

Migration vers le cloud

Procédure rédigée par : CHERIF Ahmed

Table des matières

I -Contexte du projet	2
I.1 – Définitions des besoins	2
I.2 – Avantage de la migration vers le cloud	2
I.3 – Comprendre l'existant	3
I.4 – L'architecture cible.....	4
II - Préparation pour la migration	6
II.1 - Clarifier les rôles et les responsabilités en utilisant une matrice RACI	6
II.2 - La communication et la coordination entre les différentes équipes	7
II.3 - Validation du Projet et Planning de préparation à la migration	8
II.4 - La stratégie de migration à adopter	9
III - Les principales étapes de la migration	9
III.1 – La Pre-migration	9
III.2 – La migration	11
III.2 – La Post-migration	12
IV - Roll back	13
IV.1 - Les raisons qui poussent au Roll back.....	13
IV.2 - Procédure de retour en arrière	14
V - Mise à jour des systèmes dans le cloud	16

I-\ Contexte du projet

1-\ Définition des besoins :

Nuova Impresa (NI) veut migrer ses services vers le cloud puisque le système d'exploitation utilisé sur tous ses serveurs arrive en fin de support, aussi elle veut réduire ses coûts et optimiser la disponibilité de ses services.

Pour l'instant ses serveurs applicatifs sont hébergés en interne. NI a décidé de profiter de la mise à jour de son système d'exploitation pour migrer ses serveurs vers une offre IAAS dans le cloud.

Ma mission est d'accompagner cette entreprise dans tous les phases de la migration de ses services vers le cloud.

2-\ les avantages de la migration vers le cloud :

Optimisation des coûts

Il est possible de réaliser d'importantes économies en termes de ressources, de maintenance et de coûts immobiliers, sans compter la possibilité d'optimiser les charges de travail pour que leur exploitation coûte moins cher.

Flexibilité et scalabilité

Les organisations ne paient que pour les ressources cloud qu'elles utilisent, ce qui signifie qu'elles n'ont pas besoin de payer et d'entretenir des ressources informatiques qu'elles n'utilisent qu'occasionnellement.

Lors des pics de demande ou lorsque l'organisation a besoin de ressources de calcul plus puissantes, elle peut modifier ses ressources instantanément, à la demande.

Sécurité renforcée

De nombreux cloud publics disposent de fonctionnalités de sécurité intégrées et d'outils de sécurité cloud spécialisés pour garantir la protection des ressources d'une organisation. Dans de nombreux cas, les correctifs de sécurité sont appliqués automatiquement par le fournisseur de cloud.

Conformité

Certaines plateformes cloud proposent des offres spécialisées afin de répondre plus facilement aux exigences de conformité, ce qui est idéal pour les secteurs très réglementés comme la finance, la santé et l'administration.

Sauvegarde, récupération et basculement

La plupart des fournisseurs de cloud contribuent à améliorer la continuité des activités en proposant des fonctionnalités de sauvegarde et de récupération intégrées, en un seul clic. Certains fournisseurs permettent également de stocker des sauvegardes dans différentes régions géographiques.

