HashiCorp

Mise en œuvre d'un modèle opérationnel cloud

Parvenir le plus rapidement à créer de la valeur dans un datacenter multi-cloud moderne

Résumé

Le moment est venu de mettre le cloud à profit. Pour prospérer dans une ère d'architecture multi-cloud, stimulée par la transformation digitale, l'informatique d'entreprise doit abandonner les processus ITIL afin de mettre en place des systèmes en libre-service pour l'excellence DevOps.

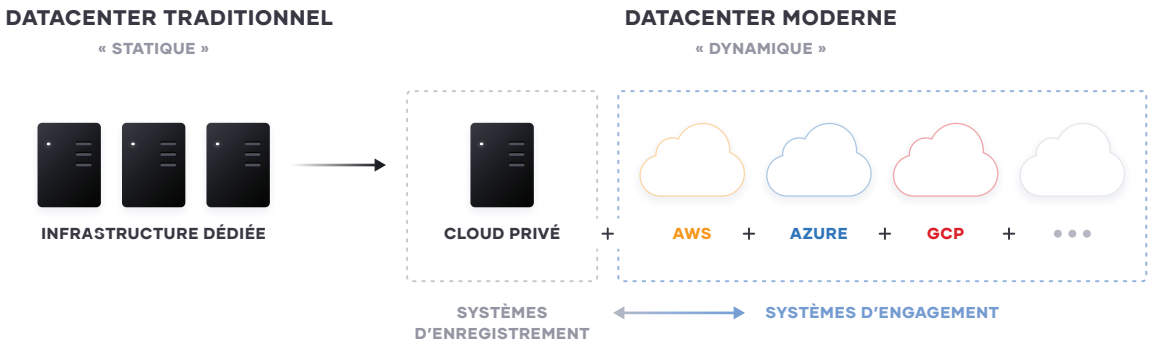
Pour la plupart des entreprises, les efforts de transformation digitale ont comme moteur d'offrir une plus grande valeur aux clients et au business, et cela à une très grande échelle. L'implication pour l'informatique d'entreprise est alors un passage de l'optimisation des coûts à l'optimisation de la vitesse. Le cloud fait inévitablement partie de ce changement car il offre la possibilité de déployer rapidement des services à la demande avec une échelle illimitée.

Pour créer le plus rapidement de la valeur avec le cloud, les entreprises doivent réfléchir à la manière d'industrialiser le processus de mise à disposition d'applications sur chaque couche du cloud : adopter un modèle opérationnel cloud et ajuster les ressources humaines, processus et outils.

Dans ce livre blanc, nous examinons les implications du modèle opérationnel cloud et présentons des solutions pour que les équipes informatiques adoptent ce modèle à travers l'infrastructure, la sécurité, la mise en réseau et la livraison d'applications.

Transition vers un datacenter multi-cloud

La transition vers les environnements cloud et multi-cloud est une transition générationnelle pour l'informatique. Cette transition implique le passage de serveurs largement dédiés dans un datacenter privé à un ensemble de capacités de calcul disponibles à la demande. Alors que la plupart des entreprises ont commencé avec un fournisseur cloud unique, il existe de bonnes raisons d'utiliser des services auprès d'autres fournisseurs et, inévitablement, la plupart des organisations Global 2000 en utiliseront plus d'un, soit par conception, soit par le biais de fusions et acquisitions.



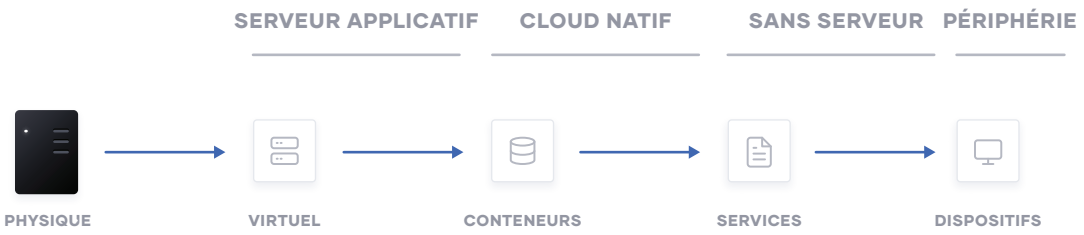
Le cloud présente une opportunité d'optimisation de la vitesse et de l'évolutivité pour les nouveaux « systèmes d'engagement », les applications conçues pour engager les clients et les utilisateurs. Ces nouvelles applications constituent l'interface principale du client pour s'engager avec une entreprise et sont parfaitement adaptées à la livraison dans le cloud, car elles ont tendance à :

- Avoir des caractéristiques d'utilisation dynamiques, avoir besoin d'ajuster les charges par ordres de grandeur pendant de courtes périodes.
- Être sous pression pour créer et itérer rapidement. Un grand nombre de ces nouveaux systèmes peuvent être éphémères, et offrir une expérience utilisateur spécifique autour d'un événement ou d'une campagne.

Pour la plupart des entreprises, ces systèmes d'engagement doivent se connecter aux « systèmes d'enregistrement » existants — les bases de données commerciales principales et les applications internes, qui continuent souvent à résider sur l'infrastructure dans les datacenters existants. En conséquence, les entreprises finissent par un ensemble hybride, un mélange de multiples environnements cloud publics et privés.

Le défi pour la plupart des entreprises est alors la façon de livrer ces applications dans le cloud uniformément tout en garantissant le moins de friction possible entre les différentes équipes de développement.

Aggravant davantage ce défi, les primitives sous-jacentes ont évolué pour passer de la manipulation de machines virtuelles dans un environnement autonome, à la manipulation de « ressources » cloud dans un environnement partagé. Les entreprises ont ensuite des modèles opérationnels concurrents pour maintenir leur domaine existant, tout en développant la nouvelle infrastructure cloud.

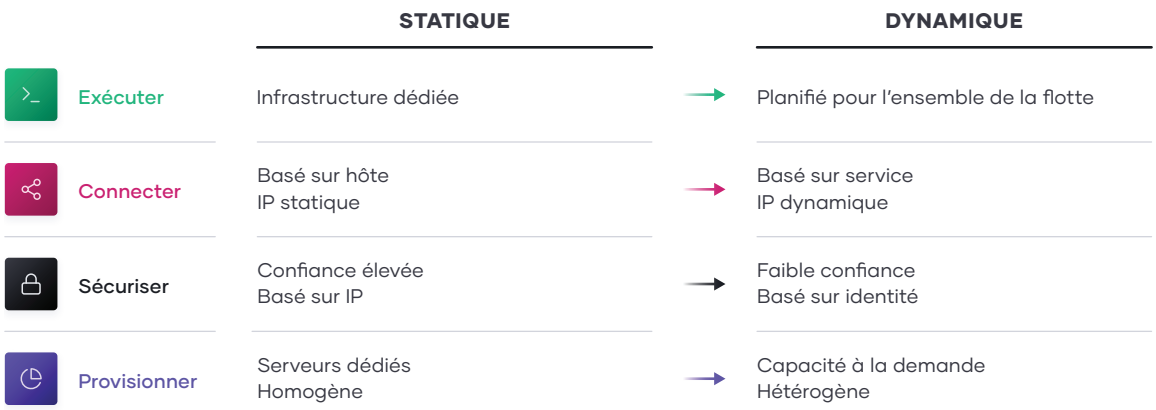


Pour le cloud computing, il doit exister des workflows uniformes qui peuvent être réutilisés à grande échelle entre plusieurs fournisseurs cloud. Cela nécessite :

- Ensembles d'instructions uniformes pour le provisionnement
- Identité pour la sécurité et les connexions réseau
- Privilèges et droits de sorte qu'ils puissent être déployés et exécutés

