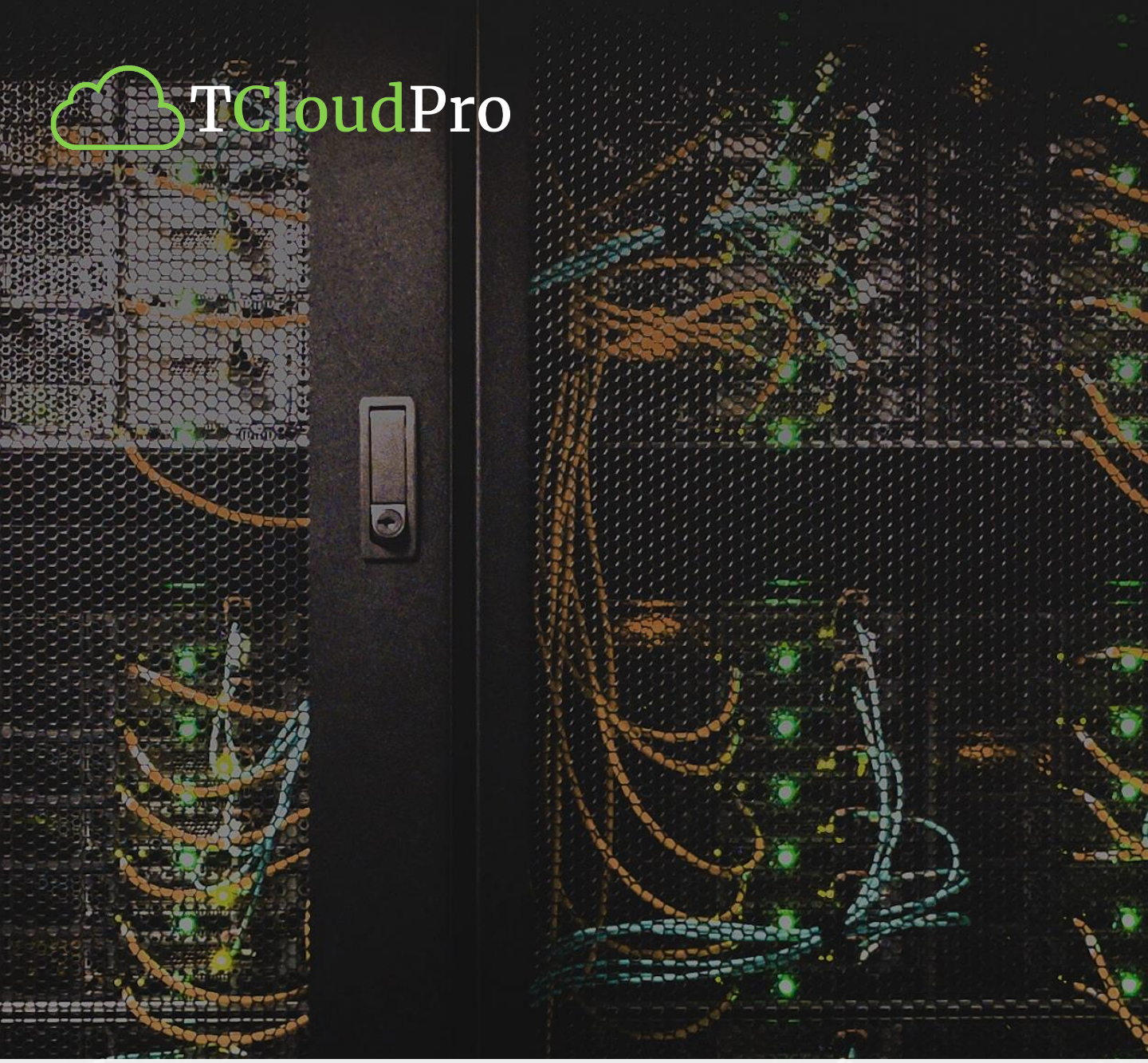
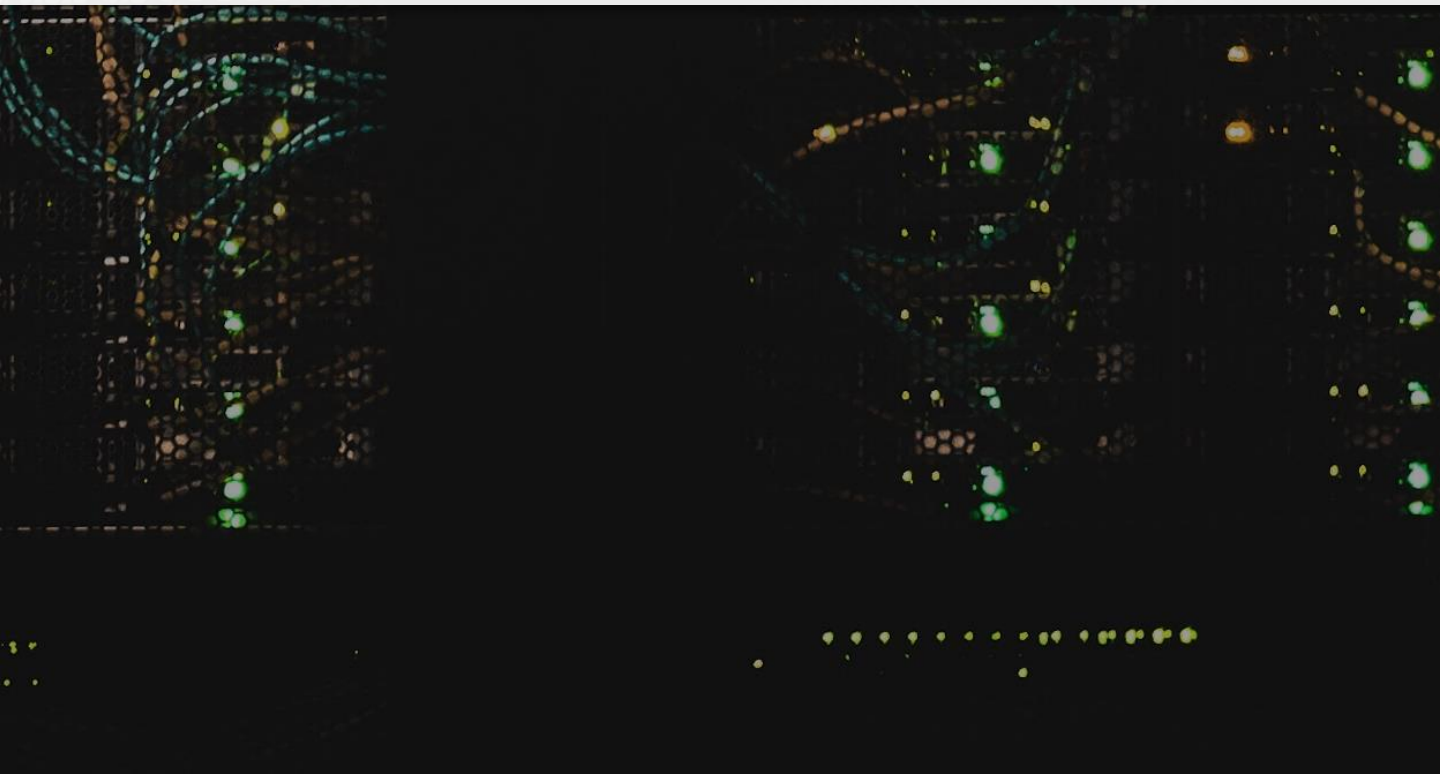