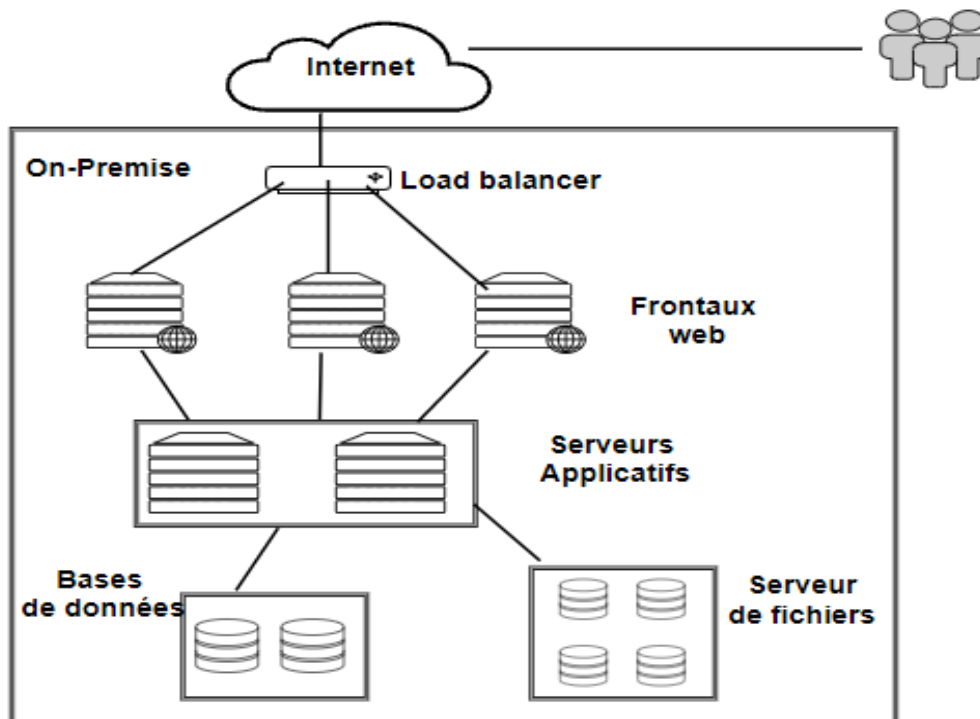
Gestion et surveillance simplifiées

Les organisations peuvent gérer et surveiller leur centre de données local et leurs ressources cloud à partir d'un seul écran si le fournisseur de cloud propose un outil de gestion centralisé.

3-\ Comprendre l'existant :

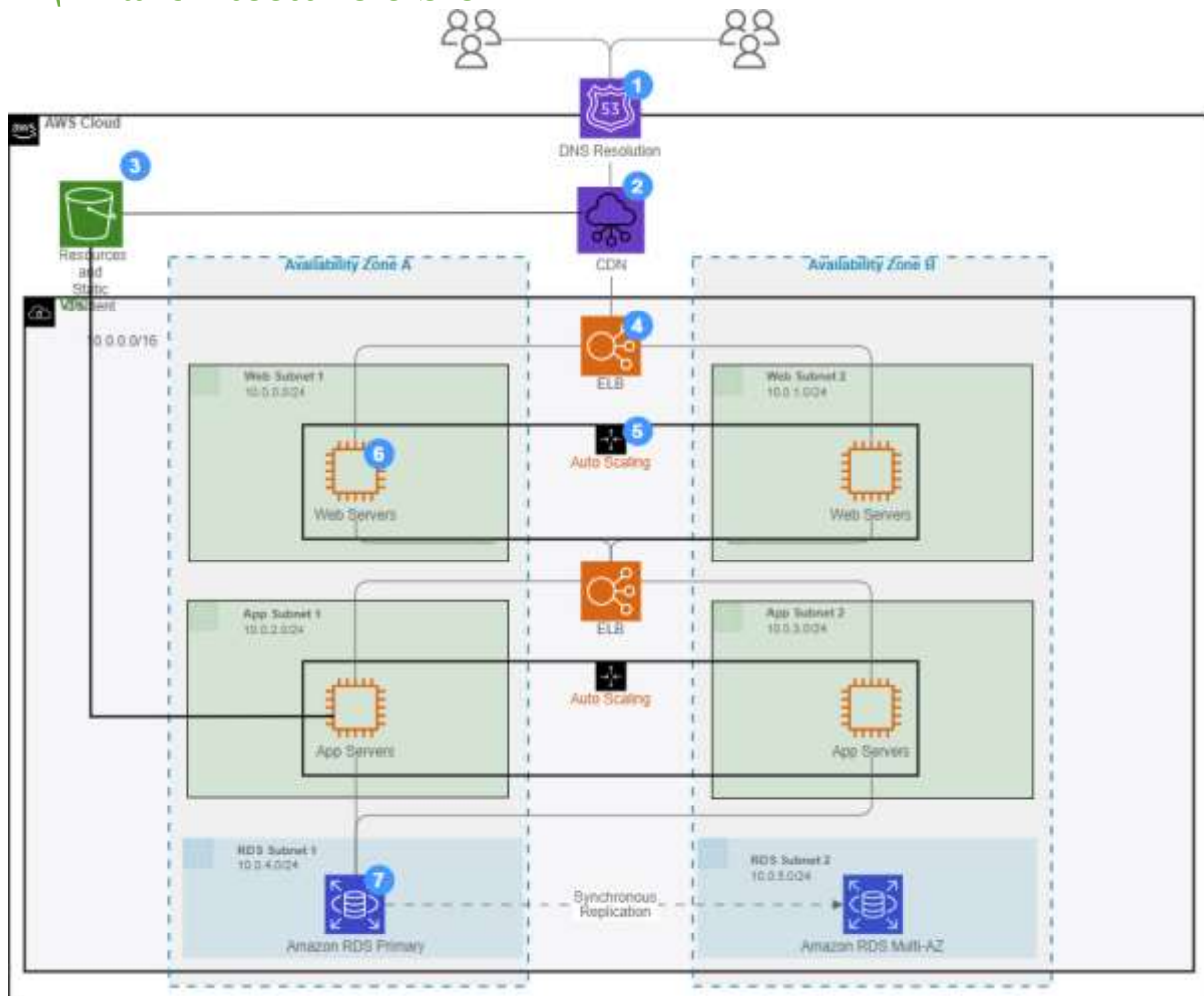
L'architecture de la plate-forme est la suivante :

