11 questions à poser avant de choisir une solution de gestion des identités

Choisir une solution de gestion des identités et des accès (Identity Access Management - IAM) engage votre organisation sur plusieurs années. Infrastructure dédiée ou partagée, hébergement européen, modèles de coût, réversibilité, conformité réglementaire : autant de critères que vos prestataires ne mettront pas nécessairement en avant. Ce document réunit les questions à poser et les signaux d'alerte à repérer dans les réponses.

> **Comment utiliser ce document**
> Posez ces 11 questions à chaque prestataire IAM que vous évaluez, puis comparez les réponses. Une réponse évasive, ou l'absence de réponse, est en soi une information.

HÉBERGEMENT ET SOUVERAINETÉ

01 Où sont physiquement hébergées mes données d'identité ?

L'annuaire des utilisateurs, les empreintes de mots de passe, les jetons de session et les journaux de connexion comptent parmi les données les plus sensibles de votre système d'information (SI) : leur compromission ouvre l'accès à toutes vos applications. Certains fournisseurs annoncent « Europe » tout en sous-traitant à des infrastructures hors Union européenne. Demandez le pays précis, le datacenter, et la liste des sous-traitants hébergeurs.

Signal d'alerte – *réponse vague (« nos datacenters européens »), refus de préciser où sont stockés l'annuaire et les secrets, ou recours à Amazon Web Services (AWS) / Microsoft Azure / Google Cloud (GCP) sans localisation garantie.*

02 Mes données sont-elles exposées aux lois extraterritoriales américaines (Cloud Act, FISA) ?

Deux textes américains s'appliquent aux fournisseurs de droit américain, quel que soit le lieu de stockage. Le Cloud Act (2018) permet aux autorités d'exiger l'accès aux données qu'ils détiennent. Le Foreign Intelligence Surveillance Act, ou FISA, (section 702) sert de base aux programmes de surveillance visant les personnes non américaines - c'est ce texte qui a conduit la Cour de justice de l'Union européenne à invalider le Privacy Shield en 2020 (arrêt Schrems II). Okta/Auth0, Microsoft et tout fournisseur à maison-mère américaine y sont soumis.

Signal d'alerte – *le prestataire est une société américaine ou la filiale d'une société américaine. La conformité RGPD et l'hébergement en Europe ne suffisent pas à écarter ce risque.*

03 Mon annuaire d'identités est-il isolé ou mutualisé avec d'autres clients ?

Sur une plateforme d'identité, la mutualisation (multi-tenant) signifie que vos comptes, vos secrets et vos jetons cohabitent avec ceux d'autres organisations dans une même base. Cela expose à des risques de voisinage : fuite entre locataires, corrélation de journaux, indisponibilité partagée. Une instance dédiée isole entièrement votre annuaire (application, base de données, système de fichiers).

Signal d'alerte – *le prestataire ne peut pas confirmer l'isolation complète de votre annuaire, ou stocke les identités de plusieurs clients dans une base partagée.*

CONFORMITÉ ET RÉGLEMENTATION

04 Quelles certifications s'appliquent, et couvrent-elles la solution que j'achète ?

ISO 27001 (gestion de la sécurité de l'information), HDS (hébergeur de données de santé), SecNumCloud (qualification ANSSI) ou SOC 2 attestent d'une maturité auditée par un tiers. Point clé : une certification porte souvent sur la plateforme ou le fournisseur, pas sur chaque produit et certaines (comme HDS) peuvent faire l'objet d'un contrat distinct, facturé en sus. Demandez le périmètre exact et les conditions d'application à votre solution.

Signal d'alerte – *certifications présentées sans préciser leur périmètre, confusion entre certification de la plateforme et de la solution achetée, ou conditions (contrat ou coût supplémentaire) passées sous silence.*

05 Le service fournit-il les éléments nécessaires à ma conformité NIS2 ?

La directive NIS2 impose de maîtriser sa chaîne d'approvisionnement numérique. Votre IAM en fait partie : vous devez pouvoir documenter les mesures de sécurité de votre prestataire et ses procédures de notification d'incident lors d'un audit.

