



Migration de F5 BIG-IP vers F5 BIG-IP VE sur le cloud AWS

AWS Conseils prescriptifs



AWS Conseils prescriptifs: Migration de F5 BIG-IP vers F5 BIG-IP VE sur le cloud AWS

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d'Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n'est pas d'Amazon, d'une manière susceptible de créer une confusion parmi les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Introduction	1
Résultats commerciaux ciblés	2
Évaluation des coûts et des compétences liés à la migration	3
Évaluation des coûts de licence et d'instance	3
Évaluation AWS et base de connaissances F5	4
Cartographie des applications et conception de l'architecture	6
Cartographie des applications	6
Planification de l'architecture	11
Planification de la migration	14
Décider des éléments à migrer	14
Détartrage de vos configurations	15
Choix du type d'instance	17
Principaux points de décision	18
Vue d'ensemble de la migration	19
Migration des données	22
Migration d'une configuration complète	22
Migration d'une configuration partielle	24
Déploiements haute densité sans Elastic IPs	25
Interconnecter votre VPCs	26
Connexion à votre AWS infrastructure	30
Ressources	33
Historique du document	34
Glossaire	35
#	35
A	36
B	39
C	41
D	44
E	48
F	51
G	53
H	54
I	56
L	58

M	59
O	64
P	66
Q	69
R	70
S	73
T	77
U	78
V	79
W	79
Z	81
.....	lxxxii

Migration de F5 BIG-IP vers F5 BIG-IP VE sur le cloud AWS

Suresh Veragoni, Amazon Web Services (AWS)

Novembre 2020 ([historique du document](#))

Ce guide fournit une vue d'ensemble des étapes, de l'architecture, des outils et des considérations relatifs à la migration des solutions de sécurité et de gestion du trafic F5 BIG-IP vers le cloud Amazon Web Services (AWS). AWS [F5 BIG-IP](#) est une collection de produits conçus autour de solutions de disponibilité, de contrôle d'accès et de sécurité. Ils fonctionnent sur le [système d'exploitation de gestion du trafic \(TMOS\) F5](#).

Vos solutions de sécurité et de gestion du trafic F5 BIG-IP sont migrées vers le AWS cloud en utilisant les stratégies de migration de [réhébergement et de replateforme issues des sept stratégies de migration](#) courantes (7 R). La charge de travail F5 sera migrée en réhébergeant un environnement existant et en utilisant certains aspects de la replateforme, tels que la découverte de services et les intégrations d'API.

Ce guide décrit les quatre principales étapes de votre migration.

- [Évaluation des coûts et des compétences liés à la migration](#)— comprendre les coûts de la migration et les connaissances requises en matière de AWS produits et services F5.
- [Cartographie des applications et conception de l'architecture](#)— évaluez la façon dont vos applications s'intègrent et concevez l'architecture de leur futur environnement.
- [Planification de la migration](#)— utilisez un plan de haut niveau pour votre migration et prenez les décisions clés concernant les éléments à migrer.
- [Migration des données](#)— déployez les configurations disponibles pour la migration des charges de travail F5 BIG-IP vers le AWS Cloud et migrez vos données.

Pour un aperçu complet des étapes de migration, consultez le modèle [Migrer une charge de travail F5 BIG-IP vers F5 BIG-IP VE sur le AWS cloud sur le site Web du guide prescriptif](#). AWS

Ce guide est destiné aux équipes d'ingénierie technique et d'architecture qui migrent les solutions de sécurité et de gestion du trafic F5 vers le AWS cloud.

Résultats commerciaux ciblés

Organisations choisissent de migrer vers le AWS cloud pour accroître leur agilité et leur résilience. Cette migration présente des avantages importants mais comporte également des risques qu'il convient de réduire. Plus précisément, le risque et la complexité liés à l'adoption du cloud augmentent lorsque des services applicatifs importants, tels que la gestion du trafic ou la sécurité, sont divisés.

Si vous migrez les charges de travail F5 BIG-IP vers le AWS cloud, vous pouvez vous concentrer sur l'agilité et adopter des modèles opérationnels à forte valeur ajoutée dans l'ensemble de votre architecture d'entreprise. Vous créez également un avantage net pour votre adoption du cloud, car vos environnements technologiques peuvent être fédérés.

Vous pouvez également créer un avantage commercial en limitant la multiplication des fournisseurs ou des outils. Cela réduit les risques lorsque vous migrez une application, car cela limite ou supprime les modifications apportées au chemin de données, aux fonctionnalités, aux outils et au modèle opérationnel de votre environnement source.

Évaluation des coûts et des compétences liés à la migration

Avant de décider de migrer vos solutions de sécurité et de gestion du trafic F5 BIG-IP vers le AWS cloud, vous devez évaluer les coûts de la migration et évaluer les compétences requises.

Les sections suivantes fournissent un résumé des coûts de migration potentiels, ainsi qu'un aperçu des connaissances relatives aux produits AWS et services F5 dont votre équipe aura besoin.

Rubriques

- [Évaluation des coûts de licence et d'instance](#)
- [Évaluation AWS et base de connaissances F5](#)

Évaluation des coûts de licence et d'instance

Le coût d'exécution des charges de travail F5 BIG-IP dans le AWS cloud varie en fonction de vos coûts combinés de licence et d'instance. Lorsque vous migrez vers le AWS cloud, vous devez faire correspondre vos licences existantes et activer les fonctionnalités de votre système source vers le système de destination.

Les produits F5 ont plusieurs modèles de licence, mais vos exigences commerciales et techniques se recoupent généralement avec les modèles suivants : Bring Your Own License (BYOL), place de marché, offre privée, abonnement et contrats de licence d'entreprise (ELA).

Le coût de migration variera également selon que vous utilisez des instances pay-as-you-go payantes annuellement ou que vous avez conclu un accord individuel avec celles-ci AWS. Il est important de noter que le coût d'une licence F5 peut également changer en fonction du modèle et de vos besoins individuels.

Vous pouvez utiliser le [calculateur de AWS prix](#) pour estimer vos coûts de fonctionnement potentiels. Les trois exemples suivants donnent un aperçu des coûts des AWS instances et de l'infrastructure.

- [F5 BIG-IP petit — 100 Mbits/s](#)
- [F5 BIG-IP moyen — 200 Mbits/s](#)
- [F5 BIG-IP large — 800 Mbits/s](#)

Évaluation AWS et base de connaissances F5

Avant de commencer à migrer votre charge de travail F5 BIG-IP, vous devez vous assurer que votre équipe connaît les produits et services suivants AWS ainsi que les produits et services F5.

AWS produits et services

- [CloudFormation](#) vous aide à créer et à provisionner des déploiements AWS d'infrastructure de manière prévisible et répétée.
- [Amazon CloudWatch](#) fournit une solution de surveillance fiable, évolutive et flexible que vous pouvez commencer à utiliser en quelques minutes.
- [Amazon Elastic Compute Cloud \(Amazon EC2\)](#) est un service Web qui fournit une capacité de calcul redimensionnable pour vous permettre de créer et d'héberger vos systèmes logiciels.
- [Gestion des identités et des accès AWS \(IAM\)](#) est un service Web permettant de contrôler de manière sécurisée l'accès aux AWS services.
- [AWS Landing Zone](#) est une solution qui aide les clients à configurer rapidement un AWS environnement multi-comptes sécurisé basé sur les AWS meilleures pratiques.
- [Amazon Simple Storage Service \(Amazon S3\)](#) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- [AWS Security Token Service \(AWS STS\)](#) vous permet de demander des informations d'identification temporaires à privilèges limités pour les utilisateurs.
- [AWS Transit Gateway](#) est un service hautement disponible et évolutif destiné à consolider la configuration de routage Amazon VPC pour Région AWS une hub-and-spoke architecture.
- [Amazon Virtual Private Cloud \(Amazon VPC\)](#) vous aide à lancer AWS des ressources dans un réseau virtuel que vous avez défini.

Important

Votre équipe doit comprendre les différentes manières de connecter un ou plusieurs clouds privés virtuels (VPCs) aux centres de données existants, ainsi que la manière de créer des ressources dans votre AWS infrastructure. Pour plus d'informations à ce sujet, consultez les [options de connectivité Network-to-Amazon VPC](#) dans la documentation Amazon VPC.

Produits et services F5

- Le [système d'exploitation de gestion du trafic \(F5 TMOS\)](#) est la base logicielle de tous les produits de réseau ou de trafic de F5.
- [Le gestionnaire de trafic local \(F5 LTM\)](#) vous aide à contrôler le trafic réseau en sélectionnant la bonne destination en fonction des performances, de la sécurité et de la disponibilité du serveur.
- Global Traffic Manager (F5 GTM) distribue les requêtes DNS et d'applications utilisateur en fonction des politiques de l'entreprise, des conditions de service du centre de données et du cloud, de l'emplacement des utilisateurs et des performances des applications.
- [Access Policy Manager \(F5 APM\)](#) sécurise, simplifie et centralise l'accès aux applications et aux données APIs, où que se trouvent les utilisateurs et leurs applications.
- [Application Security Manager \(F5 ASM\)](#) est un pare-feu d'applications Web flexible qui sécurise les applications Web dans les environnements de cloud traditionnels, virtuels et privés.
- [Advanced Firewall Manager \(F5 AFM\)](#) atténue les menaces réseau avant qu'elles ne perturbent les ressources critiques du centre de données.
- [Le F5 BIG-IQ](#) fournit un point de contrôle central pour les appareils physiques et virtuels F5, ainsi que pour les solutions qui s'exécutent sur ceux-ci.

Cartographie des applications et conception de l'architecture

Les sections suivantes vous aident à comprendre comment vos applications s'intègrent dans leur environnement existant et comment concevoir leur nouvelle architecture.

Rubriques

- [Cartographie des applications](#)
- [Planification de l'architecture](#)

Cartographie des applications

Il n'existe pas d'approche standard lorsque vous migrez des applications et leurs dépendances associées vers le AWS Cloud. Le tableau suivant fournit un aperçu des principales considérations relatives aux différentes applications couramment migrées vers le cloud avec des charges de travail F5 BIG-IP. AWS

Type de demande	Cas d'utilisation	Action suggérée
Applications personnalisées ou commerciales off-the-shelf (COT)	<p>Vous envisagez soit de fermer un centre de données ou une instance de colocation après avoir migré des applications vers le AWS cloud, soit d'exécuter une combinaison de AWS produits ou de services sur site. Vous n'avez pas l'intention de moderniser ces applications.</p> <p>Vous avez peut-être intégré le contrôleur de livraison d'applications (ADC) F5 dans le cadre de la logique de l'application et vous avez exigé qu'il porte la même logique vers le AWS cloud.</p>	<p>Passez en revue les configurations F5 actuelles et répartissez-les en composants d'application qui doivent être migrés.</p> <p>Assurez-vous de correspondre au modèle de licence utilisé, que ce soit par le biais des modules ou du programme F5 Good, Better, Best (GBB).</p>

Type de demande	Cas d'utilisation	Action suggérée
	Les composants de l'application peuvent ou non être migrés en même temps.	
Applications soumises à des exigences de conformité ou de sécurité élevées	<p>Bien que ces applications puissent être réhébergées, replateformées ou réarchitecturées, elles nécessiteront des protections avancées.</p> <p>Ces protections avancées peuvent inclure la protection comportementale, la sécurité des applications mobiles, la détection avancée des bots, l'intelligence IP approfondie et le filtrage des données de réponse en sortie.</p>	<p>Si vous utilisez déjà F5 ASM, assurez-vous de migrer la politique de sécurité ou de conformité.</p> <p>S'il s'agit d'une nouvelle application, vous devez évaluer le meilleur moyen de tirer parti de F5 ASM ou F5 Web Application Firewall (F5 WAF).</p>
Applications de nouvelle génération ou natives du cloud hébergées sur Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS) ou Amazon EC2 hébergeant K8S	Ces applications nécessitent un réglage des protocoles, tels que les réseaux mobiles ou autres types de réseaux présentant des pertes, des optimisations HTTP, des plans de données programmables (iRules) ou des services avancés qui alignent les algorithmes d'équilibrage de charge.	Pour l'entrée de conteneurs, voir F5 Container Ingress Services dans la documentation F5.

Type de demande	Cas d'utilisation	Action suggérée
Espace de noms fédéré ou applications hybrides	<p>Il s'agit d'applications dans lesquelles la fourniture du niveau de présentation est fédérée dans le cadre d'un déploiement hybride, ou dans lesquelles les services consommés sont fournis dans le cadre d'un déploiement hybride.</p> <p>Par exemple, vous pouvez utiliser F5 GTM avec F5 LTM sur site et avoir tiré parti des fonctionnalités avancées de F5 GTM pour cartographier des dépendances complexes et une logique avancée quant à l'emplacement vers lequel envoyer les clients.</p>	<p>Ce déploiement doit comporter au moins deux systèmes DNS F5 ou F5 Distributed Cloud DNS.</p> <p>Le déploiement nécessitera la création d'un ou de plusieurs VPCs dans le AWS Cloud.</p> <p>Un VPC devra être mappé dans le système en tant que centre de données. Cela peut être plusieurs VPCs si vous utilisez une conception de VPC de transit.</p>

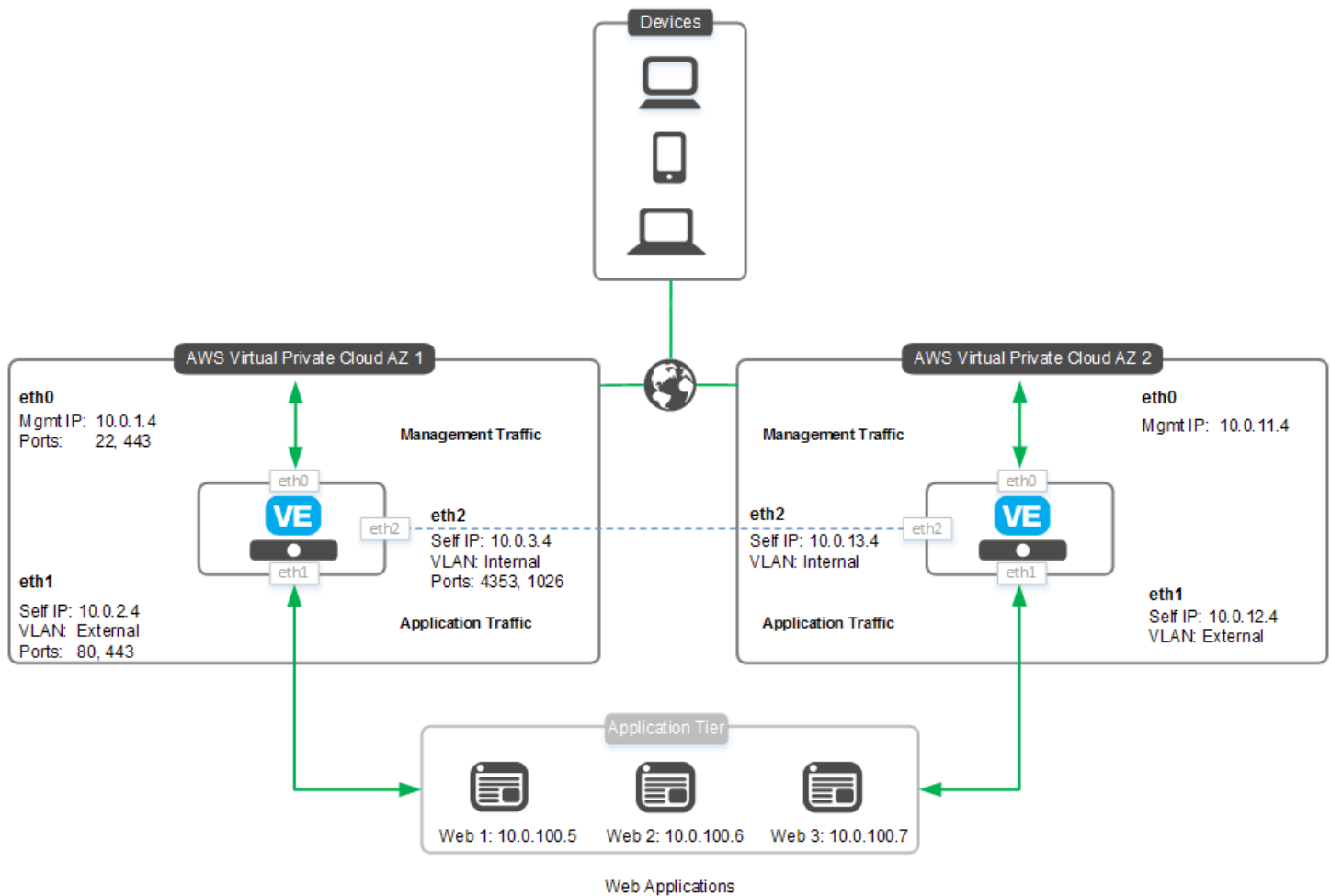
Type de demande	Cas d'utilisation	Action suggérée
Applications optimisées pour les performances	Applications susceptibles d'avoir des profils hautement optimisés au niveau de la session (L4) et des couches applicatives (L7), applications mobiles ou lorsque vous êtes concerné par une latence accrue, des optimisations HTTP (SPDY) et une compression en raison de la migration vers et depuis le cloud. AWS	<p>Cela nécessite le déploiement du système F5 LTM exécutant des serveurs virtuels de type standard (proxy TTCP complet) ou supérieur (proxy d'application tel que HTTP), avec un faible trafic symétrique entre les serveurs d'applications et les clients.</p> <p>Le trafic peut être traité par une traduction d'adresse réseau source (SNAT), ou les instances F5 BIG-IP peuvent être la passerelle par défaut pour l'instance et la table de routage.</p>
Application interne sur plusieurs zones de disponibilité, haute disponibilité (HA) mais pas de DNS	Vous devez déployer une application et souhaitez prendre en charge le cross-zone pour une disponibilité accrue, mais vous ne souhaitez pas utiliser le DNS et vous ne pouvez pas modifier l'adresse IP.	Vous devrez utiliser des passerelles client dans le VPC reliées à une passerelle privée virtuelle pour annoncer l'espace d'adressage étranger, ainsi que le modèle F5 Advanced HA iApp pour manipuler la table de routage. Les systèmes F5 peuvent être les passerelles client dans le VPC ou une solution tierce peut être la passerelle client.

