité

La mise en place de cette gestion des horaires apporte, en plus de celui économique, un aspect de **sécurité**. Effectivement, actuellement (basculement vers la gestion des horaires non effectué), les instances sont maintenues en état de mise en ligne continuellement, tous les jours de la semaine, et ce sans interruption (hormis dysfonctionnements et incidents). De ce fait, ces dernières sont possiblement à disposition de faire l'**objet d'une attaque à tout moment** de la journée, quelque que soit l'heure.

Ici, la gestion des horaires permettant de mettre hors ligne les instances ne devant pas faire l'objet d'une raison de maintien opérationnel à une heure dite, ces dernières **ne sont donc plus vulnérables à une quelconque attaque du fait de leur état**, sur les périodes de mise hors ligne (elles ne sont plus visibles sur le réseau, en interne à l'environnement AWS, en externe par le biais de nos LAN et de nos passerelles privées AWS ; ou bien par internet directement, par le biais de nos passerelles publiques AWS).

Pour conclure, la mise en place de cette politique de gestion des horaires de mise en ligne des instances permet de **réduire l'intervalle d'attaques** malveillantes sur les instances, réduisant donc grandement les possibilités des risques d'attaques sur notre réseau cloud.

B. Bénéfice budgétaire

Aujourd'hui, le budget alloué afin de maintenir notre infrastructure cloud sur notre environnement AWS est en partie engendré par le **maintien en ligne de nos ressources EC2** (actuellement 109 instances).

De ce fait, une réflexion sur l'**optimisation de ces coûts** a été étudiée par mes soins. À la suite de cette dernière, détaillée ci-dessus, et à l'aide de la mise en place d'une **politique de gestion des horaires** de mise en ligne des instances EC2 par le biais d'un script, nous pouvons en conclure l'estimation du **coût économisé** ci-dessous :

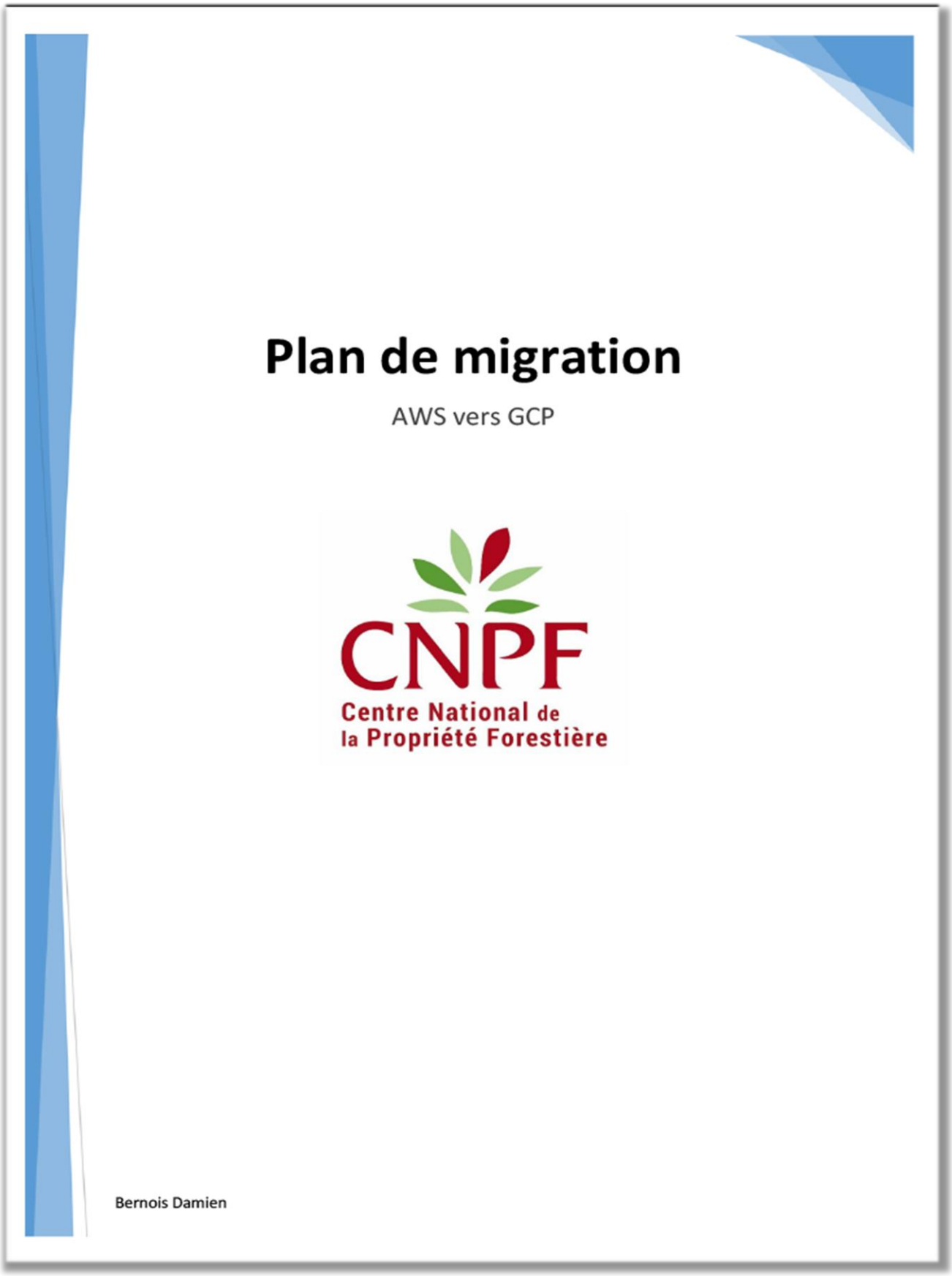
- Coût total initialement engendré par le maintien des ressources EC2 (instances) est ~ 7 347.24 $ (estimation du prix en avril 2025), soit ~ **6 551,72 €**.
- Coût du maintien des instances (à la suite de la mise en place de la politique de gestion des horaires de ces dernières) est de 4 533.61 $, soit **4 042,73€**.