- Un répartiteur de charge répartit les requêtes sur un ensemble de frontaux web
- Les frontaux web transfèrent les requêtes à un cluster de serveurs applicatifs
- Les serveurs applicatifs communiquent avec :
 - Un cluster de serveurs de fichiers qui gère le stockage d'environ 1To de données
 - Un cluster de serveurs de bases de données qui gère le stockage d'environ 5Go de données (dump texte non compressé)



Une solution On-premise consiste à héberger son infrastructure IT dans ses propres locaux. Par ce choix, vous gardez un contrôle absolu sur vos datas et vos applications. En revanche il faudra alors traiter les sujets de sécurité, sauvegarde, disponibilité et continuité de service sans oublier la performance d'accès. Bien entendu, cela nécessite un investissement initial accompagné des compétences nécessaires pour mettre en place et piloter l'architecture technique.

4-\ L'architecture cible



1- DNS Résolution

Les requêtes DNS de l'utilisateur sont traitées par Amazon Route 53, un service DNS (Domain Name System) hautement disponible. Le trafic réseau est acheminé vers l'infrastructure exécutée dans Amazon Web Services.

2- CDN

Le contenu statique, en continu et dynamique est fourni par Amazon CloudFront, un réseau mondial d'emplacements périphériques également connu sous le nom de réseau de diffusion de contenu (CDN). Les demandes sont automatiquement

acheminées vers l'emplacement périphérique le plus proche, de sorte que le contenu est livré avec les meilleures performances possibles.

3- Storage Service S3 :

Les ressources et le contenu statique utilisés par l'application Web sont stockés sur Amazon Simple Storage Service (S3), une infrastructure de stockage hautement durable conçue pour le stockage de données critiques et primaires.

4- Elastic Load Balancing (ELB)

Les requêtes HTTP sont d'abord gérées par Elastic Load Balancing (ELB), qui distribue automatiquement le trafic d'application entrant entre plusieurs instances Amazon Elastic Compute Cloud (EC2) dans les zones de disponibilité (AZ). Il permet une tolérance aux pannes encore plus grande dans vos applications, fournissant de manière transparente la quantité de capacité d'équilibrage de charge nécessaire en réponse au trafic applicatif entrant.

5- Auto-Scaling

Les serveurs Web et les serveurs d'applications sont déployés dans un groupe Auto-Scaling. Auto Scaling ajuste automatiquement votre capacité à la hausse ou à la baisse en fonction des conditions que vous définissez. Avec Auto Scaling, vous pouvez vous assurer que le nombre d'instances Amazon EC2 que vous utilisez augmente de manière transparente pendant les pics de demande pour maintenir les performances et diminue automatiquement pendant la demande pour minimiser les coûts.

6- Instance Amazon EC2

Les serveurs Web et les serveurs d'applications sont déployés sur les instances Amazon EC2. La plupart des organisations sélectionneront une Amazon Machine Image (AMI), puis la personnaliseront en fonction de leurs besoins. Cette AMI personnalisée deviendra alors le point de départ du futur développement Web.

7- RDS

Pour fournir une haute disponibilité, la base de données relationnelle qui contient les données de l'application est hébergée de manière redondante sur un déploiement multi-AZ (zones de disponibilité multiples - A et B ici) d'Amazon Relational Database Service (Amazon RDS).

II-\ Préparation pour la migration

1- Clarifier les rôles et les responsabilités en utilisant une matrice RACI

Lors de la migration vers le cloud. Il est nécessaire de comprendre le processus opérationnel et de savoir qui est responsable de quoi. Une façon de s'assurer que tout le monde comprend les rôles et les responsabilités est d'utiliser une matrice responsable, accountable, consultée et informée (RACI). Une matrice RACI est un moyen courant de mettre en œuvre un cadre de droits de décision pour clarifier les rôles et les responsabilités des processus clés.

La matrice montre les activités clés sous forme de lignes et les parties participantes sous forme de colonnes. Pour chaque partie participante, il faut indiquer si elle est responsable, accountable, consultée ou informée :

Responsable : la personne ou l'équipe qui est responsable d'exécuter et terminer les tâches

Accountable : la personne ou l'équipe qui prend les décisions et exécute les actions sur la (les) tâche (s).

