Abilian
CS LAB

OPEN INTEROP

Fiche détaillée, domaine 2 : cloud

Stefane Fermigier (Abilian SAS) · 30 octobre 2026 · DRAFT

Version 0.4
Licence CC BY 4.0

1. État de l'art

1.1 Paysage du cloud en France et en Europe

Le marché du cloud en Europe est dominé par les hyperscalers américains. Selon Synergy Research (juillet 2025), Amazon, Microsoft et Google en détiennent environ 70 % et les fournisseurs européens environ 15 %, une part stable depuis 2022 après une baisse continue depuis 2017. L'écosystème européen compte néanmoins une douzaine de fournisseurs significatifs : en France, OVHcloud, Scaleway, Outscale (Dassault Systèmes), Clever Cloud, Rapid.Space ; on trouve ailleurs en Europe Hetzner, IONOS, Exoscale, StackIT, Open Telekom Cloud, UpCloud, CloudSigma, Fuga Cloud, entre autres.

Le constat partagé est clair : **le verrouillage (vendor lock-in) par les services managés propriétaires est le principal frein à la portabilité et à la souveraineté**. Les clients qui utilisent des services spécifiques AWS (Lambda, DynamoDB, SQS, etc.) ou Azure (Cosmos DB, Azure Functions, etc.) ne peuvent pas migrer sans réécriture applicative significative.

Le cadre juridique a changé depuis la première version de cette fiche. Le chapitre VI du Data Act s'applique depuis le 12 septembre 2025. Il oblige les fournisseurs de services de traitement de données à permettre le changement de fournisseur : préavis et période de transition encadrés, export des données et des actifs numériques exportables, frais de changement réduits au coût réel puis supprimés à compter du 12 janvier 2027. Le règlement fixe l'obligation ; il ne dit pas comment vérifier qu'une sortie a effectivement réussi. Les travaux de cette fiche visent ce point.

1.2 Standards existants par couche

Couche conteneurs, orchestration et virtualisation

Spécifications d'images de conteneurs (OCI)

Standard	Statut	Évaluation
OCI (Image, Runtime, Distribution)	Mature, gouvernance Linux Foundation	Interopérabilité effective au niveau image : une image OCI tourne sur tout runtime conforme

Plateformes d'orchestration et de virtualisation

Plateforme	Origine	Maturité	Notes
CloudStack	Apache Software Foundation	Mature	Plateforme IaaS ; déploiements significatifs en Europe (Leaseweb…)
Kubernetes	Origine Google, versée à la CNCF en 2015	Mature	Orchestration de conteneurs ; écosystème associé : Helm Charts (packaging), CAPI / Cluster API (gestion déclarative multi-infrastructure)
OpenNebula	OpenNebula Systems (Espagne)	Mature	IaaS unifiée (VMs, conteneurs, multi-cloud) ; CERN et recherche européenne
OpenStack	OpenInfra Foundation, forte empreinte européenne (Cleura, OVHcloud, Open Telekom Cloud, StackIT, T-Systems…)	Mature	IaaS de référence pour le cloud privé/souverain européen
Proxmox VE	Proxmox Server Solutions (Autriche)	Mature	Virtualisation KVM + LXC avec gestion de cluster
SlapOS	Nexedi (France)	Mature	Orchestration distribuée décentralisée (sans plan de contrôle central), POSIX-based ; utilisée en production par Rapid.Space
XCP-ng	Vates (France)	Mature	Fork open source de Citrix XenServer (Xen)

Constat : Au niveau **image** (OCI), la couche est interopérable et la gouvernance est neutre. Au niveau **orchestration et virtualisation**, plusieurs plateformes matures coexistent avec des paradigmes différents (décentralisé / centralisé, IaaS / virtualisation, conteneurs / VMs). La fiche propose des profils (observabilité, secrets, adoption de SECA…) qui visent à rester implémentables au-dessus de chacune.

