S3NS

PERFORMANCE
INNOVATION
CONFIANCE

Anticipez votre transition vers le Cloud de Confiance

Scénarios de migration et considérations associées

Une solution cloud THALES x Google Cloud

Executive Summary

Depuis ses débuts, S3NS a fréquemment été confronté à deux questions, étroitement liées, de la part de ses clients.

- Premièrement, sera-t-il facile de redéployer sur le Cloud de Confiance de S3NS des workloads déjà déployés sur l'offre "Contrôles Locaux avec S3NS" ou Google Cloud Platform ?
- Deuxièmement, que faudra-t-il pour déployer des cas d'utilisation hybride entre le Cloud de Confiance de S3NS et Contrôles Locaux ou Google Cloud Platform ?

Cette dernière question, soulevée par de nombreux clients déjà matures dans leur stratégie de souveraineté, souligne en effet la nécessité de travailler avec des données de différents niveaux de sensibilité pour certains cas d'usage, par exemple pour faire de l'analytique ou Business Intelligence entre des données sensibles et d'autres peu ou non sensibles.

La réponse courte à ces deux questions est la suivante :

- L'adoption de Contrôles Locaux avec S3NS aujourd'hui peut constituer comme une première étape importante dans le parcours de migration, accélérant la transition future vers le Cloud de Confiance de S3NS
- Les clients qui ont déjà adopté la technologie GCP pourront tirer parti de leurs connaissances et des capacités de déploiement automatisées de GCP (notamment par le biais d'interfaces programmatiques et d'API, et d'Infrastructure as Code). Les workloads pourront être ré-instanciées dans le Cloud de Confiance de S3NS avec un minimum d'efforts.
- L'effort exact dépendra de l'architecture des applications et de la manière dont elles sont déployées dans ces environnements.
- Certains paramètres doivent être anticipés en amont pour faciliter cette opération : architecture, capacités de déploiement automatisé, volume de données, bande passante du réseau....

Ce document vise à fournir des conseils préalables pour optimiser et faciliter les déploiements des cas d'utilisation et pour assister les clients dans l'accélération de leur transition future à travers diverses solutions technologiques de GCP (Cloud de Confiance de S3NS / Contrôles Locaux de S3NS / Google Cloud Platform).

Les étapes clés de la migration vers le Cloud de Confiance de S3NS sont les suivantes :

- Définition du périmètre et inventaire des données : définissez la nature et la sensibilité de vos données
- Planification de l'architecture de vos workloads : 3 archétypes principaux de destination en fonction de votre application et/ou de la sensibilité de vos données.
- Utilisation des interfaces programmatiques et des API de Google Cloud similaires entre les trois solutions
- Terraform Infrastructure as Code : le fait de disposer d'une API compatible avec GCP sera bénéfique pour vos développeurs et vous évitera de devoir former à nouveau vos ingénieurs pour la création de vos environnements Cloud de Confiance
- Provisionnement : avec l'Infrastructure as Code, vous pouvez réutiliser des scripts existants pour provisionner le Cloud de Confiance de S3NS à partir de Google Cloud Platform ou Contrôles Locaux.

- Migration des données : plusieurs facteurs sont à prendre en compte lors de la migration vers le Cloud de Confiance de S3NS, notamment le volume de données, la bande passante du réseau et l'emplacement des données.

En comprenant et en exploitant les meilleures pratiques décrites dans ce document, les entreprises vont pouvoir planifier à l'avance - et en toute confiance - leur migration vers le Cloud de Confiance de S3NS.

INTRODUCTION

Pour soutenir la transformation numérique, les organisations peuvent utiliser des services de cloud computing qui offrent des avantages en termes d'échelle, d'innovation de service, de coût et de durabilité par rapport à l'infrastructure informatique existante.

Cependant, l'utilisation de ces services doit permettre aux organisations de répondre à des exigences strictes en matière de sécurité et de confidentialité des données.

Grâce à son partenariat unique avec Google Cloud, S3NS propose deux solutions qui permettent aux organisations de répondre aux exigences de conformité françaises pour différents workloads :

- **Contrôles Locaux avec S3NS** - La puissance de Google Cloud, en France, avec des garanties supplémentaires apportées par Google Cloud et des contrôles par S3NS (notamment la gestion de clés externe utilisées pour le chiffrement des données clients), permettant aux entreprises de réduire les risques, de renforcer la conformité et d'entamer dès maintenant la transition vers le Cloud de Confiance.

- **Le Cloud de Confiance de S3NS** - La puissance de Google Cloud, en France, opérée et sécurisée par S3NS, visant à être qualifié SecNumCloud, le plus haut niveau de certification délivré par le gouvernement français, conformément à la stratégie nationale française.

Pour de nombreuses organisations, une interrogation cruciale est de savoir si elles peuvent investir en toute confiance dans des déploiements cloud actuels tout en préservant la possibilité de migrer vers un Cloud de Confiance à l'avenir.
La réponse est OUI. S3NS a conçu le Cloud de Confiance de manière à réduire au maximum le temps d'ingénierie et les nouveaux investissements nécessaires pour les utilisateurs existants de Contrôles Locaux avec S3NS / Google Cloud.