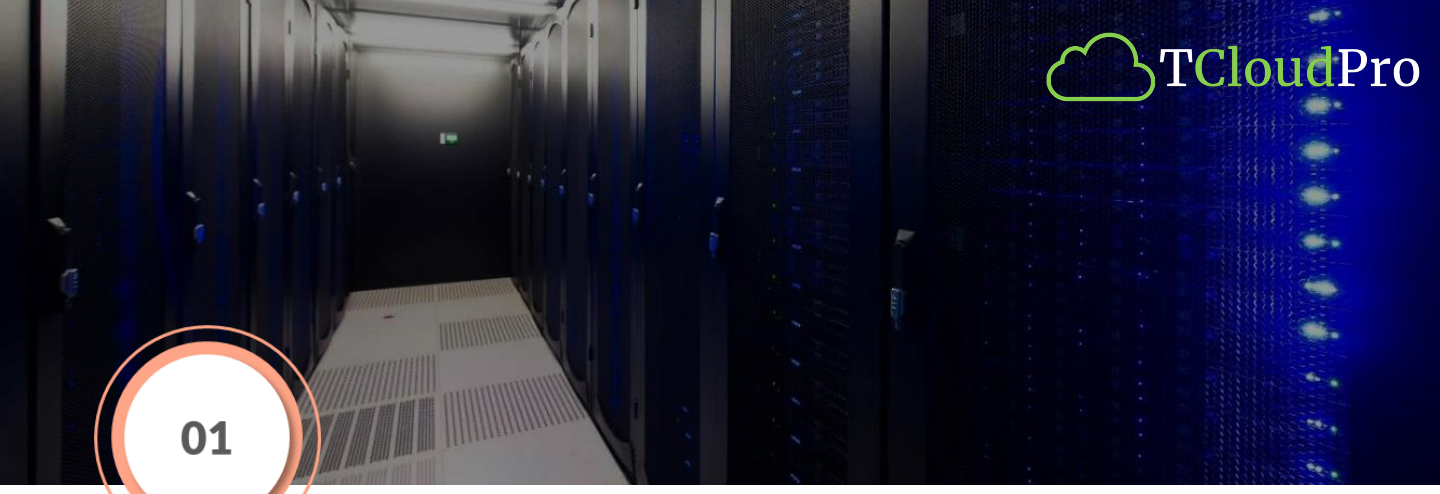