Couche Control Plane / API IaaS (LACUNE MAJEURE)

Standard / Spécification	Statut	Évaluation
SECA (Sovereign European Cloud API)	Émergent	Initiative européenne la plus prometteuse : modèle déclaratif (spec/status), RBAC intégré, spécification OpenAPI développée en ouvert. Lancée en mars 2025 par Aruba, IONOS et Dynamo ; adoption encore limitée à ses initiateurs
API OpenStack	Mature, standard de fait (privé)	APIs impératives, complexes, liées à une implémentation
OCCI	Inactif	Précurseur qui n'a pas atteint l'adoption

Constat : L'absence d'API IaaS unifiée est le verrou structurel. Chaque fournisseur a sa propre API pour créer une VM, un réseau, un volume. SECA est la tentative la plus récente et la mieux architecturée. L'enjeu est de l'amener à une adoption critique parmi les fournisseurs européens.

Couche Infrastructure as Code

Standard / Interface	Statut	Évaluation
HCL (HashiCorp Configuration Language)	Standard de fait	Langage sous-jacent d'OpenTofu et Terraform
TOSCA (OASIS)	Mature, faible adoption	Standard formel trop complexe

Constat : HCL (via OpenTofu) est le standard de fait mais reste un langage lié à un écosystème d'outillage spécifique, pas un standard formel. Côté empaquetage et description fonctionnelle d'environnements, Guix (France/INRIA) et Nix (Pays-Bas) offrent par ailleurs une approche déclarative complémentaire avec garantie de reproductibilité des builds.

Couche services managés (LACUNE MAJEURE)

Service	Standard existant	Problème
Stockage objet	**API S3** (de fait)	Fonctionne pour l'usage courant : quasi tous les clouds l'implémentent. Spécification contrôlée par AWS seul ; écarts de couverture et de comportement lors d'une sortie complète. Un profil de réversibilité est en cours (cf. §1.4)
Observabilité	**OpenTelemetry** (CNCF)	Modèle de données et protocole (OTLP) stables, logs compris ; formats applicatifs encore hétérogènes et pas d'API de consultation commune
Événements	**CloudEvents** (CNCF)	Adoption encore faible
Gestion de secrets	Aucun	API Vault/OpenBao = inspiration, pas un standard
Bases de données managées	Aucun	Chaque provider a sa propre API
Files d'attente	Aucun	SQS, Azure Service Bus, etc. tous incompatibles
Fonctions serverless	Aucun	Lambda, Cloud Functions, Azure Functions : APIs incompatibles
DNS managé	Aucun standard d'API	Chaque provider a sa propre API

Constat : Au-delà du stockage objet (API S3 de fait), il n'existe quasiment aucun standard d'API pour les services managés. C'est ici que le lock-in est le plus fort.

1.3 Matrice du marché cloud européen

L'analyse de 12 fournisseurs européens révèle :

- **Largement disponibles :** VMs (KVM/Xen, OpenNebula, OpenStack, Proxmox, XCP-ng), stockage bloc, stockage objet S3-compatible, orchestration managée
- **Inégalement couverts :** équilibrage de charge, VPC, DNS managé, IAM avancé
- **Rarement disponibles :** serverless, NoSQL managé, files d'attente managées, PaaS complet
- **Quasi-absents :** équivalents de Firebase/Amplify, entrepôts de données, requêtes serverless

L'interopérabilité cloud européenne est donc aujourd'hui possible pour les cas simples (VMs, orchestration, stockage objet S3-compatible), mais pas pour les architectures applicatives avancées. Même pour les cas simples, la compatibilité annoncée reste à vérifier : le §1.4 le montre sur le stockage objet.

