



PERFORMANCE
INNOVATION
CONFIANCE

CONTROLES LOCAUX AVEC S3NS

Une solution cloud **THALES** x Google Cloud

ÉDITION
2023

INTRODUCTION

L'informatique en nuage (ou Cloud computing) est une formidable opportunité pour accélérer la transformation des entreprises et des administrations, et contribuer à leur compétitivité économique. En 2020, les dépenses mondiales des entreprises en services d'infrastructure cloud ont dépassé pour la première fois les achats de matériels et de logiciels pour Datacenters¹.

En mai 2021, le gouvernement français a présenté sa stratégie nationale pour le cloud² pour répondre au triple enjeu de transformation, compétitivité et souveraineté des organisations publiques et privées. Celle-ci inclut notamment :

- la doctrine cloud au centre, qui fait du cloud un prérequis pour tout projet numérique de l'État, afin d'accélérer la transformation publique
- le label « cloud de confiance », qui définit le plus haut niveau de protection pour les données des français, avec des mesures à la fois juridiques et techniques.

Au-delà des technologies et des offres de services, c'est aussi un changement de culture qui s'engage, afin que les équipes projet et les ingénieurs inscrivent les opportunités du cloud dans leurs pratiques professionnelles au quotidien.

Partageant le même constat, Thales, acteur français reconnu mondialement en matière de hautes technologies au service de la confiance, et Google Cloud, leader mondial des nouvelles technologies au service de l'accès à l'information, ont décidé de s'allier pour offrir le meilleur des deux mondes aux organisations françaises. Aujourd'hui voit la naissance de S3NS, joint-venture créée et dédiée à ce partenariat.

Vous l'avez compris, nous avons souhaité, main dans la main, favoriser la modernisation, la compétitivité, l'innovation de l'État et du tissu économique français avec des choix forts :

- 1) Viser la labellisation SecNumCloud de l'ANSSI de notre offre « cloud de confiance »,
- 2) Favoriser le développement de l'écosystème local d'entreprises de toutes tailles du secteur des technologies, à la fois éditeurs logiciels et entreprises de services numériques,
- 3) Favoriser l'adoption de ces solutions en formant le plus grand nombre à ces nouvelles méthodes de travail.

Nous avons le plaisir de proposer à nos clients dès cette année une première offre technologique commune, détaillée dans ce livre blanc.

Cette offre permet dès aujourd'hui aux entreprises et aux organisations publiques de bénéficier d'un premier niveau de confiance sur la plateforme de Google Cloud en France. Cela représente une étape clé unique sur le marché vers le cloud de confiance ; en attendant la mise en place de la labellisation SecNumCloud.



Anthony Cirot
Directeur Général Google Cloud France



Walter Cappilati
Président de S3NS

SYNTHESE

Répondre aux exigences de sécurité et de confidentialité des institutions publiques et entreprises privées françaises est une priorité pour Thales et Google Cloud.

Pour répondre à ces exigences, Thales et Google Cloud ont créé S3NS, une nouvelle société de droit français majoritairement détenue et entièrement contrôlée par Thales, dont Google est actionnaire extrêmement minoritaire. La mission de S3NS est de fournir des solutions cloud de pointe permettant aux organisations d'atteindre leurs exigences en termes de souveraineté numérique, sans compromis sur leurs performances, leur capacité d'innovation ou leur conformité. S3NS et Google Cloud collaborent en particulier au développement d'une solution destinée à être qualifiée « cloud de confiance » (conforme aux exigences SecNumCloud).

La première solution disponible depuis début 2023 Contrôles locaux avec S3NS, est destinée aux institutions publiques et aux entreprises privées françaises à la recherche d'une sécurité et d'un contrôle renforcés et souhaitant commencer dès maintenant leur trajectoire vers le cloud de confiance. Cette offre n'a pas vocation à être qualifiée « cloud de confiance ».