Pour une transition progressive et rapide vers le Cloud de Confiance de S3NS, il est recommandé de démarrer dès maintenant, en accomplissant les premières étapes de la migration vers la plateforme S3NS / Google Cloud, puis de se concentrer sur un petit nombre de considérations et d'étapes supplémentaires pour accélérer la migration vers le Cloud de Confiance de S3NS, si cela s'avère nécessaire. Au cours de cette période, les équipes vont acquérir des connaissances et une expertise essentielle qui seront immédiatement mises en pratique dans l'environnement Cloud de Confiance de S3NS.

Dans ce document, nous passerons brièvement en revue les considérations initiales pour les migrations vers le cloud, en accordant une attention particulière aux aspects spécifiques et aux étapes à suivre pour une migration ultérieure vers le Cloud de Confiance de S3NS.

Adoption du Cloud et Migration Initiale des Workloads

Les organisations peuvent maintenir leur rythme d'adoption du cloud et aborder en toute confiance l'évolution des exigences des réglementations en matière de conformité en adoptant une approche combinant la classification des données, la sélection de solutions cloud adaptées à leurs besoins, l'automatisation, ainsi qu'une compréhension des options de migration pour répondre aux éventuelles évolutions des besoins.

Pour amorcer votre transition vers le cloud, il existe de nombreuses options que vous pouvez envisager. Un framework très connu, "*Les Six Rs*", décrit les options possibles :

- **Rehost** : Migrer votre application et de vos données “as-is” ("lift and shift")
- **Replatformer** : Redéfinir certains éléments pour tirer parti du cloud ("horizontal scaling")
- **Refactor** : Revoir l’architecture complète de l'application pour l'adapter au cloud.
- **Retain** : Conserver certains éléments on-premise - idéal pour les migrations de longue durée
- **Retirer** : Exclure les fonctionnalités obsolètes (ne pas effectuer leur migration)
- **Rachat** : Remplacer certaines fonctionnalités par une option "cloud" tierce.

Dans le présent document, nous supposons que l'option choisie consistera à migrer les workloads vers le cloud.

Ensuite, il convient d'effectuer un inventaire et une classification des données associées aux workloads à migrer. La sensibilité de ces données déterminera les exigences en matière de contrôle et de conformité pour le déploiement cloud, ainsi que les services cloud les plus appropriés.

Une autre réflexion concerne l'automatisation du déploiement en adoptant une approche basée sur l'Infrastructure as Code. Traditionnellement, la gestion de l'infrastructure informatique impliquait souvent des processus manuels. Cependant, avec les déploiements cloud, qui reposent sur des logiciels, l'automatisation est bien plus accessible. L'infrastructure as code (IaC) introduit la possibilité pour les organisations de provisionner et de gérer les ressources des datacenters en utilisant des fichiers facilement interprétables. Sans une approche IaC, les déploiements et les migrations dans le cloud restent des processus manuels, ce qui les rend nettement plus complexes, susceptibles d'erreurs ou de configurations incorrectes, et risqués.

Ces considérations et démarches préliminaires sont indispensables à toute migration on-premise vers le cloud. Si vous souhaitez adopter le Cloud de Confiance de S3NS, il ne sera pas nécessaire de répéter ces étapes pour passer d'un système on-premise à Google Cloud ou aux Contrôles Locaux de S3NS.

Présentation du Cloud de Confiance de S3NS

Le reste de ce document se concentre sur les considérations spécifiques et les étapes d'une migration vers le Cloud de Confiance de S3NS.

Conformément à la définition des exigences SecNumCloud les plus récentes, le Cloud de Confiance de S3NS est exploité par une société dédiée, nouvellement créée en vertu du droit français, détenue en majorité par Thales.

Le Cloud de Confiance de S3NS est hébergé en France, dans une infrastructure séparée de Google Cloud Platform, avec un réseau et des serveurs distincts, contrôlés et exploités par S3NS. Il est physiquement et logiquement séparé des environnements publics de Google Cloud Platform.

Les deux modèles les plus courant pour migrer vers et/ou travailler avec le Cloud de Confiance de S3NS seront :

1) **La Migration** : déplacer des workloads depuis des solutions on-premises, privés ou publics (y compris Google Cloud Platform) vers le Cloud de Confiance de S3NS.

2) **L'Hybridation** : Assurer la compatibilité entre les workloads on-premise ou sur le cloud avec ceux hébergés dans le Cloud de Confiance de S3NS.

La Migration vers le Cloud de Confiance : Vue d'Ensemble

Une migration réussie requiert une planification minutieuse. Il est essentiel de commencer par comprendre l'architecture et les exigences de classification des données des workloads concernés. Ensuite, il convient de déterminer comment répliquer les ressources des workloads dans le nouvel environnement, de migrer les scripts d'administration et autres orchestrations, ainsi que de transférer les données.