1.4 Le stockage objet, premier cas traité (atelier du 9 octobre 2026)

L'atelier Open Interop du 9 octobre 2026 (Track 6, « Connecting the Clouds ») a pris le stockage objet comme premier cas de réversibilité. Ses résultats valent au-delà de ce service :

- **Une déclaration ne suffit pas.** Une offre « compatible S3 » doit préciser les fonctions qu'elle prend en charge et apporter une preuve sur ce périmètre. L'acheteur doit pouvoir exécuter, ou faire exécuter, un test versionné sur un jeu de données connu et obtenir un rapport vérifiable.
- **Des critères obligatoires, sans compensation.** Aucune conformité si un objet manque, si son contenu est corrompu ou si un droit interdit devient autorisé. Les autres mesures (durée totale, débit utile, reprise, automatisation, coût) sont publiées à part. Le score global pondéré est reporté ; la doctrine proposée exclut d'ailleurs toute moyenne pondérée pour la conformité. Par ailleurs, un seuil universel de débit serait prématuré.
- **Des comportements, pas seulement des interfaces.** L'ETag ne prouve pas l'intégrité : le test calcule sa propre empreinte. Les droits se comparent par leur effet sur les accès. L'application du client doit fonctionner chez le nouveau fournisseur après révocation de ses accès à l'ancien.
- **Quatre verdicts** par critère : conforme, non conforme, non applicable, non concluant. Le dernier distingue une panne de l'environnement de test d'un défaut du service.
- **Preuve technique et contrat.** Le kit de test apporte une preuve technique. Son intégration à un contrat demande une rédaction propre : périmètre, mesure, conditions de test, conséquences d'un écart.

L'atelier a produit un profil, sept exigences, une scorecard et six scénarios de test (CTK-01 à CTK-06, le dernier à affiner). Le projet S4 (*Sovereign S3*) les détaille dans une série de notes : synthèse, constat et propositions, contrats comportementaux, scorecard, scénarios de test. Son kit de test de conformité, le CTK S4, met en œuvre les cinq premiers scénarios. Ses premiers essais montrent l'utilité de la démarche. Garage est conforme au niveau de base, sauf sur les lectures conditionnelles (`If-Match`) qu'il ignore ; il ne prend pas en charge les étiquettes d'objet. Ceph RGW, sur son moteur de stockage autonome, ne termine jamais la lecture de certains objets multiparties. Le client AWS de référence rejette par défaut, depuis janvier 2025, les réponses de plusieurs services compatibles. Aucun de ces écarts n'apparaît dans une déclaration de compatibilité.

2. Analyse des besoins de l'écosystème français

2.1 Pain points identifiés

Les frustrations ci-dessous sont des **retours qualitatifs** issus des échanges du CSF, des discussions Cigref/TOSIT, des consultations ARCEP et de l'étude OPIIEC sur l'interopérabilité (cf. note de vision et état de l'art pour les références). Elles n'ont pas fait l'objet d'un sondage quantitatif dédié et seront à corroborer par un travail empirique ultérieur. Le cadrage stratégique général est celui de l'**interopérabilité opposable** (cf. note de positionnement Abilian, novembre 2025 : *« L'interopérabilité, clé de l'efficacité collaborative et de la souveraineté »*).

Côté clients (DSI, architectes) :

1. **« Migrer d'AWS/Azure vers un cloud français, c'est réécrire l'application »** : les services managés propriétaires créent une dépendance technique profonde.
2. **« On ne peut pas comparer objectivement les offres cloud »** : absence de vocabulaire commun pour décrire les capacités des fournisseurs (pas de « dataspace d'infrastructure »).
3. **« Le multi-cloud, c'est gérer N APIs différentes »** : les équipes DevOps doivent maintenir des configurations spécifiques par fournisseur.

4. « **Les logs sont dans un format différent sur chaque cloud** » : la supervision multi-cloud est un cauchemar opérationnel.
5. « **Les secrets (clés API, certificats) sont verrouillés chez le provider** » : la migration des secrets est un risque opérationnel.

Côté fournisseurs cloud français/européens :

6. « **On ne peut pas rivaliser avec les hyperscalers service par service** » : mais un front commun d'interopérabilité permettrait de combiner les forces.
7. « **Les clients nous demandent d'être compatibles Terraform, mais chaque provider écrit son propre plugin** » : duplication d'effort colossale.
8. « **Il n'y a pas de label ou de certification d'interopérabilité** » : pas de moyen de prouver sa portabilité aux clients.

Côté acheteurs (atelier du 9 octobre 2026) :

9. « « **Compatible S3 » ne précise pas les fonctions prises en charge** » : l'acheteur ne peut ni comparer les offres ni vérifier, avant de signer, qu'une sortie sera possible.

