Sécurité du Cloud Lifesize

Gustavo Villardi

Avril 2019

lifesize

Data Centers

- Hébergé sur des data centers
  - 99.99% de disponibilité
- Sécurité physique
  - Accès contrôlé 24h/24 et 7j/7 par biométrique/vidéo
- Sécurité logique
  - Multi pare-feu, IPS, IDS, protection anti-DDoS, analyses fréquentes des vulnérabilités
  - Lifesize passe des contrats avec des agences externes pour des tests PEN annuels du service.

Data Centers

- Certifications de haut niveau :
  - ISO 27001 - Sécurité physique, sécurité de l'information, disponibilité des services
  - ISO 27017 - Sécurité de l'information pour les fournisseurs de services cloud
  - ISO 27018 - Protection de la sécurité de l'information et de la vie privée
  - ASC - L'assurance de la sécurité dans le Cloud Computing
  - SOC - Audit annuel sur l'intégrité et la sécurité des données ainsi que sur les processus internes
  - PCI - Autorisé à gérer les données des cartes de crédit
  - HIPAA - Autorisé à gérer l'information sur la santé

Confidentialité des données

- Exigence de l'UE :
  - Conformité avec le règlement général de la CE sur la protection des données (GDPR) qui remplacera la directive 95/46 et garantira l'harmonisation des réglementations en matière de protection des données de tous les pays de l'UE.

- Accord international de principes pour la protection des données personnelles entre l'UE et les États-Unis
  - Sphère de sécurité États-Unis-UE - Invalidée par la CE en octobre 2015
  - US-EU Privacy Shield - Lifesize et ses sous-traitants certifiés (11/2016)
  - RGPD - Lifesize et sous-traitants certifiés (05/2018)

aws

lifesize

Confidentialité des données

- Données conservées par Lifesize
  - Administrateur
    - e-mail, nom, téléphone, adresse, société et éventuellement le mot de passe
  - Utilisateurs
    - e-mail, nom et éventuellement le mot de passe
  - Appels
    - Peuvent être enregistrés en option si la fonction est activée par l'administrateur.
    - Métadonnées de base des appels stockés afin que les administrateurs clients puissent accéder aux rapports d'utilisation.
  - Enregistrement du serveur
    - Conservé à des fins de missions de soutien technique et de dépannage.
  - Chat
    - Enregistré éventuellement si la fonction est activée par l'administrateur.