Consulté : personnes ou équipes qui doivent être consultées avant la mise en œuvre des changements.

Informé : personnes ou équipes qui doivent être informés des changements

AIC : Administrateur Infrastructure et Cloud

ASR : Administrateur Système et Réseaux

ES : Equipe Support

ED : Equipe Développement

RACI	AIC	ASR	ES	ED
Fonctions				
Établir des indicateurs de performance clés pour la migration vers le cloud	RA	C		
Établir des critères de base de performance	RA	R	C	
Créer un plan de migration des données	RA	R	C	C
Installer les composants nécessaires	RA	R	C	
Sauvegarde des fichiers de configuration	RA	R	I	I
Assurer les performances du réseau	RA	R	I	

Effectuer une liste de contrôle de sécurité post-installation	RA	RA	C	C
Vérifier le contrôle d'accès à distance	C	RA	C	
Fournir des besoins de dimensionnement de sauvegarde	I	CI	RA	R
Mise à jour de l'application et ajouter des micro-services	I	I	I	RA
Basculer sur la production	RA	R	I	I

Autres intervenants :

- Le chef de projet organise et conduit le projet de bout en bout. Il assume la responsabilité des différentes phases, depuis la traduction des besoins utilisateurs en spécifications fonctionnelles et techniques, jusqu'à la recette utilisateur, voire la mise en production.
- Comité de direction a pour mission est de travailler sur la vision à long terme de l'entreprise et de prendre des décisions stratégiques. Les membres se rassemblent alors régulièrement lors de réunions ou séminaires pour faire le point sur les ressources financières, matérielles et humaines afin d'optimiser et d'améliorer les performances de l'entreprise.

2-\ La communication et la coordination entre les différentes équipes

Toutes les équipes sont concernées par le projet. Chaque membre de l'équipe IT a une ou plusieurs interventions dans les phases de migrations. Donc il y a un planning mis à la disposition pour toutes les équipes en indiquant le ou les jours d'interventions ; aussi le chef de projet peut intervenir à tous moments pour faire la coordination entre les équipes.

Le chef de projet réalise des réunions quotidiennes pour suivre l'avancement du projet avec les différentes équipes pour avoir le même niveau d'information.

3-\ Validation du Projet et Planning de préparation à la migration

Avant de commencer le planning de la migration, nous avons des données importantes à communiquer au comité de décision :

- Un environnement de test a été établi dans le cloud et les résultats étaient concluante. Cela montre bien que ce projet est faisable.
- Aussi les licences des systèmes d'exploitation vont être bientôt expirées. Donc le moment idéal pour faire les changements (moins de dépenses).

Ces données vont pousser le comité de décision à bien étudier le projet de point de vue rentabilité, budget et valider la date de début du projet.

Ce planning prend en considération seulement la partie communication et logistique, et non pas la partie technique.

Actions et procédures	Acteurs	Date
<ul style="list-style-type: none">• Le comité de décision à valider la date de commencement du projet et réunion avec les différents intervenants.• Meeting avec les métiers kick off meeting (réunion de lancement du projet)• Planification des différentes actions pour la migration et programmer les jours d'interventions de chaque équipe dans cette phase.• Discuter les prix des ressources utilisée• Faire un inventaire approximatif des dépenses mensuel pour l'utilisation des ressources sur le cloud	Comité de décision + Chef de projet + Equipes IT	J - 15
<ul style="list-style-type: none">• Envoi du planning aux différentes équipes en indiquant les jours et l'horaire de leurs interventions.• Envoi d'une note pour le gardien pour l'ouverture de l'entreprise pendant le weekend puisque l'arrêt de l'application et la migration va être effectuer pendant les 2 jours samedi et dimanche.	Comité de décision + Chef de projet + Equipes IT + Gardien	J - 14

4-\ La stratégie de migration à adopter

Après des réunions et des études avec des experts du domaine, le comité de décision a choisi la stratégie de migration **Rehost**

Rehost (lift and shift) : il s'agit de redéployer l'existant à l'identique (as is) dans le cloud. Cette méthode repose essentiellement sur le service IaaS et permet un démarrage rapide dans le cloud. Plutôt adaptée à un contexte où l'on souhaite réduire les coûts sans forcément tirer pleinement parti des avantages du cloud.