Comme évoqué précédemment, migrer vers le Cloud de Confiance de S3NS est facilité lorsque les workloads sont déjà hébergés sur Google Cloud Platform ou Contrôles Locaux. En adoptant les meilleures pratiques ci-dessous, les entreprises peuvent planifier à l'avance - et en toute sérénité - leur migration vers le Cloud de Confiance de S3NS.

Définition du champ d'application

Avant de lancer un projet de migration vers le Cloud de Confiance de S3NS, il est essentiel de définir le champ d'application :

- Inventaire de l'infrastructure existante et des données.
    - La nature et la sensibilité des données seront déterminantes pour savoir s'il convient de les migrer vers le Cloud de Confiance de S3NS ou de les laisser dans leur environnement actuel.
    - Une classification précise est fondamentale pour prendre une décision éclairée sur la pertinence de la migration des données
- Les politiques de sécurité internes, les réglementations ou les normes du marché applicables à l'inventaire et à la classification des données aideront également à déterminer quelles données doivent être migrées vers le Cloud de Confiance de S3NS.
- Si l'on considère une approche de "lift & shift" et en prenant en compte la structure du modèle de données, il est envisageable que certaines données non critiques requièrent une migration pour maintenir la cohérence et éviter toute transformation de l'application.

Considérer l'architecture de vos workloads

Lors de la transition vers le Cloud de Confiance de S3NS, trois archétypes majeurs de destination se distinguent. Le choix d'un archétype pour un workload spécifique peut dépendre à la fois de son architecture actuelle, qu'elle soit monolithique ou fragmentée en plusieurs services autonomes, et des exigences de conformité relatives aux données qu'il gère.

Migration complète des workloads

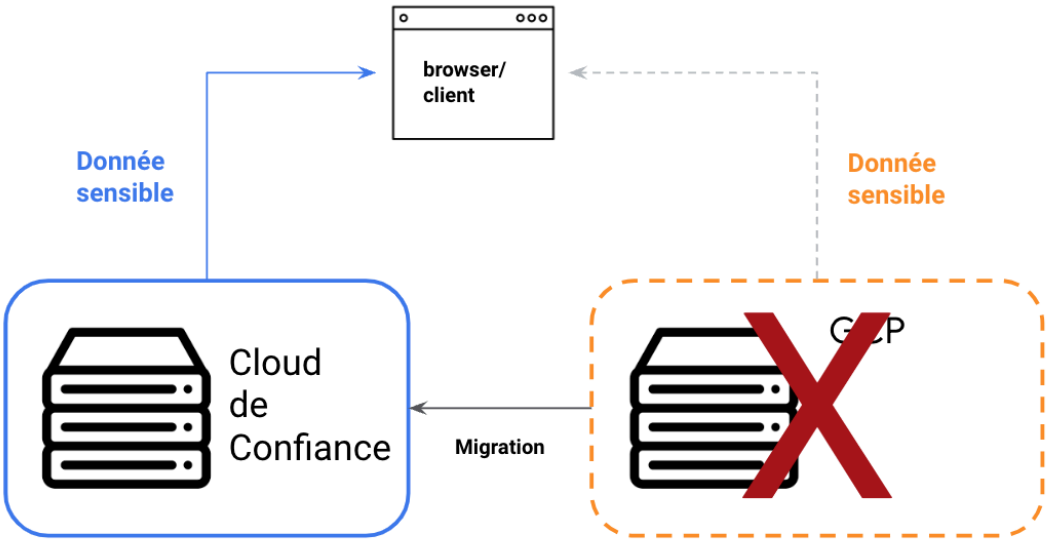

Figure (1) : Migration complète des workloads

Dans ce scénario, un workload déjà présent sur Google Cloud Platform ou Contrôles Locaux peut être transféré entièrement vers le Cloud de Confiance de S3NS. Une fois la migration effectuée, la source d'origine du workload peut être désactivée.