  26,18 $ (coût log CloudWatch) + 449.08 $ (coût engendré « RECETTE ») + 119.04 $ (coût engendré « PREPRODUCTION ») + 3 218.3 $ (coût engendré « PRODUCTION »)
- Coût économisé à l'aide de cette dernière est de 2 900.44 $, soit **2 586,39 €**.

  449.08 $ (coût économisé « RECETTE ») + 119.04 $ (coût économisé « PREPRODUCTION ») + 2 332.32 $ (coût économisé « PRODUCTION »)

Bernois Damien

G. Plan de migration (GCP)



Retour au chapitre *Retour à la table des matières*

RÉPUBLIQUE FRANÇAISE

CNPF

Table des matières

Bernois Damien

CONTEXTE

Dans le cadre du projet de migration de notre infrastructure cloud actuelle hébergée sur l'environnement AWS vers celui de GCP, nous avons convenu d'utiliser la solution native proposée par chacun de ces deux environnements.

Cette dernière s'appuie sur l'accessibilité des APIs internes à ces deux derniers afin d'assurer une migration de l'environnement source de façon sécurisée, efficace, intègre et sans aucun impact sur la continuité des services.

Cette solution à faible coût assure à tout organisme une migration structurée, sécurisée et optimale en passant par un tunnel VPN privé mettant en communication le compte AWS (par l'intermédiaire d'un user IAM, avec les bons droits d'accès, créé en amont) et l'environnement GCP).

Ce plan de migration se divisera en 2 parties clés, donc chacune d'elles sera détaillée ci-dessous, telles que :

- Création des droits d'accès aux ressources du compte AWS pour l'environnement GCP.
- Récupération et réplication des ressources AWS sur l'environnement GCP.