III-\ Les principales étapes de la migration

La planification doit couvrir les principales étapes du processus de migration de l'entrepôt de données de base et toutes les tâches qu'elles impliquent. Les principales étapes du processus sont les suivantes :

- Préparation pré-migration : préparer l'infrastructure de l'environnement de production (réseau, instances, sécurité, base de données)
- Stratégie et exécution de la migration : restaurer le dernier backup de la base de données et de système de fichiers et déconnecter de l'infrastructure on-premise et rediriger tous les trafics vers la nouvelle infrastructure et commencer de tester le fonctionnement de l'application.
- Post-migration : c'est l'étape de supervision de l'application, de supporter et corriger s'il y a un incident aussi la formation des toutes les équipes sur l'utilisation de cette nouvelle infrastructure et sur le cloud d'une façon générale.

1-\ Pre-migration

Actions et procédures	Acteurs	Date
<p>Création des comptes et des droits d'accées sur le cloud</p> <ul style="list-style-type: none">• Gestion des utilisateurs• Accès partagés à un compte sur plusieurs utilisateurs.• Accès par ressources• Création de policies <p>Remarque : le module utilisé : IAM (Identity and Access Management)</p>	<p>AIC + ASR</p>	<p>J - 13</p>

Création des groupes de sécurités (nom de chaque groupe + descriptions) Ajouter des règles à chaque groupe	AIC + ASR	J - 12
Création d'un groupe de sous réseaux pour la base de données. Création d'un groupe de sous réseaux pour les serveurs fichiers. Création d'un groupe de sous réseaux pour les serveurs applicatifs. Création d'un groupe de sous réseaux pour les Frontaux web	AIC + ASR	J - 11
Création de la base de données (le service RDS) Paramétrer et configurer cette instance (la taille 6 GO), l'utilisateur de la base de données (administrateur de la BD), le nombre d'instance (choisir 2 instances) Connexion à l'instance principale et importer ma base de données	AIC + ASR	J -10
Création des serveurs de fichier (le service S3) Création d'un compartiment. Importer tous les documents.	AIC + ASR	J - 8
Création des instances pour les serveurs applicatifs EC2 Création d'un Template pour le serveur application : Ce Template contient : <ul style="list-style-type: none"> • Toutes les dépendances qu'on doit installer pour que l'application tourne. Par exemple : php et ses bibliothèques • L'installation de l'application. Lancer 2 instances	AIC + ASR	J - 6
Création des instances pour les Frontaux web EC2 Création d'un Template pour un serveur Frontal. Ce Template contient : <ul style="list-style-type: none"> • L'installation du serveur web • La configuration du serveur web • La configuration de la certificat ssl pour la connexion https • Configuration d'une adresse IP virtuelle primaire/secondaire pour rediriger les frontaux en cas de basculement sur panne. Lancer 3 instances	AIC + ASR	J - 5
Création d'un groupe Target et lui affecter les VMs Frontaux web Creation d'un load balancers (Application Load Balancer)	AIC + ASR	J - 3

Création et configuration de l'auto-scaling	AIC + ASR	J - 2
Teste et validation du fonctionnement de l'application	AIC + ASR	J - 1

2-\ Migration

La Migration va être effectuée pendant le weekend où l'activité de l'entreprise est quasiment arrêtée (la phase de migration va durer 2 jours le samedi et le dimanche)

Actions et procédures	Acteurs	Date
Arrêt de service pour l'ancienne infrastructure	AIC + ASR	J Samedi
Prendre un full-backup de la base de données et l'importer dans le serveur base de données primaire du cloud	AIC + ASR	J Samedi 2 heures
Exporter un réplicat de cette base de données vers le serveur base de données secondaire du cloud et synchroniser les deux serveurs SGBD	AIC + ASR	J Samedi 30 minutes
Récupérer les documents qui ont été modifiés ou ajoutés depuis j-9 vers le serveur de fichiers	AIC + ASR	J Samedi 30 minutes
Mettre à jour le DNS du Load Balancers	AIC + ASR	J Samedi 30 minutes
Mettre à jour tous les nouvelles adresses IP et DNS	AIC + ASR	J Samedi 30 minutes
Validation de KPI : La gestion du temps consacré à la planification et à la supervision du processus de migration	AIC + ASR	J Samedi 30 minutes
Lancer l'application, et commencer à faire les premiers tests	AIC + ASR	J Samedi 1 heures
Pointer tous les outils de monitoring vers la nouvelle Infrastructure et Activer la surveillance	AIC + ASR	J Samedi 30 minutes

Validation des KPI d'infrastructure mesurent l'utilisation du matériel et du réseau <ul style="list-style-type: none"> • Utilisation de la mémoire • Performance du disque • Latence du réseau • Le load-balancing 	AIC + ASR	J Dimanche 2 heures
Validation de Kpi : la performance de l'application : <ul style="list-style-type: none"> • Taux d'erreur (requêtes échouées/total des requêtes) • Disponibilité • Latence • Nombre de temps morts • Débit 	AIC + ASR	J Dimanche 2 heures