Utilisation hybride des workloads

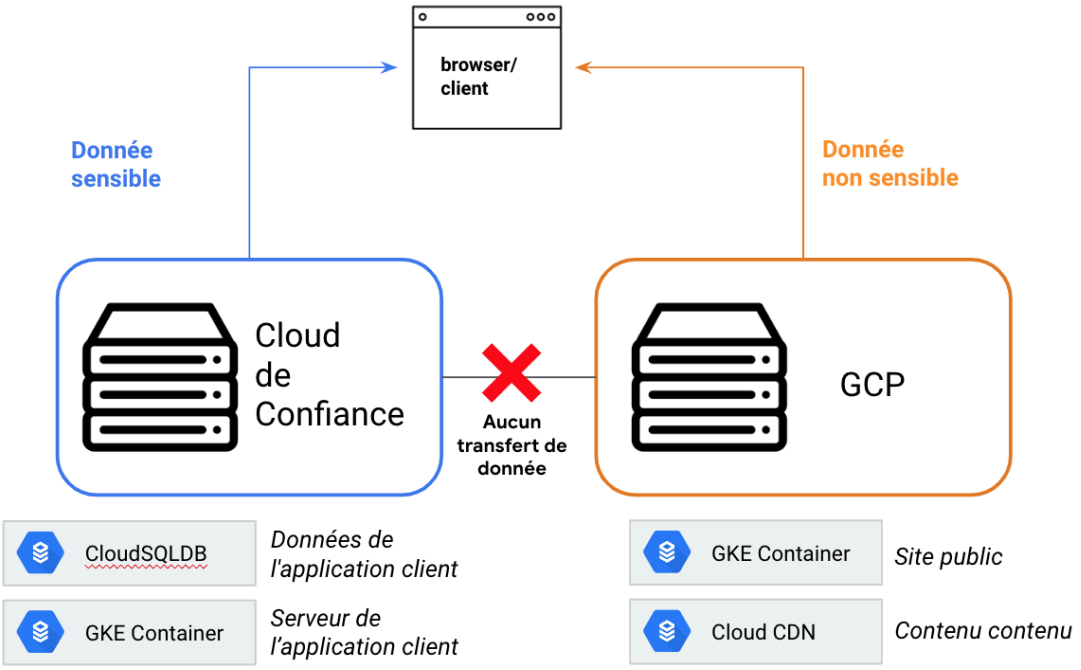

Figure (2) : Utilisation hybride des workloads

Dans un scénario hybride, seules certaines parties des workloads peuvent être déplacées vers le Cloud de Confiance de S3NS, les autres parties restant sur Google Cloud Platform ou Contrôles Locaux. Les parties des workloads qui sont migrées sont souvent celles contenant des données sensibles, soumises à des exigences de conformité telles que des informations d'identification personnelle.

Le schéma ci-dessus montre un exemple où la base de données et le serveur d'application d'une application orientée client peuvent être déplacés vers le Cloud de Confiance de S3NS, tandis que les parties moins sensibles des workloads - comme un site web public ou un contenu CDN statique - peuvent rester à leur emplacement initial.

Il convient de souligner qu'aucun transfert de données d'exécution n'est requis entre les workloads du Cloud de Confiance et ceux demeurant sur Contrôles Locaux. En optant pour cette approche, en les adressant de façon unique via le DNS, l'utilisateur final bénéficie d'une expérience transparente, similaire à celle affichée dans leur navigateur ou leur application client.

Workload connecté à l'extérieur

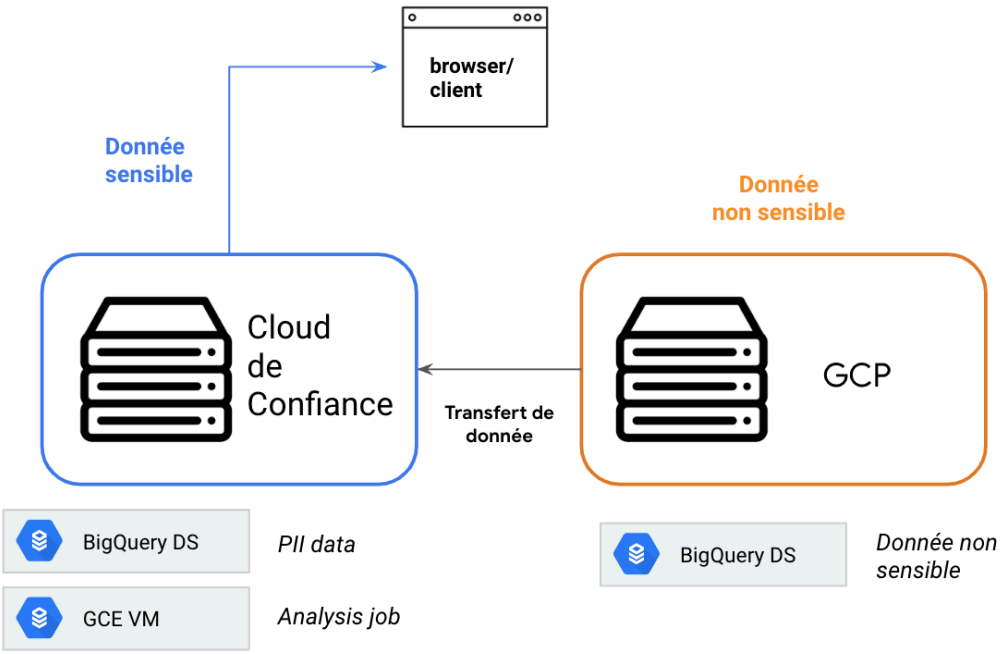

Figure (3): workload connecté à l'extérieur

En ce qui concerne les workloads analytiques/de traitement, il peut être nécessaire d'agréger les données nécessaires à partir de sources multiples. Il est essentiel de garder à l'esprit que les données les plus sensibles ne doivent jamais être transférées vers un environnement qui ne respecte pas leurs exigences en matière de conformité. À cet égard, la direction de tout transfert doit être soigneusement considérée.