L'offre Contrôles locaux avec S3NS permet de bénéficier des services Google Cloud avec les mêmes niveaux de performance que la version publique. En outre, l'offre permet de localiser les données des clients en France ou en Europe à leur demande, et limite à du personnel de l'Union européenne l'accès aux données clients pour leur administration et leur support technique. Elle rend possible un contrôle cryptographique de l'accès aux données via un service de gestion externe des clés de chiffrement opéré par S3NS. Cette première offre apporte les bénéfices d'une automatisation supplémentaire permettant de simplifier les opérations, d'une auditabilité et d'une transparence additionnelles afin d'accroître la confiance des clients dans les opérations du cloud.

Les offres de S3NS se veulent compatibles : nous prévoyons d'une part de mettre à disposition sur la future offre cloud de confiance les services d'ores et déjà disponibles dans l'offre Contrôles locaux avec S3NS, et d'autre part de proposer un redéploiement facilité de Contrôles locaux avec S3NS vers le cloud de confiance.

En résumé, Contrôles locaux avec S3NS vous permet dès maintenant d'appliquer des mesures de sécurité additionnelles, de renforcer votre conformité et d'accélérer votre transition vers le cloud de confiance.

DESCRIPTIF DE L'OFFRE

Contrôles locaux avec S3NS permet de répondre aux principales exigences de contrôle et de transparence lors de l'utilisation de Google Cloud.

Pour ce faire, Contrôles locaux avec S3NS permet d'automatiser le déploiement de fonctionnalités sur Google Cloud concernant :

- la localisation des données en France ou dans l'UE, selon les préférences du client
- un contrôle cryptographique sur l'accès aux données, via le contrôle des clés de chiffrement par le client et l'externalisation des clés maître
- la localisation du support technique d'abord par Google Cloud depuis l'Union Européenne, puis par S3NS à partir de fin de novembre 2023

Ces contrôles peuvent être définis à la maille de la charge de travail, garantissant qu'ils peuvent être appliqués et respectés de manière sélective.

Localisation des données

Les règles et contrôles d'organisation de Google Cloud prennent en charge le stockage des données client au repos au sein de la région France (ou de régions UE choisies par le client). Les politiques sont configurées automatiquement lors de la création d'une charge de travail, ce qui réduit le risque de mauvaise configuration qui pourrait entraîner le stockage involontaire de données en dehors de la région choisie.

Contrôle cryptographique sur l'accès aux données

Le contrôle cryptographique de l'accès aux données est réalisé grâce à l'utilisation de justifications d'accès aux clés (Key Access Justifications) avec le support par Google Cloud d'un gestionnaire de clés externes (External Key Manager).

La fonctionnalité de Key Access Justifications permet aux utilisateurs de refuser aux administrateurs Google Cloud l'accès à leurs données sans raison particulière, même dans des situations généralement exemptées du contrôle du client, telles que des pannes ou des réponses à des demandes de données de tiers. Pour ce faire, elle fournit de manière automatique aux clients une raison claire pour laquelle les données doivent être déchiffrées, qu'ils peuvent utiliser pour décider programmatiquement d'utiliser ou non leurs clés externalisées et ainsi autoriser l'accès à leurs données.

En combinant les Key Access Justifications avec l'External Key Manager, les clients bénéficient :

- d'une visibilité sur chaque demande d'utilisation de clé externalisée, permettant aux données (ex. un bucket Cloud Storage) de passer de l'état chiffré au repos à l'état in-use, avec une justification de cette demande
- d'un mécanisme explicite pour décider ou non d'utiliser leur clé externalisée dans le contexte de cette demande via une politique automatisée qu'ils auront définie
- d'un engagement de Google Cloud à protéger l'intégrité des contrôles et des justifications d'accès

Cela signifie qu'il n'y a aucun moyen direct pour Google Cloud de déchiffrer les données client au repos sans approbation, cette approbation pouvant être refusée sans raison particulière. Par exemple, un client peut décider qu'une justification ne correspond pas à sa politique ou nécessite une approbation supplémentaire de ses équipes sécurité, juridiques ou de protection des données.