Infrastructure et Sécurité.

Les piliers de nos services et de notre plateforme.

TSIFi 6 rue de Porstrein , Port de commerce 29200 Brest 02 90 91 45 74 contact@tsifi.com www.tsifi.com





01

Nos centres de données.

Les lieux où sont hébergés nos serveurs.

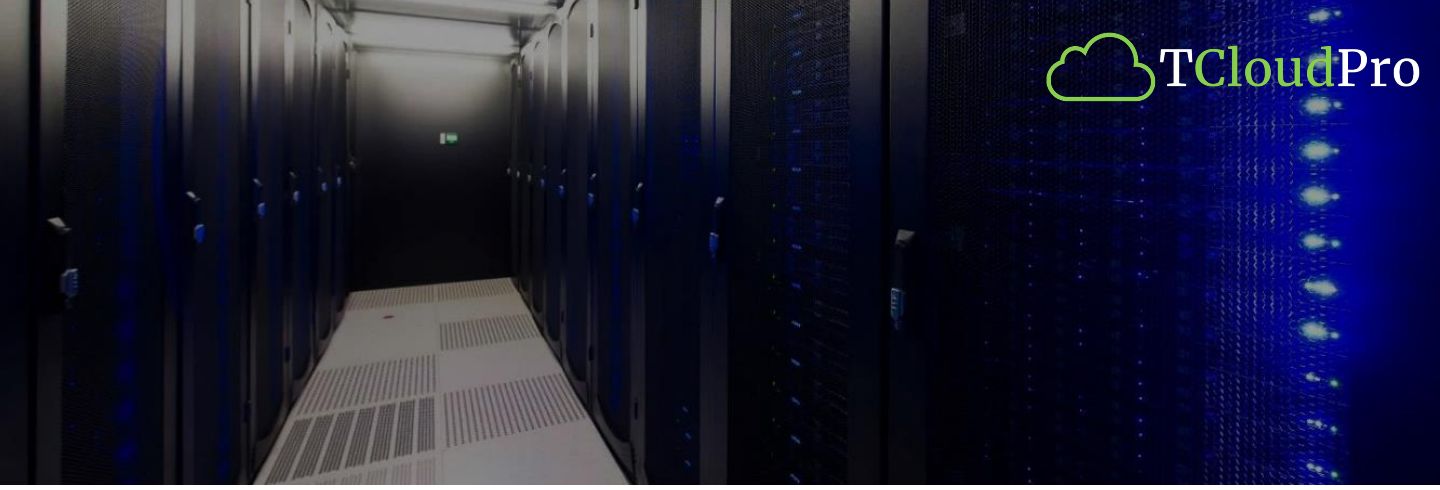
Nous hébergeons notre plateforme et notre infrastructure dans des centres de données européens ultramodernes choisis en fonction de critères stricts de sécurité, de qualité, de rendement et de connectivité.

En France, notre infrastructure est située à Paris, tandis qu'en Espagne, nos centres de données sont situés à Madrid. Comptant probablement parmi les plus avancés construits à ce jour, ils sont une référence au niveau européen. Ce sont tous des **centres de données neutres**, avec une large gamme de connectivité qui permet d'offrir une plus grande redondance et une plus grande disponibilité en termes de connexion.