Type de demande	Cas d'utilisation	Action suggérée
WAF ou applications IDS/IPS	Ces applications nécessitent des fonctionnalités de sécurité avancées telles que des signatures SNORT, des protections contre les robots, des ensembles de règles WAF approfondis et complexes (plus de 2 900 signatures) et l'intégration d'un scanner de sécurité.	Choisissez un CloudFormation modèle de topologie qui répond aux besoins de l'application (haute disponibilité AWS Auto Scaling , autonomie), puis créez et validez la politique de sécurité appropriée.
La sécurité et les services transitent par les applications VPC	<p>Il s'agit d'une variante d'un VPC de transit dans lequel vous centralisez la sécurité et les services pour Internet ou l'intranet, et vous les associez à d'autres VPCs</p> <p>Cette topologie peut être utilisée avec les autres types d'applications et listes de cas d'utilisation. Il est utilisé pour réduire la surface d'attaque Internet de la structure VPC d'une entreprise, centraliser les contrôles et séparer les tâches. Il est également utilisé pour insérer des applications avancées et des services de sécurité entre un VPC spécifique, un autre VPCs VPC et Internet.</p>	Déployez un VPC de transit avec les exigences de visibilité de l'adresse IP du VPC homologue (application).

Type de demande	Cas d'utilisation	Action suggérée
Sécurité du DNS, applications express et hybrides	Répliquez des tables de recherche DNS sécurisées et cohérentes dans le AWS cloud et dans le centre de données avec la capacité de gérer de gros volumes de requêtes DNS ; de survivre à une interruption de connexion directe via Direct Connect ; un DNS géré de manière centralisée et basé sur des règles dans l'ensemble de l'environnement ; la mise en cache DNS et la validation et la sécurité du protocole DNS (DNSSEC).	Utilisez les meilleures pratiques pour déployer le DNS et traiter chaque VPC comme un centre de données virtuel.

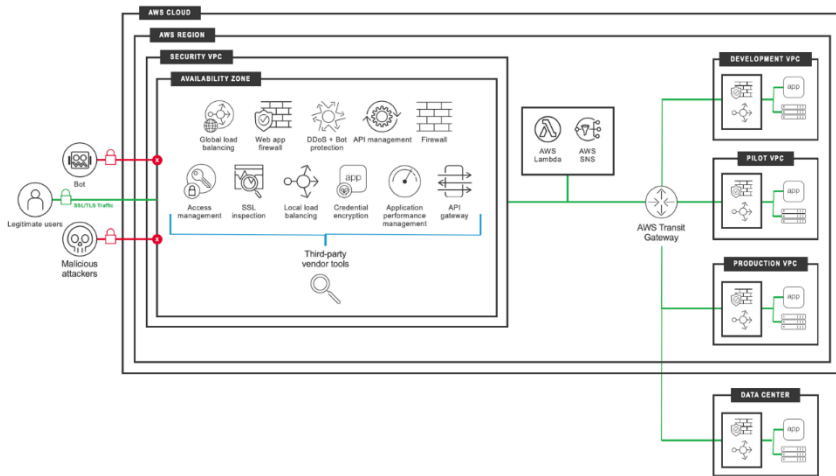
Planification de l'architecture

Le schéma suivant montre l'architecture de base du VPC Edge et de l'application VPCs connectés par AWS Transit Gateway. Ils VPCs peuvent faire partie du même compte ou de comptes différents.



Par exemple, une zone d'atterrissage déploie généralement un compte réseau qui contrôlera la périphérie VPCs. Cette architecture permet aux utilisateurs de tirer parti des politiques, des processus et des plateformes communs à l'ensemble de la suite d'applications.

Le schéma suivant montre deux instances d'interface réseau (NIC) issues d'une charge de travail BIG-IP F5 déployée dans un cluster de secours actif. Vous pouvez ajouter des interfaces réseau plus élastiques à ces systèmes, dans la limite du nombre d'instances. F5 vous recommande d'utiliser un modèle multi-AZ pour votre déploiement afin d'éviter toute défaillance de la zone de disponibilité.



Planification de la migration

La planification de votre processus de migration est essentielle pour garantir une migration fluide et réussie. Les sections suivantes décrivent comment planifier votre migration, ainsi que les principales considérations à prendre en compte à cet égard.

Rubriques

- [Décider des éléments à migrer](#)
- [Détartrage de vos configurations](#)
- [Choix du type d'instance](#)
- [Principaux points de décision](#)
- [Vue d'ensemble de la migration](#)

Décider des éléments à migrer

Lorsque vous migrez, vous devez décider quelles charges de travail sont essentielles, quelles charges de travail sont « agréables à avoir » mais pas essentielles, et quelles charges de travail ne sont pas nécessaires et peuvent être supprimées [une fois la migration terminée](#).

Une partie importante de votre processus décisionnel impliquera les exigences individuelles que vous avez en matière d'automatisation, d'API, d'outillage et d'autres processus. Vous devrez également tenir compte des exigences fonctionnelles et de performance de votre organisation.

Par exemple, vous avez peut-être utilisé des plateformes matérielles partagées dans un centre de données existant avec des partitions utilisateur. Toutefois, votre migration peut nécessiter que les services s'exécutent sur des systèmes qui ne sont pas aussi largement partagés en raison des limites de performances liées au passage de solutions accélérées par le matériel. Par exemple, les transactions SSL (Secure Sockets Layer) par seconde (TPS) peuvent nécessiter qu'un certain service ne s'exécute pas sur un système partagé.

Après avoir identifié et documenté les applications à migrer ainsi que leurs exigences, vous devez préparer vos systèmes sources en appliquant les meilleures pratiques suivantes.

- Exécutez la même version de F5 TMOS que celle que vous utiliserez dans le AWS cloud. [La version 14.1](#) ou ultérieure est recommandée, mais [la version 13.1](#) ou ultérieure peut également être

utilisée. Bien que vous puissiez migrer la version [12.1.x](#), vous pouvez rencontrer des problèmes de sécurité, d'automatisation et de maintenabilité.

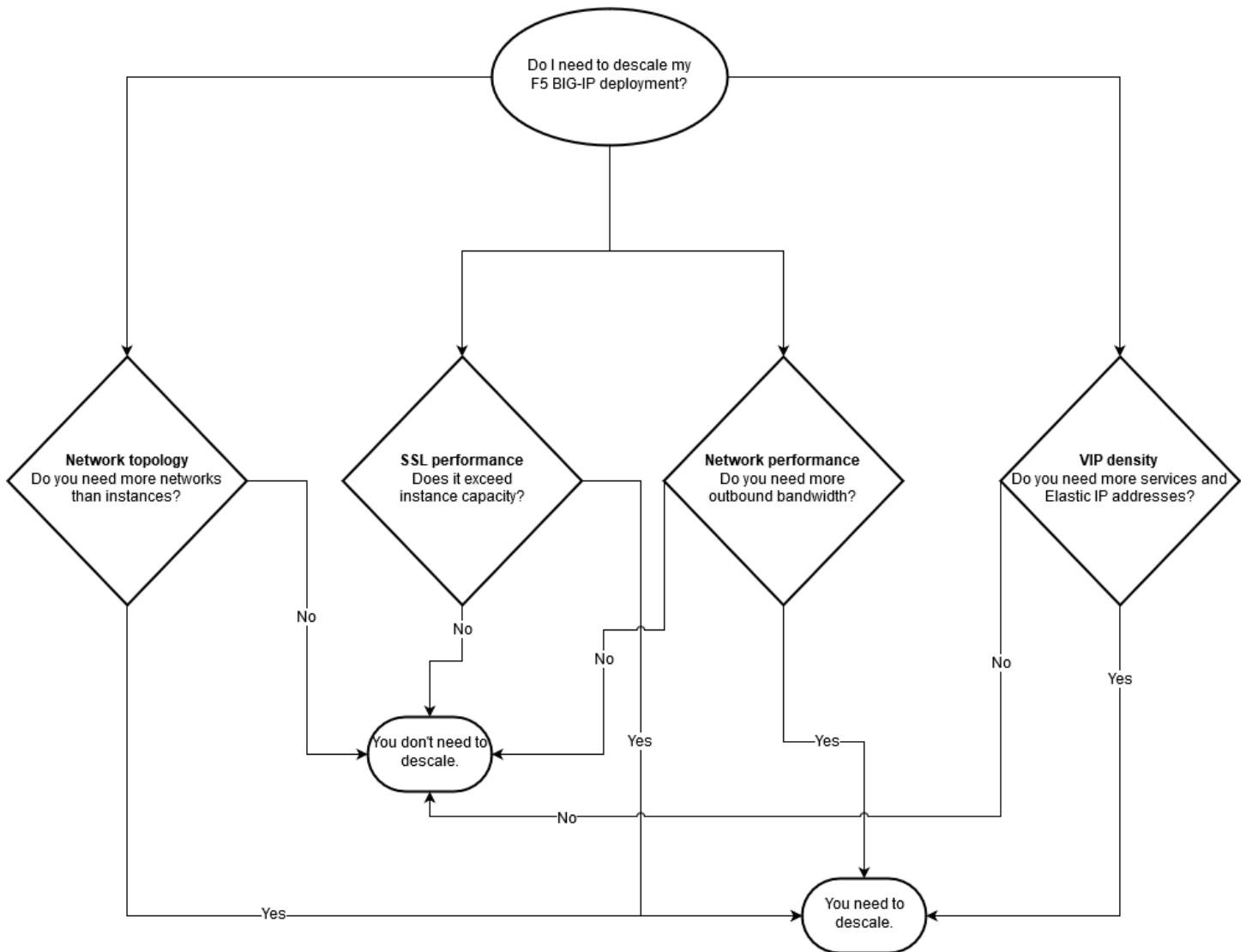
- Disposez de sauvegardes valides de toutes les configurations de chaque appareil. Étant donné que la sauvegarde du serveur d'entreprise Univention (UCS) contient des attributs et des objets spécifiques au centre de données (tels que des adresses IP, des nœuds ou des membres du pool), F5 vous recommande de créer un fichier de commandes shell (SCF) pour modifier et fusionner les configurations.
- Conservez des copies de sauvegarde de tous les certificats de sécurité pertinents et envisagez de passer du chiffrement RSA au chiffrement ECC pour de meilleures performances.
- Disposez de mesures de performance détaillées au niveau du serveur virtuel pour la mise à l'échelle et la planification des capacités.
- Optez pour une solution [F5 Global Server Load Balancing \(GSLB\)](#) pour le passage du centre de données au cloud. AWS
- Comprenez l'impact de la migration d'un modèle d'appliance matérielle vers un modèle logiciel et virtualisé en termes de performances, d'évolutivité et de haute disponibilité.
- Ayez défini les exigences relatives à ce qui sera migré vers le AWS cloud et tenez compte des considérations suivantes.
 - Sachez que toute migration vers le AWS cloud nécessite de décider si des configurations complètes ou partielles seront migrées. Généralement, un déplacement partiel à la fois est plus efficace.
 - Déterminez quels itinéraires et quelles adresses IP seront modifiés.
 - Identifiez les pools SNAT à remplacer par F5 SNAT Automap.

Vous devriez également envisager de consulter [AWS des partenaires](#) ou l'équipe des services professionnels de F5. Cela contribuera à garantir une forte probabilité de réussite de la migration.

Détartrage de vos configurations

Le « détartrage » signifie le déplacement d'une configuration F5 BIG-IP vers une configuration inférieure ou plus rentable, en fonction des fonctionnalités ou des mesures requises après vos premières découvertes. Vous devez évaluer soigneusement toutes ces options car elles auront un impact sur l'architecture et le nombre d'instances requises.

Le schéma suivant vous aide à évaluer si le détartrage est adapté à vos besoins et exigences.



La migration créera également de nouvelles considérations dans les domaines suivants.

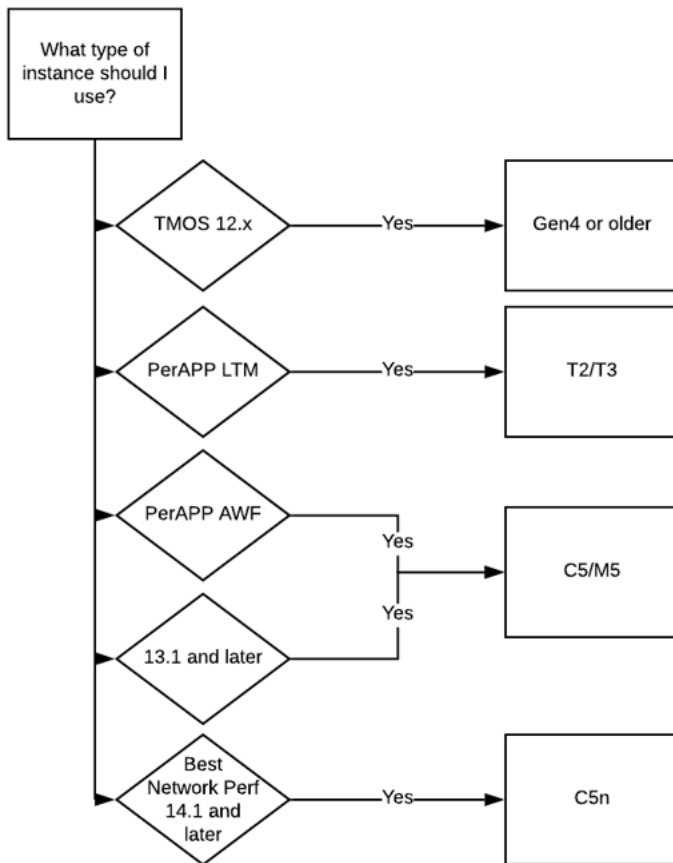
- Topologie réseau : actuellement VLANs, les 802.1q balises AWS ne sont pas prises en charge. Le nombre d'interfaces d'instance (moins une pour la gestion) limite le nombre de réseaux qu'une instance peut prendre en charge. Si vous avez besoin d'une topologie spécifique, vous devez l'évaluer par rapport aux différentes instances prises en charge par F5 dans le AWS Cloud.
- Performances SSL — Les appliances et les châssis F5 ont des performances SSL supérieures à ce qui peut être accompli avec x86. Vous devez évaluer les exigences SSL agrégées et par serveur virtuel.
- Performances du réseau : vous devez évaluer les caractéristiques agrégées, sortantes et internes du réseau. AWS les types d'instance présentent des caractéristiques de réseau différentes (faible, moyenne, élevée, jusqu'à X ou dédiée) qui doivent être prises en compte. Il existe également

des limites quant à la quantité de trafic qu'une instance peut envoyer en provenance ou via une connexion directe.

- Densité VIP — Si vous avez un plus grand nombre d'adresses IP virtuelles (VIPs), vous devez tenir compte de la limite d'instances au nombre d'adresses VIPs pouvant être mappées aux interfaces réseau.
- Connexion simultanée : le nombre maximum de connexions que les instances peuvent prendre en charge est limité.
- État de session : différentes applications utilisent différents types de persistance. Les applications dynamiques et apatrides modifieront les méthodes utilisées pour passer à l'état partagé, ce qui peut avoir un impact sur l'échelle des in/out opérations.

Choix du type d'instance

F5 prend en charge plusieurs types d'instances et le choix de l'instance à utiliser peut s'avérer une décision complexe. Pour la plupart des migrations, c5n.2x1 c5n.4x1 ce seront les choix d'instance les plus courants, car ils offrent une combinaison de performances réseau, de densité du processeur, de densité d'interface et du nombre de ces IPs éléments pouvant être pris en charge sur l'instance. Le schéma suivant fournit des exemples des instances à choisir, en fonction des produits F5 que vous utilisez.



Principaux points de décision

De nombreux aspects de la migration doivent être pris en compte, mais avant de commencer la migration de votre charge de travail F5 BIG-IP, posez-vous les questions suivantes pour clarifier le processus de migration.

Qui sont les utilisateurs de vos applications ?

Déterminez s'il s'agit d'utilisateurs internes (ne passant pas par une adresse IP élastique) ou externes (passant par une adresse IP élastique). Si les utilisateurs sont internes, déterminez si l'application peut utiliser le DNS pour faire face à la défaillance d'une zone de disponibilité ou à un déploiement actif. Vous devez également vérifier si vous devez utiliser un autre modèle de conception permettant à un sous-réseau de couvrir plusieurs zones de disponibilité.

Quelles parties de vos applications seront migrées vers le AWS cloud ?

Déterminez si l'ensemble de l'application est en cours de déplacement ou uniquement le niveau de présentation. Vous devez également prendre en compte les dépendances supplémentaires liées à la sécurité et à l'espace de noms DNS. Votre évaluation doit déterminer ce qui serait requis à partir de la topologie du réseau. En outre, déterminez les exigences d'un accord de niveau de service (SLA) en cas d'événement survenant au niveau de la zone de disponibilité, du VPC ou de la région. AWS

Pourquoi l'application migre-t-elle ?