Grâce à ces contrôles, les clients sont les décisionnaires ultimes de l'accès à leurs données car :

- les données des services Google Cloud proposés sont toujours chiffrées au repos
- le niveau le plus élevé dans la hiérarchie des clés maître (Key Encryption Keys) est géré exclusivement par S3NS, et ces clés sont stockées en dehors de l'infrastructure technique de Google Cloud
- les demandes d'utilisation des clés sont automatiquement accompagnées d'une justification et les clients disposent de moyens programmatiques pour les refuser le cas échéant, pour toute raison qu'ils jugent nécessaire.
- les Key Access Justifications sont détaillées afin que les clients puissent comprendre ce qu'il advient de leurs données (ex. CUSTOMER_INITIATED_SUPPORT lorsque le client soumet un ticket d'assistance et que l'accès à ses données est nécessaire pour résoudre le problème)

S3NS augmente les capacités de contrôle cryptographique disponibles sur Google Cloud pour l'External Key Manager et le Key Access Justifications.

Tout d'abord, S3NS fournit un service d'External Key Manager dédié et élastique, qui réduit le temps et les efforts auxquels les clients Google Cloud sont confrontés pour configurer de manière optimale la gestion des clés externes (généralement 60 à 90 jours voire plus). S3NS opère l'External Key Manager et est responsable de son maintien en conditions de sécurité et de modernité, ce qui constitue un avantage supplémentaire pour le client.

Ensuite, S3NS fournit une inscription automatisée au service de Key Access Justification, ce qui réduit le temps et les efforts auxquels les clients de Google Cloud sont confrontés lors de la configuration de Key Access Justification (généralement plus de 21 jours).

Enfin, S3NS peut définir et gérer les politiques Key Access Justification selon les meilleures pratiques, par exemple pour refuser les demandes d'accès de tiers par défaut. À l'avenir, S3NS prévoit d'offrir des fonctionnalités supplémentaires telles que l'examen et la corrélation des journaux Key Access Justification, et la définition de politiques plus granulaires spécifiques par client.

Transparence et approbation des accès

Les journaux d'accès (Access Transparency Logs) enregistrent les actions que le support et les ingénieurs de Google Cloud entreprennent dans les rares cas où ils ont besoin d'accéder au contenu ou aux configurations du client. Les entrées des Access Transparency Logs incluent des détails tels que la ressource et l'action effectuée, l'heure de l'action, la raison de l'action et des informations sur la personne demandant l'accès.

L'approbation d'accès (Access Approval) garantit que le support et les ingénieurs de Google Cloud obtiennent l'approbation explicite des clients à chaque fois qu'ils ont besoin d'accéder au contenu client. L'approbation est signée cryptographiquement pour garantir son intégrité. Elle fournit également une vue historique de toutes les demandes qui ont été approuvées, rejetées ou expirées.

À la discrétion du client, S3NS pourra recevoir des rapports proactifs sur l'état des contrôles d'accès aux données sur la plateforme Google Cloud via les Access Transparency Logs. À l'avenir, S3NS pourra recevoir des rapports détaillés qui pourront être utilisés pour fournir des informations supplémentaires aux clients.

Support technique

Les exigences des clients peuvent s'étendre au support client : certains clients exigent de la transparence, du contrôle et la restriction du personnel de support à l'Union Européenne ou à la France lorsqu'ils soumettent une demande de support ou lors d'une assistance technique.

Les clients de l'offre Contrôles locaux avec S3NS pourront obtenir un support réalisé uniquement par du personnel situé en Union Européenne (avec des exceptions possibles pour les rares cas de support avancé). Ces restrictions s'étendent au personnel chargé des opérations et du support technique, afin de protéger les données client.

S3NS prendra en charge le support technique, francophone, à partir de novembre 2023.

Ce niveau de service n'est pas proposé par Google Cloud sur son offre standard.