Le diagramme ci-dessus montre un exemple avec plusieurs ensembles de données BigQuery. L'un d'eux se trouve sur le Cloud de Confiance de S3NS, où des données sensibles des clients peuvent être stockées. L'autre se trouve sur Google Cloud Platform ou Contrôles Locaux, où sont stockées des données moins sensibles.

Pour garantir une analyse sécurisée de ces datasets, il est impératif que le pipeline d'analyse soit hébergé dans l'environnement le plus sécurisé, à savoir le Cloud de Confiance de S3NS. Par ailleurs, les données nécessaires à l'analyse ne doivent être extraites de leurs sources que pour être introduites dans le pipeline d'analyse sur le Cloud de Confiance de S3NS. Elles ne doivent généralement pas être poussées (*pushed*) dans le Cloud de Confiance de S3NS, car cela impliquerait que les informations d'identification pour accéder au Cloud de Confiance de S3NS pourraient être stockées ou utilisées dans des environnements moins sensibles.

Mise à jour de l'utilisation de la ligne de commande et des scripts

Les utilisateurs de Google Cloud et de Contrôles Locaux de S3NS disposent de plusieurs interfaces pour gérer leur infrastructure cloud. La console basée sur l'interface utilisateur simplifie la découverte des fonctionnalités et des capacités de chaque plateforme, offrant ainsi une expérience intuitive. Tandis que les interfaces programmatiques telles que l'interface de ligne de commande (CLI) gcloud et les API de services cloud jouent un rôle central dans l'automatisation des workflows DevOps.

L'interface de commande gcloud a été mise à jour pour prendre en charge le Cloud de Confiance de S3NS, de sorte qu'un seul outil peut être utilisé pour gérer l'infrastructure à travers Google Cloud, Contrôles Locaux de S3NS, et le Cloud de Confiance de S3NS.
La syntaxe des commandes de l'interface gcloud sera cohérente pour les trois solutions, à de rares exceptions près. Pour les développeurs qui travaillent sur ces plateformes, le fait de disposer d'une CLI unique simplifie les flux de travail et réduit la complexité et le temps nécessaire pour la migration des workloads entre les plateformes. Dans la majorité des cas, lorsqu'il s'agit de migrer des scripts existants qui exploitent la CLI gcloud vers le Cloud de Confiance, La seule modification nécessaire consistera à actualiser les informations d'identification du service afin qu'elles soient reconnues par le Cloud de Confiance. Il ne sera pas nécessaire de modifier explicitement les noms de domaine des API de service nommées par gcloud, ces informations sont automatiquement dérivées des informations d'identification du compte Cloud de Confiance.

En d'autres termes, il est aussi aisé de changer la plateforme cloud sur laquelle gcloud effectue des modifications que de changer d'identifiant. Dans cet exemple, deux identifiants sont stockés dans gcloud, et l'identifiant actif est défini pour Google Cloud :

```
$ gcloud auth list
  Credentialed Accounts
ACTIVE  ACCOUNT                              UNIVERSE_DOMAIN
*       google_user@betterenergy.fr          googleapis.com
        s3ns_user@betterenergy.fr            apis-s3ns.fr
```

En changeant de compte avec gcloud config set account, la CLI envoie désormais des commandes au Cloud de Confiance :

```
$ gcloud config set account s3ns_user@betterenergy.fr
$ gcloud auth list
  Credentialed Accounts
ACTIVE  ACCOUNT                              UNIVERSE_DOMAIN
        google_user@betterenergy.fr          googleapis.com
*       s3ns_user@betterenergy.fr            apis-s3ns.fr
```

Portage des intégrations programmatiques

Pour les intégrations programmatiques existantes avec les services Google Cloud également disponibles dans le Cloud de Confiance, le portage de ces intégrations peuvent souvent être adaptées avec quelques ajustements, voire sans aucun, pour s'intégrer parfaitement. Pour les intégrations qui appellent directement les API de service, la mise à jour impliquera principalement l'ajustement de la méthode d'authentification et du nom de domaine complet pour les requêtes d'API. Pour les intégrations utilisant les bibliothèques client de Google Cloud, les modifications seront encore plus simples : il suffira de vérifier que la bibliothèque client est à jour et de mettre à jour les informations d'identification nécessaires pour se connecter au Cloud de Confiance de S3NS.

Appels directs d'API

Lors du portage d'intégrations qui font directement appel aux API de service, la première étape consiste à examiner la méthode d'authentification utilisée par le script ou l'automatisation. Le Cloud de Confiance prend en charge l'authentification via le Service Account, Workforce Identity ou Workload Identity. Contrairement à Google Cloud ou à Contrôle Locaux de S3NS, il ne prend pas en charge l'utilisation des comptes d'utilisateur Google.

Le prochain changement potentiel nécessaire consistera à actualiser les noms de domaine pleinement qualifiés utilisés pour se connecter aux points d'extrémité de l'API du service Cloud de Confiance. Les services Contrôles Locaux ou Google Cloud utilisent le nom de domaine de base `googleapis.com.` Cependant, ce nom de domaine de base est différent dans Cloud de Confiance : `apis-s3ns.fr`. Par exemple, l'API Compute Engine utilise le sous-domaine `compute` et le domaine pleinement qualifié `compute.googleapis.com` dans Google Cloud. Au sein du Cloud de Confiance, ce service utilisera également le sous-domaine `compute`, mais le domaine pleinement qualifié sera `compute.apis-s3ns.fr`.