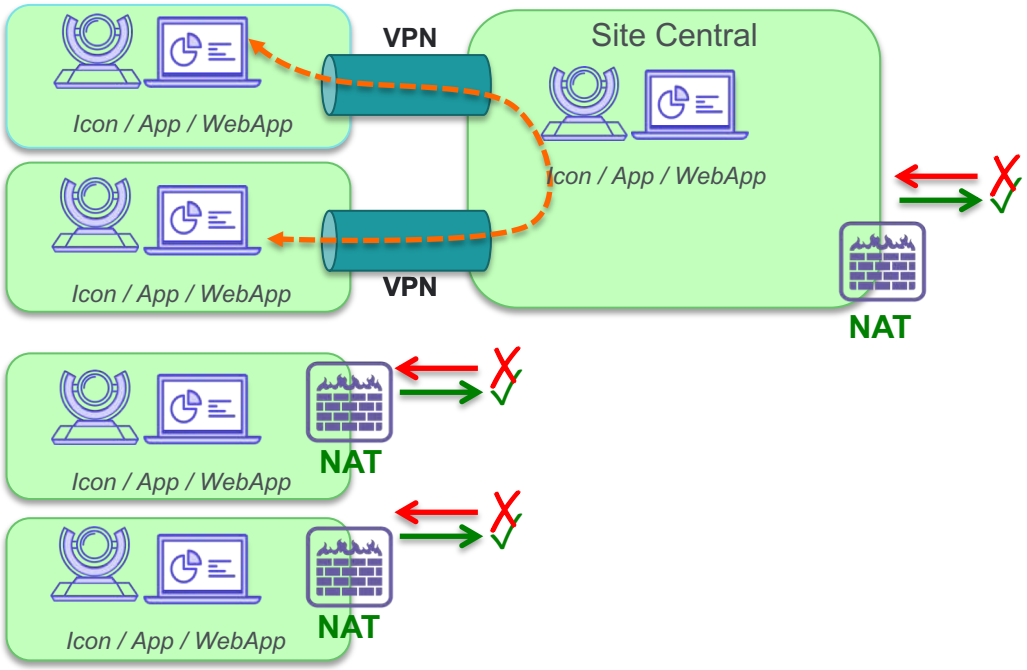
lifesize

Trafic sortant contrôlé uniquement

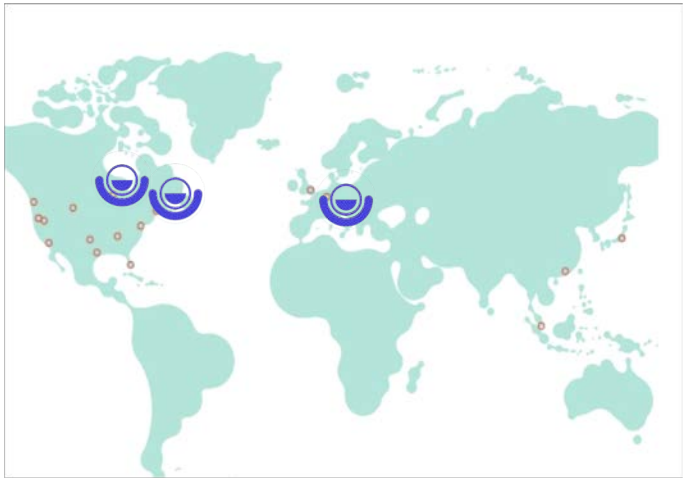
- Aucun trafic entrant requis
  - La connexion sortante établie au démarrage du client/système de salle est maintenue en permanence.
- Ouverture du trafic sortant vers les microservices Lifesize identifiés
  - Services disponibles par l'intermédiaire des FQDN (pas d'adresses IP statiques)

lifesize

Direct Media



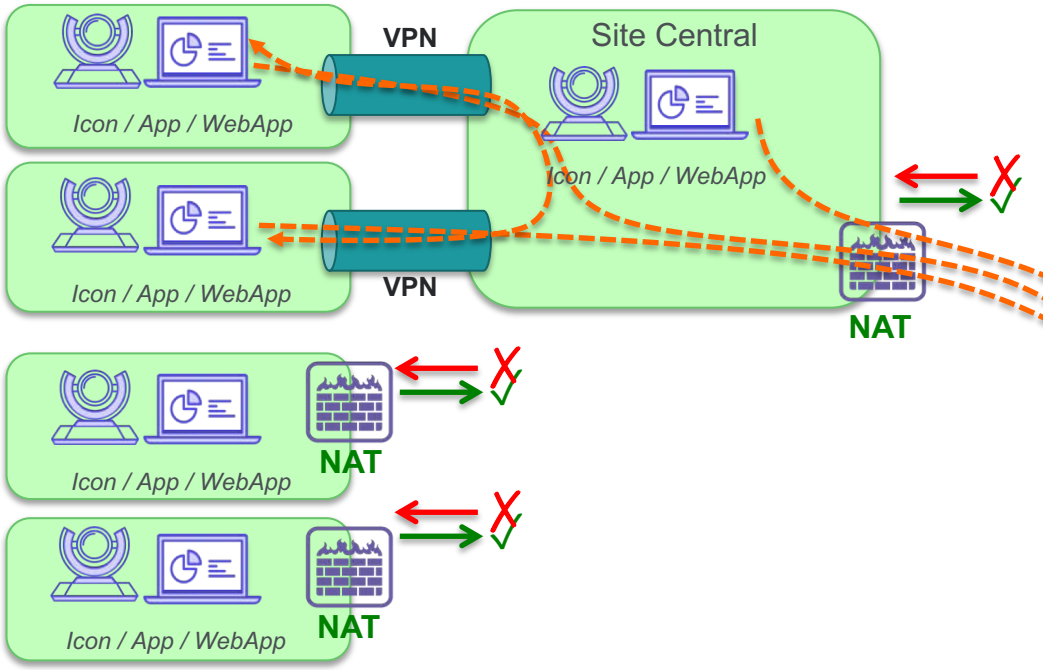
- Les appels P2P restent sur le réseau privé client