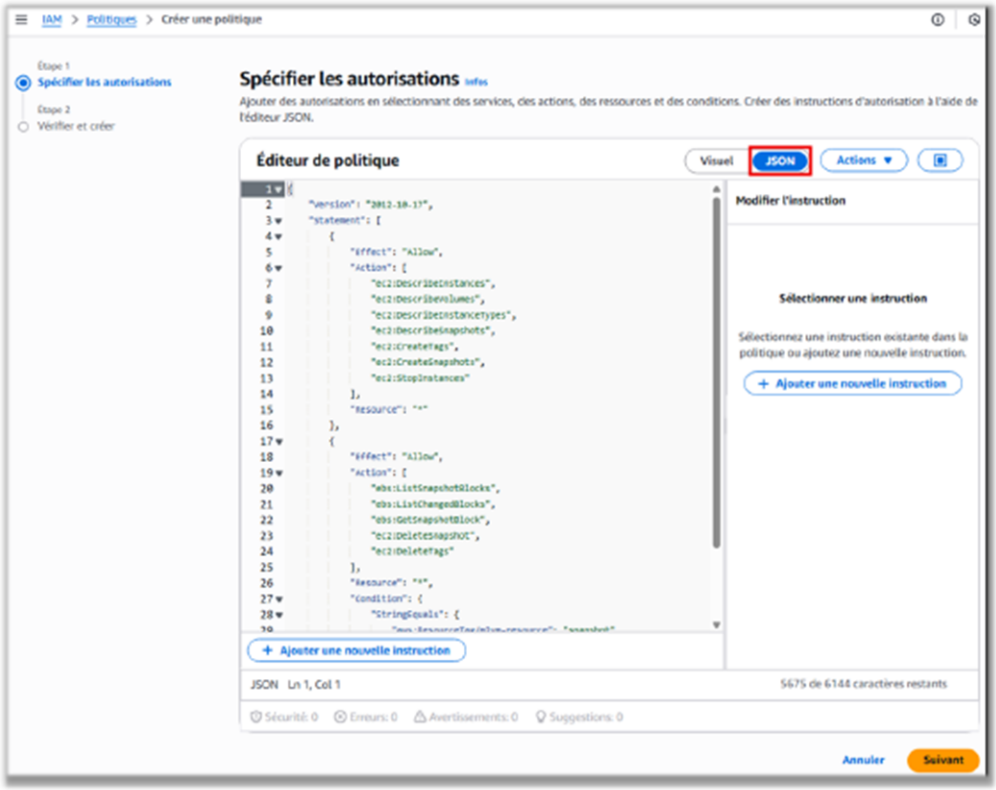
Bernois Damien

Retour au chapitre Retour à la table des matières

➢ Création des droits d'accès

Afin d'assurer la **communication entre les deux environnements cloud**, il est nécessaire de créer en amont un **utilisateur IAM**, ayant les ressources nécessaires aux ressources hébergées sur AWS, afin que GCP puisse créer sa source de migration à partir du lien de communication que lui fournit cet utilisateur interne à notre compte AWS.

➢ Création de la politique d'accès :



Bernois Damien

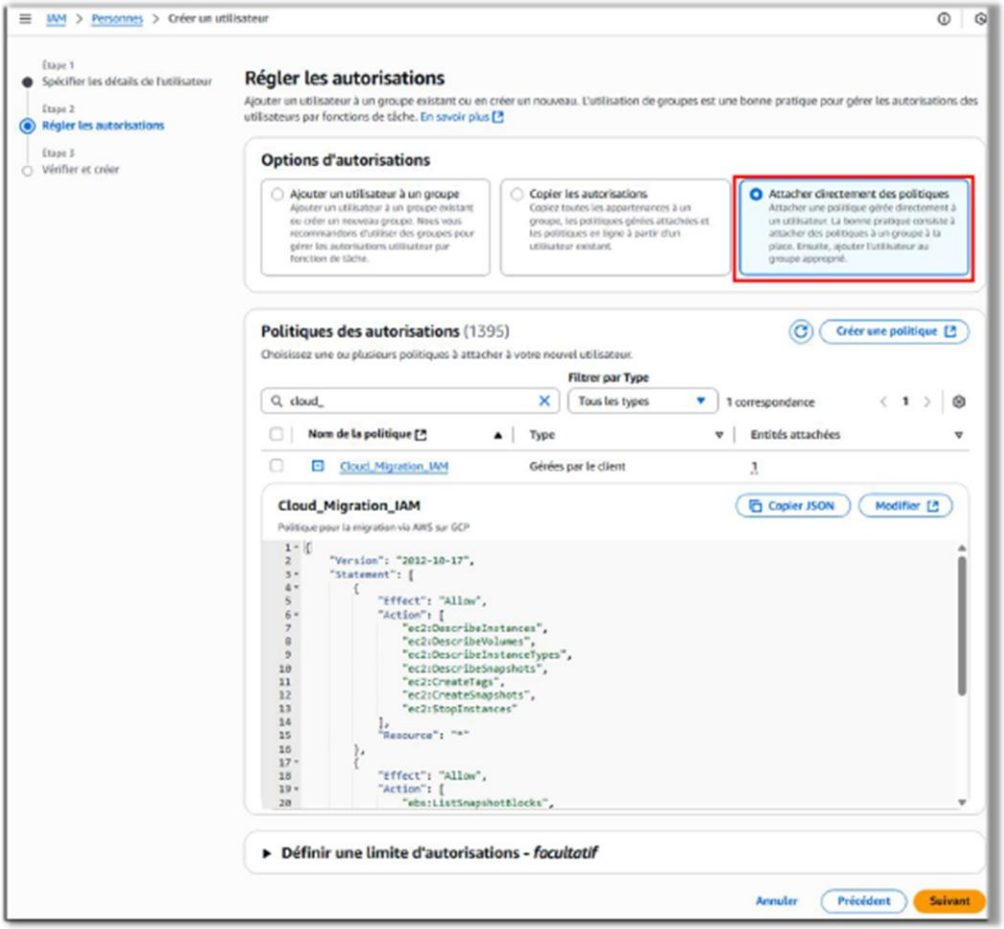
Retour au chapitre Retour à la table des matières