Après ces modifications, les calls API existants resteront opérationnels, à condition que le service soit disponible dans le Cloud de Confiance. Les noms des types de ressources dans le Cloud de Confiance seront cohérents avec ceux de Google Cloud.

Bibliothèques client

Les bibliothèques client Google simplifient l'accès aux API de service dans Google Cloud et Cloud de Confiance de S3NS. Ces bibliothèques sont disponibles pour un certain nombre de langages de programmation et réduisent la quantité de code nécessaire à l'intégration avec Google et/ou le Cloud de Confiance.

Comme pour les intégrations qui lancent les calls API de service du Cloud de Confiance, les intégrations qui utilisent les bibliothèques client nécessiteront également une authentification à l'aide de Service Account, Workforce Identity, ou Workload Identity lors de la connexion aux API du Cloud de Confiance.

Contrairement aux intégrations qui lancent les calls sur les API de service, les programmes utilisant une bibliothèque client ne nécessitent aucune modification manuelle du nom de domaine utilisé pour se connecter aux API de service du Cloud de Confiance. Au lieu de cela, la bibliothèque client récupère le nom de domaine correct à partir des informations d'identification utilisées pour s'authentifier auprès du Cloud de Confiance et crée les noms de domaine entièrement qualifiés appropriés pour les call d'API de service en fonction de la configuration de la bibliothèque client et des méthodes utilisées. Pour les intégrations

Google Cloud existantes, cela signifie qu'il suffit de mettre à jour la bibliothèque client vers une version prenant en charge le Cloud de Confiance et de configurer l'authentification avec le Cloud de Confiance.
Aucun ajustement supplémentaire du code n'est requis.

Déployer avec Terraform

L'approche du Cloud de Confiance, avec ses API compatibles avec GCP, présente un avantage significatif pour les clients qui utilisent Terraform. Grâce à cette base, Google a pu élargir son offre Terraform pour inclure le Cloud de Confiance. Cela signifie que les clients existants de Google Cloud Platform et de Contrôles Locaux qui utilisent Terraform n'ont pas besoin de s'intégrer à un nouveau fournisseur Terraform ou de former à nouveau leurs ingénieurs et architectes cloud, simplifiant ainsi la migration des configurations d'infrastructure.

La migration avec Terraform de Google Cloud Platform ou de Contrôles Locaux vers le Cloud de Confiance de S3NS doit tenir compte de quatre éléments clés :

1) Où Terraform s'exécute
2) Configurer le fournisseur Terraform pour qu'il se connecte au Cloud de Confiance de S3NS
3) Le provisionnement des ressources dans le Cloud de Confiance de S3NS
4) La Gestion des différences de services et de ressources dans le Cloud de Confiance de S3NS

L'Environnement

Étant donné que des informations sensibles ou même des identifiants d'accès au cloud peuvent être présents dans les fichiers de configuration et d'état de Terraform, il convient de réfléchir à l'endroit où ces fichiers seront stockés et utilisés par Terraform afin de s'assurer qu'ils seront traités de manière conforme. Terraform offre une polyvalence qui permet aux clients de déployer ses versions open source et Enterprise dans le Cloud de Confiance de S3NS ou dans d'autres environnements adaptés aux données sensibles, tels que les déploiements on-premise. Terraform Cloud, cependant, stockera les fichiers d'état sur une infrastructure gérée par Hashicorp, une société basée aux États-Unis, et, en tant que tel, peut ne pas convenir aux workloads de SecNumCloud.

Connexion

Tout d'abord, examinons un exemple simple dans lequel Terraform est configuré pour pointer vers Google Cloud Platform ou Contrôles Locaux :

```
// a provider that points to Google Cloud Platform or S3NS Local Controls
// uses service account credentials contained in the referenced file
provider "google" {
  project                 = "projectABC"
  region                  = "europe-west9"
  credentials             = "${file("google.json")}"
}
```

Pour diriger vers le Cloud de Confiance de S3NS, il suffit d'ajouter une nouvelle entrée `provider google` avec un `alias` :

```
// a provider that points to Google Cloud Platform or S3NS Local Controls
// uses service account credentials contained in the referenced file
provider "google" {
  project                 = "projectABC"
  region                  = "europe-west9"
  credentials             = "${file("google.json")}"
}

// a provider that points to S3NS Trusted Cloud
provider "google" {
  alias                   = "s3nscloud"
  project                 = "s3ns:projectXYZ"
  region                  = "u-france-east1"
  ... // TODO authentication details; see below
}
```

Grâce à l'utilisation d'`alias`, les clients de Terraform peuvent configurer une deuxième instance du fournisseur google spécifiquement pour le Cloud de Confiance de S3NS, avec ses propres paramètres distincts, y compris les informations d'authentification. Une fois ajouté, il reste à définir la méthode d'authentification à utiliser pour accéder au Cloud de Confiance de S3NS, les deux méthodes les plus fréquentes sont :

Utiliser un compte de service du Cloud de Confiance S3NS

En utilisant un fichier de compte de service JSON généré par le Cloud de Confiance de S3NS, une seule ligne d'informations d'identification peut être ajoutée à l'entrée du nouveau fournisseur Terraform. Étant donné que ce fichier contient également les détails du domaine API spécifique au Cloud de Confiance de S3NS, toutes les ressources provisionnées via ce fournisseur seront automatiquement dirigées vers le Cloud de Confiance de S3NS.