2.2 Besoins structurels

- **Permettre la portabilité applicative** : qu'un client puisse migrer d'un cloud à un autre sans réécriture, au moins pour les briques standardisables.
- **Créer un front commun européen** : les clouds européens ont intérêt à s'allier sur la couche d'interopérabilité pour se différencier collectivement des hyperscalers.
- **Outiller la commande publique** : pour la circulaire du Premier ministre n° 6519/SG du 5 février 2026, la réversibilité est « un élément-clé dans le choix des solutions » que les contrats doivent prendre en compte ; le Data Act impose le changement de fournisseur. Il n'existe pourtant aucun référentiel technique pour vérifier qu'une sortie réussit. L'atelier du 9 octobre prévoit une proposition d'annexe contractuelle pour le stockage objet en décembre 2026.
- **Promouvoir l'interopérabilité opposable** : obtenir que les exigences d'interopérabilité se vérifient par des tests reproductibles (cf. doctrine, principe 1), dans les marchés comme dans l'application du Data Act.

2.3 Priorisation des besoins

Besoin	Urgence	Impact	Faisabilité
Réversibilité du stockage objet (profil S4)	Haute	Élevé	Haute (en cours depuis octobre 2026)
Standard d'API de logs / observabilité	Haute	Élevé	Haute (OpenTelemetry comme base)
Standard de gestion de secrets	Haute	Élevé	Moyenne (API Vault comme inspiration)
API IaaS unifiée (SECA ou équivalent)	Stratégique	Très élevé	Moyenne (SECA existe, adoption à construire)
Indicateur de portabilité / interopérabilité	Haute	Élevé	Moyenne (méthode éprouvée sur le stockage objet, à étendre service par service)
Standard d'API pour services managés avancés	Stratégique	Très élevé	Faible (champ vierge)

3. Propositions concrètes

Chaque chantier proposé suit la proposition de doctrine : il livre un profil, une implémentation de référence quand il n'en existe pas, une suite de tests de conformité libre et un modèle de déclaration de conformité (principe 4).

Prérequis transverses : Tous les chantiers cloud s'appuient sur les livrables de la fiche transverse :

- **T1 (Identité OIDC/SCIM)** est le socle d'authentification pour les control planes cloud, y compris l'authentification JWT exigée par SECA (cf. CL3). L'identité d'un orchestrateur (OIDC) se distingue de la signature des requêtes d'un service comme S3. OAuth 2.1 restant un projet de l'IETF, toute exigence formelle immédiate s'appuie sur OAuth 2.0 et ses extensions de sécurité publiées (RFC 9700).
- **T2 (Style guide API REST)** définit les conventions communes (pagination, filtrage, erreurs, versioning) que les APIs de CL1/CL2/CL3 doivent respecter.
- **T4 (Notifications)** fournit le format CloudEvents réutilisable pour la supervision (lien avec CL1) et les événements de control plane.

3.1 Chantier CL1 : Standard de logs et observabilité

Objectif : Un administrateur peut consulter les logs de n'importe quel cloud européen avec le même outil et le même format.

Base : OpenTelemetry (CNCF)

Actions :

1. **Profil Open Interop d'observabilité** : rédiger un profil fondé sur OpenTelemetry qui spécifie :
   - Le format de log structuré obligatoire (JSON-L, schéma OpenTelemetry Logs)
   - Les champs obligatoires (timestamp, severity, resource, trace_id, etc.)
   - La distinction logs d'infrastructure vs. logs de sécurité
2. **API de consultation** : spécifier une API REST (OpenAPI) permettant de requêter, filtrer et exporter les logs de manière standardisée, indépendamment du backend de stockage.
3. **Implémentation de référence** : développer un collecteur/proxy open source implémentant cette API, avec des connecteurs pour 2-3 clouds européens.
4. **Suite de tests** : outil de validation de conformité, avec un modèle de déclaration de conformité.

Livrables : Profil documenté, spécification OpenAPI, implémentation de référence, suite de tests, modèle de déclaration.