- Politique (JSON) :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSnapshots",
                "ec2:CreateTags",
                "ec2:CreateSnapshots",
                "ec2:StopInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ebs:GetSnapshotBlock",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/m2vm-resource": "snapshot"
                }
            }
        }
    ]
}
```

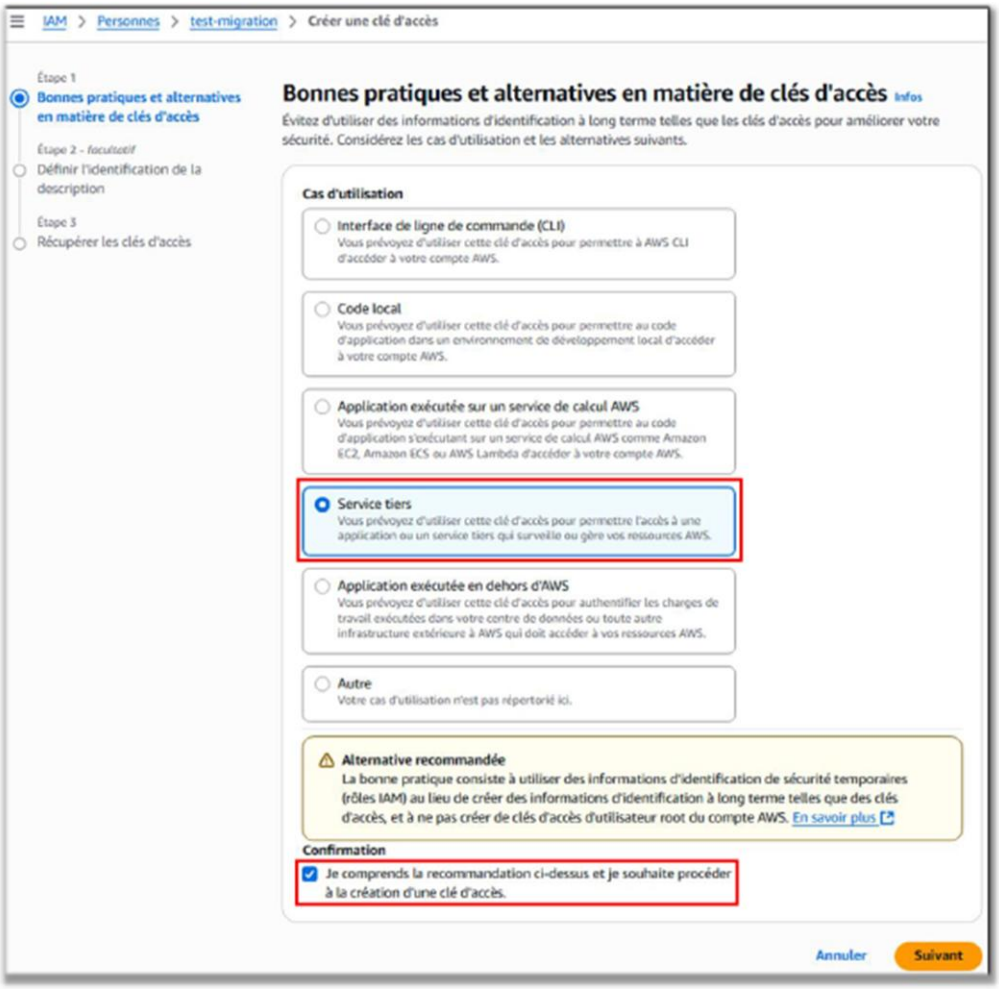
Bernois Damien

➢ Création de l'utilisateur :