Vous êtes peut-être en train de migrer votre application parce que vous fermez des centres de données ou parce que vous souhaitez plus d'élasticité. Déterminez si l'application est en train de migrer pour disposer d'une architecture par application, par rapport aux modèles monolithiques partagés courants dans de nombreux centres de données. Il convient également de réfléchir aux efforts de modernisation qui devraient être déployés parallèlement à la migration.

Où est effectuée la migration de l'application ?

Déterminez si l'application doit passer à un seul VPC avec une ou deux zones de disponibilité. Déterminez la topologie du VPC homologue ou de transit, ainsi que la nécessité de déploiements multirégionaux. Cela aura un impact sur la conception du modèle de migration.

Vue d'ensemble de la migration

Avant de commencer la migration, il est utile de définir l'ensemble du processus à partir d'un niveau élevé. Voici un exemple des étapes que vous pouvez suivre pour migrer une charge de travail F5 BIG-IP vers le cloud. AWS Vous trouverez des étapes et des processus plus détaillés pour une migration F5 BIG-IP dans le modèle [Migrer une charge de travail F5 BIG-IP vers F5 BIG-IP VE sur le cloud. AWS](#)

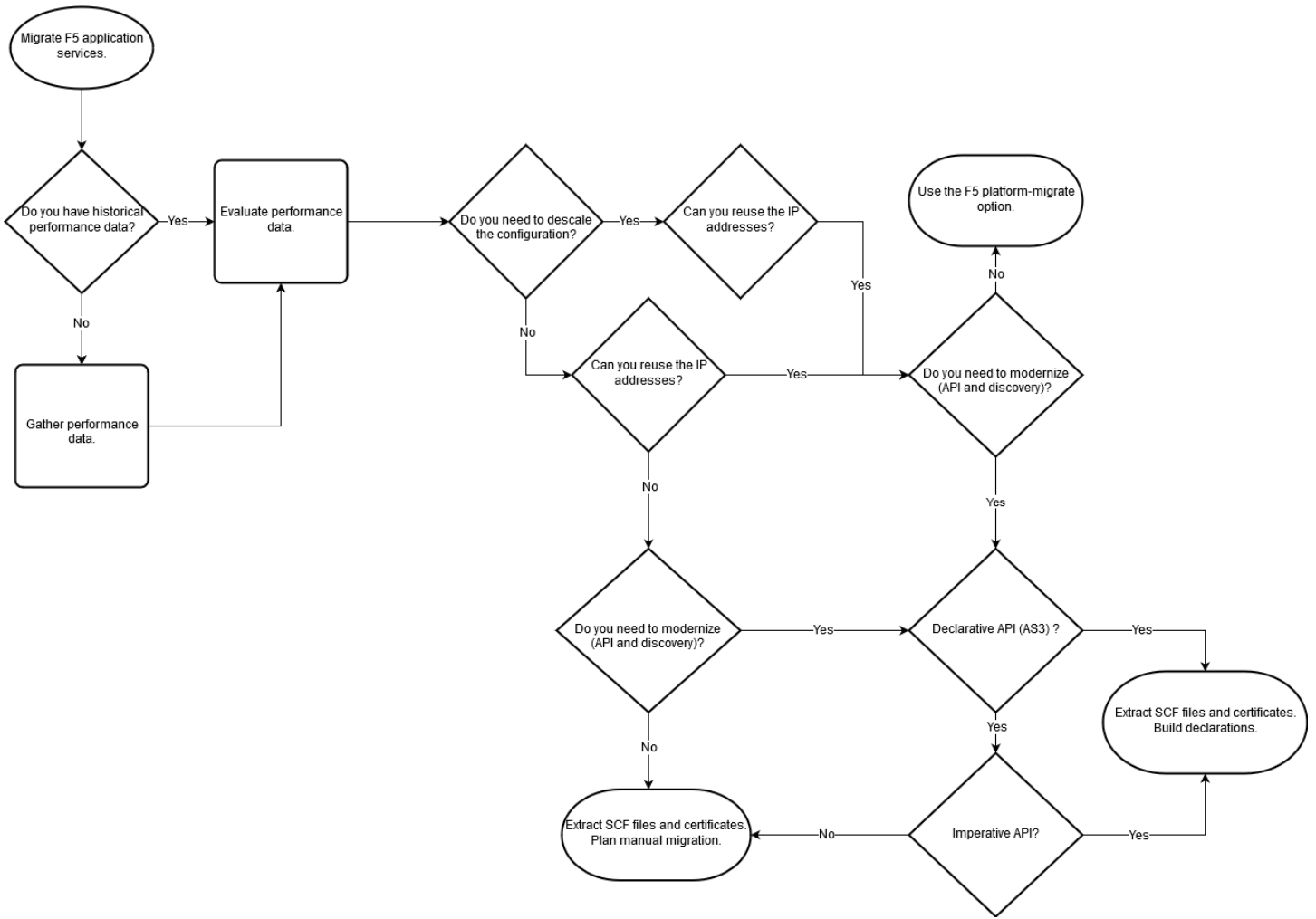
1. Déployez le nombre requis VPCs en fonction de vos besoins individuels. Cela peut être manuel ou automatisé via un outil tel que [AWS Landing Zone](#).
2. Évaluez les licences, les utilisations et les configurations F5 actuelles.
3. Évaluez les candidatures publiques et internes.
4. Évaluez les configurations F5 actuelles.
5. Évaluez les exigences en matière de taille et d'adresse IP, puis choisissez le nombre et le type de F5 et d' AWS instances requis.
6. Identifiez la stratégie de migration à déployer. Par exemple, levage et changement de vitesse ; levage, changement de vitesse et modernisation ; ou hybride.

7. Évaluez et identifiez la conception du DNS.
8. Évaluez comment le trafic sera dirigé vers l'application s'il existe à la fois sur site et dans le AWS cloud.
9. Effectuez les déploiements initiaux d'instances F5 à l'aide AWS CloudFormation de modèles.
10. Modifiez les déploiements pour répondre aux exigences topologiques grâce à des interfaces réseau élastiques et à des tables de routage supplémentaires.
11. Alignez les adresses IP élastiques sur celles de vous-même IPs ou de gestion IPs, et planifiez le mappage des adresses IP élastiques vers les adresses IP virtuelles (VIP).
12. Créez des adresses secondaires sur des interfaces réseau élastiques pour VIPs.
13. Appliquez des adresses secondaires dans le AWS cloud.
14. Mappez les adresses IP Elastic à l'adresse secondaire pour VIPs.
15. Extrayez les configurations et compilez une liste d'objets à déplacer.
16. Déployez les configurations sur F5 BIG-IP.
17. Mappez les adresses secondaires à VIPs.
18. Testez le trafic.
19. Testez le basculement.
20. Si vous créez un système hybride, assurez-vous d'intégrer le système dans F5 DNS.

⚠ Important

L'accès aux points de terminaison de AWS l'API est requis. Les adresses IP NAT ou Elastic sont également requises pour garantir une haute disponibilité au sein des zones de disponibilité ou entre celles-ci.

Le schéma suivant montre le flux de processus de haut niveau pour une migration F5 BIG-IP.



Migration des données

Toutes les migrations doivent itérer sur une configuration et créer l'arbre de dépendances. Lorsque vous utilisez un seul fichier de configuration, tout est fait pour vous. Si vous utilisez l'[API TMSH](#), vous devrez itérer et créer l'arbre de dépendances. Les sections suivantes décrivent les différentes options et configurations disponibles lors de la migration d'une charge de travail F5 BIG-IP.

Rubriques

- [Migration d'une configuration complète](#)
- [Migration d'une configuration partielle](#)
- [Déploiements haute densité sans Elastic IPs](#)
- [Interconnecter votre VPCs](#)
- [Connexion à votre AWS infrastructure](#)

Migration d'une configuration complète

Dans cette approche, vous prenez une configuration d'un système existant et vous la migrez vers un nouveau système. Ce processus copiera une configuration existante, des adresses IP, des certificats, des clés, des phrases de passe et des informations d'identification de connexion.

La principale raison de la migration d'une configuration complète est le remplacement d'un like-for-like système, tel qu'une mise à niveau matérielle ou un RMA. En général, ces concepts ne s'appliquent pas au AWS cloud.

Vous pouvez utiliser des fichiers UCS ou SCF pour migrer une configuration complète, et les tableaux suivants fournissent un aperçu des avantages et des inconvénients de leur utilisation.

Utiliser un fichier UCS ou qkview

Avantages	Inconvénients
Tous les fichiers sont déplacés sous forme d'archive unique.	Le principal cas d'utilisation d'un fichier UCS serait de remplacer un périphérique défaillant. L'archive contient des informations spécifiques

Avantages	Inconvénients
	<p>es au périphérique susceptibles de rendre la charge de travail F5 BIG-IP inaccessible.</p>
<p>Les comptes utilisateurs locaux sont préservés . S'ils sont intégrés à votre Active Directory, la configuration est préservée.</p>	<p>Si vous avez configuré une intégration d'annuaires, il se peut que vous rencontriez des problèmes d'accès. Si vous n'avez pas accès aux mots de passe des utilisateurs, vous pouvez également rencontrer des problèmes d'accès.</p>
<p>Toutes les configurations de serveurs virtuels sont préservées.</p>	<p>Vous devrez peut-être modifier les adresses IP de l'appareil, des serveurs virtuels et des membres du pool.</p>
<p>La structure du fichier est préservée.</p>	<p>Vous devez savoir quels fichiers modifier.</p> <p>Ce processus est plus complexe qu'un SCF ou un object-by-object déménagement.</p> <p>Risque d'erreur accru, notamment un redéploiement ou un échec du chargement de la configuration.</p> <p>Conçu pour les flux de travail de remplacement complets du système.</p>

Utiliser un fichier SCF

Avantages	Inconvénients
<p>Crée un fichier texte de la configuration.</p>	<p>Des modifications seront nécessaires car le fichier comporte des propriétés spécifiques au périphérique qui peuvent avoir un impact sur l'accès si le fichier est simplement chargé.</p>

Avantages	Inconvénients
Facilement modifiable dans n'importe quel éditeur de texte Unix ou Linux.	Vous devez comprendre la configuration et la structure du fichier pour effectuer les modifications.
Le fichier de configuration présente l'ordre correct des opérations de chargement.	
Vous pouvez facilement trouver les objets à migrer.	
	Vous devez savoir quelles parties du fichier supprimer pour éviter qu'elles ne remplacent les configurations spécifiques à l'appareil.

Migration d'une configuration partielle

Lorsque vous choisissez de migrer une configuration partielle, vous utiliserez un fichier TMSH ou SCF comme point de départ. Vous devrez également rechercher les objets que vous souhaitez déplacer et les compiler dans le bon ordre. Le tableau suivant décrit les avantages et les inconvénients de la migration d'une configuration partielle.

Avantages	Inconvénients
Les configurations peuvent être analysées et des corrections peuvent être apportées au fur et à mesure de l'avancement du travail.	La connaissance des objets F5 et des structures de fichiers est requise. Vous devez également être capable de lire iRules.
Les modifications de configuration peuvent être groupées.	
Résolution plus facile des problèmes de chargement de configuration.	La migration prend du temps.
Réduction du risque de blocage de l'accès à l'appareil.	
Il est plus facile de déplacer la configuration vers une topologie appropriée.	
	La modification des fichiers ou l'extraction des informations peuvent prendre beaucoup de temps.

Avantages	Inconvénients
Il est plus facile de traiter les partitions d'administrateur et de router les domaines car il s'agit d'un fichier plat.	
La structure de fichier plat permet d'utiliser les outils de texte Linux si vous souhaitez rechercher et remplacer des adresses IP par programmation.	

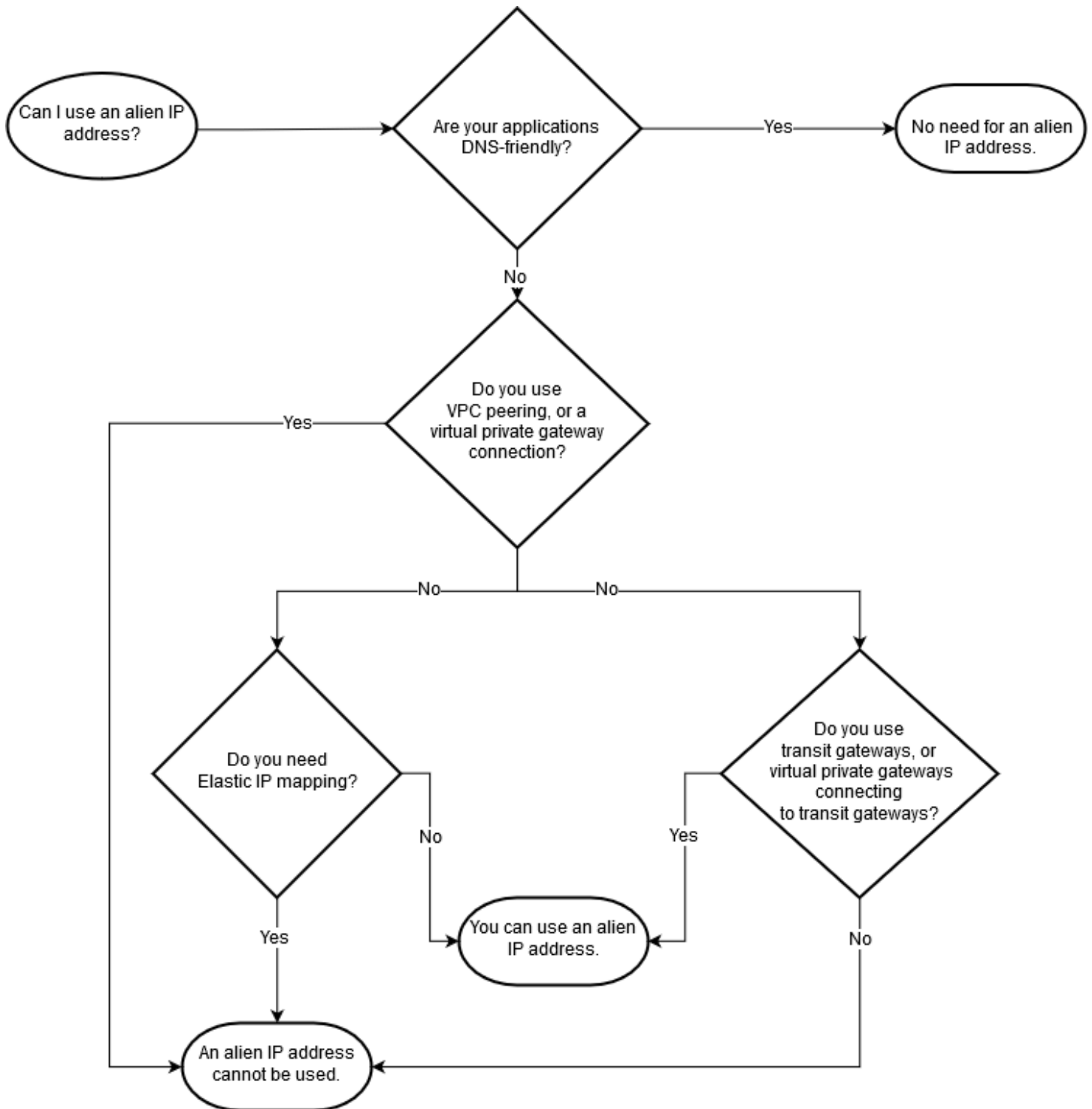
Déploiements haute densité sans Elastic IPs

Si vous avez besoin de déploiements très denses, vous pouvez utiliser les indicateurs de performance et ces applications ne nécessitent pas l'utilisation d'Elastic IPs. C'est ce que l'on appelle une « adresse IP étrangère ».

Une adresse IP étrangère est un réseau ou une plage de sous-réseaux externe au bloc CIDR du VPC et auquel F5 mappe des services virtuels. Les adresses IP étrangères ne fonctionnent pas dans tous les scénarios, mais peuvent être utilisées pour une densité élevée de serveurs virtuels. Avant de pouvoir utiliser une adresse IP étrangère, les ressources suivantes sont requises.

- Un sous-réseau pour héberger les applications
- Un déploiement F5 BIG-IP avec une extension Cloud Failover pour gérer les itinéraires
- Un itinéraire dans les tables de AWS routage pointant vers les interfaces réseau élastiques

L'utilisation d'adresses IP étrangères a des implications sur la façon dont vous vous interconnectez VPCs aux autres VPCs, ainsi que sur la manière dont vous pouvez vous interconnecter VPCs à vos centres de données. Le schéma suivant permet de déterminer si une adresse IP étrangère est requise.



Interconnecter votre VPCs

Les tableaux suivants présentent les principales considérations à prendre en compte lors de l'interconnexion de votre VPCs.