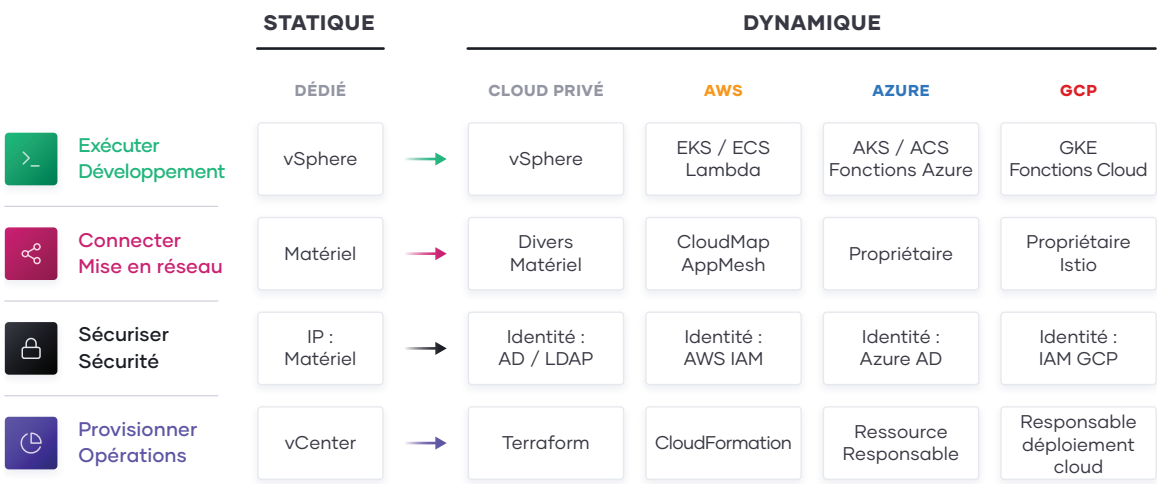
Implications du modèle opérationnel cloud

L'implication essentielle de la transition vers le cloud est le passage d'une infrastructure « statique » à une infrastructure « dynamique » : d'une focalisation sur la configuration et la gestion d'une flotte statique de ressources informatiques, au provisionnement, à la sécurisation, connexion et exécution de ressources dynamiques à la demande.



En décomposant cette implication, et en travaillant sur les différentes couches, divers changements d'approche deviennent implicites :

- **Provisionner.** La couche infrastructure passe de l'exécution de serveurs dédiés à l'évolutivité limitée vers un environnement dynamique où les organisations peuvent facilement s'adapter à une demande accrue en activant des milliers de serveurs et en s'ajustant lorsqu'ils ne sont plus utilisés. Alors que les architectures et les services deviennent plus distribués, le volume des nœuds de calcul augmente considérablement.
- **Sécuriser.** La couche de sécurité passe d'un monde fondamentalement « à forte confiance », appliquée par un périmètre et un pare-feu solides à un environnement « faible confiance » « Zero Trust » sans périmètre clair ou statique. En conséquence, l'hypothèse fondamentale de la sécurité passe d'une sécurité basée sur IP à l'utilisation d'un accès aux ressources basé sur l'identité. Ce changement est très perturbant pour les modèles de sécurité traditionnels.
- **Connecter.** La couche réseau passe d'une grande dépendance à l'emplacement physique et à l'adresse IP des services et applications à l'utilisation d'un registre dynamique des services pour la découverte, segmentation et composition. Une équipe informatique d'entreprise n'a pas le même contrôle sur le réseau, ou les emplacements physiques des ressources informatiques, et doit penser à la connectivité basée sur les services.
- **Exécuter.** La couche d'exécution passe du déploiement d'artefacts vers un serveur d'applications statique au déploiement d'applications avec un planificateur vers un ensemble d'infrastructures provisionné à la demande. De plus, de nouvelles applications sont devenues des collections de services qui sont provisionnées dynamiquement et empaquetées de plusieurs manières : cela allant des machines virtuelles aux conteneurs.



Pour relever ces défis, ces équipes doivent poser les questions suivantes :

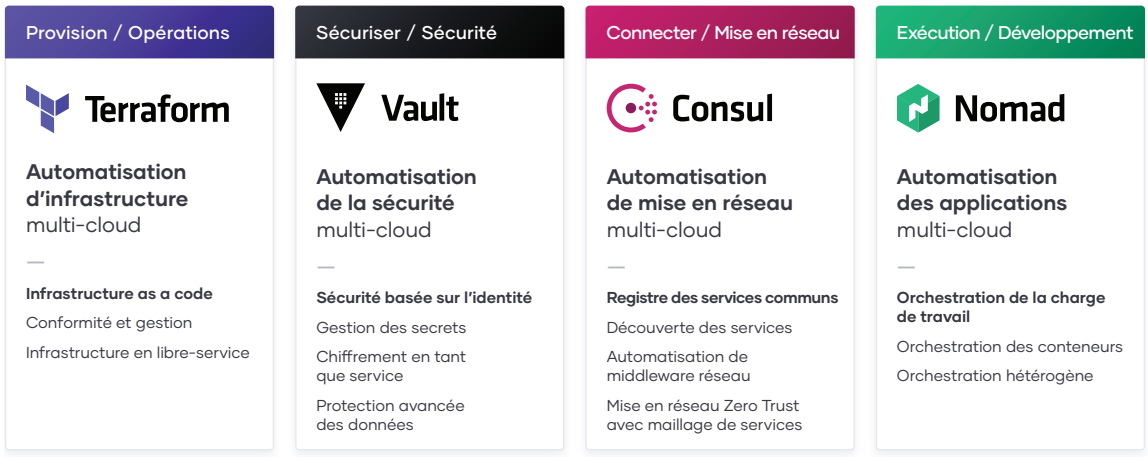
- **Personnes.** Comment pouvons-nous permettre à une équipe de travailler dans un environnement multi-cloud efficacement, où les connaissances pourraient être appliquées uniformément, quelle que soit la cible ?
- **Processus.** Comment positionner les services informatiques centraux en libre service comme accélérateur de business, plutôt qu'un frein à base de tickets, tout en maintenant la conformité et la gouvernance ?
- **Outils.** Comment pouvons-nous tirer le meilleur parti de la valeur des capacités disponibles des fournisseurs cloud dans la poursuite d'une meilleure valeur client et commerciale ?

Mise en œuvre d'un modèle opérationnel cloud

Alors que les implications du modèle opérationnel cloud ont une incidence sur les équipes en charge de l'infrastructure, de la sécurité, du réseau et des applications, nous constatons une tendance récurrente dans les entreprises à établir des services centraux partagés (centres d'excellence) afin de fournir l'infrastructure dynamique nécessaire à chaque couche pour une fourniture réussie des applications.

Alors que les équipes fournissent chaque service partagé pour le modèle opérationnel cloud, la vélocité informatique augmente. Plus la maturité du cloud est grande, plus la vitesse est rapide.

L'EXPANSION DE L'UTILISATION DE LA PILE HASHICORP ACCROÎT LA MATURITÉ ET LA VITESSE POUR NOS CLIENTS

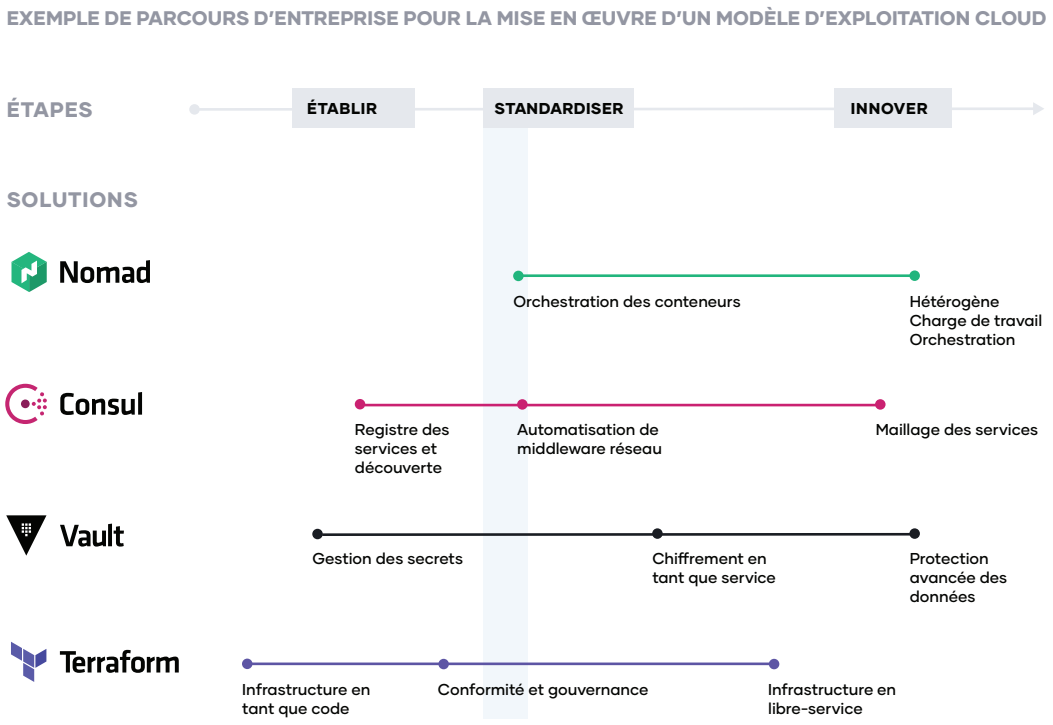


Le parcours typique que les clients ont adopté, lorsqu'ils mettent en œuvre un modèle opérationnel cloud, implique trois étapes majeures :