3-\ Post-migration

Actions et procédures	Acteurs	Date
Accompagner l'équipe de support et vérifier les indicateurs retournés par les outils de monitoring. Relevé les incidents Mettre à jour certains indicateurs si nécessaire.	AIC + ASR + ES	J+1
Formation des équipes IT à AWS	AIC + ASR + ES + ED	J+2
Audit de sécurité Vérifier s'il y a une faille de sécurité non détecté	AIC + ASR	J+3
Démanteler de l'infrastructure on-premise	AIC + ASR	J+30

IV-\ Roll back

Après la migration, on peut s'affronter à différents types de problèmes (techniques, sécurités, financières), parfois on se trouve à l'obligation de faire un retour en arrière et revenir à l'ancienne infrastructure, donc l'administrateur cloud doit prévoir une procédure de Roll-back.

La phase de migration est faite pendant le week-end c'est-à-dire en 2 jours (le taux de l'utilisation de l'application est bas) donc la plupart des actions vont être effectuées pendant le samedi, par contre le dimanche matin est réservé pour valider les indicateurs KPI (Key Performance Indicator)

Si les valeurs des indicateurs ne sont pas satisfaisantes par exemple :

- **Taux d'erreur élevée**
- **L'application n'est pas disponible**
- **Latence dans le chargement de l'application**
- **La performance de disque**

L'administrateur cloud est dans l'obligation de contacter le comité de décision et d'aller vers un Roll-back

1-\ D'autres raisons qui poussent au Roll back

Les coûts cachés

Les coûts de gestion d'une solution de cloud sont très souvent sous-estimés par les entreprises. En principe, les fournisseurs de solutions cloud affichent un tarif pour le stockage de base et la sécurisation des données. Dans la pratique, s'ajoutent bien souvent à ce tarif des frais liés au transit ou au déplacement des données et applications, mais aussi à la personnalisation des services, la maintenance ou encore le conseil.

La sécurité

Si les principaux fournisseurs de solution cloud du marché possèdent des hauts standards en matière de sécurité, de nombreuses entreprises ignorent que la protection de leurs données et applications relève de leur responsabilité. En cas de perte de données liée à un sinistre majeur, l'hébergeur ne saurait être tenu pour responsable.

La performance

Le transfert des données des entreprises, réparties dans plusieurs datacenters au niveau local et dans le cloud, engendre des latences. Lorsque celles-ci sont trop

élevées, elles occasionnent des ralentissements, voire la perte de connexion à certaines applications.

Le contrôle

La maintenance et le contrôle des données et des applications les plus utilisées par l'entreprise sont simplifiés dans son propre environnement où les coûts sont fixes et prévisibles. Pour certaines entreprises, le département IT peut mieux faire face aux problèmes potentiels lorsque les données sont dans leurs propres datacenters. Par conséquent, pour les organisations concernées, si le contrôle promis par le fournisseur de solution n'est pas satisfaisant, il peut être pertinent de rapatrier leurs données sur leur site.