VPC de sécurité avec peering VPC		VPC de sécurité avec Transit Gateway AWS		VPC de sécurité avec interconnexion VPN	
Avantages	Désavantages	Avantages	Inconvénients	Avantages	Inconvénients
<ul style="list-style-type: none"> • Facile et rapide à configurer • Routage simple • Redondance élevée • Bande passante élevée 	<ul style="list-style-type: none"> • Prend uniquement en charge le trafic provenant des plages CIDR attribuées par VPC • Impossible d'insérer une inspection de sécurité entre VPCs • Complexes à gérer à grande échelle (tous les sont point-to-point) 	<ul style="list-style-type: none"> • Facile à configurer • Routage flexible sans SNAT • Redondance élevée • Bande passante élevée • Facile à gérer à grande échelle 	<ul style="list-style-type: none"> • Le routage est plus complexe (tables de routage VPC et tables de routage AWS Transit Gateway) • Topologie complexe pour insérer une inspection de sécurité entre VPCs 	<ul style="list-style-type: none"> • Routage flexible sans SNAT • Insertion facile de l'inspection de sécurité entre VPCs 	<ul style="list-style-type: none"> • Faible bande passante • Basculement complexe dépendant du fournisseur • Complexes à gérer à grande échelle (tous les sont point-to-point)

Client (envoi le SYN)	AWS Transit Gateway	Appariage de VPC	VPN entre VPCs	Vue d'ensemble de la solution et problèmes éventuels
Internet ou Direct Connect	N/A	N/A	N/A	Le trafic traverse une passerelle Internet, ou passerelle virtuelle. Il n'est pas

Client (envoi le SYN)	AWS Transit Gateway	Appairage de VPC	VPN entre VPCs	Vue d'ensemble de la solution et problèmes éventuels
pour assurer le service dans un VPC unique doté d'un sous-réseau public ou privé.				nécessaire de dépasser la limite du VPC. Le VPC agit comme un réseau stub conçu. Le trafic entre sur site et le AWS cloud (Direct Connect VPN).
Internet ou Direct Connect dans un VPC avec des clients dans un autre VPC VPCs (par exemple, des membres du pool dans un autre VPC), pas de SNAT.	Oui	Non	Oui	<p>AWS Transit Gateway ou VPNs autorisez le trafic à contourner le filtre d'appairage VPC que seul un VPC assigné peut passer. CIDRs</p> <p>Les solutions VPN seront limitées. Pas de routage multichemin à coût égal (ECMP) (un seul itinéraire) et pas de bande passante (environ 1,2 Go de seconde par tunnel, en général un seul tunnel).</p>
Internet ou Direct Connect vers un service dans un VPC avec des clients dans un autre VPC VPCs (par exemple, des membres du pool dans un autre VPC), avec SNAT.	Oui (mais pas obligatoire)	Oui	Oui (mais pas obligatoire)	<p>Étant donné que l'interconnexion entre le VPCs trafic Sees provenant du VPC est attribuée CIDRs, n'importe laquelle fonctionnera.</p> <p>Les solutions VPN seront limitées. Pas d'ECMP (une seule route) et pas de bande passante (environ 1,2 Go de seconde par tunnel, en général un seul tunnel).</p>
À l'intérieur du VPC pour le service dans le même VPC.	N/A	N/A	N/A	Tout le trafic est limité à un seul VPC. L'interconnexion n'est pas requise.

Client (envoi le SYN)	AWS Transit Gateway	Appairage de VPC	VPN entre VPCs	Vue d'ensemble de la solution et problèmes éventuels
À l'intérieur d'un VPC vers un VPC de service. Le service se trouve dans le VPC CIDR de destination.	Oui (mais pas obligatoire)	Oui	Oui (mais pas obligatoire)	Étant donné que l'interconnexion entre le VPCs trafic Sees provenant du VPC est attribuée CIDRs, n'importe laquelle fonctionnera.
À l'intérieur d'un VPC vers un VPC de service. Le service se situe en dehors de la gamme VPC CIDR.	Oui	Non	Oui	Étant donné que l'interconnexion entre le VPCs trafic Sees provenant du VPC est attribuée CIDRs, n'importe laquelle fonctionnera. Les solutions VPN seront limitées. Pas d'ECMP (une seule route) et pas de bande passante (environ 1,2 Go de seconde par tunnel, en général un seul tunnel).
À l'intérieur d'un seul VPC connecté à un service Internet.	N/A	N/A	N/A	Le trafic provient d'un CIDR attribué par VPC. Si les constructions Elastic IP, NAT ou de table de routage sont intégrées, le trafic circulera.
À l'intérieur d'un VPC vers un service Internet, routage sortant via un VPC de sécurité ou d'inspection.	Oui	Non	Oui	Étant donné que l'interconnexion entre le trafic SEE provenant de VPCs l'extérieur d'une plage CIDR attribuée par VPC, le peering VPC ne peut pas être utilisé. Les solutions VPN seront limitées. Pas d'ECMP (une seule route) et pas de bande passante (environ 1,2 Go de seconde par tunnel, en général un seul tunnel).

Connexion à votre AWS infrastructure

Le tableau suivant indique les principaux points à prendre en compte lorsque vous vous connectez à votre nouvelle AWS infrastructure lors d'une migration F5 BIG-IP.

Méthode de connectivité	Support du protocole de routage	Limites de bande passante	Adressage IP du terminal (public, privé ou les deux)	Support pour l'espace d'adresse extraterrestre	Support multi-VPC pour une seule connexion	Support multirégional
Internet	N/A	Vous créez un lien vers AWS, 5 Go de secondes par instance sortante	Public	Non	Oui	Oui
VPN - VPC	Statique, BGP	IPsec limites (environ 1,2 GB-seconde par tunnel)	Privé	Oui (vous devez configurer un IPsec tunnel supplémentaire entre le F5 BIG-IP du VPC et la passerelle virtuelle connectée au VPC).	Non	Non

Méthode de connectivité	Support du protocole de routage	Limites de bande passante	Adressage IP du terminal (public, privé ou les deux)	Support pour l'espace d'adresse extraterrestre	Support multi-VPC pour une seule connexion	Support multirégional
VPN et AWS Transit Gateway	Statique, BGP	IPsec limites (environ 1,2 GB-seconde par tunnel)	Privé	Oui	Oui	Non (si la passerelle de transit est prolongée, elle sera affectée)
AWS Direct Connect - VPC	Statique, BGP	Direct Connect limites (prend en charge le collage), instances individuelles limitées à 5 Go-secondes	les deux	Non	Non	Non

Méthode de connectivité	Support du protocole de routage	Limites de bande passante	Adressage IP du terminal (public, privé ou les deux)	Support pour l'espace d'adresse extraterrestre	Support multi-VPC pour une seule connexion	Support multirégional
Direct Connect - passerelle	Statique, BGP	Direct Connect limites (prend en charge le collage), instances individuelles limitées à 5 Go-secondes	les deux	Non	Oui	Oui
Direct Connect gateway - AWS Transit Gateway (limité à plusieurs AWS régions)	Statique, BGP	Direct Connect limites (prend en charge le collage), instances individuelles limitées à 5 Go-secondes	Confirmation verbale de l'équipe d'AWS architectes	Oui	Oui	Limité à plusieurs régions

Ressources

Documentation F5

- [Extension F5 Cloud Failover](#)
- [Streaming de télémétrie F5](#)
- [Laboratoire de topologie F5](#)
- [F5 Application Services on AWS : présentation \(vidéo\)](#)
- [Guide de l'utilisateur de l'extension F5 Application Services 3](#)
- [F5 Devcentral GitHub](#)
- [Wiki REST F5 iControl](#)
- [Vue d'ensemble F5 des fichiers de configuration uniques \(11.x - 15.x\)](#)
- [Livres blancs F5](#)
- [Présentation de l'option « platform-migrate » de l'archive UCS](#)
- [Centre de connaissances F5 BIG-IP Cloud Edition](#)

AWS resources

- [F5 sur Marketplace AWS](#)
- [F5 BIG-IP VE activé AWS : démarrage rapide](#)

AWS Partenaires

- [F5 activé AWS](#)

Guides et modèles connexes

- [Migrer une charge de travail F5 BIG-IP vers F5 BIG-IP VE sur le cloud AWS](#)

Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide. Pour être averti des mises à jour à venir, abonnez-vous à un [fil RSS](#).

Modification	Description	Date
Publication initiale	—	16 novembre 2020

AWS Glossaire des directives prescriptives

Les termes suivants sont couramment utilisés dans les stratégies, les guides et les modèles fournis par les directives AWS prescriptives. Pour suggérer des entrées, veuillez utiliser le lien [Faire un commentaire](#) à la fin du glossaire.

Nombres

7 R

Sept politiques de migration courantes pour transférer des applications vers le cloud. Ces politiques s'appuient sur les 5 R identifiés par Gartner en 2011 et sont les suivantes :

- **Refactorisation/réarchitecture** : transférez une application et modifiez son architecture en tirant pleinement parti des fonctionnalités natives cloud pour améliorer l'agilité, les performances et la capacité de mise à l'échelle. Cela implique généralement le transfert du système d'exploitation et de la base de données. Exemple : migrez votre base de données Oracle sur site vers l'édition compatible avec Amazon Aurora PostgreSQL.
- **Replateformer (déplacer et remodeler)** : transférez une application vers le cloud et introduisez un certain niveau d'optimisation pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle sur site vers Amazon Relational Database Service (Amazon RDS) pour Oracle dans le AWS Cloud
- **Racheter (rachat)** : optez pour un autre produit, généralement en passant d'une licence traditionnelle à un modèle SaaS. Exemple : migrez votre système de gestion de la relation client (CRM) vers Salesforce.com.
- **Réhéberger (lift and shift)** : transférez une application vers le cloud sans apporter de modifications pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle sur site vers Oracle sur une instance EC2 dans le AWS Cloud
- **Relocaliser (lift and shift au niveau de l'hyperviseur)** : transférez l'infrastructure vers le cloud sans acheter de nouveau matériel, réécrire des applications ou modifier vos opérations existantes. Vous migrez des serveurs d'une plateforme sur site vers un service cloud pour la même plateforme. Exemple : migrer une Microsoft Hyper-V application vers AWS.
- **Retenir** : conservez les applications dans votre environnement source. Il peut s'agir d'applications nécessitant une refactorisation majeure, que vous souhaitez retarder, et d'applications existantes que vous souhaitez retenir, car rien ne justifie leur migration sur le plan commercial.

- Retirer : mettez hors service ou supprimez les applications dont vous n'avez plus besoin dans votre environnement source.

A

ABAC

Voir contrôle [d'accès basé sur les attributs](#).

services abstraits

Consultez la section [Services gérés](#).

ACIDE

Voir [atomicité, consistance, isolation, durabilité](#).

migration active-active

Méthode de migration de base de données dans laquelle la synchronisation des bases de données source et cible est maintenue (à l'aide d'un outil de réplication bidirectionnelle ou d'opérations d'écriture double), tandis que les deux bases de données gèrent les transactions provenant de la connexion d'applications pendant la migration. Cette méthode prend en charge la migration par petits lots contrôlés au lieu d'exiger un basculement ponctuel. Elle est plus flexible mais demande plus de travail qu'une migration [active-passive](#).

migration active-passive

Méthode de migration de base de données dans laquelle les bases de données source et cible sont synchronisées, mais seule la base de données source gère les transactions liées à la connexion des applications pendant que les données sont répliquées vers la base de données cible. La base de données cible n'accepte aucune transaction pendant la migration.

fonction d'agrégation

Fonction SQL qui agit sur un groupe de lignes et calcule une valeur de retour unique pour le groupe. Des exemples de fonctions d'agrégation incluent SUM et MAX.

AI

Voir [intelligence artificielle](#).

AIOps

Voir les [opérations d'intelligence artificielle](#).

anonymisation

Processus de suppression définitive d'informations personnelles dans un ensemble de données. L'anonymisation peut contribuer à protéger la vie privée. Les données anonymisées ne sont plus considérées comme des données personnelles.

anti-motif

Solution fréquemment utilisée pour un problème récurrent lorsque la solution est contre-productive, inefficace ou moins efficace qu'une alternative.

contrôle des applications

Une approche de sécurité qui permet d'utiliser uniquement des applications approuvées afin de protéger un système contre les logiciels malveillants.

portefeuille d'applications

Ensemble d'informations détaillées sur chaque application utilisée par une organisation, y compris le coût de génération et de maintenance de l'application, ainsi que sa valeur métier. Ces informations sont essentielles pour [le processus de découverte et d'analyse du portefeuille](#) et permettent d'identifier et de prioriser les applications à migrer, à moderniser et à optimiser.

intelligence artificielle (IA)

Domaine de l'informatique consacré à l'utilisation des technologies de calcul pour exécuter des fonctions cognitives généralement associées aux humains, telles que l'apprentissage, la résolution de problèmes et la reconnaissance de modèles. Pour plus d'informations, veuillez consulter [Qu'est-ce que l'intelligence artificielle ?](#)

opérations d'intelligence artificielle (AIOps)

Processus consistant à utiliser des techniques de machine learning pour résoudre les problèmes opérationnels, réduire les incidents opérationnels et les interventions humaines, mais aussi améliorer la qualité du service. Pour plus d'informations sur son AIOps utilisation dans la stratégie de AWS migration, consultez le [guide d'intégration des opérations](#).

chiffrement asymétrique

Algorithme de chiffrement qui utilise une paire de clés, une clé publique pour le chiffrement et une clé privée pour le déchiffrement. Vous pouvez partager la clé publique, car elle n'est pas utilisée pour le déchiffrement, mais l'accès à la clé privée doit être très restreint.

atomicité, cohérence, isolement, durabilité (ACID)

Ensemble de propriétés logicielles garantissant la validité des données et la fiabilité opérationnelle d'une base de données, même en cas d'erreur, de panne de courant ou d'autres problèmes.

contrôle d'accès par attributs (ABAC)

Pratique qui consiste à créer des autorisations détaillées en fonction des attributs de l'utilisateur, tels que le service, le poste et le nom de l'équipe. Pour plus d'informations, consultez [ABAC pour AWS](#) dans la documentation Gestion des identités et des accès AWS (IAM).

source de données faisant autorité

Emplacement où vous stockez la version principale des données, considérée comme la source d'information la plus fiable. Vous pouvez copier les données de la source de données officielle vers d'autres emplacements à des fins de traitement ou de modification des données, par exemple en les anonymisant, en les expurgant ou en les pseudonymisant.

Zone de disponibilité

Un emplacement distinct au sein d'une Région AWS réseau isolé des défaillances dans d'autres zones de disponibilité et fournissant une connectivité réseau peu coûteuse et à faible latence aux autres zones de disponibilité de la même région.

AWS Cadre d'adoption du cloud (AWS CAF)

Un cadre de directives et de meilleures pratiques visant AWS à aider les entreprises à élaborer un plan efficace pour réussir leur migration vers le cloud. AWS La CAF organise ses conseils en six domaines prioritaires appelés perspectives : les affaires, les personnes, la gouvernance, les plateformes, la sécurité et les opérations. Les perspectives d'entreprise, de personnes et de gouvernance mettent l'accent sur les compétences et les processus métier, tandis que les perspectives relatives à la plateforme, à la sécurité et aux opérations se concentrent sur les compétences et les processus techniques. Par exemple, la perspective liée aux personnes cible les parties prenantes qui s'occupent des ressources humaines (RH), des fonctions de dotation en personnel et de la gestion des personnes. Dans cette perspective, la AWS CAF fournit des conseils pour le développement du personnel, la formation et les communications afin de préparer l'organisation à une adoption réussie du cloud. Pour plus d'informations, veuillez consulter le [site Web AWS CAF](#) et le [livre blanc AWS CAF](#).

AWS Cadre de qualification de la charge de travail (AWS WQF)

Outil qui évalue les charges de travail liées à la migration des bases de données, recommande des stratégies de migration et fournit des estimations de travail. AWS Le WQF est inclus avec

AWS Schema Conversion Tool (AWS SCT). Il analyse les schémas de base de données et les objets de code, le code d'application, les dépendances et les caractéristiques de performance, et fournit des rapports d'évaluation.

B

mauvais bot

Un [bot](#) destiné à perturber ou à nuire à des individus ou à des organisations.

BCP

Consultez la section [Planification de la continuité des activités](#).

graphique de comportement

Vue unifiée et interactive des comportements des ressources et des interactions au fil du temps. Vous pouvez utiliser un graphique de comportement avec Amazon Detective pour examiner les tentatives de connexion infructueuses, les appels d'API suspects et les actions similaires. Pour plus d'informations, veuillez consulter [Data in a behavior graph](#) dans la documentation Detective.

système de poids fort

Système qui stocke d'abord l'octet le plus significatif. Voir aussi [endianité](#).

classification binaire

Processus qui prédit un résultat binaire (l'une des deux classes possibles). Par exemple, votre modèle de machine learning peut avoir besoin de prévoir des problèmes tels que « Cet e-mail est-il du spam ou non ? » ou « Ce produit est-il un livre ou une voiture ? ».

filtre de Bloom

Structure de données probabiliste et efficace en termes de mémoire qui est utilisée pour tester si un élément fait partie d'un ensemble.

déploiement bleu/vert

Stratégie de déploiement dans laquelle vous créez deux environnements distincts mais identiques. Vous exécutez la version actuelle de l'application dans un environnement (bleu) et la nouvelle version de l'application dans l'autre environnement (vert). Cette stratégie vous permet de revenir rapidement en arrière avec un impact minimal.

bot

Application logicielle qui exécute des tâches automatisées sur Internet et simule l'activité ou l'interaction humaine. Certains robots sont utiles ou bénéfiques, comme les robots d'exploration Web qui indexent des informations sur Internet. D'autres robots, appelés « bots malveillants », sont destinés à perturber ou à nuire à des individus ou à des organisations.

botnet

Réseaux de [robots](#) infectés par des [logiciels malveillants](#) et contrôlés par une seule entité, connue sous le nom d'herder ou d'opérateur de bots. Les botnets sont le mécanisme le plus connu pour faire évoluer les bots et leur impact.

branche

Zone contenue d'un référentiel de code. La première branche créée dans un référentiel est la branche principale. Vous pouvez créer une branche à partir d'une branche existante, puis développer des fonctionnalités ou corriger des bogues dans la nouvelle branche. Une branche que vous créez pour générer une fonctionnalité est communément appelée branche de fonctionnalités. Lorsque la fonctionnalité est prête à être publiée, vous fusionnez à nouveau la branche de fonctionnalités dans la branche principale. Pour plus d'informations, consultez [À propos des branches](#) (GitHub documentation).

accès par brise-vitre

Dans des circonstances exceptionnelles et par le biais d'un processus approuvé, c'est un moyen rapide pour un utilisateur d'accéder à un accès auquel Compte AWS il n'est généralement pas autorisé. Pour plus d'informations, consultez l'indicateur [Implementation break-glass procedures](#) dans le guide Well-Architected AWS .

stratégie existante (brownfield)

L'infrastructure existante de votre environnement. Lorsque vous adoptez une stratégie existante pour une architecture système, vous concevez l'architecture en fonction des contraintes des systèmes et de l'infrastructure actuels. Si vous étendez l'infrastructure existante, vous pouvez combiner des politiques brownfield (existantes) et [greenfield](#) (inédites).

cache de tampon

Zone de mémoire dans laquelle sont stockées les données les plus fréquemment consultées.

capacité métier

Ce que fait une entreprise pour générer de la valeur (par exemple, les ventes, le service client ou le marketing). Les architectures de microservices et les décisions de développement

peuvent être dictées par les capacités métier. Pour plus d'informations, veuillez consulter la section [Organisation en fonction des capacités métier](#) du livre blanc [Exécution de microservices conteneurisés sur AWS](#).

planification de la continuité des activités (BCP)

Plan qui tient compte de l'impact potentiel d'un événement perturbateur, tel qu'une migration à grande échelle, sur les opérations, et qui permet à une entreprise de reprendre ses activités rapidement.