1. **Établir les bases cloud** – Au fur et à mesure que vous commencez votre transition vers le cloud, les exigences immédiates consistent à approvisionner l'infrastructure cloud en adoptant l'infrastructure as code et en s'assurant qu'elle est sécurisée avec une solution de gestion des secrets. Il s'agit du strict nécessaire qui vous permettra de construire une architecture cloud adaptable et véritablement dynamique qui soit évolutive.

2. **Standardiser sur un ensemble de services partagés** – Lorsque la consommation cloud commencera à prendre de l'ampleur, vous devrez mettre en œuvre et standardiser sur un ensemble de services partagés afin de tirer pleinement profit de ce que le cloud a à offrir. Cela pose également des défis concernant la gouvernance et la conformité, car la nécessité de définir des règles de contrôle d'accès et des exigences de suivi devient de plus en plus importante.

3. **Innover en utilisant une architecture logique commune** – Lorsque vous adoptez pleinement le cloud et que vous dépendez des services et applications cloud comme principaux systèmes d'engagement, il devient nécessaire de créer une architecture logique commune. Cela nécessite un control plane qui se connecte à l'écosystème étendu des solutions cloud et fournit intrinsèquement une sécurité et une orchestration avancées entre les services et les clouds multiples.

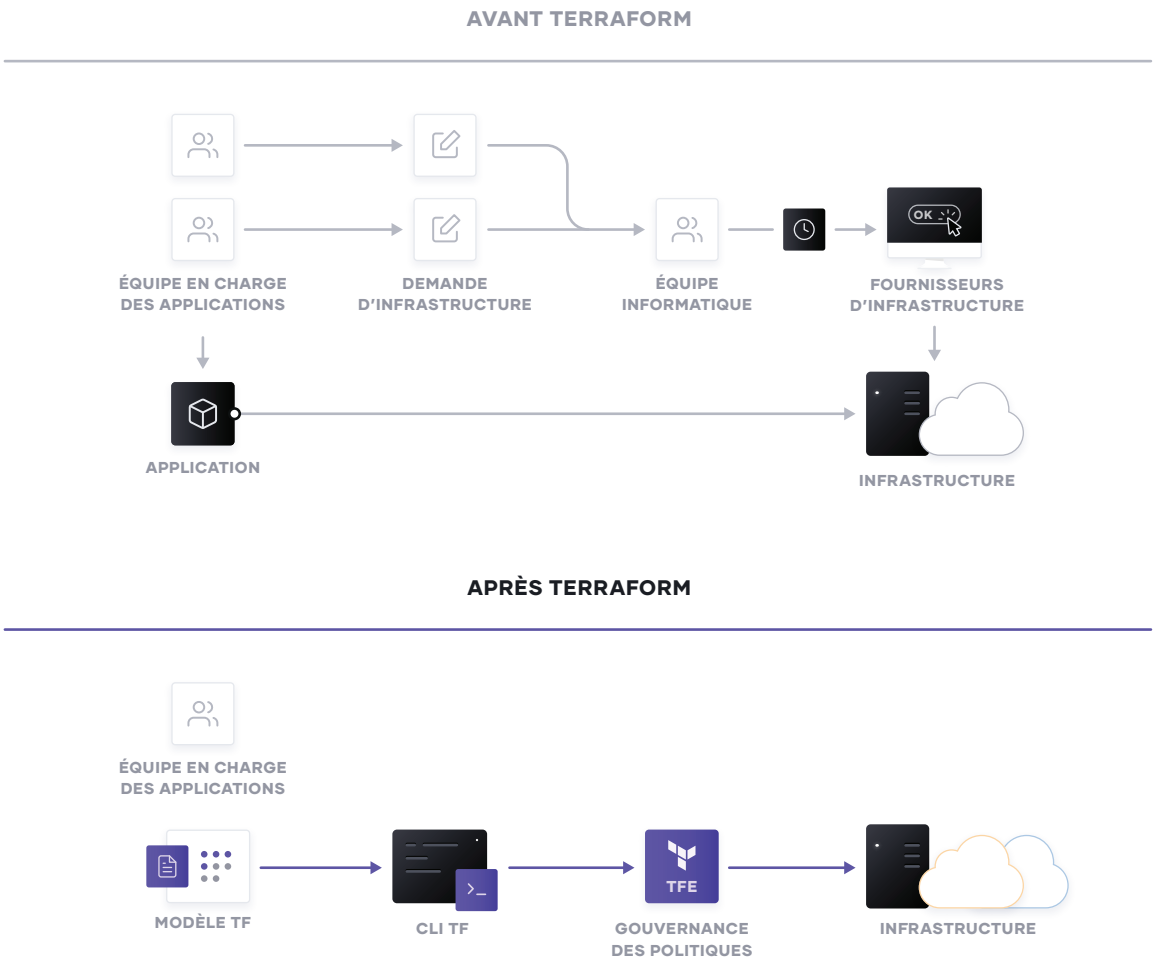


Ce qui suit est le parcours étape par étape que nous avons vu adopter avec succès par des organisations

Étape 1 : Provisionnement des infrastructures multi-cloud

La base pour l'adoption du cloud est le provisionnement de l'infrastructure. HashiCorp Terraform est le produit de provisionnement cloud le plus utilisé au monde et il peut être utilisé pour provisionner l'infrastructure pour toute application utilisant un éventail de providers pour toute plateforme cible.

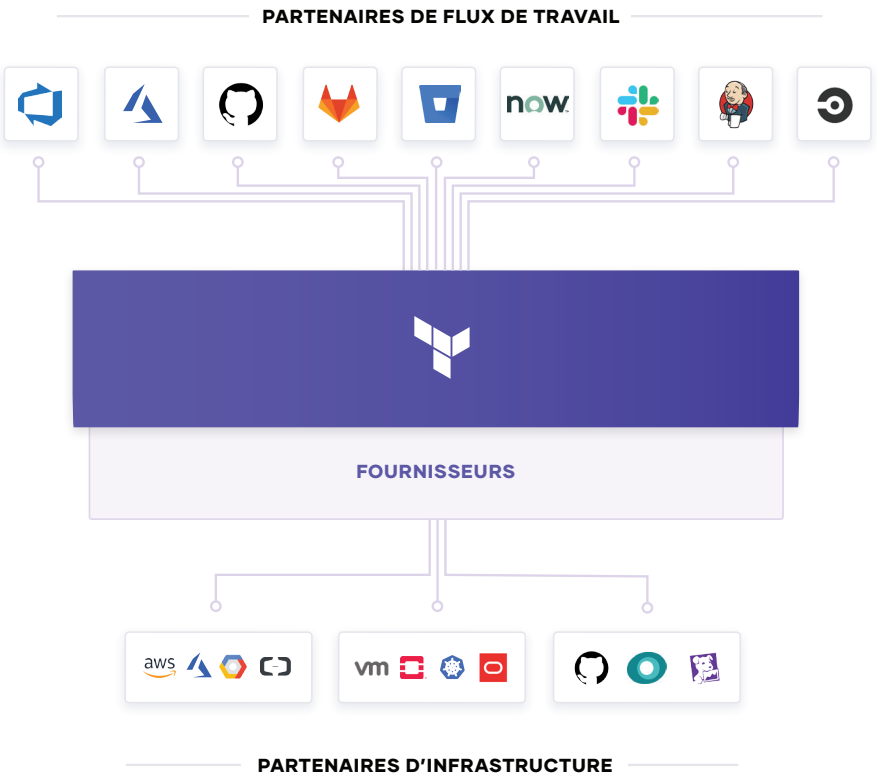
Afin d'obtenir des services partagés pour le provisionnement des infrastructures, les équipes informatiques doivent commencer par mettre en œuvre une infrastructure reproductible par le biais de l'infrastructure as code, puis y superposer les workflows de conformité et de gouvernance afin de garantir des contrôles appropriés.