.

```
provider "google" {
  alias                   = "s3nscloud"
  project                 = "s3ns:projectXYZ"
  region                  = "u-france-east1"

  // SA credentials (and API domain context) for S3NS Trusted Cloud
  credentials             = "${file("s3ns.json")}"
}
```

Utilisation d'un jeton d'accès à partir de Hashicorp Vault

Une autre approche consiste à obtenir un jeton d'accès basé sur un JWT via Hashicorp Vault. Les clients devront veiller à sélectionner le bon jeton pour le fournisseur aliasé et de spécifier le paramètre `universe_domain` pour diriger les appels de provisionnement vers les ressources associées au fournisseur aliasé dans Terraform.

```
provider "google" {
  alias                 = "s3nscloud"
  project               = "s3ns:projectXYZ"
  region                = "u-france-east1"

  // token from Hashicorp Vault & defining the universe domain
  access_token          = data.vault_generic_secret.gcp.data[“token”]
  universe_domain       = "apis-s3ns.fr"
}
```

Grâce à ces options de configuration, les clients peuvent choisir d'utiliser Terraform dans l'un des scénarios suivants :

- Provisionnement pour Google Cloud Platform ou Contrôles Locaux de S3NS
- Provisionnement dans le Cloud de Confiance de S3NS
- Provisionnement un cloud ou l’autre en sélectionnant l’emplacement des ressources

Provisionnement

Maintenant que la connexion et l'authentification au Cloud de Confiance de S3NS sont configurées, le provisionnement des ressources peut débuter.

Provisionnement du Cloud de Confiance de S3NS

Pour choisir l'emplacement de création d'une nouvelle ressource, il suffit de spécifier l'univers cible dans le champ du fournisseur. En supposant que le Cloud de Confiance de S3NS a été défini dans les étapes précédentes comme `google.s3nscloud`, l'exemple suivant illustre la création d'un nouveau bucket GCS dans ce cloud.

.

```
resource "google_storage_bucket" "default" {
  provider              = google.s3nscloud
  name                  = "shiny-new-bucket"
  location              = "u-france-east1"
  force_destroy         = true
}
```

Migration de la ressource vers le Cloud de Confiance de S3NS

Pour migrer une ressource de Contrôles Locaux de S3NS ou GCP vers le Cloud de Confiance de S3NS (voir schéma "*Migration complète des workloads*"), il suffit généralement de copier-coller la définition avec un champ `field` mis à jour et d'ajuster la `region` ou `location` comme il convient.
Par exemple :

```
// existing bucket in Google Cloud Platform
resource "google_storage_bucket" "default" {
  provider               = google
  name                   = "original-bucket"
  location               = "europe-west9"
  force_destroy          = true
}

// new bucket in s3ns Trusted Cloud
resource "google_storage_bucket" "default" {
  provider               = google.s3nscloud
  name                   = "new-bucket"
  location               = "u-france-east1"
  force_destroy          = true
}
```

Remarque : dans certains cas, la disponibilité des fonctionnalités peut différer entre Contrôles Locaux de S3NS / GCP et le Cloud de Confiance de S3NS, ce qui peut nécessiter des changements supplémentaires dans la définition des ressources Terraform. Reportez-vous à la documentation dans un tel scénario.

Une fois que les données ont été migrées (voir la section " *Déplacement des données* " ci-dessous), la définition de la ressource d'origine peut être supprimée, ce qui entraîne son déprovisionnement.

```
~~// existing bucket in Google Cloud Platform~~
~~resource "google_storage_bucket" "default" {~~
~~  provider               = google~~
~~  name                   = "original-bucket"~~
~~  location               = "europe-west9"~~
~~  force_destroy          = true~~
~~}~~

// new bucket in s3ns Trusted Cloud
resource "google_storage_bucket" "default" {
  provider               = google.s3nscloud
  name                   = "new-bucket"
  location               = "u-france-east1"
  force_destroy          = true
}
```

Gestion des ressources entre Contrôles Locaux S3NS/GCP et le Cloud de Confiance de S3NS

Les ressources pour un même workload peuvent être réparties entre Contrôles Locaux de S3NS / GCP et le Cloud de Confiance de S3NS en fonction des exigences de classification des données. Pour ce faire, il suffit de sélectionner les champs `provider` et `région/location` pour spécifier la cible souhaitée.