Délai : 6-9 mois.

3.2 Chantier CL2 : Standard de gestion de secrets

Objectif : Les secrets (clés API, certificats, mots de passe) sont gérés via une API standard, portable entre fournisseurs.

Inspiration : API HashiCorp Vault / OpenBao

Actions :

1. **Analyse de l'API Vault/OpenBao** : extraire un sous-ensemble minimal de fonctionnalités (CRUD de secrets, rotation, audit log, politiques d'accès) formant un standard d'API.
2. **Spécification OpenAPI** : publier une spécification formelle de l'API de coffre-fort, avec des profils de conformité (basique, avancé).
3. **POC multi-cloud** : démontrer la portabilité de secrets entre 2 clouds européens via cette API standard.

4. **Intégration IaC** : fournir un provider OpenTofu implémentant cette API standard.

Livrables : Spécification OpenAPI, POC, provider OpenTofu.

Délai : 6-9 mois.

3.3 Chantier CL3 : Adoption et extension de SECA

Objectif : Faire de SECA (ou d'une spécification dérivée) le standard d'API IaaS adopté par les clouds européens, en particulier français.

Actions :

1. **Évaluation technique de SECA** : analyse approfondie de la spécification actuelle et de ses éléments de conformité, identification des forces (modèle déclaratif, RBAC, OpenAPI) et des lacunes (couverture fonctionnelle, PaaS, services managés).
2. **Engagement des fournisseurs français** : organiser avec OVHcloud, Scaleway, Outscale, Clever Cloud et Rapid.Space un atelier sur SECA, sur le modèle de celui du 9 octobre 2026 sur le stockage objet, pour évaluer la spécification et recueillir leurs besoins.
3. **Extensions proposées** :
   - Extension PaaS (déploiement d'applications, pas seulement d'infrastructure)
   - Extension services managés (bases de données, files d'attente)
   - Mécanisme de discovery (catalogue de capacités d'un fournisseur)
4. **Contribution à la spécification** : les extensions développées sont contribuées au projet SECA pour renforcer l'adoption européenne.
5. **Complémentarité TOSCA** : valider la complémentarité SECA/TOSCA via un POC d'orchestration.

Livrables : Rapport d'évaluation, propositions d'extensions, POC SECA + TOSCA.

Délai : 9-12 mois.

3.4 Chantier CL4 : Indicateur d'interopérabilité cloud

Objectif : Permettre de mesurer objectivement le niveau d'interopérabilité et de réversibilité d'un fournisseur cloud, service par service.

Méthode : celle que l'atelier du 9 octobre 2026 a définie pour le stockage objet (cf. §1.4), appliquée à chaque service :

1. **Profil et contrats comportementaux** : le sous-ensemble de l'API retenu, les fonctions que le fournisseur peut revendiquer et les comportements attendus lors d'une sortie.
2. **Scorecard** : des critères obligatoires de conformité sans compensation possible, plus des mesures publiées séparément avec leurs conditions. D'éventuels niveaux se définiraient par les critères obligatoires satisfaits, jamais par une moyenne.
3. **Suite de tests** : scénarios versionnés, jeux de données reproductibles, quatre verdicts, rapport assez complet pour qu'un tiers reproduise l'essai.
4. **Indicateur** : calculé à partir des rapports de conformité, selon une méthode publique (doctrine, §5.4) ; la preuve relève d'un des trois niveaux de la doctrine (autoévaluation, vérification, essai croisé).
5. **Publication** : matrice comparative des fournisseurs, mise à jour à chaque campagne d'essais croisés.

Premier cas : réversibilité du stockage objet (projet S4). Le calendrier proposé par l'atelier prévoit un TechSprint début novembre 2026, des essais croisés entre au moins deux fournisseurs fin novembre, puis un profil V0.1 et une proposition d'annexe contractuelle en décembre. Le CTK S4 couvre déjà les scénarios CTK-01 à CTK-05 (cf. §1.4).

Cas suivants : stockage bloc et images de machines virtuelles, bases de données managées, puis les services couverts par CL1 et CL2 une fois leurs profils publiés.