Infrastructure as Code reproductible

Le premier objectif d'un service partagé pour le provisionnement des infrastructures est de permettre la livraison d'infrastructures reproductibles par le biais d'infrastructure as code, fournissant ainsi aux équipes DevOps un moyen de planifier et de provisionner des ressources dans les flux de travail CI/CD en utilisant des outils familiers.

Les équipes DevOps peuvent créer des modèles Terraform qui indiquent la configuration des services depuis une ou plusieurs plateformes cloud. Terraform s'intègre à tous les principaux outils de gestion de configuration afin de permettre un traitement granulaire fin à la suite du provisionnement des ressources sous-jacentes. Enfin, les modèles peuvent être étendus avec les services de nombreux autres fournisseurs ISV pour inclure des agents de monitoring, des systèmes de surveillance des performances applicatives (APM), des outils de sécurité, DNS et des réseaux de diffusion de contenu, etc. Une fois définis, les modèles peuvent être provisionnés ainsi que requis de manière automatisée. Ce faisant, Terraform devient la *lingua franca* et un workflow commun pour les équipes qui fournissent des ressources dans le cloud public et privé.



Pour l'informatique en libre-service, le découplage du processus de création de modèle et du processus de provisionnement réduit considérablement le temps pris pour toute application en direct, car les développeurs n'ont plus besoin d'attendre l'approbation du service en charge des opérations, tant qu'ils utilisent un modèle pré-approuvé.

Conformité et gestion

Pour la plupart des équipes, il est également nécessaire d'appliquer des politiques sur le type d'infrastructure créé, et de définir la manière dont elles sont utilisées et les équipes à utiliser. La politique Sentinel de HashiCorp en tant que framework de code assure la conformité et la gouvernance sans nécessiter de changement dans le workflow global de l'équipe, et est également définie en tant que code, permettant ainsi une meilleure collaboration et une plus grande compréhension pour les DevSecOps.

Sans policy as code, les organisations ont recours à un processus d'examen basé sur des tickets pour approuver les changements. Les développeurs attendent ainsi des semaines ou plus pour provisionner l'infrastructure et cela conduit à des goulots d'étranglement. La notion de policy as code permet de résoudre ce problème en séparant définition de la politique et exécution de la politique.

Les équipes centralisées codifient les politiques en appliquant les meilleures pratiques de sécurité, de conformité et opérationnelles pour l'ensemble du provisionnement cloud. L'application automatisée des politiques garantit que les changements sont conformes sans créer de goulot d'étranglement manuel.

Étape 2 : Sécurité multi-cloud

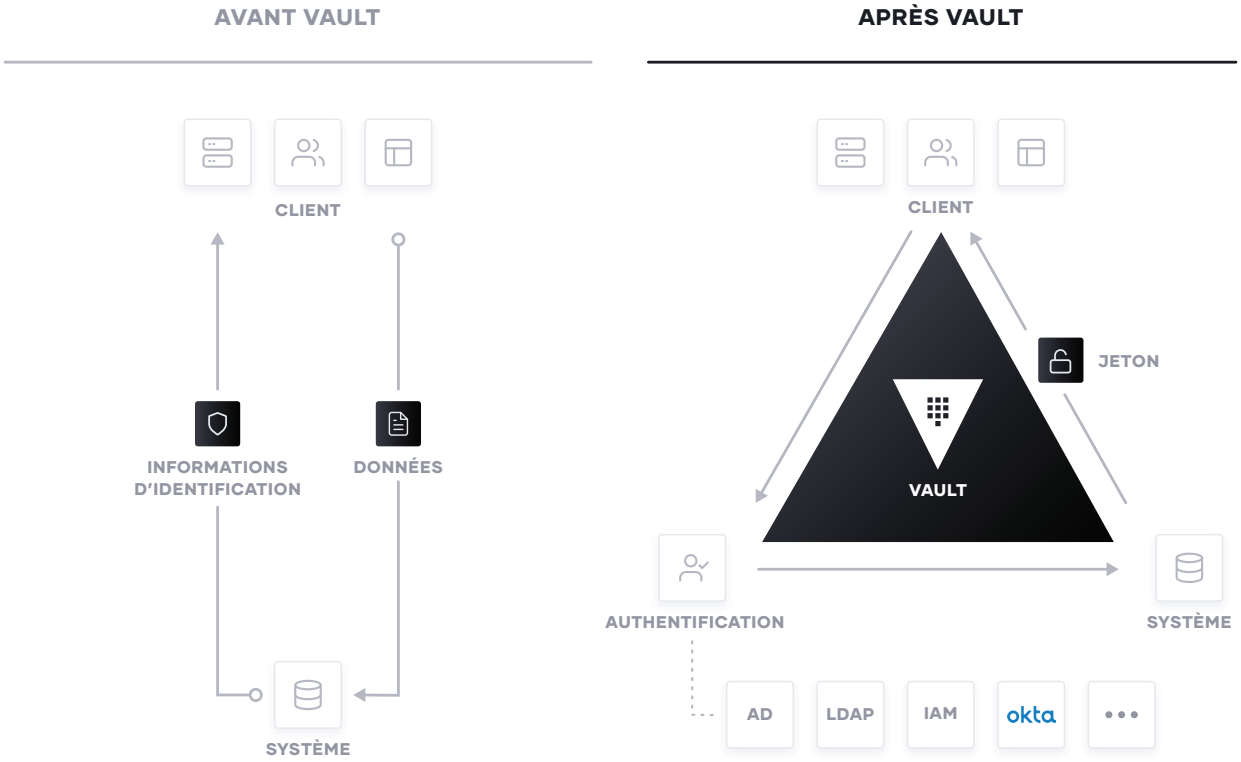
Une infrastructure cloud dynamique implique un passage d'une identité basée sur l'hôte à une identité basée sur les applications, avec des réseaux à faible confiance ou Zero Trust sur plusieurs clouds sans un périmètre réseau clair.

Dans le monde de la sécurité traditionnelle, nous avons supposé des réseaux internes à forte confiance, ce qui a entraîné un fort blindage en bordure, sans grande protection en interne. Avec l'approche moderne « Zero Trust », nous œuvrons pour renforcer également l'intérieur. Cela exige que les applications soient explicitement authentifiées, autorisées à récupérer des secrets et à effectuer des opérations sensibles, et auditées étroitement.

HashiCorp Vault permet aux équipes de stocker et de contrôler rigoureusement l'accès aux tokens, mots de passe, certificats et clés de chiffrement pour la protection des machines et des applications. Cela fournit une solution complète de gestion des secrets. Plus encore, Vault aide à protéger les données au repos et les données en transit. Vault expose une API de haut niveau à des fins cryptographiques pour permettre aux développeurs de sécuriser les données sensibles sans exposer les clés de chiffrement. Vault peut également agir comme autorité de certification, afin de fournir des certificats dynamiques à court terme pour sécuriser les communications avec SSL/TLS. Enfin, Vault permet une transmission d'identité entre différentes plateformes, telles que Active Directory sur site et AWS IAM, pour permettre aux applications de fonctionner dans les limites des plateformes.

Vault est largement utilisé, y compris dans le secteur boursier, par les grandes organisations financières, les chaînes hôtelières, et tout ce qui est entre les deux pour assurer la sécurité dans un modèle opérationnel cloud.