Dans l'exemple ci-dessous, un bucket GCS moins sensible (par exemple, hébergeant du contenu statique) peut être défini dans la configuration Terraform juste à côté d'un bucket contenant des informations plus sensibles (par exemple, PII). Chacun cible l'environnement approprié afin de répondre aux besoins de conformité.

```
// static data in Google Cloud Platform
resource "google_storage_bucket" "default" {
  provider               = google
  name                   = "static-bucket"
  location               = "europe-west9"
  force_destroy          = true
}

// sensitive data in s3ns Trusted Cloud
resource "google_storage_bucket" "default" {
  provider               = google.s3nscloud
  name                   = "sensitive-bucket"
  location               = "u-france-east1"
  force_destroy          = true
}
```

Différences d'univers

Dans certains cas, la configuration Terraform existante gère des types de ressources dans Google Cloud Platform ou Contrôles Locaux qui ne sont pas encore disponibles dans le Cloud de Confiance de S3NS.

Dans ce cas, pendant les phases d'exécution `terraform plan` et/ou `terraform apply`, le fournisseur Terraform renverra des messages d'erreur pour indiquer qu'un type de ressource ou un service déclaré n'est pas encore disponible :

```
$ terraform plan
Error: Invalid resource type

  on main.tf line 16, in resource "google_cloud_run_service" "default":
  16: resource "google_cloud_run_service" "default" {

The resource “google_cloud_run_service” is not available in universe_domain “apis-s3ns.fr”
```

Déplacement des données

Une fois que l'infrastructure du workload est déployée dans le Cloud de Confiance de S3NS, vous pouvez commencer à migrer les données souhaitées depuis Google Cloud ou Contrôles Locaux. Il est important de bien réfléchir à toutes les tâches nécessaires pour identifier, préparer, extraire et transférer les données afin de faciliter l'ensemble du processus.

Le présent document part du principe que les données seront transférées d'une plateforme à l'autre en utilisant le même ensemble de services cloud dans les deux environnements. Les activités nécessitant l'adoption de nouveaux services, la modernisation des workloads ou d'autres changements ne sont pas abordés dans ce document.

La première activité à mener consiste à déterminer quelles données seront transférées sur la base de l'exercice d'inventaire et de classification décrit précédemment - qui aura inclus l'identification de la sensibilité des données et les dépendances des données. Une fois que les données susceptibles d'être transférées ont été identifiées, plusieurs facteurs auront un impact sur le transfert, notamment les suivants :

- Volume de données
- Bande passante du réseau
- Contraintes de temps liées au transfert de données
- Localisation des données

La durée du transfert des données dépend à la fois du volume des données à transférer et de la capacité de la bande passante du réseau. Cette durée est essentielle car elle déterminera potentiellement le temps d'arrêt nécessaire pour migrer l'application et si ce temps d'arrêt peut être géré dans le cadre des SLO/SLA du workload. La vitesse de la bande passante du réseau dépend de la qualité de la connectivité entre l'environnement source (Google Cloud ou Contrôles Locaux) et l'environnement cible (Cloud de Confiance de S3NS). Plusieurs solutions sont possibles pour établir cette connexion, chacune leurs spécificités. Les deux options les plus courantes sont les suivantes :

Internet en accès public

VPN Cloud : le VPN Cloud offre un tunnel IPSec sécurisé entre deux sites sur le réseau internet public. Cette solution peut être implémentée de manière flexible et à moindre coût. Afin d'augmenter la bande passante du réseau, plusieurs tunnels IPSec peuvent être établis. Chaque tunnel VPN Cloud prend en charge jusqu'à 250 000 paquets par seconde pour la somme du trafic entrant et sortant. En fonction de la taille moyenne des paquets dans le tunnel, 250 000 paquets par seconde équivalent à une bande passante de 1 Gbps à 3 Gbps.

Pour plus d'informations sur le transfert de données volumineuses, consultez ce lien : https://cloud.google.com/architecture/migration-to-google-cloud-transferring-your-large-datasets?hl=fr

Quels que soient le scénario et le type de données à migrer, il est fortement recommandé de protéger les données pendant le processus de transfert en utilisant le cryptage en transit (c'est-à-dire en utilisant des connexions conformes au protocole TLS).

Conclusion

Les organisations peuvent accélérer leur transition vers le cloud tout en restant flexibles face aux changements réglementaires en cours.

Une migration vers le Cloud de Confiance de S3NS est grandement simplifiée si les workloads sont déjà sur Google Cloud Platform ou sur Contrôles Locaux.

En exploitant les bonnes pratiques décrites dans ce document, vous aurez en mémoire ces grandes étapes :

- Définition du champ d'application et inventaire des données
- Planification de l'architecture de workloads autour de modèles spécifiques
- Utilisation des interfaces programmatiques et des API de Google Cloud
- Terraform Infrastructure as Code
- Provisionnement
- Migration / déplacement des données

Les entreprises peuvent planifier longtemps à l'avance - et en toute confiance - leur migration vers le Cloud de Confiance de S3NS.

PERFORMANCE
INNOVATION
CONFIANCE