Signal d'alerte – *le prestataire ne peut fournir ni certification, ni mesures de sécurité documentées, ni procédure de notification d'incident exploitables pour votre propre dossier de conformité.*

06 Qui est responsable des mises à jour de sécurité, et comment les vulnérabilités sont-elles suivies ?

Les failles sur Keycloak ou ses bibliothèques sous-jacentes font l'objet de vulnérabilités publiques référencées (CVE). En modèle autogéré, c'est à votre équipe de corriger. En modèle managé, vérifiez qui prend en charge les correctifs et comment le suivi des vulnérabilités est organisé.

Signal d'alerte – *le prestataire ne précise pas qui déploie les correctifs, ni comment les vulnérabilités sont surveillées et traitées.*

DISPONIBILITÉ ET SÉCURITÉ DU SERVICE

07 Quel est le SLA de disponibilité, et que couvre-t-il ?

Un SLA à 99,9 % représente environ 9h d'indisponibilité autorisée par an ; à 99,99 %, moins d'une heure. Vérifiez le périmètre couvert, le traitement des fenêtres de maintenance, et l'existence de pénalités contractuelles en cas de dépassement.

Signal d'alerte – *SLA inférieur à 99,9 %, maintenance non planifiée intégrée au calcul de disponibilité, ou absence de compensation contractuelle.*

08 Quelles méthodes d'authentification forte sont proposées ?

Un service d'identité doit couvrir l'authentification multifacteur sans dépendance à une technologie unique : clés d'accès (passkeys) et WebAuthn, codes temporaires à usage unique, application mobile d'authentification, ainsi que l'authentification par élévation (step-up), qui exige un facteur supplémentaire uniquement pour les actions sensibles. Vérifiez l'étendue des méthodes disponibles et leur compatibilité avec vos usages.

Signal d'alerte – *authentification multifacteur limitée à une application maison, absence de clés d'accès (passkeys) / WebAuthn, ou méthodes reposant sur une technologie propriétaire.*

RÉVERSIBILITÉ ET STANDARDS OUVERTS

09 Puis-je récupérer l'intégralité de mes identités, empreintes de mots de passe comprises ?

Sur un service d'identité, la réversibilité ne se limite pas à exporter la liste des utilisateurs : sans les empreintes de mots de passe, une migration contraint tous vos utilisateurs à réinitialiser leur accès. Demandez le format d'export (par exemple l'export de realm JSON pour Keycloak), le périmètre exact des données récupérables, et les conditions d'export des secrets.

Signal d'alerte – *empreintes de mots de passe non exportables, export des secrets restreint selon le forfait ou seulement sur demande, format propriétaire, ou absence de procédure de migration documentée.*

10 La solution repose-t-elle sur des standards d'identité ouverts, et sait-elle fédérer mes annuaires existants ?

OAuth 2.0, OpenID Connect (OIDC) et SAML v2 garantissent l'interopérabilité avec vos applications ; la fédération LDAP / Active Directory et l'intermédiation avec d'autres fournisseurs d'identité évitent de dupliquer vos comptes. Une solution qui n'implémente ces standards que partiellement, ou via des extensions propriétaires, vous enferme dans son écosystème.

Signal d'alerte – *support partiel des standards, absence de SAML v2, ou fédération LDAP / Active Directory et intermédiation limitées à des connecteurs propriétaires.*

COÛT TOTAL ET MODÈLE TARIFAIRE

11 Le tarif est-il transparent et prévisible, et que couvre-t-il exactement ?

Les modèles par utilisateur actif mensuel (MAU) ou par utilisateur provisionné peuvent générer des surprises en cas de croissance ou de pic. Vérifiez l'existence d'une grille publique, le préavis en cas de hausse et vos options si le prix augmente. Distinguez ensuite ce qui est compris dans le prix affiché de ce qui relève d'options payantes (niveau de service garanti [SLA], support, migration), et vérifiez l'existence éventuelle de frais de sortie.

Signal d'alerte – *absence de grille publique, hausses sans préavis, options critiques (SLA, support 24/7) non distinguées du tarif de base, ou frais de sortie en cas de résiliation.*