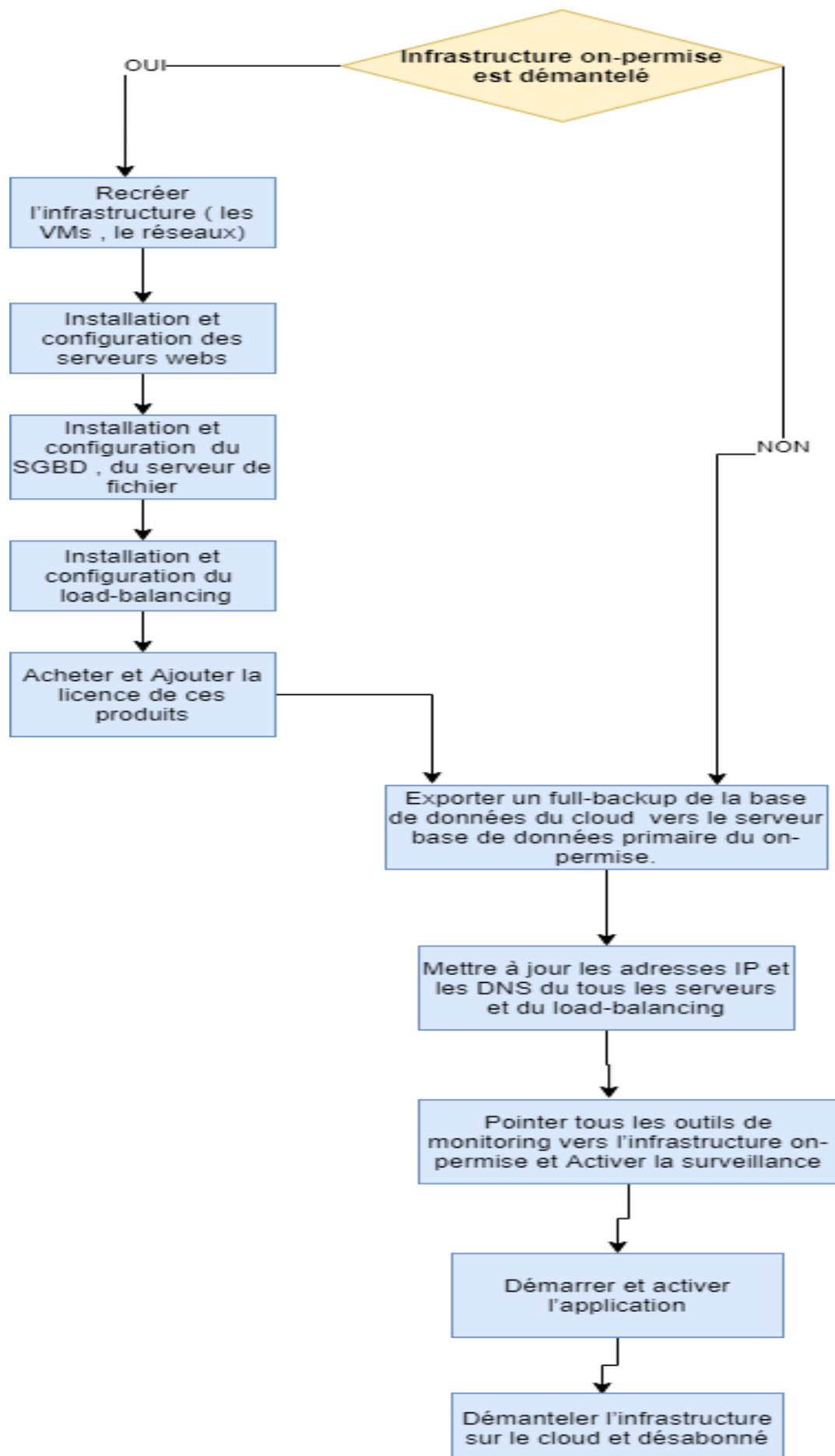
2-\ Procédure de retour en arrière

L'infrastructure on-permise n'est pas démantelé :

- 1-\ Prendre un full-backup de la base de données du cloud et l'importer dans le serveur base de données primaire du on-permise.
- 2-\ mettre à jour les adresses IP et les DNS de tous les serveurs et du load-balancing
- 3-\ Pointer tous les outils de monitoring vers l'infrastructure on-permise et Activer la surveillance
- 4-\ Démarrer et activer l'application.
- 5-\ Démanteler l'infrastructure sur le cloud et désabonné

L'infrastructure on-permise est démantelé :

- 1-\ Recréer l'infrastructure (les VMs , le réseaux)
- 2-\ Installation et configuration des serveurs webs , du SGBD , du serveur de fichier, du load-balancing
- 3-\ Acheter les licences de ces produits
- 4-\ Prendre un full-backup de la base de données du cloud et l'importer dans le serveur base de données primaire du on-permise.
- 5-\ mettre à jour les adresses IP et les DNS de tous les serveurs et du load-balancing
- 6-\ Pointer tous les outils de monitoring vers l'infrastructure on-permise et Activer la surveillance
- 7-\ Démarrer et activer l'application.
- 8-\ Démanteler l'infrastructure sur le cloud et désabonné



V-\ Mise à jour des systèmes dans le cloud

Les mises à jour des systèmes d'exploitation offrent de nombreux avantages. Tout est question de révisions. Celles-ci peuvent inclure la réparation des failles de sécurité découvertes et la correction ou la suppression de bogues informatiques. Les mises à jour peuvent ajouter de nouvelles fonctionnalités à vos appareils et supprimer celles qui sont obsolètes, aussi améliorer les fonctionnalités et optimiser le fonctionnement ou les performances.