C

CAF

Voir le [cadre d'adoption du AWS cloud](#).

déploiement de Canary

Diffusion lente et progressive d'une version pour les utilisateurs finaux. Lorsque vous êtes sûr, vous déployez la nouvelle version et remplacez la version actuelle dans son intégralité.

CCo E

Voir [le Centre d'excellence du cloud](#).

CDC

Voir [capture des données de modification](#).

capture des données de modification (CDC)

Processus de suivi des modifications apportées à une source de données, telle qu'une table de base de données, et d'enregistrement des métadonnées relatives à ces modifications. Vous pouvez utiliser la CDC à diverses fins, telles que l'audit ou la réplication des modifications dans un système cible afin de maintenir la synchronisation.

ingénierie du chaos

Introduire intentionnellement des défaillances ou des événements perturbateurs pour tester la résilience d'un système. Vous pouvez utiliser [AWS Fault Injection Service \(AWS FIS\)](#) pour effectuer des expériences qui stressent vos AWS charges de travail et évaluer leur réponse.

CI/CD

Découvrez [l'intégration continue et la livraison continue](#).

classification

Processus de catégorisation qui permet de générer des prédictions. Les modèles de ML pour les problèmes de classification prédisent une valeur discrète. Les valeurs discrètes se distinguent toujours les unes des autres. Par exemple, un modèle peut avoir besoin d'évaluer la présence ou non d'une voiture sur une image.

chiffrement côté client

Chiffrement des données localement, avant que la cible ne les Service AWS reçoive.

Centre d'excellence du cloud (CCoE)

Une équipe multidisciplinaire qui dirige les efforts d'adoption du cloud au sein d'une organisation, notamment en développant les bonnes pratiques en matière de cloud, en mobilisant des ressources, en établissant des délais de migration et en guidant l'organisation dans le cadre de transformations à grande échelle. Pour plus d'informations, consultez les [CCoarticles électroniques](#) du blog sur la stratégie AWS Cloud d'entreprise.

cloud computing

Technologie cloud généralement utilisée pour le stockage de données à distance et la gestion des appareils IoT. Le cloud computing est généralement associé à la technologie [informatique de pointe](#).

modèle d'exploitation du cloud

Dans une organisation informatique, modèle d'exploitation utilisé pour créer, faire évoluer et optimiser un ou plusieurs environnements cloud. Pour plus d'informations, consultez la section [Création de votre modèle d'exploitation cloud](#).

étapes d'adoption du cloud

Les quatre phases que les entreprises traversent généralement lorsqu'elles migrent vers AWS Cloud :

- **Projet** : exécution de quelques projets liés au cloud à des fins de preuve de concept et d'apprentissage
- **Base** : réaliser des investissements fondamentaux pour accélérer votre adoption du cloud (par exemple, créer une zone de landing zone, définir un CCo E, établir un modèle opérationnel)
- **Migration** : migration d'applications individuelles
- **Réinvention** : optimisation des produits et services et innovation dans le cloud

Ces étapes ont été définies par Stephen Orban dans le billet de blog [The Journey Toward Cloud-First & the Stages of Adoption](#) publié sur le blog AWS Cloud Enterprise Strategy. Pour plus d'informations sur leur lien avec la stratégie de AWS migration, consultez le [guide de préparation à la migration](#).

CMDB

Consultez la base de [données de gestion des configurations](#).

référentiel de code

Emplacement où le code source et d'autres ressources, comme la documentation, les exemples et les scripts, sont stockés et mis à jour par le biais de processus de contrôle de version. Les référentiels cloud courants incluent GitHub ou Bitbucket Cloud. Chaque version du code est appelée branche. Dans une structure de microservice, chaque référentiel est consacré à une seule fonctionnalité. Un seul pipeline CI/CD peut utiliser plusieurs référentiels.

cache passif

Cache tampon vide, mal rempli ou contenant des données obsolètes ou non pertinentes. Cela affecte les performances, car l'instance de base de données doit lire à partir de la mémoire principale ou du disque, ce qui est plus lent que la lecture à partir du cache tampon.

données gelées

Données rarement consultées et généralement historiques. Lorsque vous interrogez ce type de données, les requêtes lentes sont généralement acceptables. Le transfert de ces données vers des niveaux ou classes de stockage moins performants et moins coûteux peut réduire les coûts.

vision par ordinateur (CV)

Domaine de l'[IA](#) qui utilise l'apprentissage automatique pour analyser et extraire des informations à partir de formats visuels tels que des images numériques et des vidéos. Par exemple, Amazon SageMaker AI fournit des algorithmes de traitement d'image pour les CV.

dérive de configuration

Pour une charge de travail, une modification de configuration par rapport à l'état attendu. Cela peut entraîner une non-conformité de la charge de travail, et cela est généralement progressif et involontaire.

base de données de gestion des configurations (CMDB)

Référentiel qui stocke et gère les informations relatives à une base de données et à son environnement informatique, y compris les composants matériels et logiciels ainsi que leurs

configurations. Vous utilisez généralement les données d'une CMDB lors de la phase de découverte et d'analyse du portefeuille de la migration.

pack de conformité

Ensemble de AWS Config règles et d'actions correctives que vous pouvez assembler pour personnaliser vos contrôles de conformité et de sécurité. Vous pouvez déployer un pack de conformité en tant qu'entité unique dans une région Compte AWS et, ou au sein d'une organisation, à l'aide d'un modèle YAML. Pour plus d'informations, consultez la section [Packs de conformité](#) dans la AWS Config documentation.

intégration continue et livraison continue (CI/CD)

Processus d'automatisation des étapes de source, de construction, de test, de préparation et de production du processus de publication du logiciel. CI/CD est communément décrit comme un pipeline. CI/CD peut vous aider à automatiser les processus, à améliorer la productivité, à améliorer la qualité du code et à accélérer les livraisons. Pour plus d'informations, veuillez consulter [Avantages de la livraison continue](#). CD peut également signifier déploiement continu. Pour plus d'informations, veuillez consulter [Livraison continue et déploiement continu](#).

CV

Voir [vision par ordinateur](#).

D

données au repos

Données stationnaires dans votre réseau, telles que les données stockées.

classification des données

Processus permettant d'identifier et de catégoriser les données de votre réseau en fonction de leur sévérité et de leur sensibilité. Il s'agit d'un élément essentiel de toute stratégie de gestion des risques de cybersécurité, car il vous aide à déterminer les contrôles de protection et de conservation appropriés pour les données. La classification des données est une composante du pilier de sécurité du AWS Well-Architected Framework. Pour plus d'informations, veuillez consulter [Classification des données](#).

dérive des données

Une variation significative entre les données de production et les données utilisées pour entraîner un modèle ML, ou une modification significative des données d'entrée au fil du temps. La dérive

des données peut réduire la qualité, la précision et l'équité globales des prédictions des modèles ML.

données en transit

Données qui circulent activement sur votre réseau, par exemple entre les ressources du réseau.

maillage de données

Un cadre architectural qui fournit une propriété des données distribuée et décentralisée avec une gestion et une gouvernance centralisées.

minimisation des données

Le principe de collecte et de traitement des seules données strictement nécessaires. La pratique de la minimisation des données AWS Cloud peut réduire les risques liés à la confidentialité, les coûts et l'empreinte carbone de vos analyses.

périmètre de données

Ensemble de garde-fous préventifs dans votre AWS environnement qui permettent de garantir que seules les identités fiables accèdent aux ressources fiables des réseaux attendus. Pour plus d'informations, voir [Création d'un périmètre de données sur AWS](#).

prétraitement des données

Pour transformer les données brutes en un format facile à analyser par votre modèle de ML. Le prétraitement des données peut impliquer la suppression de certaines colonnes ou lignes et le traitement des valeurs manquantes, incohérentes ou en double.

provenance des données

Le processus de suivi de l'origine et de l'historique des données tout au long de leur cycle de vie, par exemple la manière dont les données ont été générées, transmises et stockées.

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt des données

Un système de gestion des données qui prend en charge les informations commerciales, telles que les analyses. Les entrepôts de données contiennent généralement de grandes quantités de données historiques et sont généralement utilisés pour les requêtes et les analyses.

langage de définition de base de données (DDL)

Instructions ou commandes permettant de créer ou de modifier la structure des tables et des objets dans une base de données.

langage de manipulation de base de données (DML)

Instructions ou commandes permettant de modifier (insérer, mettre à jour et supprimer) des informations dans une base de données.

DDL

Voir [langage de définition de base](#) de données.

ensemble profond

Sert à combiner plusieurs modèles de deep learning à des fins de prédiction. Vous pouvez utiliser des ensembles profonds pour obtenir une prévision plus précise ou pour estimer l'incertitude des prédictions.

deep learning

Un sous-champ de ML qui utilise plusieurs couches de réseaux neuronaux artificiels pour identifier le mappage entre les données d'entrée et les variables cibles d'intérêt.

defense-in-depth

Approche de la sécurité de l'information dans laquelle une série de mécanismes et de contrôles de sécurité sont judicieusement répartis sur l'ensemble d'un réseau informatique afin de protéger la confidentialité, l'intégrité et la disponibilité du réseau et des données qu'il contient. Lorsque vous adoptez cette stratégie AWS, vous ajoutez plusieurs contrôles à différentes couches de la AWS Organizations structure afin de sécuriser les ressources. Par exemple, une defense-in-depth approche peut combiner l'authentification multifactorielle, la segmentation du réseau et le chiffrement.

administrateur délégué

Dans AWS Organizations, un service compatible peut enregistrer un compte AWS membre pour administrer les comptes de l'organisation et gérer les autorisations pour ce service. Ce compte est appelé administrateur délégué pour ce service. Pour plus d'informations et une liste des services compatibles, veuillez consulter la rubrique [Services qui fonctionnent avec AWS Organizations](#) dans la documentation AWS Organizations .

déploiement

Processus de mise à disposition d'une application, de nouvelles fonctionnalités ou de corrections de code dans l'environnement cible. Le déploiement implique la mise en œuvre de modifications dans une base de code, puis la génération et l'exécution de cette base de code dans les environnements de l'application.

environnement de développement

Voir [environnement](#).

contrôle de détection

Contrôle de sécurité conçu pour détecter, journaliser et alerter après la survenue d'un événement. Ces contrôles constituent une deuxième ligne de défense et vous alertent en cas d'événements de sécurité qui ont contourné les contrôles préventifs en place. Pour plus d'informations, veuillez consulter la rubrique [Contrôles de détection](#) dans *Implementing security controls on AWS*.

cartographie de la chaîne de valeur du développement (DVSM)

Processus utilisé pour identifier et hiérarchiser les contraintes qui nuisent à la rapidité et à la qualité du cycle de vie du développement logiciel. DVSM étend le processus de cartographie de la chaîne de valeur initialement conçu pour les pratiques de production allégée. Il met l'accent sur les étapes et les équipes nécessaires pour créer et transférer de la valeur tout au long du processus de développement logiciel.

jumeau numérique

Représentation virtuelle d'un système réel, tel qu'un bâtiment, une usine, un équipement industriel ou une ligne de production. Les jumeaux numériques prennent en charge la maintenance prédictive, la surveillance à distance et l'optimisation de la production.

tableau des dimensions

Dans un [schéma en étoile](#), table plus petite contenant les attributs de données relatifs aux données quantitatives d'une table de faits. Les attributs des tables de dimensions sont généralement des champs de texte ou des nombres discrets qui se comportent comme du texte. Ces attributs sont couramment utilisés pour la contrainte des requêtes, le filtrage et l'étiquetage des ensembles de résultats.

catastrophe

Un événement qui empêche une charge de travail ou un système d'atteindre ses objectifs commerciaux sur son site de déploiement principal. Ces événements peuvent être des

catastrophes naturelles, des défaillances techniques ou le résultat d'actions humaines, telles qu'une mauvaise configuration involontaire ou une attaque de logiciel malveillant.

reprise après sinistre (DR)

La stratégie et le processus que vous utilisez pour minimiser les temps d'arrêt et les pertes de données causés par un [sinistre](#). Pour plus d'informations, consultez [Disaster Recovery of Workloads on AWS : Recovery in the Cloud in the AWS Well-Architected Framework](#).

DML

Voir [langage de manipulation de base](#) de données.

conception axée sur le domaine

Approche visant à développer un système logiciel complexe en connectant ses composants à des domaines évolutifs, ou objectifs métier essentiels, que sert chaque composant. Ce concept a été introduit par Eric Evans dans son ouvrage Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston : Addison-Wesley Professional, 2003). Pour plus d'informations sur l'utilisation du design piloté par domaine avec le modèle de figuier étrangleur, veuillez consulter [Modernizing legacy Microsoft ASP.NET \(ASMX\) web services incrementally by using containers and Amazon API Gateway](#).

DR

Voir [reprise après sinistre](#).

détection de dérive

Suivi des écarts par rapport à une configuration de référence. Par exemple, vous pouvez l'utiliser AWS CloudFormation pour [détecter la dérive des ressources du système](#) ou AWS Control Tower pour [détecter les modifications de votre zone d'atterrissage](#) susceptibles d'affecter le respect des exigences de gouvernance.

DVSM

Voir la [cartographie de la chaîne de valeur du développement](#).

E

EDA

Voir [analyse exploratoire des données](#).

EDI

Voir échange [de données informatisé](#).

informatique de périphérie

Technologie qui augmente la puissance de calcul des appareils intelligents en périphérie d'un réseau IoT. Comparé au [cloud computing, l'informatique](#) de pointe peut réduire la latence des communications et améliorer le temps de réponse.

échange de données informatisé (EDI)

L'échange automatique de documents commerciaux entre les organisations. Pour plus d'informations, voir [Qu'est-ce que l'échange de données informatisé ?](#)

chiffrement

Processus informatique qui transforme des données en texte clair, lisibles par l'homme, en texte chiffré.

clé de chiffrement

Chaîne cryptographique de bits aléatoires générée par un algorithme cryptographique. La longueur des clés peut varier, et chaque clé est conçue pour être imprévisible et unique.

endianisme

Ordre selon lequel les octets sont stockés dans la mémoire de l'ordinateur. Les systèmes de poids fort stockent d'abord l'octet le plus significatif. Les systèmes de poids faible stockent d'abord l'octet le moins significatif.

point de terminaison

Voir [point de terminaison de service](#).

service de point de terminaison

Service que vous pouvez héberger sur un cloud privé virtuel (VPC) pour le partager avec d'autres utilisateurs. Vous pouvez créer un service de point de terminaison avec AWS PrivateLink et accorder des autorisations à d'autres Comptes AWS ou à Gestion des identités et des accès AWS (IAM) principaux. Ces comptes ou principaux peuvent se connecter à votre service de point de terminaison de manière privée en créant des points de terminaison d'un VPC d'interface. Pour plus d'informations, veuillez consulter [Création d'un service de point de terminaison](#) dans la documentation Amazon Virtual Private Cloud (Amazon VPC).

planification des ressources d'entreprise (ERP)

Système qui automatise et gère les principaux processus métier (tels que la comptabilité, le [MES](#) et la gestion de projet) pour une entreprise.

chiffrement d'enveloppe

Processus de chiffrement d'une clé de chiffrement à l'aide d'une autre clé de chiffrement. Pour plus d'informations, consultez la section [Chiffrement des enveloppes](#) dans la documentation AWS Key Management Service (AWS KMS).

environnement

Instance d'une application en cours d'exécution. Les types d'environnement les plus courants dans le cloud computing sont les suivants :

- Environnement de développement : instance d'une application en cours d'exécution à laquelle seule l'équipe principale chargée de la maintenance de l'application peut accéder. Les environnements de développement sont utilisés pour tester les modifications avant de les promouvoir dans les environnements supérieurs. Ce type d'environnement est parfois appelé environnement de test.
- Environnements inférieurs : tous les environnements de développement d'une application, tels que ceux utilisés pour les générations et les tests initiaux.
- Environnement de production : instance d'une application en cours d'exécution à laquelle les utilisateurs finaux peuvent accéder. Dans un CI/CD pipeline, l'environnement de production est le dernier environnement de déploiement.
- Environnements supérieurs : tous les environnements accessibles aux utilisateurs autres que l'équipe de développement principale. Ils peuvent inclure un environnement de production, des environnements de préproduction et des environnements pour les tests d'acceptation par les utilisateurs.