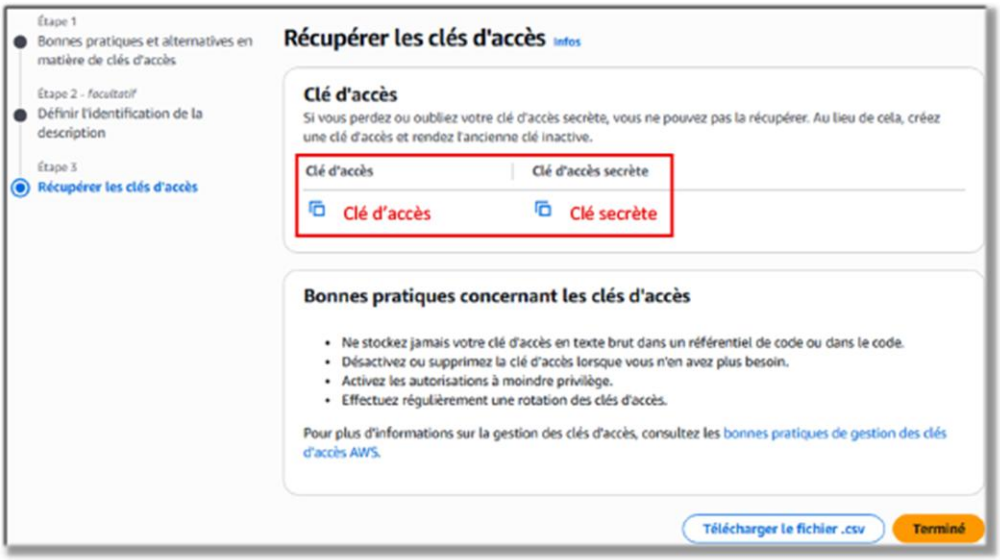
➢ Création de la clé d'accès :

Bernois Damien



Bernois Damien

Retour au chapitre Retour à la table des matières



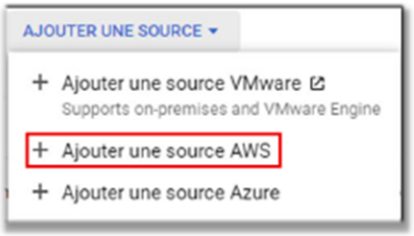
Bernois Damien

Retour au chapitre Retour à la table des matières

➢ Récupération des ressources

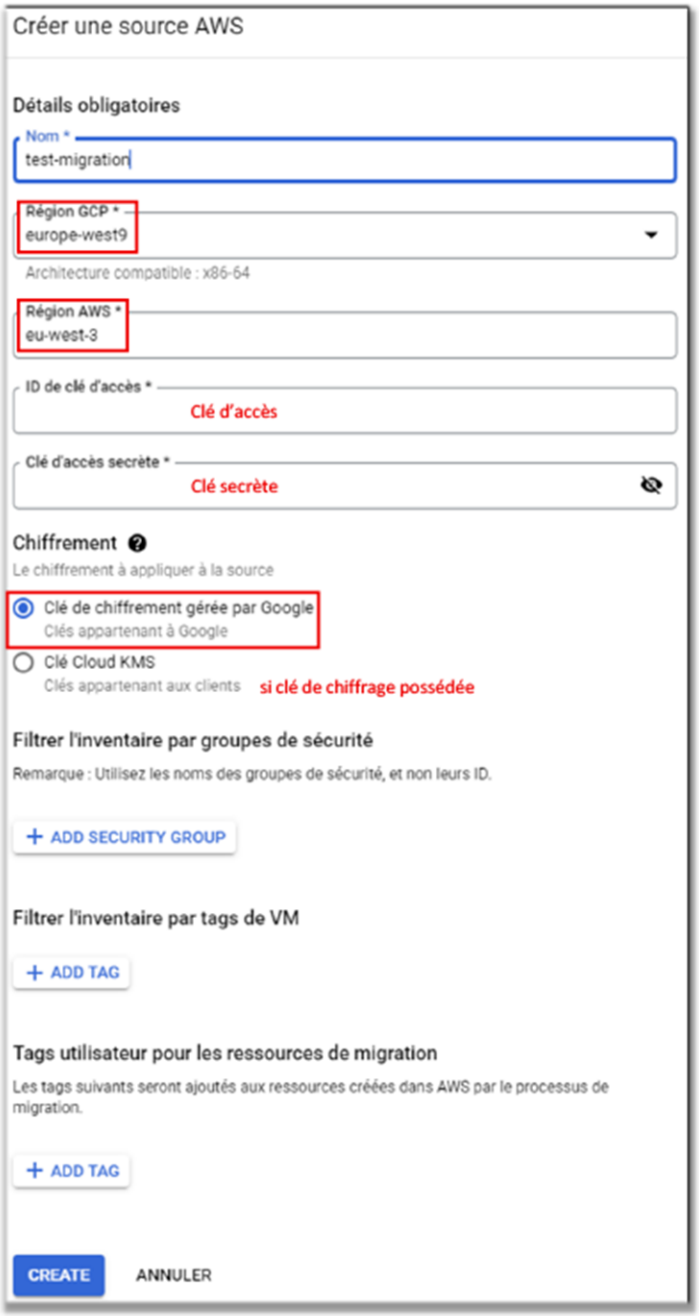
Pour cette deuxième étape, il est essentiel de configurer correctement la **source de migration** dans l'environnement GCP, afin de permettre la **communication avec l'utilisateur IAM** sur AWS et d'assurer l'**accès aux ressources hébergées**.