Par défaut, l'équilibreur de charge ELB achemine les demandes de manière uniforme vers ses zones de disponibilité. Lorsque on veut faire la Mise à jour des instances, on peut suivre les étapes suivantes :

1. Enlever temporairement une zone de disponibilité de l'équilibreur de charge exemple zone A
2. Appliquer les mises à jour sur les instances et les redémarrer ou redémarrer le service en question.
3. Ajouter cette zone de disponibilité (zone A) à l'équilibre de charge.
4. Enlever temporairement une zone de disponibilité de l'équilibreur de charge exemple zone B
5. Appliquer les mises à jour sur les instances et les redémarrer ou redémarrer le service en question.
6. Ajouter cette zone de disponibilité (zone B) à l'équilibre de charge.
7. Refaire les mêmes étapes s'il y a d'autres zone de disponibilité à mettre à jours ces instances.

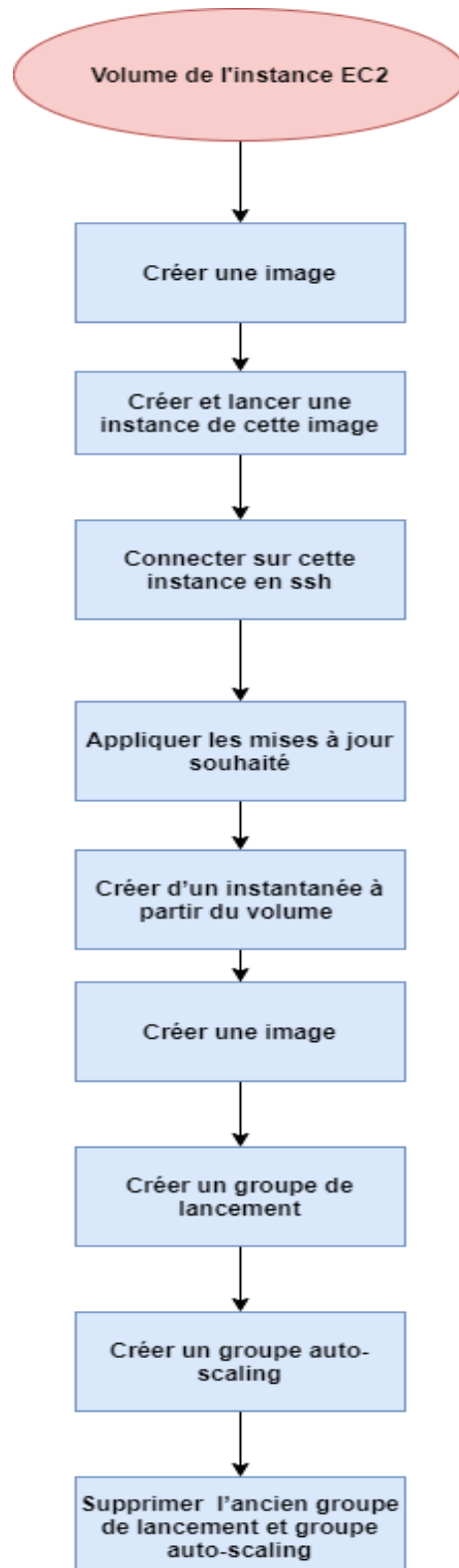
Remarque :

Lorsque on retire une zone de disponibilité du ELB, l'équilibreur de charge arrête d'acheminer les demandes vers les instances enregistrées dans cette zone de disponibilité mais continue de les acheminer vers les instances enregistrées des autres zones de disponibilité.

Démarche pour faire la mise à jour d'une instance EC2 :

1. A partir du volume créer un instantanée (snapshot)
2. A partir de cette instantanée créer une image
3. A partir de cette image créer et lancer une instance
4. Connecter sur cette instance, appliquer les mises à jour souhaité
5. Création d'un nouveau instantanée à partir du volume de la nouvelle instance et création de la nouvelle image

6. Création d'un groupe de lancement à partir de cette nouvelle image en choisissant les spécifications désirées (type d'instance, groupe de sécurité,..)
7. Création d'un groupe auto-scaling à partir ce groupe de lancement (réseau, stratégie de dimensionnement...)
8. Suppression de l'ancien groupe de lancement et groupe auto-scaling



webography

<https://azure.microsoft.com/fr-fr/overview/cloud-migration-benefits-challenges/#benefits>

<https://www.napsis.fr/actualite/cloud-on-premise/>

<https://www.connectria.com/blog/kpi-for-your-cloud-migration/>

<https://blog.atempo.com/fr/blog/les-raisons-qui-poussent-les-entreprises-%C3%A0-quitter-le-cloud>

https://docs.aws.amazon.com/fr_fr/elasticloadbalancing/latest/classic/enable-disable-az.html

https://docs.aws.amazon.com/fr_fr/prescriptive-guidance/latest/backup-recovery/ec2-backup.html