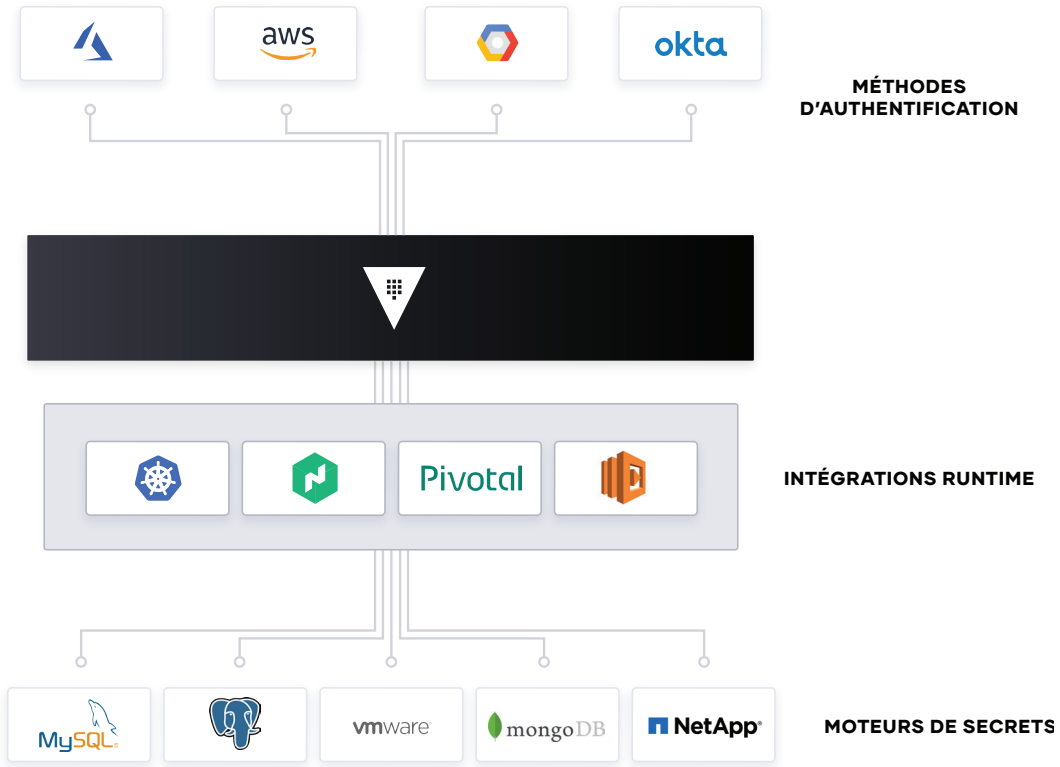
Afin de parvenir à des services partagés pour la sécurité, les équipes informatiques doivent activer des services de gestion des secrets centralisés, puis utiliser ce service pour fournir des cas d'utilisation de chiffrement en tant que service plus sophistiqués, tels que rotations de certificats et clés, et chiffrement des données en transit et au repos.



Gestion des secrets

La première étape de la sécurité cloud est généralement la gestion des secrets : stockage central, contrôle d'accès et distribution de secrets dynamique. Au lieu de se baser sur des adresses IP statiques, l'intégration avec des systèmes d'accès basés sur l'identité comme AWS IAM et Azure DAA pour l'authentification et l'accès aux services et aux ressources est cruciale.

Vault utilise des politiques pour codifier la façon dont les applications s'authentifient, les informations d'identification qu'elles sont autorisées à utiliser et la manière dont les audits doivent être effectués. Vault peut s'intégrer à un éventail de fournisseurs d'identité fiables, tels que les plateformes d'identité et de gestion d'accès (IAM) cloud, Kubernetes, Active Directory et d'autres systèmes basés sur OIDC pour l'authentification. Vault gère ensuite centralement et applique l'accès aux secrets et systèmes basés sur des sources fiables d'applications et d'identités utilisateur.



Les équipes informatiques d'entreprise doivent créer un service partagé qui permet la demande de secrets pour tout système via un workflow uniforme, audité et sécurisé.

Encryption as a Service

De plus, les entreprises doivent chiffrer les données applicatives au repos et en transit. Vault peut fournir un service d'Encrytion as a Service afin de fournir une API uniforme pour la gestion des clés et la cryptographie. Cela permet aux développeurs d'effectuer une seule intégration, puis de protéger les données dans plusieurs environnements.

Utiliser Vault comme API pour le chiffrement résout les problèmes difficiles rencontrés par les équipes de sécurité telles que la rotation des certificats et des clés. Vault permet une gestion centralisée afin de simplifier les données en transit et au repos entre les clouds et les datacenters. Cela permet de réduire les coûts au niveau des modules de sécurité matérielle coûteux (HSM) et d'augmenter la productivité avec des flux de sécurité et des normes cryptographiques uniformes dans toute l'organisation.

Bien que de nombreuses organisations fournissent un mandat aux développeurs pour chiffrer les données, elles ne fournissent pas souvent de guide ce qui laisse les développeurs construire des solutions personnalisées sans avoir une compréhension adéquate de la cryptographie. Vault offre aux développeurs une API simple qui peut être facilement utilisée, tout en offrant aux équipes de sécurité centrales les contrôles de politique et les API de gestion du cycle de vie dont elles ont besoin.

Protection avancée des données

Les organisations qui adoptent le cloud ou optent pour des environnements hybrides continuent de maintenir et de prendre en charge des services et applications sur site qui doivent effectuer des opérations cryptographiques, telles que le chiffrement des données pour le stockage au repos. Ces services ne souhaitent pas nécessairement mettre en œuvre la logique de la gestion de ces clés cryptographiques, et cherchent donc à déléguer la tâche de la gestion des clés aux fournisseurs externes. Advanced Data Protection permet aux organisations de connecter, contrôler et d'intégrer en toute sécurité les clés de chiffrement avancées, les opérations et la gestion entre l'infrastructure et Vault Enterprise, y compris la protection automatique des données dans MySQL, MongoDB, PostGresQL et d'autres bases de données utilisant le chiffrement transparent des données (TDE).

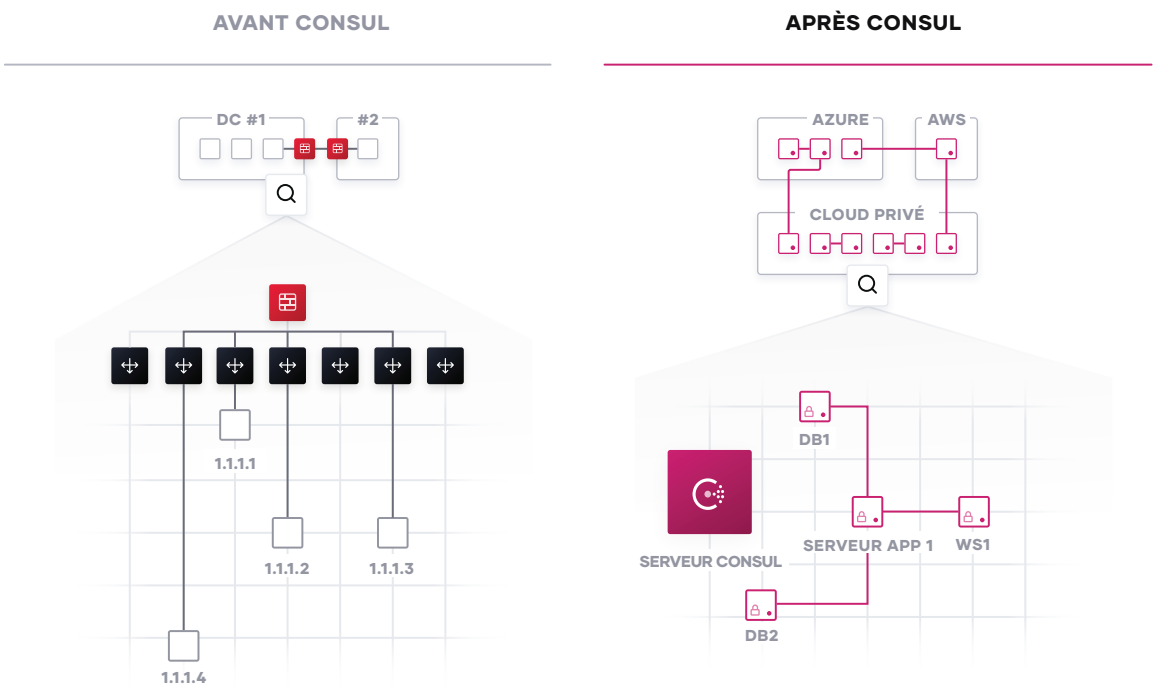
Pour les organisations ayant des exigences de sécurité élevées en matière de conformité des données (PCI DSS, HIPAA, etc.), de protection des données et de protection cryptographique des informations personnelles identifiables (ou PII), Advanced Data Protection fournit aux organisations des fonctionnalités de tokénisation des données, telles que le masquage des données, afin de protéger les données sensibles, telles que les cartes de crédit, les informations personnelles sensibles, les numéros bancaires, etc.