SERVICES CLOUD DISPONIBLES

Contrôles locaux avec S3NS fournit les produits Google Cloud Platform pour lesquels les contrôles de sécurité ci-dessus sont disponibles. Cela permettra aux clients d'utiliser les mêmes produits et services que ceux disponibles sur la plateforme standard Google Cloud, avec le contrôle et la supervision supplémentaires de S3NS, sans compromis sur les fonctionnalités ou les performances.

Disponibilité des produits

L'ensemble des produits pris en charge initialement par la solution (voir tableau ci-dessous) permettra aux clients de créer et d'exécuter des applications modernes et de migrer les charges de travail déployées sur des machines virtuelles. Les clients auront accès à des fonctionnalités de calcul basées sur des machines virtuelles ou des conteneurs, à un stockage cloud élastique et à une base de données SQL. Les services priorités pour 2023 élargiront les options offertes pour les bases de données, la gestion et l'analyse des données.

Disponibilité des produits de l'offre Contrôles locaux avec S3NS		
Disponible	Disponible en Q3/Q4 2023	Priorités pour 2024
• <i>Artifact Registry</i> • <i>BigQuery</i> • <i>Cloud Composer</i> • <i>Cloud console</i> • <i>Cloud DNS</i> • <i>Cloud IAM</i> • <i>Cloud IAP</i> • <i>Cloud Interconnect</i> • <i>Cloud Load Balancing</i> • <i>Cloud Logging</i> • <i>Cloud NAT</i> • <i>Cloud Router</i> • <i>Cloud SQL</i> • <i>Cloud Storage</i> • <i>Compute Engine</i> • <i>Dataproc</i> • <i>Key Management</i> • <i>Kubernetes Engine</i> • <i>Network Connectivity Center</i> • <i>Persistent Disk</i> • <i>Pub/Sub</i> • <i>VPC-SC</i> • <i>VPN</i>	• <i>Big Table</i> • <i>Cloud Spanner</i> • <i>Dataflow</i>	• <i>Apigee</i> • <i>Cloud Armor</i> • <i>Cloud Filestore</i> • <i>Cloud Memorystore</i> • <i>Cloud Monitoring / Stackdriver</i> • <i>Cloud Run</i> • <i>Secret Manager</i> • <i>Security Command Center</i> • <i>Vertex AI</i> <i>Planification en cours pour des services supplémentaires</i>

Cette feuille de route s'étendra progressivement à l'ensemble des services disponibles, afin de proposer des fonctionnalités supplémentaires à nos clients.

Certifications et exigences de conformité

Notre objectif est que l'offre Contrôles locaux avec S3NS bénéficie des mêmes certifications que l'offre standard de Google Cloud.

Google Cloud fait régulièrement l'objet d'une vérification indépendante sur la sécurité, la confidentialité et la conformité de la plateforme, obtenant des certifications, des attestations de conformité ou des rapports d'audit par rapport aux normes internationales. Les certifications obtenues par Google Cloud incluent notamment :

- ISO/CEI 27001:2013
- ISO/CEI 27017:2015
- ISO/CEI 27018:2019
- ISO 9001:2015
- ISO 22301:2019
- ISO 50001:2018
- SOC 1/SOC 2/SOC 3
- EU Cloud Code of Conduct niveau 2 (EU CoC)
- Payment Card Industry Data Security Standard (PCI-DSS)
- BSI Cloud Computing Compliance Criteria Catalog (C5:2020)
- Hébergement de données de santé (HDS)

Une liste complète des certifications et de la documentation relative à la conformité de Google Cloud est disponible ici : Conformité au cloud – Réglementations et certifications | Google Cloud | Google Cloud¹.