Livrables : profil et suite de tests par service, méthode de calcul de l'indicateur, première matrice comparative.

Délai : stockage objet fin 2026 ; deux services supplémentaires dans les 12 mois suivants.

3.5 Chantier CL5 : Guides d'architecture cloud-agnostique

Objectif : Fournir aux DSI et architectes des guides pratiques pour concevoir des applications portables.

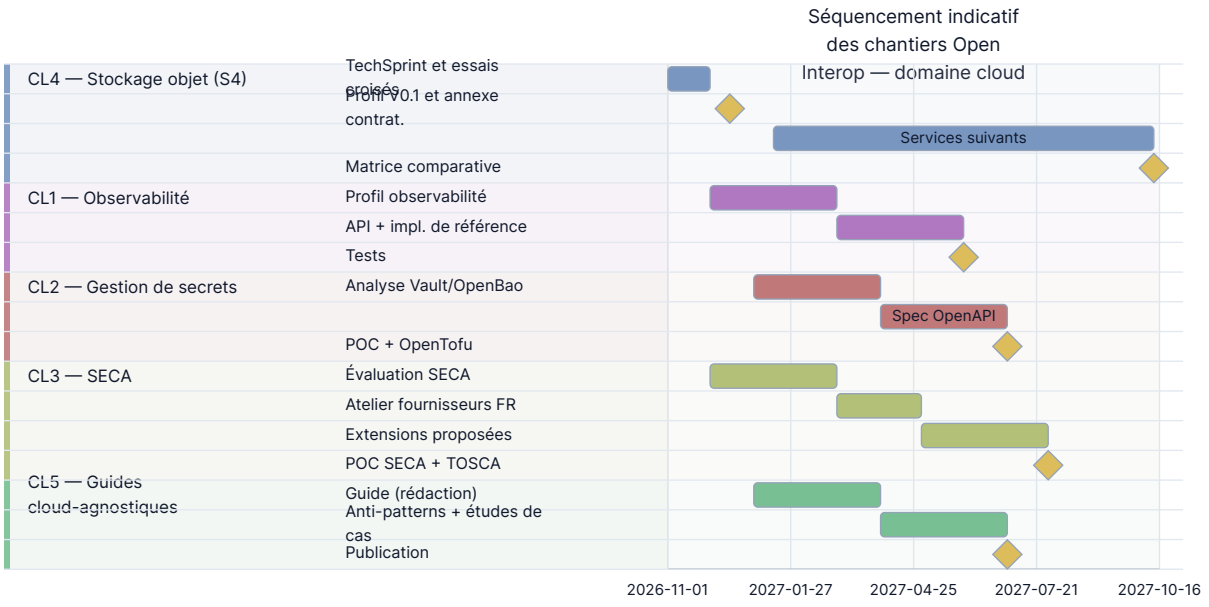
Actions :

1. **Guide de bonnes pratiques** : documenter les patrons d'architecture cloud-agnostiques :
   - Abstraction des services managés (utiliser des interfaces, pas des SDKs propriétaires)
   - Stratégie de conteneurisation : OCI au niveau image ; la plateforme d'orchestration ou de virtualisation (CloudStack, Kubernetes, OpenNebula, OpenStack, Proxmox VE, SlapOS, XCP-ng…) se choisit selon les contraintes opérationnelles et de souveraineté
   - Gestion de configuration externalisée
   - Stratégies de stockage portable (API S3 comme socle)
   - Observabilité standardisée (OpenTelemetry)
2. **Anti-patterns documentés** : recenser les pièges de lock-in les plus fréquents avec des alternatives concrètes, dont la confiance dans une compatibilité déclarée sans périmètre ni preuve.
3. **Étude de cas** : documenter 2-3 cas réels de migration entre clouds européens.

Livrables : Guide publié, fiches anti-patterns, études de cas.

Délai : 6-9 mois (peut avancer en parallèle des autres chantiers).

3.6 Vue d'ensemble et séquencement



Le séquencement initial prévoyait un démarrage en juin 2026 ; seul le chantier CL4 a démarré, par le stockage objet, en octobre. Les dates ci-dessus dépendent des participants que chaque chantier réunira (doctrine, §5.1).