Étape 3 : Réseau de services multi-cloud

Les défis de la mise en réseau dans le cloud sont souvent l'un des aspects les plus difficiles de l'adoption d'un modèle opérationnel cloud pour les entreprises. L'association d'adresses IP dynamiques, une croissance significative du trafic est-ouest au fur et à mesure qu'un modèle de microservices est adopté, et l'absence d'un périmètre réseau clair constituent un défi énorme.

HashiCorp Consul fournit une couche réseau de services multi-cloud pour connecter et sécuriser les services. Consul est un produit largement déployé, avec de nombreux clients qui exécutent bien plus de 100 000 nœuds dans leurs environnements.

Les services de mise en réseau doivent être fournis de manière centralisée, avec les équipes informatiques fournissant des capacités de services et de découverte de services. Le fait d'avoir un registre commun fournit une « carte » des services en cours d'exécution, de leur emplacement et de leur état de santé actuel. Le registre peut être interrogé de manière programmatique pour permettre la découverte de services ou l'automatisation d'API gateways, d'équilibreurs de charge, pare-feux et autres composants de middleware critiques. Ces composants de middleware peuvent être sortis de la couche réseau physique en utilisant une approche par maillage des services, où les proxies s'exécutent en périphérie afin de fournir une fonctionnalité équivalente. Les approches par maillage des services permettent de simplifier la topologie réseau, en particulier pour les topologies multi-cloud et multi-datacenters.



Découverte des services

Le point de départ de la mise en réseau dans un modèle opérationnel cloud est généralement un registre de services commun, qui fournit un répertoire en temps réel des services exécutés, de là où ils sont, et de leur état de santé actuel. Les approches traditionnelles de la mise en réseau reposent sur les équilibreurs de charge et les IP virtuelles pour fournir une abstraction de nommage afin de représenter un service avec une IP statique. Le processus de suivi de l'emplacement dans le réseau des services prend souvent la forme de feuilles de calcul, de tableaux de bord d'équilibreur de charge ou de fichiers de configuration, qui sont tous déconnectés : des processus manuels imparfaits.

Pour Consul, chaque service est enregistré de façon programmatique et les interfaces DNS et API sont fournies afin de permettre l'identification de tout service par d'autres services. Le contrôle d'intégrité intégré surveillera l'état de santé de chaque instance de service afin que l'équipe informatique puisse déterminer la disponibilité de chaque instance et que Consul puisse empêcher le routage du trafic vers des instances de service défaillantes.

Consul peut être intégré à d'autres services qui gèrent le trafic nord-sud existant, tels que des équilibreurs de charges traditionnels, et des plateformes d'applications distribuées comme Kubernetes, afin de fournir un service de registre et de découverte uniforme dans les environnements multi-datacenters, cloud et plateformes.

Automatisation de middleware réseau

L'étape suivante consiste à réduire la complexité opérationnelle avec le middleware réseau existant via l'automatisation du réseau. Au lieu d'un processus manuel basé sur des tickets pour reconfigurer les équilibreurs de charge et les pare-feu chaque fois qu'il y a un changement des emplacements ou configurations du réseau de services, Consul peut automatiser ces opérations réseau. Ceci est obtenu en permettant aux périphériques middleware réseau de s'abonner aux changements de service du registre de services, ce qui permet une infrastructure hautement dynamique qui peut évoluer bien plus qu'avec les approches statiques.

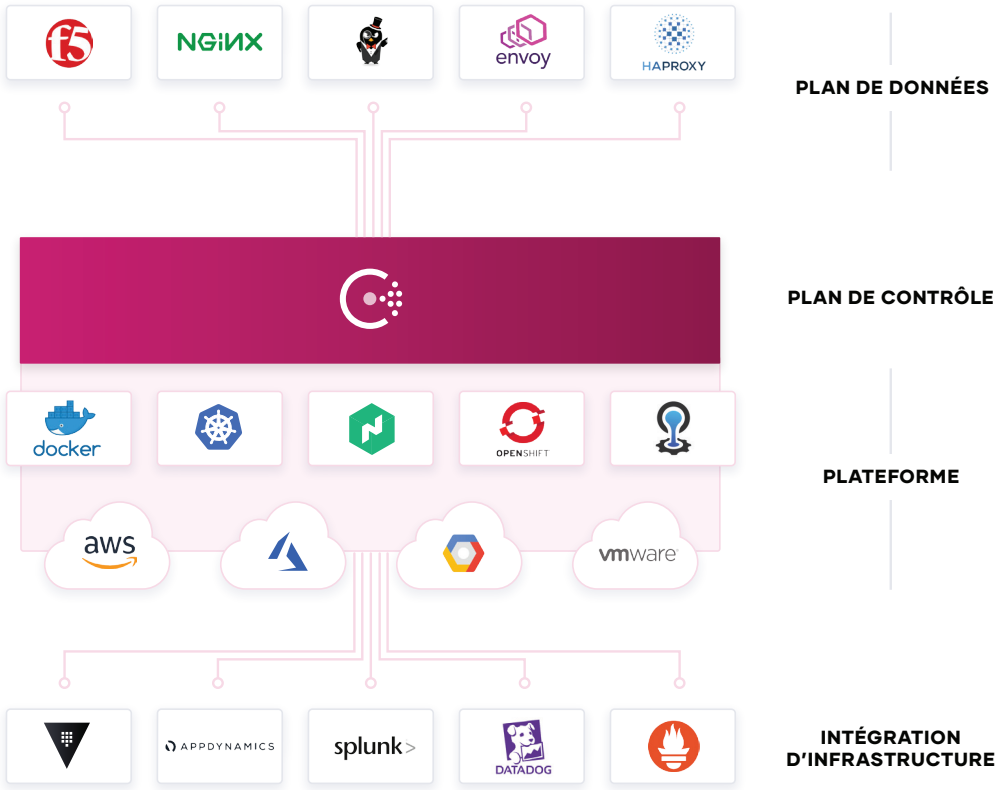
Cela dissocie le workflow entre les équipes, car les opérateurs peuvent déployer indépendamment des applications et publier sur Consul, tandis que les équipes NetOps peuvent s'abonner à Consul pour gérer l'automatisation en aval.

Mise en réseau Zero Trust avec maillage des services

Alors que les organisations continuent de passer à l'échelle avec des applications basées sur des microservices ou des applications cloud natives, l'infrastructure sous-jacente devient plus grande et plus dynamique avec une explosion du trafic est-ouest. Cela induit une prolifération de middleware réseau coûteux avec des points uniques de défaillance et des surcoûts opérationnels significatifs pour les équipes informatiques.

Consul fournit un maillage des services distribué qui déplace les fonctionnalités de routage, d'autorisation et d'autres fonctionnalités réseaux aux endpoints dans le réseau, plutôt que de les imposer par le biais du middleware. Cela rend la topologie réseau plus simple et plus facile à gérer, supprime le besoin de middleware coûteux pour le trafic est-ouest, et rend la communication de service à service beaucoup plus fiable et évolutive.

Consul est un control plane piloté par API qui s'intègre aux proxies sidecar, à côté de chaque instance de service (proxies tels que Envoy, HAProxy et NGINX). Ces proxies fournissent le data plane distribué. Ensemble, data plane et control plane permettent un modèle de réseau Zero Trust qui assure la communication de service à service avec chiffrement TLS automatique et autorisation basée sur l'identité. Les équipes de sécurité et en charge des opérations réseau peuvent définir les politiques de sécurité par le biais d'intentions avec des services logiques plutôt que des adresses IP.