L'offre Contrôles locaux avec S3NS permet aux clients d'activer des mesures supplémentaires dont la mise en œuvre est recommandée par le Comité Européen de la Protection des Données. Ces mesures supplémentaires sont :

- la localisation de vos données au repos dans des Datacenters au sein de l'Union Européenne
- la localisation des équipes support susceptibles d'accéder à vos données au sein de l'Union Européenne
- le stockage des clés de chiffrement maître de vos données au repos sous le contrôle de S3NS dans le gestionnaire de clés externe

ÉVOLUTION PREVUE DE L'OFFRE

L'offre Contrôle locaux avec S3NS sera enrichie au fil du temps. Les fonctionnalités actuellement prioritaires incluent :

- l'intégration progressive de la fonctionnalité External Key Management à l'ensemble des services Google Cloud qui stockent des données
- l'externalisation de la gestion des identités client (Bring Your Own Identity)
- les prestations de gestion des services de sécurité (Managed Security Service Provider) pour les zones d'atterrissage des clients
- l'intégration de solutions partenaires proposées par des éditeurs de logiciels indépendants (Independent Software Vendors)

Services optionnels proposés via S3NS ou ses partenaires privilégiés

S3NS travaille avec un ensemble de partenaires privilégiés pour offrir des services de sécurité complémentaires, comprenant la création d'une zone d'atterrissage sécurisée, la migration sécurisée des données client basée sur des mécanismes de chiffrement maîtrisés par S3NS, ainsi que la sécurisation et l'exploitation des applications des clients (ex. surveillance par un centre d'opération de la cybersécurité, tests d'intrusion, conseils en FinOps).

Éditeurs de logiciels indépendants (Independent Software Vendors)

Les clients de Google Cloud s'appuient aujourd'hui sur les services offerts par un écosystème de partenaires de Google Cloud, en complément des services de la plateforme Google Cloud. Développer un écosystème spécifique de partenaires autour de l'offre Contrôles locaux avec S3NS est essentiel pour offrir à nos clients ces services complémentaires de manière compatible avec des exigences accrues de sécurité. Nous partagerons prochainement les éditeurs de logiciel qui supportent l'offre contrôles Locaux avec S3NS.

CLOUD DE CONFIANCE

Une solution en cours de développement par S3NS et Google Cloud visera la certification SecNumCloud¹ (label « cloud de confiance »). Ses principales caractéristiques sont les suivantes :

- la solution sera opérée, sécurisée et commercialisée par S3NS
- les données seront hébergées dans trois Datacenters en région parisienne, dans des zones dédiées sécurisées au niveau physique et logique, et isolées du reste de l'infrastructure Google Cloud en termes de réseau
- l'infrastructure physique et logique sera entièrement opérée par S3NS, y compris les aspects cryptographie et gestion des identités de production
- l'infrastructure physique et logique sera également supervisée par un SOC PDIS.
- S3NS contrôlera les mises à jour avant leur déploiement, et assurera l'exploitation, l'administration et le support

CONCLUSION

En résumé, l'offre Contrôles locaux avec S3NS permettra aux clients d'accélérer leur trajectoire vers le cloud de confiance, en leur proposant dès maintenant :

- Une relation contractuelle avec S3NS : S3NS peut revendre les solutions Google Cloud Platform, Contrôles locaux avec S3NS, et dès à présent le futur cloud de confiance
- Une relation opérationnelle avec S3NS : support technique fourni par S3NS, sur l'External Key Manager pour commencer puis global à partir de novembre 2023, et la mise à disposition de Customer Engineers dédiés
- La mise en place d'un environnement d'intégration similaire au futur « cloud de confiance », par exemple : services disponibles, version des services, expérience utilisateur, contraintes de localisation des données
- L'anticipation de plusieurs mois de la montée en compétences des équipes client (recrutement et formation), afin de bénéficier du niveau de compétence adéquat dès le premier jour de disponibilité du cloud de confiance

Une stratégie simplifiée de redéploiement depuis la solution Contrôles locaux avec S3NS vers la future solution cloud de confiance sera disponible. Elle sera facilitée par une approche d'infrastructure as code et le soutien opérationnel des équipes de S3NS, Google Cloud et leurs partenaires privilégiés.



PERFORMANCE
INNOVATION
CONFIANCE

Contact@S3NS.io

S3NS.io

71 rue de Miromesnil
75008 Paris – France



Une solution cloud **THALES** x Google Cloud