Media trafic

lifesize

Direct Media

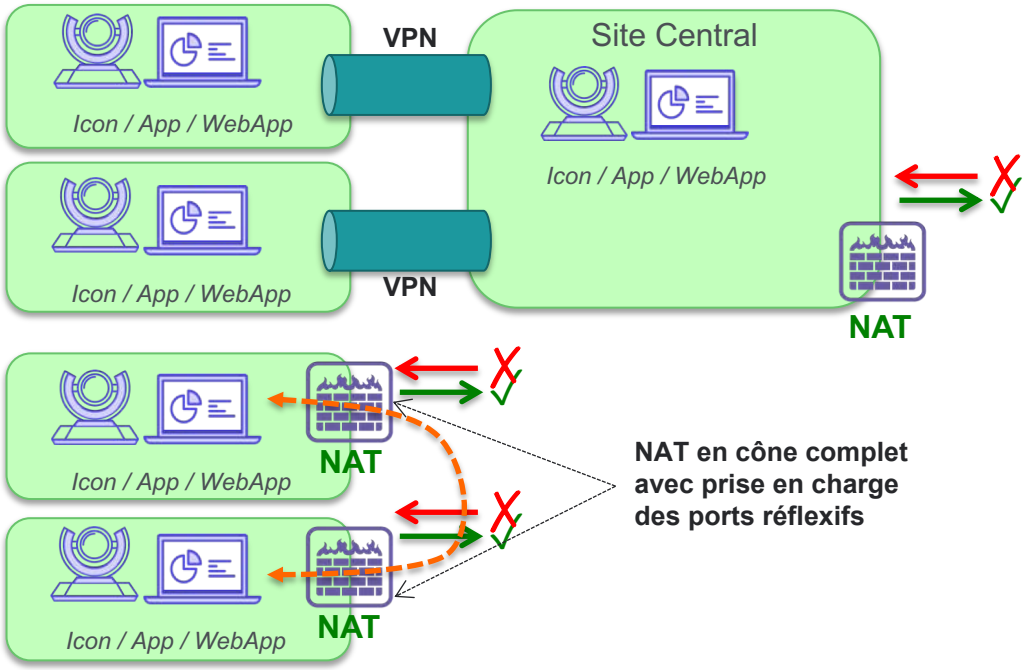


- En cas d'appels multipoints, l'appel passera par le service MP Lifesize le plus proche.

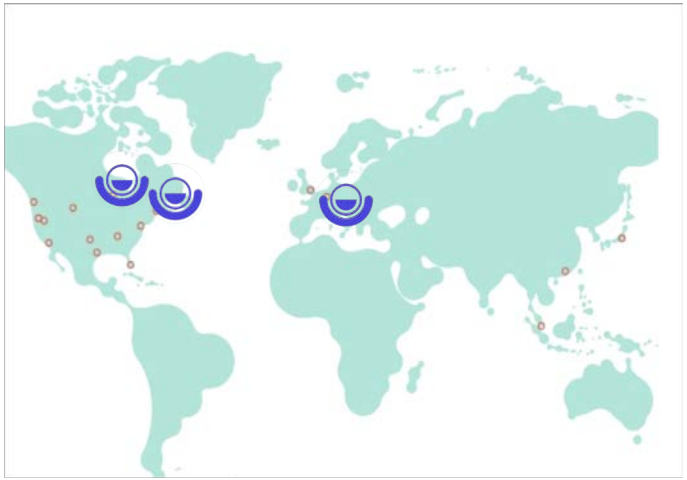
Media trafic

lifesize

Direct Media



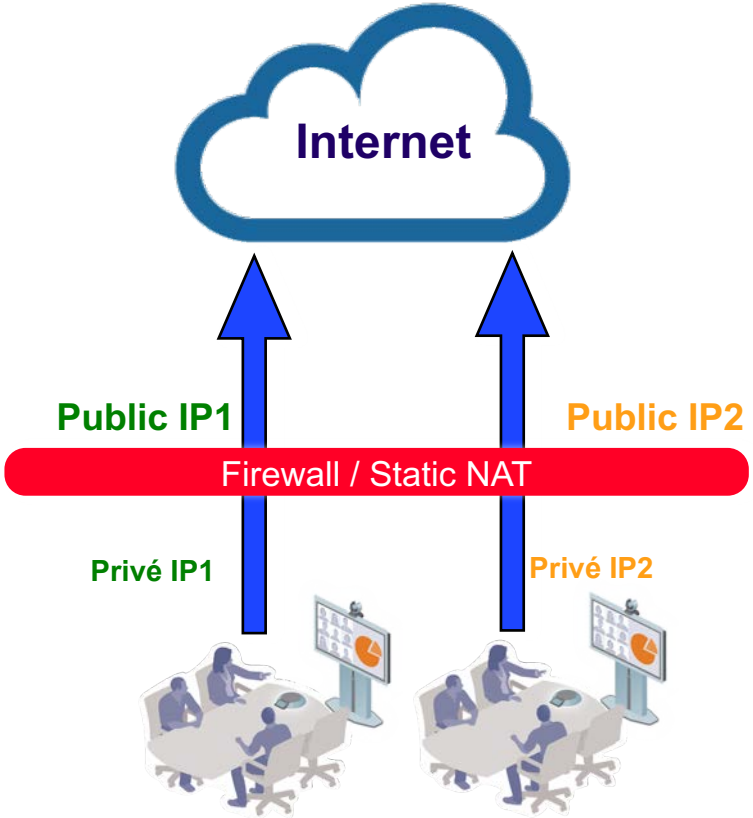
- Les appels media restent directs mais via Internet