épopée

Dans les méthodologies agiles, catégories fonctionnelles qui aident à organiser et à prioriser votre travail. Les épopées fournissent une description détaillée des exigences et des tâches d'implémentation. Par exemple, les points forts de la AWS CAF en matière de sécurité incluent la gestion des identités et des accès, les contrôles de détection, la sécurité des infrastructures, la protection des données et la réponse aux incidents. Pour plus d'informations sur les épopées dans la stratégie de migration AWS , veuillez consulter le [guide d'implémentation du programme](#).

ERP

Voir [Planification des ressources d'entreprise](#).

analyse exploratoire des données (EDA)

Processus d'analyse d'un jeu de données pour comprendre ses principales caractéristiques. Vous collectez ou agrégez des données, puis vous effectuez des enquêtes initiales pour trouver des modèles, détecter des anomalies et vérifier les hypothèses. L'EDA est réalisée en calculant des statistiques récapitulatives et en créant des visualisations de données.

F

tableau des faits

La table centrale dans un [schéma en étoile](#). Il stocke des données quantitatives sur les opérations commerciales. Généralement, une table de faits contient deux types de colonnes : celles qui contiennent des mesures et celles qui contiennent une clé étrangère pour une table de dimensions.

échouer rapidement

Une philosophie qui utilise des tests fréquents et progressifs pour réduire le cycle de vie du développement. C'est un élément essentiel d'une approche agile.

limite d'isolation des défauts

Dans le AWS Cloud, une limite telle qu'une zone de disponibilité Région AWS, un plan de contrôle ou un plan de données qui limite l'effet d'une panne et contribue à améliorer la résilience des charges de travail. Pour plus d'informations, consultez la section [Limites d'isolation des AWS pannes](#).

branche de fonctionnalités

Voir [succursale](#).

fonctionnalités

Les données d'entrée que vous utilisez pour faire une prédiction. Par exemple, dans un contexte de fabrication, les fonctionnalités peuvent être des images capturées périodiquement à partir de la ligne de fabrication.

importance des fonctionnalités

Le niveau d'importance d'une fonctionnalité pour les prédictions d'un modèle. Il s'exprime généralement sous la forme d'un score numérique qui peut être calculé à l'aide de différentes techniques, telles que la méthode Shapley Additive Explanations (SHAP) et les gradients intégrés. Pour plus d'informations, voir [Interprétabilité du modèle d'apprentissage automatique avec AWS](#).

transformation de fonctionnalité

Optimiser les données pour le processus de ML, notamment en enrichissant les données avec des sources supplémentaires, en mettant à l'échelle les valeurs ou en extrayant plusieurs ensembles d'informations à partir d'un seul champ de données. Cela permet au modèle de ML de tirer parti des données. Par exemple, si vous décomposez la date « 2021-05-27 00:15:37 » en « 2021 », « mai », « jeudi » et « 15 », vous pouvez aider l'algorithme d'apprentissage à apprendre des modèles nuancés associés à différents composants de données.

invitation en quelques coups

Fournir à un [LLM](#) un petit nombre d'exemples illustrant la tâche et le résultat souhaité avant de lui demander d'effectuer une tâche similaire. Cette technique est une application de l'apprentissage contextuel, dans le cadre de laquelle les modèles apprennent à partir d'exemples (prises de vue) intégrés dans des instructions. Les instructions en quelques étapes peuvent être efficaces pour les tâches qui nécessitent un formatage, un raisonnement ou des connaissances de domaine spécifiques. Voir également [l'invite Zero-Shot](#).

FGAC

Découvrez le [contrôle d'accès détaillé](#).

contrôle d'accès détaillé (FGAC)

Utilisation de plusieurs conditions pour autoriser ou refuser une demande d'accès.

migration instantanée (flash-cut)

Méthode de migration de base de données qui utilise la réplication continue des données par [le biais de la capture des données de modification](#) afin de migrer les données dans les plus brefs délais, au lieu d'utiliser une approche progressive. L'objectif est de réduire au maximum les temps d'arrêt.

FM

Voir le [modèle de fondation](#).

modèle de fondation (FM)

Un vaste réseau neuronal d'apprentissage profond qui s'est entraîné sur d'énormes ensembles de données généralisées et non étiquetées. FMs sont capables d'effectuer une grande variété de tâches générales, telles que comprendre le langage, générer du texte et des images et converser en langage naturel. Pour plus d'informations, voir [Que sont les modèles de base ?](#)

G

IA générative

Sous-ensemble de modèles d'[IA](#) qui ont été entraînés sur de grandes quantités de données et qui peuvent utiliser une simple invite textuelle pour créer de nouveaux contenus et artefacts, tels que des images, des vidéos, du texte et du son. Pour plus d'informations, consultez [Qu'est-ce que l'IA générative](#).

blocage géographique

Voir les [restrictions géographiques](#).

restrictions géographiques (blocage géographique)

Sur Amazon CloudFront, option permettant d'empêcher les utilisateurs de certains pays d'accéder aux distributions de contenu. Vous pouvez utiliser une liste d'autorisation ou une liste de blocage pour spécifier les pays approuvés et interdits. Pour plus d'informations, consultez [la section Restreindre la distribution géographique de votre contenu](#) dans la CloudFront documentation.

Flux de travail Gitflow

Approche dans laquelle les environnements inférieurs et supérieurs utilisent différentes branches dans un référentiel de code source. Le flux de travail Gitflow est considéré comme existant, et le [flux de travail basé sur les troncs](#) est l'approche moderne préférée.

image dorée

Un instantané d'un système ou d'un logiciel utilisé comme modèle pour déployer de nouvelles instances de ce système ou logiciel. Par exemple, dans le secteur de la fabrication, une image dorée peut être utilisée pour fournir des logiciels sur plusieurs appareils et contribue à améliorer la vitesse, l'évolutivité et la productivité des opérations de fabrication des appareils.

stratégie inédite

L'absence d'infrastructures existantes dans un nouvel environnement. Lorsque vous adoptez une stratégie inédite pour une architecture système, vous pouvez sélectionner toutes les nouvelles technologies sans restriction de compatibilité avec l'infrastructure existante, également appelée [brownfield](#). Si vous étendez l'infrastructure existante, vous pouvez combiner des politiques brownfield (existantes) et greenfield (inédites).

barrière de protection

Règle de haut niveau qui permet de régir les ressources, les politiques et la conformité au sein des unités organisationnelles (OUs). Les barrières de protection préventives appliquent des politiques pour garantir l'alignement sur les normes de conformité. Elles sont mises en œuvre à l'aide de politiques de contrôle des services et de limites des autorisations IAM. Les barrières de protection de détection détectent les violations des politiques et les problèmes de conformité, et génèrent des alertes pour y remédier. Ils sont implémentés à l'aide d'Amazon AWS Config AWS Security Hub CSPM GuardDuty AWS Trusted Advisor, d'Amazon Inspector et de AWS Lambda contrôles personnalisés.

H

HA

Découvrez [la haute disponibilité](#).

migration de base de données hétérogène

Migration de votre base de données source vers une base de données cible qui utilise un moteur de base de données différent (par exemple, Oracle vers Amazon Aurora). La migration hétérogène fait généralement partie d'un effort de réarchitecture, et la conversion du schéma peut s'avérer une tâche complexe. [AWS propose AWS SCT](#) qui facilite les conversions de schémas.

haute disponibilité (HA)

Capacité d'une charge de travail à fonctionner en continu, sans intervention, en cas de difficultés ou de catastrophes. Les systèmes HA sont conçus pour basculer automatiquement, fournir constamment des performances de haute qualité et gérer différentes charges et défaillances avec un impact minimal sur les performances.

modernisation des historiens

Approche utilisée pour moderniser et mettre à niveau les systèmes de technologie opérationnelle (OT) afin de mieux répondre aux besoins de l'industrie manufacturière. Un historien est un type de base de données utilisé pour collecter et stocker des données provenant de diverses sources dans une usine.

données de rétention

Partie de données historiques étiquetées qui n'est pas divulguée dans un ensemble de données utilisé pour entraîner un modèle d'[apprentissage automatique](#). Vous pouvez utiliser les données de blocage pour évaluer les performances du modèle en comparant les prévisions du modèle aux données de blocage.

migration de base de données homogène

Migration de votre base de données source vers une base de données cible qui partage le même moteur de base de données (par exemple, Microsoft SQL Server vers Amazon RDS for SQL Server). La migration homogène s'inscrit généralement dans le cadre d'un effort de réhébergement ou de replateforme. Vous pouvez utiliser les utilitaires de base de données natifs pour migrer le schéma.

données chaudes

Données fréquemment consultées, telles que les données en temps réel ou les données translationnelles récentes. Ces données nécessitent généralement un niveau ou une classe de stockage à hautes performances pour fournir des réponses rapides aux requêtes.

correctif

Solution d'urgence à un problème critique dans un environnement de production. En raison de son urgence, un correctif est généralement créé en dehors du flux de travail de DevOps publication habituel.

période de soins intensifs

Immédiatement après le basculement, période pendant laquelle une équipe de migration gère et surveille les applications migrées dans le cloud afin de résoudre les problèmes éventuels. En règle générale, cette période dure de 1 à 4 jours. À la fin de la période de soins intensifs, l'équipe de migration transfère généralement la responsabilité des applications à l'équipe des opérations cloud.

I

laC

Considérez [l'infrastructure comme un code](#).

politique basée sur l'identité

Politique attachée à un ou plusieurs principaux IAM qui définit leurs autorisations au sein de l'AWS Cloud environnement.

application inactive

Application dont l'utilisation moyenne du processeur et de la mémoire se situe entre 5 et 20 % sur une période de 90 jours. Dans un projet de migration, il est courant de retirer ces applications ou de les retenir sur site.

Ilo T

Voir [Internet industriel des objets](#).

infrastructure immuable

Modèle qui déploie une nouvelle infrastructure pour les charges de travail de production au lieu de mettre à jour, d'appliquer des correctifs ou de modifier l'infrastructure existante. Les infrastructures immuables sont intrinsèquement plus cohérentes, fiables et prévisibles que les infrastructures [mutables](#). Pour plus d'informations, consultez les meilleures pratiques de [déploiement à l'aide d'une infrastructure immuable](#) dans le AWS Well-Architected Framework.

VPC entrant (d'entrée)

Dans une architecture AWS multi-comptes, un VPC qui accepte, inspecte et achemine les connexions réseau depuis l'extérieur d'une application. L'[architecture AWS de référence de sécurité](#) recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

migration incrémentielle

Stratégie de basculement dans le cadre de laquelle vous migrez votre application par petites parties au lieu d'effectuer un basculement complet unique. Par exemple, il se peut que vous ne transfériez que quelques microservices ou utilisateurs vers le nouveau système dans un premier temps. Après avoir vérifié que tout fonctionne correctement, vous pouvez transférer

I

progressivement des microservices ou des utilisateurs supplémentaires jusqu'à ce que vous puissiez mettre hors service votre système hérité. Cette stratégie réduit les risques associés aux migrations de grande ampleur.

Industry 4.0

Terme introduit par [Klaus Schwab](#) en 2016 pour désigner la modernisation des processus de fabrication grâce aux avancées en matière de connectivité, de données en temps réel, d'automatisation, d'analyse et d'IA/ML.

infrastructure

Ensemble des ressources et des actifs contenus dans l'environnement d'une application.

infrastructure en tant que code (IaC)

Processus de mise en service et de gestion de l'infrastructure d'une application via un ensemble de fichiers de configuration. IaC est conçue pour vous aider à centraliser la gestion de l'infrastructure, à normaliser les ressources et à mettre à l'échelle rapidement afin que les nouveaux environnements soient reproductibles, fiables et cohérents.

Internet industriel des objets (IIoT)

L'utilisation de capteurs et d'appareils connectés à Internet dans les secteurs industriels tels que la fabrication, l'énergie, l'automobile, les soins de santé, les sciences de la vie et l'agriculture. Pour plus d'informations, voir [Élaboration d'une stratégie de transformation numérique de l'Internet des objets \(IIoT\) industriel](#).

VPC d'inspection

Dans une architecture AWS multi-comptes, un VPC centralisé qui gère les inspections du trafic réseau VPCs entre (identique ou Régions AWS différent), Internet et les réseaux locaux. L'[architecture AWS de référence de sécurité](#) recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

Internet des objets (IoT)

Réseau d'objets physiques connectés dotés de capteurs ou de processeurs intégrés qui communiquent avec d'autres appareils et systèmes via Internet ou via un réseau de communication local. Pour plus d'informations, veuillez consulter la section [Qu'est-ce que l'IoT ?](#).

interprétabilité

Caractéristique d'un modèle de machine learning qui décrit dans quelle mesure un être humain peut comprendre comment les prédictions du modèle dépendent de ses entrées. Pour plus d'informations, voir [Interprétabilité du modèle d'apprentissage automatique avec AWS](#).

IoT

Voir [Internet des objets](#).

Bibliothèque d'informations informatiques (ITIL)

Ensemble de bonnes pratiques pour proposer des services informatiques et les aligner sur les exigences métier. L'ITIL constitue la base de l'ITSM.

gestion des services informatiques (ITSM)

Activités associées à la conception, à la mise en œuvre, à la gestion et à la prise en charge de services informatiques d'une organisation. Pour plus d'informations sur l'intégration des opérations cloud aux outils ITSM, veuillez consulter le [guide d'intégration des opérations](#).

ITIL

Consultez la [bibliothèque d'informations informatiques](#).

ITSM

Voir [Gestion des services informatiques](#).

L

contrôle d'accès basé sur des étiquettes (LBAC)

Une implémentation du contrôle d'accès obligatoire (MAC) dans laquelle une valeur d'étiquette de sécurité est explicitement attribuée aux utilisateurs et aux données elles-mêmes. L'intersection entre l'étiquette de sécurité utilisateur et l'étiquette de sécurité des données détermine les lignes et les colonnes visibles par l'utilisateur.

zone de destination

Une zone d'atterrissage est un AWS environnement multi-comptes bien conçu, évolutif et sécurisé. Il s'agit d'un point de départ à partir duquel vos entreprises peuvent rapidement lancer et déployer des charges de travail et des applications en toute confiance dans leur environnement de sécurité et d'infrastructure. Pour plus d'informations sur les zones de destination, veuillez consulter [Setting up a secure and scalable multi-account AWS environment](#).

grand modèle de langage (LLM)

Un modèle d'[intelligence artificielle basé](#) sur le deep learning qui est préentraîné sur une grande quantité de données. Un LLM peut effectuer plusieurs tâches, telles que répondre à des questions, résumer des documents, traduire du texte dans d'autres langues et compléter des phrases. Pour plus d'informations, voir [Que sont LLMs](#).

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

Voir contrôle d'[accès basé sur des étiquettes](#).

principe de moindre privilège

Bonne pratique de sécurité qui consiste à accorder les autorisations minimales nécessaires à l'exécution d'une tâche. Pour plus d'informations, veuillez consulter la rubrique [Accorder les autorisations de moindre privilège](#) dans la documentation IAM.

lift and shift

Voir [7 Rs](#).

système de poids faible

Système qui stocke d'abord l'octet le moins significatif. Voir aussi [endianité](#).

LLM

Voir le [grand modèle de langage](#).

environnements inférieurs

Voir [environnement](#).

M

machine learning (ML)

Type d'intelligence artificielle qui utilise des algorithmes et des techniques pour la reconnaissance et l'apprentissage de modèles. Le ML analyse et apprend à partir de données enregistrées, telles que les données de l'Internet des objets (IoT), pour générer un modèle statistique basé sur des modèles. Pour plus d'informations, veuillez consulter [Machine Learning](#).

branche principale

Voir [succursale](#).

malware

Logiciel conçu pour compromettre la sécurité ou la confidentialité de l'ordinateur. Les logiciels malveillants peuvent perturber les systèmes informatiques, divulguer des informations sensibles ou obtenir un accès non autorisé. Parmi les malwares, on peut citer les virus, les vers, les rançongiciels, les chevaux de Troie, les logiciels espions et les enregistreurs de frappe.

services gérés

Services AWS pour lequel AWS fonctionnent la couche d'infrastructure, le système d'exploitation et les plateformes, et vous accédez aux points de terminaison pour stocker et récupérer des données. Amazon Simple Storage Service (Amazon S3) et Amazon DynamoDB sont des exemples de services gérés. Ils sont également connus sous le nom de services abstraits.

système d'exécution de la fabrication (MES)

Un système logiciel pour le suivi, la surveillance, la documentation et le contrôle des processus de production qui convertissent les matières premières en produits finis dans l'atelier.

MAP

Voir [Migration Acceleration Program](#).

mécanisme

Processus complet au cours duquel vous créez un outil, favorisez son adoption, puis inspectez les résultats afin de procéder aux ajustements nécessaires. Un mécanisme est un cycle qui se renforce et s'améliore lorsqu'il fonctionne. Pour plus d'informations, voir [Création de mécanismes](#) dans le cadre AWS Well-Architected.

compte membre

Tous, à l'exception des Comptes AWS exception du compte de gestion, qui font partie d'une organisation dans AWS Organizations. Un compte ne peut être membre que d'une seule organisation à la fois.

MAILLES

Voir le [système d'exécution de la fabrication](#).