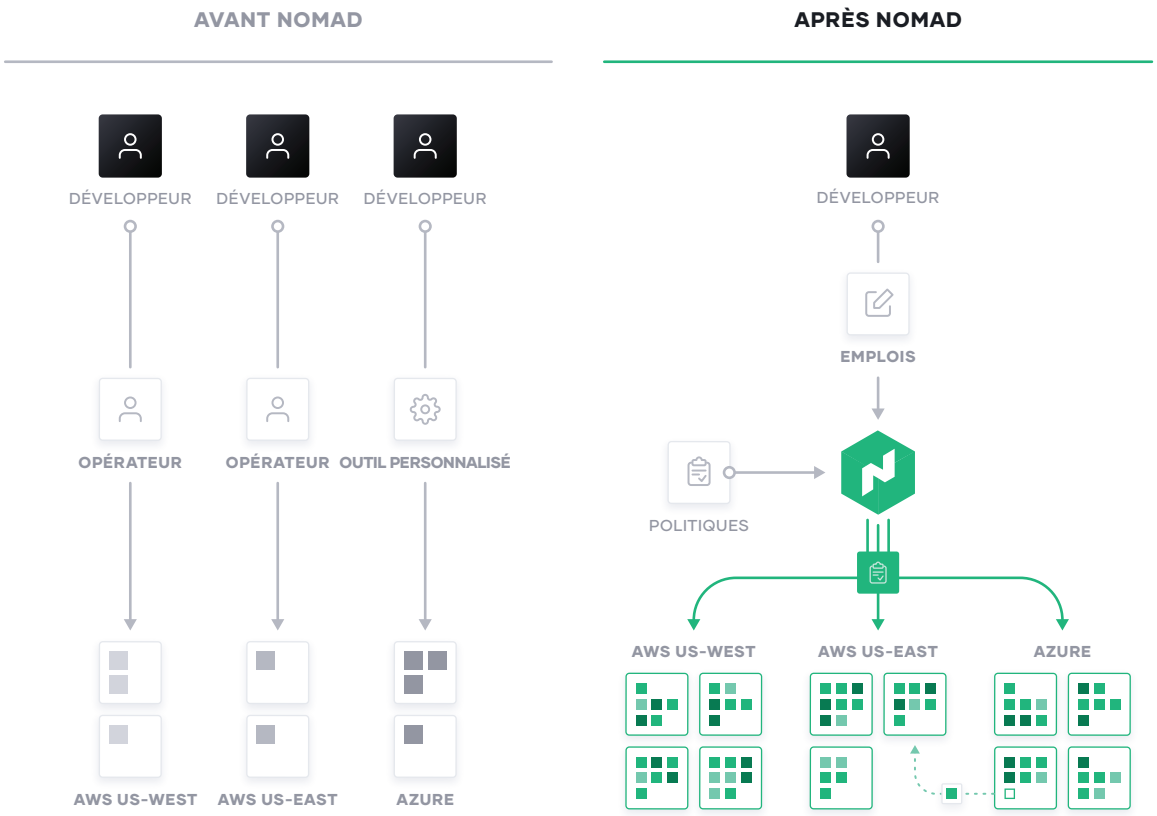


Consul permet une micro-segmentation des services pour sécuriser la communication de service à service avec chiffrement TLS automatique et autorisation basée sur l'identité. Consul peut être intégré à Vault pour la gestion centralisée des PKI et des certificats. La configuration des services est réalisée via un stockage clé/valeur piloté par API qui peut être utilisé pour configurer facilement les services au moment de l'exécution dans n'importe quel environnement.

Étape 4 : Livraison d'applications multi-cloud

Enfin, au niveau de la couche applicative, les nouvelles applications sont de plus en plus distribuées tandis que les applications traditionnelles doivent également être gérées de manière plus flexible. HashiCorp Nomad fournit un orchestrateur flexible pour déployer et gérer des applications existantes et modernes, pour tous les types de charges de travail : des services de longue durée aux lots à court terme, aux agents système.

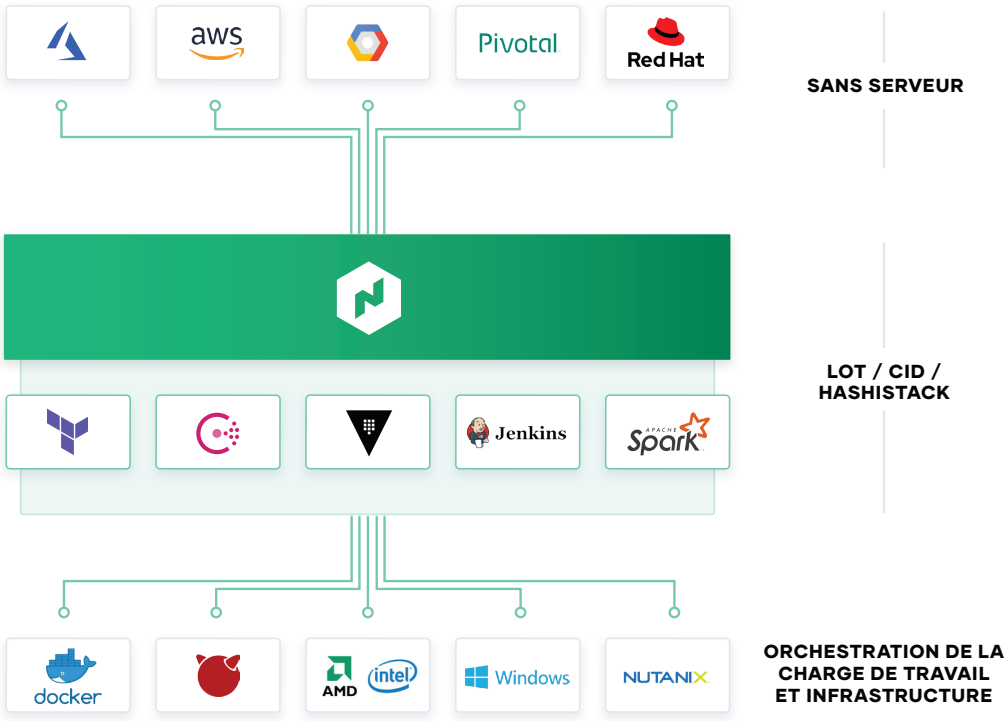
Afin d'obtenir des services partagés pour la mise à disposition des applications, les équipes informatiques doivent utiliser Nomad avec Terraform, Vault et Consul afin de permettre une mise à disposition uniforme des applications sur l'infrastructure cloud, en intégrant les exigences nécessaires en matière de conformité, de sécurité et de mise en réseau, ainsi que l'orchestration et la planification des charges de travail.



Orchestration des charges de travail mixtes

De nombreuses nouvelles charges de travail sont développées avec l'empaquetage des conteneurs dans l'intention de déployer vers Kubernetes ou d'autres plateformes de gestion de conteneurs. Pour autant de nombreuses charges de travail traditionnelles ne seront pas déplacées vers ces plateformes, ainsi que les futures applications Serverless. Nomad fournit un processus uniforme pour le déploiement de tout type de charges de travail, des machines virtuelles, aux binaires autonomes ou conteneurs. Nomad offre des avantages d'orchestration à travers ces charges de travail, telles que l'automatisation des versions, les stratégies de mise à niveau multiples, le bin packing et la résilience.

Pour les applications modernes — généralement intégrées dans les conteneurs — Nomad fournit un même workflow uniforme à grande échelle dans n'importe quel environnement. Nomad se concentre sur la simplicité et l'efficacité lors de l'orchestration et de la planification, et évite la complexité des plateformes telles que Kubernetes qui nécessitent des compétences spécialisées pour l'utilisation et résolvent uniquement les charges de travail conteneurisées.



Nomad s'intègre aux workflows CI/CD existants afin de fournir des déploiements d'applications rapides et automatiques pour les charges de travail existantes et modernes.

Calcul haute performance

Nomad est conçu pour planifier des applications avec une faible latence sur de très grands clusters. Ceci est essentiel pour les clients avec des tâches par lots volumineuses, comme cela est courant avec les charges de travail HPC (High Performance Computing). Pour le défi du million de conteneurs, Nomad a pu planifier un million d'instances de Redis sur 5 000 machines dans trois datacenters, en moins de 5 minutes. Plusieurs grands déploiements Nomad s'exécutent à des échelles encore plus grandes.