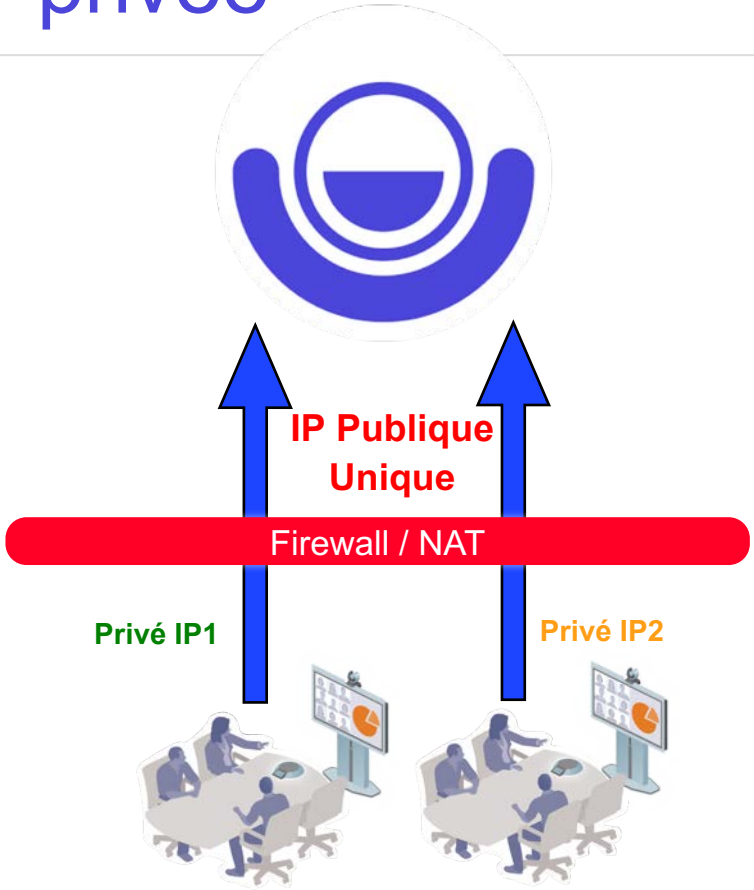


Media trafic

lifesize

Masquage de l'adresse IP privée





lifesize

Chiffrement du trafic de bout en bout

- authentification HTTPS
- Signalisation d'appel par TLS utilisant un port non standard
- Supports d'appel via SRTP / AES 128 bits utilisant des ports aléatoires renégociés au début de chaque appel
  - Clé de chiffrement à usage unique. Nouvelle clé de cryptage générée pour chaque appel
- Appels vers des terminaux externes utilisant H.323 cryptés par H.235
- Sessions enregistrées cryptées "in wire" avec AES 128 et "at rest" avec AES 256 bits.