3.7 Coopération européenne

Ces chantiers ne peuvent réussir qu'avec une dimension européenne :

- **SECA** : contribuer à la spécification et rallier les fournisseurs français
- **EuroStack** : s'appuyer sur la fondation EuroStack pour la coordination inter-pays
- **DG CNECT** : présenter les travaux pour nourrir les futures régulations (Data Act, Interoperable Europe Act)
- **APELL / OpenForum Europe** : relais de plaidoyer auprès des institutions européennes

3.8 Alignement avec le plan d'action CSF Cloud

Les chantiers ci-dessus s'inscrivent dans le plan d'action plus large du CSF sur l'interopérabilité cloud, structuré en 5 piliers :

Pilier CSF	Chantiers Open Interop correspondants
Pilier 1 : Socle technique (livre blanc, contrats sémantiques, catalogue de connecteurs)	CL1 (observabilité), CL2 (secrets), CL3 (SECA), CL5 (guides)
Pilier 2 : Preuve et conformité (Compliance Test Kit, indice d'interopérabilité, audit des boîtes noires)	CL4 (indicateur d'interopérabilité), suites de tests de CL1/CL2/CL3
Pilier 3 : Levier économique et juridique (clauses marchés publics, label EU Sovereign Cloud, lobbying ARCEP/DG CNECT)	Phase 3 proposée par la note de vision
Pilier 4 : Écosystème et formation (hackathons, référentiel de compétences OPIIEC, plateforme best practices)	CL5 (guides), hackathons d'interopérabilité
Pilier 5 : Gouvernance, Design Authority (entité experte neutre, validation des standards, lien avec le lab I4C)	Autorité technique de la doctrine proposée (§7), en lien avec l'ARCEP et le laboratoire I4C (IMT)

Éléments spécifiques du plan CSF à intégrer :

- **Contrats sémantiques** (Action 1.2 du CSF) : au-delà des APIs, définir les comportements attendus des services. Par exemple, comment un service de stockage objet doit réagir lors d'une exportation massive, quels sont les SLA de disponibilité des APIs d'interopérabilité, etc. Cela rejoint le concept d'**interopérabilité opposable** : ce sont des résultats mesurables, pas des déclarations de conformité. Une première version existe pour le stockage objet, issue de l'atelier du 9 octobre 2026.
- **Catalogue de connecteurs standards** (Action 1.3 du CSF) : identifier et référencer les connecteurs open source existants (opérateurs Kubernetes, modules OpenNebula, modules OpenStack, providers OpenTofu, recettes SlapOS, bibliothèques d'API) pour chaque couche du continuum cloud-to-edge.
- **Hackathons d'interopérabilité** (Action 4.1 du CSF) : faire collaborer des industriels consommateurs de cloud (Renault, Schneider, EDF…) avec des fournisseurs européens (OVH, Scaleway, Cloud Temple…) pour valider des cas d'usage multi-cloud concrets. Le TechSprint de novembre 2026 sur le stockage objet en est une première forme.
- **Référentiel de compétences** (Action 4.2 du CSF) : en lien avec l'OPIIEC, définir les compétences de « l'ingénierie de l'interopérabilité » et adapter l'offre de formation.

- **Design Authority** (Pilier 5 du CSF) : entité experte chargée de valider les dispositifs techniques d'interopérabilité. La doctrine proposée en ferait l'**autorité technique** d'Open Interop : elle validerait les profils et les suites de tests, délivrerait les badges, accorderait les dérogations et trancherait les différends. Elle pourrait être constituée avec le laboratoire I4C (laboratoire commun « Interoperability 4 Cloud » de l'IMT et d'acteurs industriels).