Transport télémétrique en file d'attente de messages (MQTT)

[Protocole de communication léger machine-to-machine \(M2M\), basé sur le modèle de publication/d'abonnement, pour les appareils IoT aux ressources limitées.](#)

microservice

Un petit service indépendant qui communique via un réseau bien défini APIs et qui est généralement détenu par de petites équipes autonomes. Par exemple, un système d'assurance peut inclure des microservices qui mappent à des capacités métier, telles que les ventes ou le marketing, ou à des sous-domaines, tels que les achats, les réclamations ou l'analytique. Les avantages des microservices incluent l'agilité, la flexibilité de la mise à l'échelle, la facilité de déploiement, la réutilisation du code et la résilience. Pour plus d'informations, consultez la section [Intégration de microservices à l'aide de services AWS sans serveur](#).

architecture de microservices

Approche de création d'une application avec des composants indépendants qui exécutent chaque processus d'application en tant que microservice. Ces microservices communiquent via une interface bien définie en utilisant Lightweight. APIs Chaque microservice de cette architecture peut être mis à jour, déployé et mis à l'échelle pour répondre à la demande de fonctions spécifiques d'une application. Pour plus d'informations, consultez la section [Implémentation de microservices sur AWS](#).

Programme d'accélération des migrations (MAP)

Un AWS programme qui fournit un support de conseil, des formations et des services pour aider les entreprises à établir une base opérationnelle solide pour passer au cloud, et pour aider à compenser le coût initial des migrations. MAP inclut une méthodologie de migration pour exécuter les migrations héritées de manière méthodique, ainsi qu'un ensemble d'outils pour automatiser et accélérer les scénarios de migration courants.

migration à grande échelle

Processus consistant à transférer la majeure partie du portefeuille d'applications vers le cloud par vagues, un plus grand nombre d'applications étant déplacées plus rapidement à chaque vague. Cette phase utilise les bonnes pratiques et les enseignements tirés des phases précédentes pour implémenter une usine de migration d'équipes, d'outils et de processus en vue de rationaliser la migration des charges de travail grâce à l'automatisation et à la livraison agile. Il s'agit de la troisième phase de la [stratégie de migration AWS](#).

usine de migration

Équipes interfonctionnelles qui rationalisent la migration des charges de travail grâce à des approches automatisées et agiles. Les équipes de Migration Factory comprennent généralement des responsables des opérations, des analystes commerciaux et des propriétaires, des ingénieurs de migration, des développeurs et DevOps des professionnels travaillant dans le cadre de sprints.

Entre 20 et 50 % du portefeuille d'applications d'entreprise est constitué de modèles répétés qui peuvent être optimisés par une approche d'usine. Pour plus d'informations, veuillez consulter la rubrique [discussion of migration factories](#) et le [guide Cloud Migration Factory](#) dans cet ensemble de contenus.

métadonnées de migration

Informations relatives à l'application et au serveur nécessaires pour finaliser la migration.

Chaque modèle de migration nécessite un ensemble de métadonnées de migration différent. Les exemples de métadonnées de migration incluent le sous-réseau cible, le groupe de sécurité et le AWS compte.

modèle de migration

Tâche de migration reproductible qui détaille la stratégie de migration, la destination de la migration et l'application ou le service de migration utilisé. Exemple : réorganisez la migration vers Amazon EC2 AWS avec le service de migration d'applications.

Évaluation du portefeuille de migration (MPA)

Outil en ligne qui fournit des informations pour valider l'analyse de rentabilisation en faveur de la migration vers le. AWS Cloud La MPA propose une évaluation détaillée du portefeuille (dimensionnement approprié des serveurs, tarification, comparaison du coût total de possession, analyse des coûts de migration), ainsi que la planification de la migration (analyse et collecte des données d'applications, regroupement des applications, priorisation des migrations et planification des vagues). L'[outil MPA](#) (connexion requise) est disponible gratuitement pour tous les AWS consultants et consultants APN Partner.

Évaluation de la préparation à la migration (MRA)

Processus qui consiste à obtenir des informations sur l'état de préparation d'une organisation au cloud, à identifier les forces et les faiblesses et à élaborer un plan d'action pour combler les lacunes identifiées, à l'aide du AWS CAF. Pour plus d'informations, veuillez consulter le [guide de préparation à la migration](#). La MRA est la première phase de la [stratégie de migration AWS](#).

stratégie de migration

L'approche utilisée pour migrer une charge de travail vers le AWS Cloud. Pour plus d'informations, reportez-vous aux [7 R](#) de ce glossaire et à [Mobiliser votre organisation pour accélérer les migrations à grande échelle](#).

ML

Voir [apprentissage automatique](#).

modernisation

Transformation d'une application obsolète (héritée ou monolithique) et de son infrastructure en un système agile, élastique et hautement disponible dans le cloud afin de réduire les coûts, de gagner en efficacité et de tirer parti des innovations. Pour plus d'informations, consultez [la section Stratégie de modernisation des applications dans le AWS Cloud](#).

évaluation de la préparation à la modernisation

Évaluation qui permet de déterminer si les applications d'une organisation sont prêtes à être modernisées, d'identifier les avantages, les risques et les dépendances, et qui détermine dans quelle mesure l'organisation peut prendre en charge l'état futur de ces applications. Le résultat de l'évaluation est un plan de l'architecture cible, une feuille de route détaillant les phases de développement et les étapes du processus de modernisation, ainsi qu'un plan d'action pour combler les lacunes identifiées. Pour plus d'informations, consultez la section [Évaluation de l'état de préparation à la modernisation des applications dans le AWS Cloud](#).

applications monolithiques (monolithes)

Applications qui s'exécutent en tant que service unique avec des processus étroitement couplés. Les applications monolithiques ont plusieurs inconvénients. Si une fonctionnalité de l'application connaît un pic de demande, l'architecture entière doit être mise à l'échelle. L'ajout ou l'amélioration des fonctionnalités d'une application monolithique devient également plus complexe lorsque la base de code s'élargit. Pour résoudre ces problèmes, vous pouvez utiliser une architecture de microservices. Pour plus d'informations, veuillez consulter [Decomposing monoliths into microservices](#).

MPA

Voir [Évaluation du portefeuille de migration](#).

MQTT

Voir [Message Queuing Telemetry Transport](#).

classification multi-classes

Processus qui permet de générer des prédictions pour plusieurs classes (prédiction d'un résultat parmi plus de deux). Par exemple, un modèle de ML peut demander « Ce produit est-il un livre, une voiture ou un téléphone ? » ou « Quelle catégorie de produits intéresse le plus ce client ? ».

infrastructure mutable

Modèle qui met à jour et modifie l'infrastructure existante pour les charges de travail de production. Pour améliorer la cohérence, la fiabilité et la prévisibilité, le AWS Well-Architected Framework recommande l'utilisation [d'une infrastructure immuable comme](#) meilleure pratique.

O

OAC

Voir [Contrôle d'accès à l'origine](#).

OAI

Voir [l'identité d'accès à l'origine](#).

OCM

Voir [gestion du changement organisationnel](#).

migration hors ligne

Méthode de migration dans laquelle la charge de travail source est supprimée au cours du processus de migration. Cette méthode implique un temps d'arrêt prolongé et est généralement utilisée pour de petites charges de travail non critiques.

OI

Consultez la section [Intégration des opérations](#).

OLA

Voir l'accord [au niveau opérationnel](#).

migration en ligne

Méthode de migration dans laquelle la charge de travail source est copiée sur le système cible sans être mise hors ligne. Les applications connectées à la charge de travail peuvent continuer à fonctionner pendant la migration. Cette méthode implique un temps d'arrêt nul ou minimal et est généralement utilisée pour les charges de travail de production critiques.

OPC-UA

Voir [Open Process Communications - Architecture unifiée](#).

Communications par processus ouvert - Architecture unifiée (OPC-UA)

Un protocole de communication machine-to-machine (M2M) pour l'automatisation industrielle. L'OPC-UA fournit une norme d'interopérabilité avec des schémas de cryptage, d'authentification et d'autorisation des données.

accord au niveau opérationnel (OLA)

Accord qui précise ce que les groupes informatiques fonctionnels s'engagent à fournir les uns aux autres, afin de prendre en charge un contrat de niveau de service (SLA).

examen de l'état de préparation opérationnelle (ORR)

Une liste de questions et de bonnes pratiques associées qui vous aident à comprendre, à évaluer, à prévenir ou à réduire l'ampleur des incidents et des défaillances possibles. Pour plus d'informations, voir [Operational Readiness Reviews \(ORR\)](#) dans le AWS Well-Architected Framework.

technologie opérationnelle (OT)

Systèmes matériels et logiciels qui fonctionnent avec l'environnement physique pour contrôler les opérations, les équipements et les infrastructures industriels. Dans le secteur manufacturier, l'intégration des systèmes OT et des technologies de l'information (IT) est au cœur des transformations de [l'industrie 4.0](#).

intégration des opérations (OI)

Processus de modernisation des opérations dans le cloud, qui implique la planification de la préparation, l'automatisation et l'intégration. Pour en savoir plus, veuillez consulter le [guide d'intégration des opérations](#).

journal de suivi d'organisation

Un parcours créé par AWS CloudTrail qui enregistre tous les événements pour tous les membres Comptes AWS d'une organisation dans AWS Organizations. Ce journal de suivi est créé dans chaque Compte AWS qui fait partie de l'organisation et suit l'activité de chaque compte. Pour plus d'informations, consultez [la section Création d'un suivi pour une organisation](#) dans la CloudTrail documentation.

gestion du changement organisationnel (OCM)

Cadre pour gérer les transformations métier majeures et perturbatrices du point de vue des personnes, de la culture et du leadership. L'OCM aide les organisations à se préparer et à effectuer la transition vers de nouveaux systèmes et de nouvelles politiques en accélérant

l'adoption des changements, en abordant les problèmes de transition et en favorisant des changements culturels et organisationnels. Dans la stratégie de AWS migration, ce cadre est appelé accélération du personnel, en raison de la rapidité du changement requise dans les projets d'adoption du cloud. Pour plus d'informations, veuillez consulter le [guide OCM](#).

contrôle d'accès d'origine (OAC)

Dans CloudFront, une option améliorée pour restreindre l'accès afin de sécuriser votre contenu Amazon Simple Storage Service (Amazon S3). L'OAC prend en charge tous les compartiments S3 dans leur ensemble Régions AWS, le chiffrement côté serveur avec AWS KMS (SSE-KMS) et les requêtes dynamiques PUT adressées au compartiment S3. DELETE

identité d'accès d'origine (OAI)

Dans CloudFront, une option permettant de restreindre l'accès afin de sécuriser votre contenu Amazon S3. Lorsque vous utilisez OAI, il CloudFront crée un principal auprès duquel Amazon S3 peut s'authentifier. Les principaux authentifiés peuvent accéder au contenu d'un compartiment S3 uniquement via une distribution spécifique CloudFront . Voir également [OAC](#), qui fournit un contrôle d'accès plus précis et amélioré.

ORR

Voir l'[examen de l'état de préparation opérationnelle](#).

DE

Voir [technologie opérationnelle](#).

VPC sortant (de sortie)

Dans une architecture AWS multi-comptes, un VPC qui gère les connexions réseau initiées depuis une application. L'[architecture AWS de référence de sécurité](#) recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

P

limite des autorisations

Politique de gestion IAM attachée aux principaux IAM pour définir les autorisations maximales que peut avoir l'utilisateur ou le rôle. Pour plus d'informations, veuillez consulter la rubrique [Limites des autorisations](#) dans la documentation IAM.

informations personnelles identifiables (PII)

Informations qui, lorsqu'elles sont consultées directement ou associées à d'autres données connexes, peuvent être utilisées pour déduire raisonnablement l'identité d'une personne. Les exemples d'informations personnelles incluent les noms, les adresses et les informations de contact.

PII

Voir les [informations personnelles identifiables](#).

manuel stratégique

Ensemble d'étapes prédéfinies qui capturent le travail associé aux migrations, comme la fourniture de fonctions d'opérations de base dans le cloud. Un manuel stratégique peut revêtir la forme de scripts, de runbooks automatisés ou d'un résumé des processus ou des étapes nécessaires au fonctionnement de votre environnement modernisé.

PLC

Voir [contrôleur logique programmable](#).

PLM

Consultez la section [Gestion du cycle de vie des produits](#).

policy

Objet capable de définir les autorisations (voir la [politique basée sur l'identité](#)), de spécifier les conditions d'accès (voir la [politique basée sur les ressources](#)) ou de définir les autorisations maximales pour tous les comptes d'une organisation dans AWS Organizations (voir la politique de contrôle des [services](#)).

persistance polyglotte

Choix indépendant de la technologie de stockage de données d'un microservice en fonction des modèles d'accès aux données et d'autres exigences. Si vos microservices utilisent la même technologie de stockage de données, ils peuvent rencontrer des difficultés d'implémentation ou présenter des performances médiocres. Les microservices sont plus faciles à mettre en œuvre, atteignent de meilleures performances, ainsi qu'une meilleure capacité de mise à l'échelle s'ils utilisent l'entrepôt de données le mieux adapté à leurs besoins.

évaluation du portefeuille

Processus de découverte, d'analyse et de priorisation du portefeuille d'applications afin de planifier la migration. Pour plus d'informations, veuillez consulter [Evaluating migration readiness](#).

predicate

Une condition de requête qui renvoie `true` ou `false`, généralement située dans une `WHERE` clause.

prédicat pushdown

Technique d'optimisation des requêtes de base de données qui filtre les données de la requête avant le transfert. Cela réduit la quantité de données qui doivent être extraites et traitées à partir de la base de données relationnelle et améliore les performances des requêtes.

contrôle préventif

Contrôle de sécurité conçu pour empêcher qu'un événement ne se produise. Ces contrôles constituent une première ligne de défense pour empêcher tout accès non autorisé ou toute modification indésirable de votre réseau. Pour plus d'informations, veuillez consulter [Preventative controls](#) dans *Implementing security controls on AWS*.

principal

Entité AWS capable d'effectuer des actions et d'accéder aux ressources. Cette entité est généralement un utilisateur root pour un Compte AWS rôle IAM ou un utilisateur. Pour plus d'informations, veuillez consulter la rubrique Principal dans [Termes et concepts relatifs aux rôles](#), dans la documentation IAM.

confidentialité dès la conception

Une approche d'ingénierie système qui prend en compte la confidentialité tout au long du processus de développement.

zones hébergées privées

Conteneur contenant des informations sur la manière dont vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines au sein d'un ou de plusieurs VPCs domaines. Pour plus d'informations, veuillez consulter [Working with private hosted zones](#) dans la documentation Route 53.

contrôle proactif

[Contrôle de sécurité](#) conçu pour empêcher le déploiement de ressources non conformes. Ces contrôles analysent les ressources avant qu'elles ne soient provisionnées. Si la ressource n'est pas conforme au contrôle, elle n'est pas provisionnée. Pour plus d'informations, consultez le [guide de référence sur les contrôles](#) dans la AWS Control Tower documentation et consultez la section [Contrôles proactifs dans Implémentation](#) des contrôles de sécurité sur AWS.

gestion du cycle de vie des produits (PLM)

Gestion des données et des processus d'un produit tout au long de son cycle de vie, depuis la conception, le développement et le lancement, en passant par la croissance et la maturité, jusqu'au déclin et au retrait.

environnement de production

Voir [environnement](#).

contrôleur logique programmable (PLC)

Dans le secteur manufacturier, un ordinateur hautement fiable et adaptable qui surveille les machines et automatise les processus de fabrication.

chaînage rapide

Utiliser le résultat d'une invite [LLM](#) comme entrée pour l'invite suivante afin de générer de meilleures réponses. Cette technique est utilisée pour décomposer une tâche complexe en sous-tâches ou pour affiner ou développer de manière itérative une réponse préliminaire. Cela permet d'améliorer la précision et la pertinence des réponses d'un modèle et permet d'obtenir des résultats plus précis et personnalisés.

pseudonymisation

Processus de remplacement des identifiants personnels dans un ensemble de données par des valeurs fictives. La pseudonymisation peut contribuer à protéger la vie privée. Les données pseudonymisées sont toujours considérées comme des données personnelles.

publish/subscribe (pub/sub)

Modèle qui permet des communications asynchrones entre les microservices afin d'améliorer l'évolutivité et la réactivité. Par exemple, dans un [MES](#) basé sur des microservices, un microservice peut publier des messages d'événements sur un canal auquel d'autres microservices peuvent s'abonner. Le système peut ajouter de nouveaux microservices sans modifier le service de publication.

Q

plan de requête

Série d'étapes, telles que des instructions, utilisées pour accéder aux données d'un système de base de données relationnelle SQL.

régression du plan de requêtes

Le cas où un optimiseur de service de base de données choisit un plan moins optimal qu'avant une modification donnée de l'environnement de base de données. Cela peut être dû à des changements en termes de statistiques, de contraintes, de paramètres d'environnement, de liaisons de paramètres de requêtes et de mises à jour du moteur de base de données.

R

Matrice RACI

Voir [responsable, responsable, consulté, informé \(RACI\)](#).

RAG

Voir [Retrieval Augmented Generation](#).

rançongiciel

Logiciel malveillant conçu pour bloquer l'accès à un système informatique ou à des données jusqu'à ce qu'un paiement soit effectué.

Matrice RASCI

Voir [responsable, responsable, consulté, informé \(RACI\)](#).

RCAC

Voir [contrôle d'accès aux lignes et aux colonnes](#).

réplica en lecture

Copie d'une base de données utilisée en lecture seule. Vous pouvez acheminer les requêtes vers le réplica de lecture pour réduire la charge sur votre base de données principale.

réarchitecte

Voir [7 Rs](#).

objectif de point de récupération (RPO)

Durée maximale acceptable depuis le dernier point de récupération des données. Il détermine ce qui est considéré comme étant une perte de données acceptable entre le dernier point de reprise et l'interruption du service.

objectif de temps de récupération (RTO)

Le délai maximum acceptable entre l'interruption du service et le rétablissement du service.

refactoriser

Voir [7 Rs](#).