lifesize

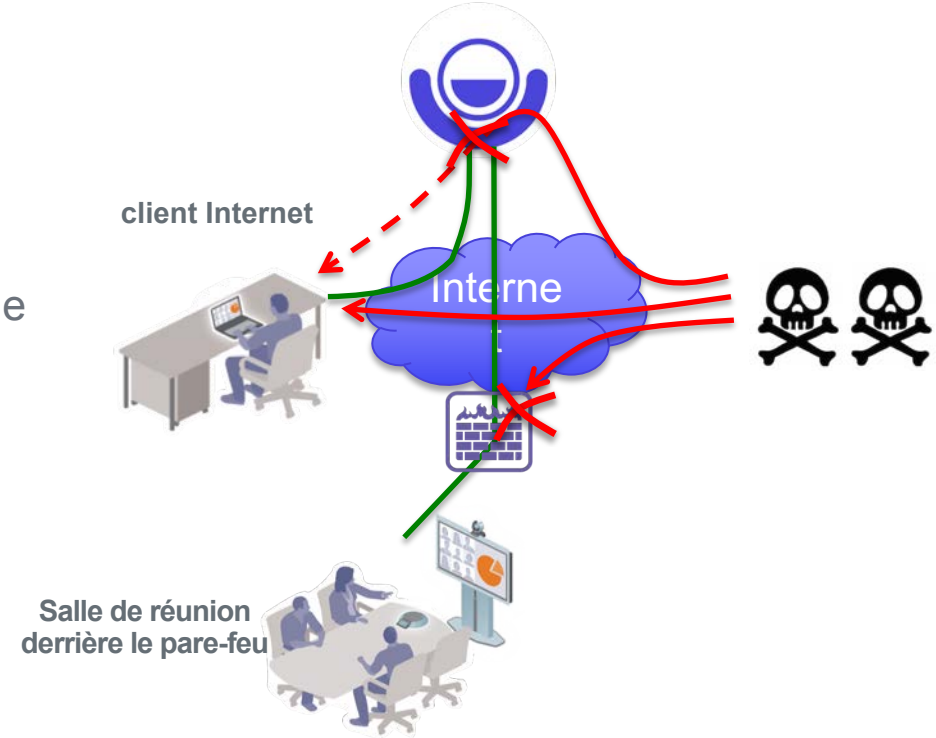
Sécurité des réunions

- Un code PIN optionnel peut être défini pour chaque VMR
- Prise en charge des VMRs à usage éphémère (One-Time Meetings)
- Prise en charge des VMRs cachées
  - seuls le créateur et les modérateurs peuvent voir ces VMRs dans leurs répertoires
- Au cours d'une réunion, un modérateur peut retirer des participants d'un appel
- Au cours d'une réunion, un modérateur peut couper le son de tous les participants
- Au cours d'une réunion, un utilisateur peut couper le son de son propre système audio et/ou vidéo

lifesize

Filtrage de l'utilisation malveillante

- Filtrage des appels SPAM via un pare-feu au niveau applicatif implémenté sur Lifesize Cloud
- Protection contre les attaques de type " homme au milieu " grâce à l'épinglage de certificats
- Limitation des domaines de messagerie valides pour se protéger contre la création de faux comptes d'utilisateur

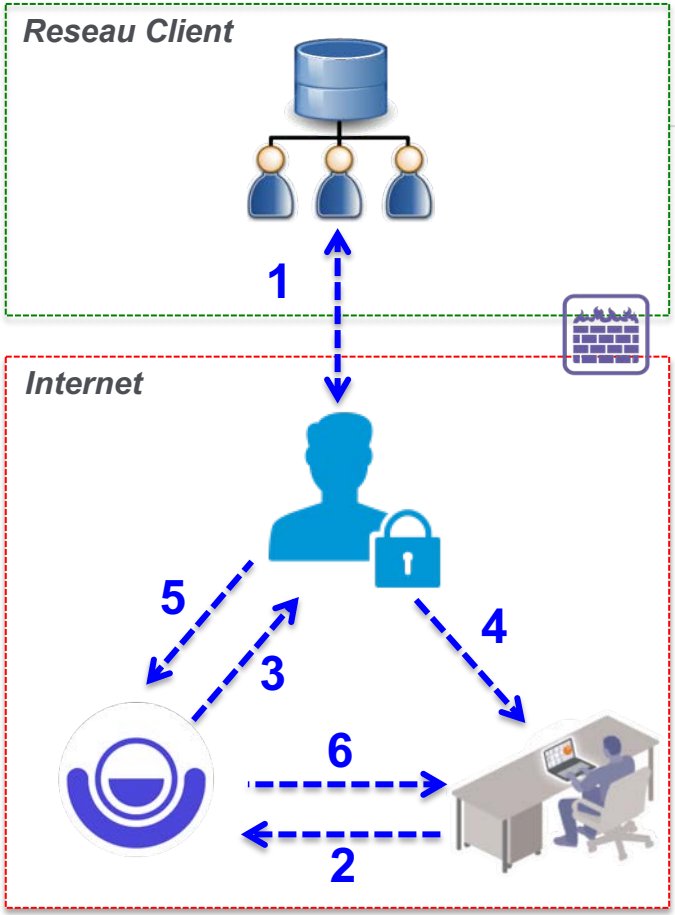


lifesize

Authentification unique (SSO)