➢ Création de la source :



Bernois Damien

Retour au chapitre Retour à la table des matières

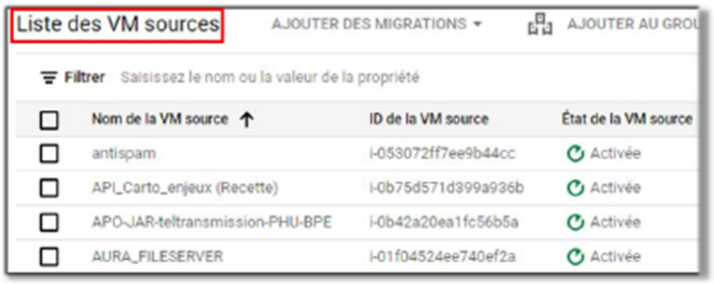


!

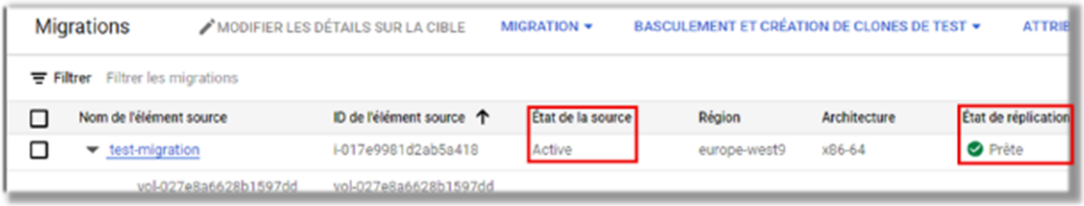
Bernois Damien

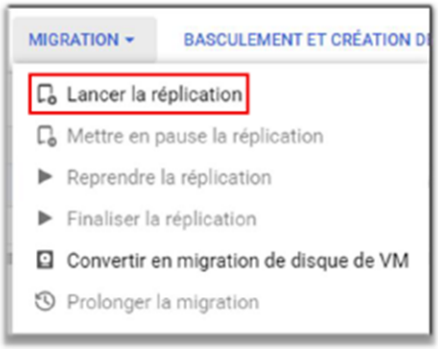
Retour au chapitre Retour à la table des matières

➢ Récupération de la source :



➢ Réplication des ressources :





Bernois Damien

Retour au chapitre Retour à la table des matières