Région

Un ensemble de AWS ressources dans une zone géographique. Chacun Région AWS est isolé et indépendant des autres pour garantir tolérance aux pannes, stabilité et résilience. Pour plus d'informations, voir [Spécifier ce que Régions AWS votre compte peut utiliser](#).

régression

Technique de ML qui prédit une valeur numérique. Par exemple, pour résoudre le problème « Quel sera le prix de vente de cette maison ? », un modèle de ML pourrait utiliser un modèle de régression linéaire pour prédire le prix de vente d'une maison sur la base de faits connus à son sujet (par exemple, la superficie en mètres carrés).

réhéberger

Voir [7 Rs](#).

version

Dans un processus de déploiement, action visant à promouvoir les modifications apportées à un environnement de production.

déplacer

Voir [7 Rs](#).

replateforme

Voir [7 Rs](#).

rachat

Voir [7 Rs](#).

résilience

La capacité d'une application à résister aux perturbations ou à s'en remettre. [La haute disponibilité et la reprise après sinistre](#) sont des considérations courantes lors de la planification de la résilience dans le AWS Cloud. Pour plus d'informations, consultez [AWS Cloud Résilience](#).

politique basée sur les ressources

Politique attachée à une ressource, comme un compartiment Amazon S3, un point de terminaison ou une clé de chiffrement. Ce type de politique précise les principaux auxquels l'accès est autorisé, les actions prises en charge et toutes les autres conditions qui doivent être remplies.

matrice responsable, redevable, consulté et informé (RACI)

Une matrice qui définit les rôles et les responsabilités de toutes les parties impliquées dans les activités de migration et les opérations cloud. Le nom de la matrice est dérivé des types de responsabilité définis dans la matrice : responsable (R), responsable (A), consulté (C) et informé (I). Le type de support (S) est facultatif. Si vous incluez le support, la matrice est appelée matrice RASCI, et si vous l'excluez, elle est appelée matrice RACI.

contrôle réactif

Contrôle de sécurité conçu pour permettre de remédier aux événements indésirables ou aux écarts par rapport à votre référence de sécurité. Pour plus d'informations, veuillez consulter la rubrique [Responsive controls](#) dans *Implementing security controls on AWS*.

retain

Voir [7 Rs](#).

se retirer

Voir [7 Rs](#).

Génération augmentée de récupération (RAG)

Technologie d'[IA générative](#) dans laquelle un [LLM](#) fait référence à une source de données faisant autorité qui se trouve en dehors de ses sources de données de formation avant de générer une réponse. Par exemple, un modèle RAG peut effectuer une recherche sémantique dans la base de connaissances ou dans les données personnalisées d'une organisation. Pour plus d'informations, voir [Qu'est-ce que RAG ?](#)

rotation

Processus de mise à jour périodique d'un [secret](#) pour empêcher un attaquant d'accéder aux informations d'identification.

contrôle d'accès aux lignes et aux colonnes (RCAC)

Utilisation d'expressions SQL simples et flexibles dotées de règles d'accès définies. Le RCAC comprend des autorisations de ligne et des masques de colonnes.

RPO

Voir l'[objectif du point de récupération](#).

RTO

Voir l'[objectif en matière de temps de rétablissement](#).

runbook

Ensemble de procédures manuelles ou automatisées nécessaires à l'exécution d'une tâche spécifique. Elles visent généralement à rationaliser les opérations ou les procédures répétitives présentant des taux d'erreur élevés.

S

SAML 2.0

Un standard ouvert utilisé par de nombreux fournisseurs d'identité (IdPs). Cette fonctionnalité permet l'authentification unique fédérée (SSO), afin que les utilisateurs puissent se connecter AWS Management Console ou appeler les opérations de l' AWS API sans que vous ayez à créer un utilisateur dans IAM pour tous les membres de votre organisation. Pour plus d'informations sur la fédération SAML 2.0, veuillez consulter [À propos de la fédération SAML 2.0](#) dans la documentation IAM.

SCADA

Voir [Contrôle de supervision et acquisition de données](#).

SCP

Voir la [politique de contrôle des services](#).

secret

Dans AWS Secrets Manager des informations confidentielles ou restreintes, telles qu'un mot de passe ou des informations d'identification utilisateur, que vous stockez sous forme cryptée. Il comprend la valeur secrète et ses métadonnées. La valeur secrète peut être binaire, une chaîne unique ou plusieurs chaînes. Pour plus d'informations, voir [Que contient le secret d'un Secrets Manager ?](#) dans la documentation de Secrets Manager.

sécurité dès la conception

Une approche d'ingénierie système qui prend en compte la sécurité tout au long du processus de développement.

contrôle de sécurité

Barrière de protection technique ou administrative qui empêche, détecte ou réduit la capacité d'un assaillant d'exploiter une vulnérabilité de sécurité. Il existe quatre principaux types de contrôles de sécurité : [préventifs](#), [détectifs](#), [réactifs](#) et [proactifs](#).

renforcement de la sécurité

Processus qui consiste à réduire la surface d'attaque pour la rendre plus résistante aux attaques. Cela peut inclure des actions telles que la suppression de ressources qui ne sont plus requises, la mise en œuvre des bonnes pratiques de sécurité consistant à accorder le moindre privilège ou la désactivation de fonctionnalités inutiles dans les fichiers de configuration.

système de gestion des informations et des événements de sécurité (SIEM)

Outils et services qui associent les systèmes de gestion des informations de sécurité (SIM) et de gestion des événements de sécurité (SEM). Un système SIEM collecte, surveille et analyse les données provenant de serveurs, de réseaux, d'appareils et d'autres sources afin de détecter les menaces et les failles de sécurité, mais aussi de générer des alertes.

automatisation des réponses de sécurité

Action prédéfinie et programmée conçue pour répondre automatiquement à un événement de sécurité ou y remédier. Ces automatisations servent de contrôles de sécurité [détectifs](#) ou [réactifs](#) qui vous aident à mettre en œuvre les meilleures pratiques en matière AWS de sécurité. Parmi les actions de réponse automatique, citons la modification d'un groupe de sécurité VPC, l'application de correctifs à une instance Amazon EC2 ou la rotation des informations d'identification.

chiffrement côté serveur

Chiffrement des données à destination, par celui Service AWS qui les reçoit.

Politique de contrôle des services (SCP)

Politique qui fournit un contrôle centralisé des autorisations pour tous les comptes d'une organisation dans AWS Organizations. SCPs définissent des garde-fous ou des limites aux actions qu'un administrateur peut déléguer à des utilisateurs ou à des rôles. Vous pouvez les utiliser SCPs comme listes d'autorisation ou de refus pour spécifier les services ou les actions autorisés ou interdits. Pour plus d'informations, consultez la section [Politiques de contrôle des services](#) dans la AWS Organizations documentation.

point de terminaison du service

URL du point d'entrée pour un Service AWS. Pour vous connecter par programmation au service cible, vous pouvez utiliser un point de terminaison. Pour plus d'informations, veuillez consulter la rubrique [Service AWS endpoints](#) dans Références générales AWS.

contrat de niveau de service (SLA)

Accord qui précise ce qu'une équipe informatique promet de fournir à ses clients, comme le temps de disponibilité et les performances des services.

indicateur de niveau de service (SLI)

Mesure d'un aspect des performances d'un service, tel que son taux d'erreur, sa disponibilité ou son débit.

objectif de niveau de service (SLO)

Mesure cible qui représente l'état d'un service, tel que mesuré par un indicateur de [niveau de service](#).

modèle de responsabilité partagée

Un modèle décrivant la responsabilité que vous partagez en matière AWS de sécurité et de conformité dans le cloud. AWS est responsable de la sécurité du cloud, alors que vous êtes responsable de la sécurité dans le cloud. Pour de plus amples informations, veuillez consulter [Modèle de responsabilité partagée](#).

SIEM

Consultez les [informations de sécurité et le système de gestion des événements](#).

point de défaillance unique (SPOF)

Défaillance d'un seul composant critique d'une application susceptible de perturber le système.

SLA

Voir le contrat [de niveau de service](#).

SLI

Voir l'indicateur de [niveau de service](#).

SLO

Voir l'objectif de [niveau de service](#).

split-and-seed modèle

Modèle permettant de mettre à l'échelle et d'accélérer les projets de modernisation. Au fur et à mesure que les nouvelles fonctionnalités et les nouvelles versions de produits sont définies, l'équipe principale se divise pour créer des équipes de produit. Cela permet de mettre à l'échelle les capacités et les services de votre organisation, d'améliorer la productivité des développeurs et de favoriser une innovation rapide. Pour plus d'informations, voir [Approche progressive de la modernisation des applications dans](#) le AWS Cloud

SPOF

Voir [point de défaillance unique](#).

schéma en étoile

Structure organisationnelle de base de données qui utilise une grande table de faits pour stocker les données transactionnelles ou mesurées et utilise une ou plusieurs tables dimensionnelles plus petites pour stocker les attributs des données. Cette structure est conçue pour être utilisée dans un [entrepôt de données](#) ou à des fins de business intelligence.

modèle de figuier étrangleur

Approche de modernisation des systèmes monolithiques en réécrivant et en remplaçant progressivement les fonctionnalités du système jusqu'à ce que le système hérité puisse être mis hors service. Ce modèle utilise l'analogie d'un figuier de vigne qui se développe dans un arbre existant et qui finit par supplanter son hôte. Le schéma a été [présenté par Martin Fowler](#) comme un moyen de gérer les risques lors de la réécriture de systèmes monolithiques. Pour obtenir un exemple d'application de ce modèle, veuillez consulter [Modernizing legacy Microsoft ASP.NET \(ASMX\) web services incrementally by using containers and Amazon API Gateway](#).

sous-réseau

Plage d'adresses IP dans votre VPC. Un sous-réseau doit se trouver dans une seule zone de disponibilité.

contrôle de supervision et acquisition de données (SCADA)

Dans le secteur manufacturier, un système qui utilise du matériel et des logiciels pour surveiller les actifs physiques et les opérations de production.

chiffrement symétrique

Algorithme de chiffrement qui utilise la même clé pour chiffrer et déchiffrer les données.

tests synthétiques

Tester un système de manière à simuler les interactions des utilisateurs afin de détecter les problèmes potentiels ou de surveiller les performances. Vous pouvez utiliser [Amazon CloudWatch Synthetics](#) pour créer ces tests.

invite du système

Technique permettant de fournir un contexte, des instructions ou des directives à un [LLM](#) afin d'orienter son comportement. Les instructions du système aident à définir le contexte et à établir des règles pour les interactions avec les utilisateurs.

T

tags

Des paires clé-valeur qui agissent comme des métadonnées pour organiser vos AWS ressources. Les balises peuvent vous aider à gérer, identifier, organiser, rechercher et filtrer des ressources. Pour plus d'informations, veuillez consulter la rubrique [Balisage de vos AWS ressources](#).

variable cible

La valeur que vous essayez de prédire dans le cadre du ML supervisé. Elle est également qualifiée de variable de résultat. Par exemple, dans un environnement de fabrication, la variable cible peut être un défaut du produit.

liste de tâches

Outil utilisé pour suivre les progrès dans un runbook. Liste de tâches qui contient une vue d'ensemble du runbook et une liste des tâches générales à effectuer. Pour chaque tâche générale, elle inclut le temps estimé nécessaire, le propriétaire et l'avancement.

environnement de test

Voir [environnement](#).

entraînement

Pour fournir des données à partir desquelles votre modèle de ML peut apprendre. Les données d'entraînement doivent contenir la bonne réponse. L'algorithme d'apprentissage identifie des modèles dans les données d'entraînement, qui mettent en correspondance les attributs des données d'entrée avec la cible (la réponse que vous souhaitez prédire). Il fournit un modèle de ML

qui capture ces modèles. Vous pouvez alors utiliser le modèle de ML pour obtenir des prédictions sur de nouvelles données pour lesquelles vous ne connaissez pas la cible.

passerelle de transit

Un hub de transit réseau que vous pouvez utiliser pour interconnecter vos réseaux VPCs et ceux sur site. Pour plus d'informations, voir [Qu'est-ce qu'une passerelle de transit](#) dans la AWS Transit Gateway documentation.

flux de travail basé sur jonction

Approche selon laquelle les développeurs génèrent et testent des fonctionnalités localement dans une branche de fonctionnalités, puis fusionnent ces modifications dans la branche principale. La branche principale est ensuite intégrée aux environnements de développement, de préproduction et de production, de manière séquentielle.

accès sécurisé

Accorder des autorisations à un service que vous spécifiez pour effectuer des tâches au sein de votre organisation AWS Organizations et dans ses comptes en votre nom. Le service de confiance crée un rôle lié au service dans chaque compte, lorsque ce rôle est nécessaire, pour effectuer des tâches de gestion à votre place. Pour plus d'informations, consultez la section [Utilisation AWS Organizations avec d'autres AWS services](#) dans la AWS Organizations documentation.

réglage

Pour modifier certains aspects de votre processus d'entraînement afin d'améliorer la précision du modèle de ML. Par exemple, vous pouvez entraîner le modèle de ML en générant un ensemble d'étiquetage, en ajoutant des étiquettes, puis en répétant ces étapes plusieurs fois avec différents paramètres pour optimiser le modèle.

équipe de deux pizzas

Une petite DevOps équipe que vous pouvez nourrir avec deux pizzas. Une équipe de deux pizzas garantit les meilleures opportunités de collaboration possible dans le développement de logiciels.

U

incertitude

Un concept qui fait référence à des informations imprécises, incomplètes ou inconnues susceptibles de compromettre la fiabilité des modèles de ML prédictifs. Il existe deux types

d'incertitude : l'incertitude épistémique est causée par des données limitées et incomplètes, alors que l'incertitude aléatoire est causée par le bruit et le caractère aléatoire inhérents aux données.

tâches indifférenciées

Également connu sous le nom de « levage de charges lourdes », ce travail est nécessaire pour créer et exploiter une application, mais qui n'apporte pas de valeur directe à l'utilisateur final ni d'avantage concurrentiel. Les exemples de tâches indifférenciées incluent l'approvisionnement, la maintenance et la planification des capacités.

environnements supérieurs

Voir [environnement](#).

V

mise à vide

Opération de maintenance de base de données qui implique un nettoyage après des mises à jour incrémentielles afin de récupérer de l'espace de stockage et d'améliorer les performances.

contrôle de version

Processus et outils permettant de suivre les modifications, telles que les modifications apportées au code source dans un référentiel.

Appairage de VPC

Une connexion entre deux VPCs qui vous permet d'acheminer le trafic en utilisant des adresses IP privées. Pour plus d'informations, veuillez consulter la rubrique [Qu'est-ce que l'appairage de VPC ?](#) dans la documentation Amazon VPC.

vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

W

cache actif

Cache tampon qui contient les données actuelles et pertinentes fréquemment consultées. L'instance de base de données peut lire à partir du cache tampon, ce qui est plus rapide que la lecture à partir de la mémoire principale ou du disque.

données chaudes

Données rarement consultées. Lorsque vous interrogez ce type de données, des requêtes modérément lentes sont généralement acceptables.

fonction de fenêtre

Fonction SQL qui effectue un calcul sur un groupe de lignes liées d'une manière ou d'une autre à l'enregistrement en cours. Les fonctions de fenêtre sont utiles pour traiter des tâches, telles que le calcul d'une moyenne mobile ou l'accès à la valeur des lignes en fonction de la position relative de la ligne en cours.

charge de travail

Ensemble de ressources et de code qui fournit une valeur métier, par exemple une application destinée au client ou un processus de backend.

flux de travail

Groupes fonctionnels d'un projet de migration chargés d'un ensemble de tâches spécifique. Chaque flux de travail est indépendant, mais prend en charge les autres flux de travail du projet. Par exemple, le flux de travail du portefeuille est chargé de prioriser les applications, de planifier les vagues et de collecter les métadonnées de migration. Le flux de travail du portefeuille fournit ces actifs au flux de travail de migration, qui migre ensuite les serveurs et les applications.

VER

Voir [écrire une fois, lire plusieurs](#).

WQF

Voir le [cadre AWS de qualification de la charge](#) de travail.

écrire une fois, lire plusieurs (WORM)

Modèle de stockage qui écrit les données une seule fois et empêche leur suppression ou leur modification. Les utilisateurs autorisés peuvent lire les données autant de fois que nécessaire, mais ils ne peuvent pas les modifier. Cette infrastructure de stockage de données est considérée comme [immuable](#).

Z

exploit Zero-Day

Une attaque, généralement un logiciel malveillant, qui tire parti d'une [vulnérabilité de type « jour zéro »](#).

vulnérabilité « jour zéro »

Une faille ou une vulnérabilité non atténuée dans un système de production. Les acteurs malveillants peuvent utiliser ce type de vulnérabilité pour attaquer le système. Les développeurs prennent souvent conscience de la vulnérabilité à la suite de l'attaque.

invite Zero-Shot

Fournir à un [LLM](#) des instructions pour effectuer une tâche, mais aucun exemple (plans) pouvant aider à la guider. Le LLM doit utiliser ses connaissances pré-entraînées pour gérer la tâche. L'efficacité de l'invite zéro dépend de la complexité de la tâche et de la qualité de l'invite. Voir également les instructions [en quelques clics](#).

application zombie

Application dont l'utilisation moyenne du processeur et de la mémoire est inférieure à 5 %. Dans un projet de migration, il est courant de retirer ces applications.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.