Références

Standards et spécifications — Conteneurs et orchestration

- **OCI** (Open Container Initiative) — Image, Runtime, Distribution Specs (Linux Foundation). https://opencontainers.org/
- **Kubernetes** — Documentation officielle (CNCF, projet d'origine Google), inclut Helm Charts et Cluster API. https://kubernetes.io/docs/reference/

Plateformes d'orchestration et de virtualisation européennes

- **OpenNebula** — Plateforme IaaS unifiée (Espagne, OpenNebula Systems) ; utilisée notamment au CERN. https://opennebula.io/
- **OpenStack** — Plateforme IaaS open source (OpenInfra Foundation), forte empreinte européenne. https://www.openstack.org/
- **Proxmox VE** — Plateforme de virtualisation KVM+LXC (Autriche, Proxmox Server Solutions). https://www.proxmox.com/en/proxmox-virtual-environment/
- **SlapOS** — Orchestration distribuée décentralisée (Nexedi, France) ; utilisée en production par Rapid.Space. https://slapos.nexedi.com/
- **XCP-ng** — Fork open source de Citrix XenServer (Vates, France). https://xcp-ng.org/

Standards et spécifications — APIs cloud et IaC

- **SECA** (Sovereign European Cloud API) — Aruba, IONOS, Dynamo (mars 2025). https://www.secapi.cloud/
- **OCCI** (Open Cloud Computing Interface) — OGF. https://occi-wg.org/
- **TOSCA** — OASIS. https://www.oasis-open.org/committees/tosca/
- **OpenTofu** — Fork open source de Terraform. https://opentofu.org/
- **Crossplane** — IaC basé sur Kubernetes (CNCF). https://www.crossplane.io/
- **HCL** (HashiCorp Configuration Language) — Spécification. https://github.com/hashicorp/hcl

Standards et spécifications — Services et observabilité

- **OpenTelemetry** — CNCF. https://opentelemetry.io/
- **CloudEvents** — CNCF. https://cloudevents.io/
- **OpenBao** — Fork communautaire de Vault. https://openbao.org/
- **API S3** — Documentation AWS (interface de fait). https://docs.aws.amazon.com/AmazonS3/latest/API/
- **OAuth 2.0 Security Best Current Practice** — RFC 9700 (BCP 240), IETF, janvier 2025.

Réglementation et marché

- Règlement (UE) 2023/2854 (Data Act), chapitre VI : changement de fournisseur de services de traitement de données ; applicable depuis le 12 septembre 2025, suppression des frais de changement au 12 janvier 2027.

- Synergy Research Group, *European Cloud Providers' Local Market Share Now Holds Steady at 15%*, juillet 2025.

Analyses et documents de travail

- Comparaison SECA / OCCI / OpenStack / TOSCA, note diffusée au CSF en septembre 2025
- Matrice des fonctionnalités du cloud européen — https://pad.cloud.abilian.com/s/z3OQJl9ZP
- Note CSF sur l'interopérabilité (S. Fermigier, nov. 2025) — https://pad.cloud.abilian.com/s/HLoX9YJ7V
- CNLL, « Interopérabilité cloud : le CNLL prend position » — https://cnll.fr/news/interoperabilite-cloud-le-cnll-prend-position/ (2024)
- Notes S4 du GT Cloud, issues de l'atelier du 9 octobre 2026 : position, contrats comportementaux, scorecard, scénarios de test
- CTK S4, kit de test de conformité du profil S4 (*Sovereign S3*)

Fournisseurs cloud européens (référencés dans la matrice)

OVHcloud (https://www.ovhcloud.com/), Scaleway (https://www.scaleway.com/), Hetzner (https://www.hetzner.com/), IONOS (https://www.ionos.com/), Exoscale (https://www.exoscale.com/), Open Telekom Cloud (https://open-telekom-cloud.com/), Rapid.Space (https://rapid.space/), StackIT (https://www.stackit.de/), Upcloud (https://upcloud.com/), CloudSigma (https://www.cloudsigma.com/), etc.

Documents Open Interop

- Note de vision Open Interop
- État de l'art des standards d'interopérabilité
- Fiche transverse (chantier T1 = socle identité commun à CL1/CL2/CL3 ; T2 = style guide API pour les control planes cloud)
- Fiche collaboratif
- Fiche cybersécurité
- Proposition de doctrine pour Open Interop