Basé sur le protocole SAML 2.0

1. Le fournisseur d'identité (IdP) se synchronise avec le serveur d'annuaire du client
2. L'utilisateur s'identifie par email (pas de mot de passe)
3. Lifesize Cloud envoie une demande d'authentification au client IdP
4. IdP demande les identifiants de l'utilisateur (mot de passe, jeton, carte à puce, etc.) et valide la réponse.
5. IdP indique à Lifesize Cloud de permettre à l'utilisateur de se connecter au service
6. Lifesize Cloud autorise la connexion de l'utilisateur

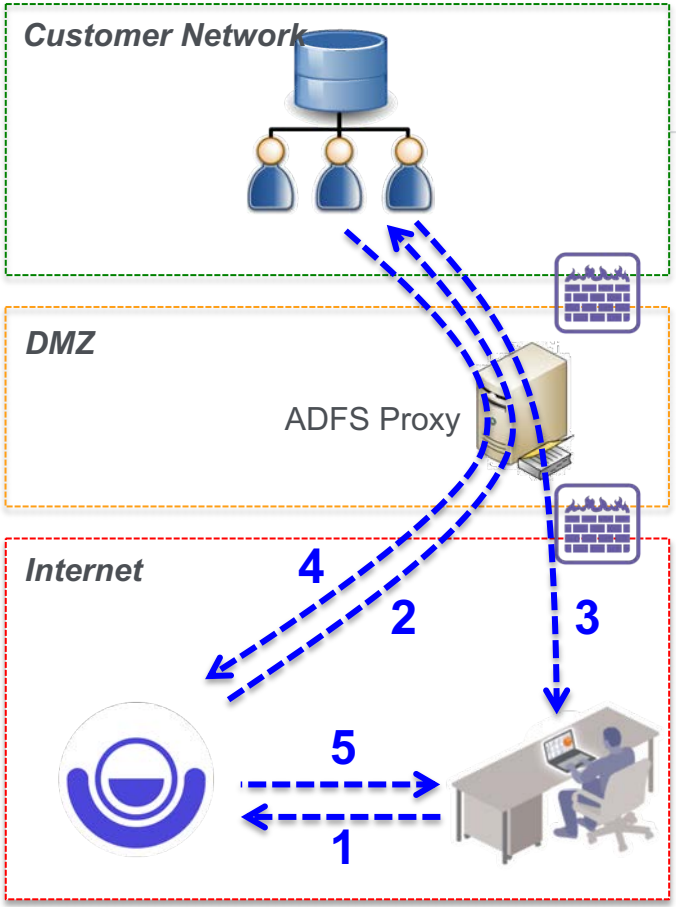


lifesize

Authentification unique (SSO)

Basé sur Active Directory Federation Services V2.0 ou V3.0

1. L'utilisateur s'identifie par email (pas de mot de passe)
2. Lifesize Cloud envoie une demande d'authentification au client ADFS via son proxy ADFS.
3. L'ADFS demande les informations d'identification de l'utilisateur par l'intermédiaire du serveur mandataire de l'ADFS et valide la réponse.
4. L'ADFS indique à Lifesize Cloud de permettre à l'utilisateur de se connecter au service
5. Lifesize Cloud autorise la connexion de l'utilisateur



lifesize

Authentification unique (SSO)

SSO SAML v2 supporté avec :

Active Directory Federation Services

v2.0 / v3.0

onelogin

BITIUM

Centrify

okta

Ping Identity

salesforce

OpenIAM Identity and Access Management

Microsoft Azure

stoneware

Google Apps

lifesize

Merci!

© 2019 Lifesize, Inc. All rights reserved. – CONFIDENTIAL

Documentation de référence

- Haute disponibilité des centres de données :
  - https://aws.amazon.com/pt/ec2/sla/

- Certifications des data centers :
  - https://aws.amazon.com/compliance/data-privacy-faq/
  - https://aws.amazon.com/compliance/iso-27001-faqs
  - https://aws.amazon.com/compliance/