Nomad permet aux applications hautes performances d'utiliser facilement une API pour consommer de la capacité dynamiquement, ce qui permet un partage efficace des ressources pour les applications d'analyse de données telles que Spark. La planification à faible latence garantit que les résultats sont disponibles en temps opportun et réduit le gaspillage de ressources.

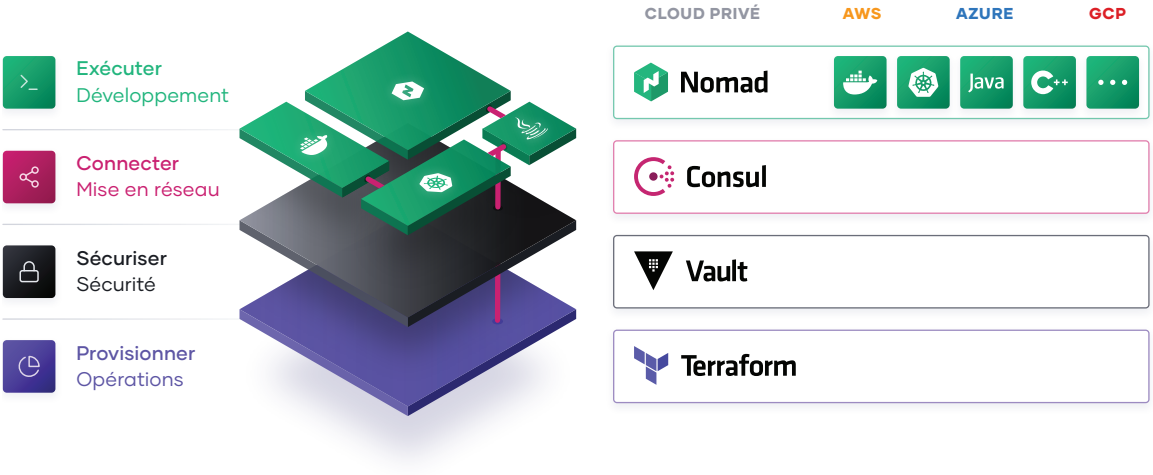
Orchestration de charges de travail multi-datacenters

Nomad est multi-région et multi-cloud par conception, avec un workflow uniforme pour le déploiement de toute charge de travail. Au fur et à mesure que les équipes déploient des applications globales sur plusieurs datacenters, ou dans les limites du cloud, Nomad fournit une orchestration et planification pour ces applications, prises en charge par les ressources de l'infrastructure, de sécurité et de mise en réseau afin de garantir que l'application est déployée avec succès.

Étape 5 : Processus de livraison d'applications industrialisé

Au final, ces services partagés entre l'infrastructure, la sécurité, la mise en réseau et l'exécution des applications présentent un processus industrialisé pour la livraison des applications, tout en tirant parti de la nature dynamique de chaque couche cloud.

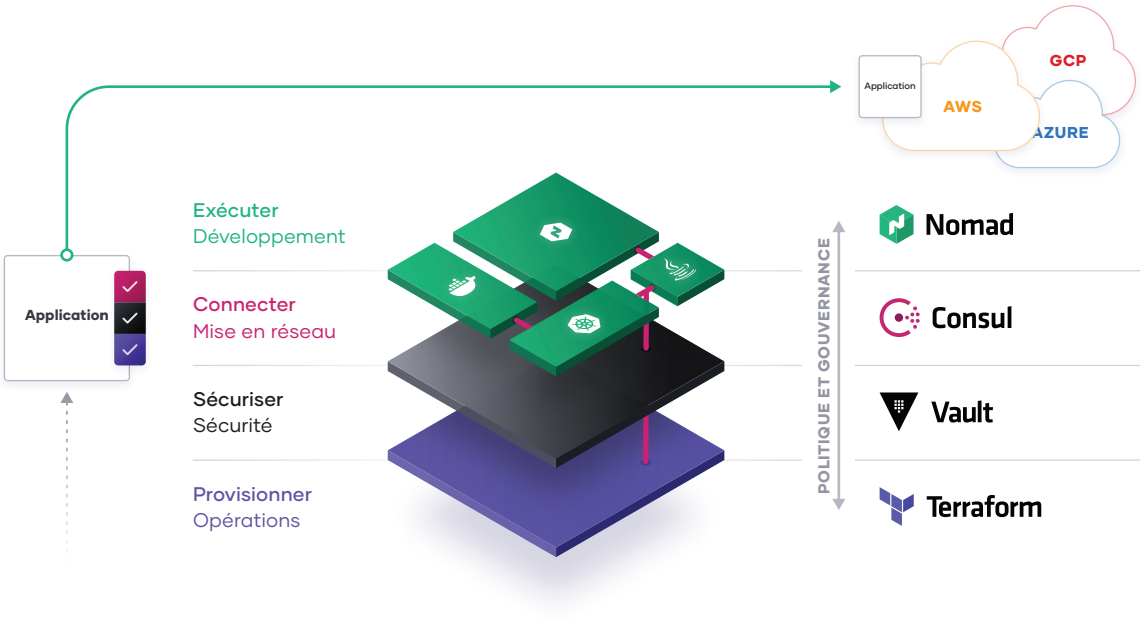
L'adoption du modèle opérationnel cloud permet une informatique en libre-service, entièrement conforme et gouvernée, afin que les équipes livrent des applications plus rapidement.



Conclusion

Un modèle opérationnel cloud commun constitue une transition inévitable pour les entreprises visant à maximiser leurs efforts de transformation numérique. La suite d'outils HashiCorp cherche à fournir des solutions pour chaque couche cloud afin de permettre aux entreprises de réaliser cette transition vers un modèle opérationnel cloud.

L'informatique d'entreprise doit évoluer en abandonnant les points de contrôle basés sur ITIL, qui mettent l'accent sur l'optimisation des coûts, en se transformant vers un système en libre-service dont l'objectif est de réduire latence des opérations. Cela est possible en fournissant des services partagés sur chaque couche cloud conçus pour aider les équipes à offrir une nouvelle valeur commerciale et client rapidement.



Créer le chemin le plus rapide vers la création de valeur dans un datacenter multi-cloud moderne grâce à l'adoption d'un modèle opérationnel cloud commun signifie modifier les caractéristiques de l'informatique d'entreprise :

- **Personnes : Passer à des compétences multi-cloud**
  - Réutiliser les compétences de gestion interne des datacenters et les fournisseurs cloud uniques et les appliquer uniformément dans n'importe quel environnement.
  - Adopter DevSecOps et d'autres pratiques agiles pour livrer continuellement des systèmes de plus en plus éphémères et distribués.

- **Processus : Passage à l'informatique en libre-service**
  - Positionner l'informatique centrale comme un service partagé axé sur la vitesse de livraison des applications : expédier les logiciels plus rapidement et avec un risque minimal.
  - Établir des centres d'excellence sur chaque couche cloud pour la fourniture en libre-service de capacités.

- **Outils : Passage à des environnements dynamiques**
  - Utiliser des outils qui soutiennent l'augmentation de l'éphéméralité et la distribution de l'infrastructure et des applications, et qui soutiennent les workflows critiques plutôt que d'être liés à des technologies spécifiques.
  - Fournir des outils de politique et de gouvernance afin de faire correspondre la rapidité de livraison et la conformité pour gérer les risques dans un environnement libre-service.

À propos de HashIcorp

HashiCorp est le leader dans le secteur des logiciels d'automatisation d'infrastructure multi-cloud. La suite logicielle HashiCorp permet aux entreprises d'adopter des flux de travail uniformes pour provisionner, sécuriser, connecter et exécuter n'importe quelle infrastructure pour n'importe quelle application. Les outils Open Source de HashiCorp : Vagrant, Packer, Terraform, Vault, Consul et Nomad sont téléchargés des dizaines de millions de fois chaque année et sont largement adoptés par les entreprises du Global 2000. Les versions d'entreprise de ces produits améliorent les outils open source avec des fonctionnalités qui favorisent la collaboration, les opérations, la gouvernance et les fonctionnalités multi-datacenter. L'entreprise a son siège à San Francisco et est appuyée par Mayfield, GGV Capital, Redpoint Ventures, True Ventures, IVP et Bessemer Venture Partners. Pour plus d'informations, visitez le site : **www.hashicorp.com** ou suivez HashiCorp sur Twitter : **@HashiCorp**.


HashiCorp