En outre, ils sont soumis à des mesures de sécurités strictes concernant l'accès physique, les conditions environnementales et l'alimentation électrique, afin de garantir une qualité de service optimale.

Sécurité physique.

L'accès physique, limité et autorisé uniquement sur autorisation préalable, fait l'objet d'un contrôle 24/7 par vidéosurveillance et par du personnel de sécurité.



Mesures de sécurité :

- Agents de sécurité 24/24.
- Enregistrement continu 24/7.
- Détecteur de métaux et tourniquet d'entrée pour l'accès au CTD.
- Caméras extérieures et intérieures (portes d'accès, couloirs).

Contrôle d'accès :

- 5 couches de sécurité physique (accès périmétrique, bâtiment, locaux techniques, armoires rack, etc.).

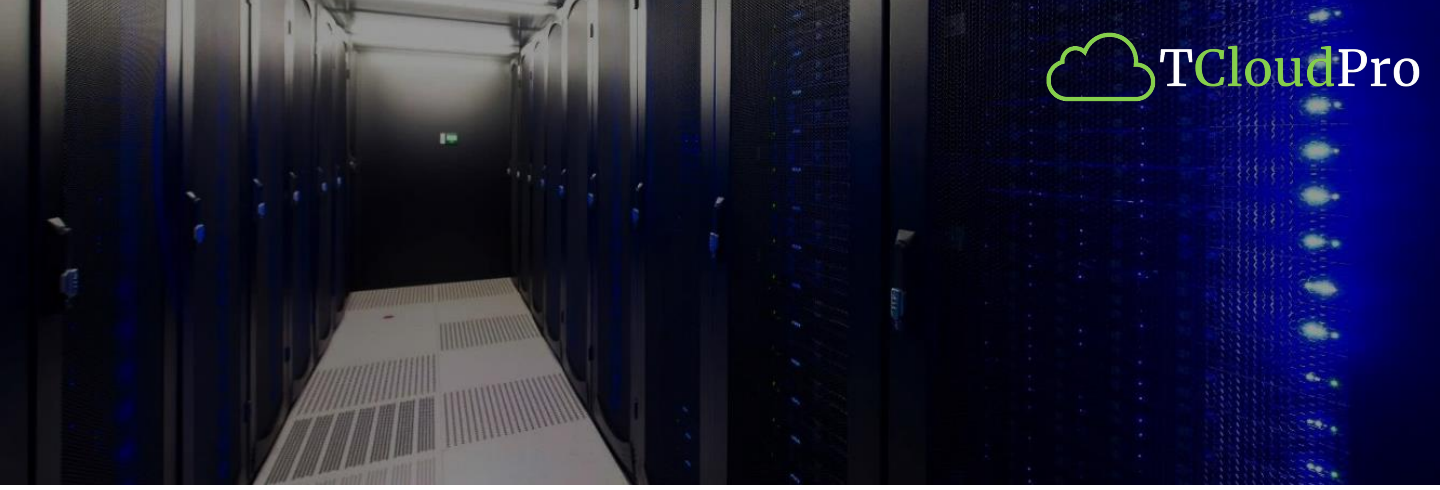
Contrôles environnementaux.

Les équipements informatiques sont installés et surveillés dans des **environnements contrôlés** avec des niveaux de température et d'humidité définis par contrat (SLA) :

- Refroidissement continu (24/24).
- Équipement de climatisation redondant.
- Température de 21 °C et humidité relative de 50 %.

Tous les serveurs disposent de **systèmes anti-incendies** conçus pour éteindre tout incendie en quelques secondes et sans résidus :

- Détecteurs de fumée.
- Démarrage automatique des systèmes d'extinction.
- Boutons manuels d'arrêt d'urgence dans tous les locaux.
- Détecteurs optiques et ioniques avec système VESDA.
- Alarmes surveillées 24/7.



Énergie.

Nos centres de données sont équipés de **connexions redondantes au réseau électrique** et de **générateurs diesel cinétiques** dimensionnés pour répondre aux besoins énergétiques de l'ensemble du bâtiment et des infrastructures qui s'y trouvent.

Certifications de nos centres de données.

ISO 14001

Systèmes de management environnemental

ISO 22301

Sécurité et résilience

ISO 27001

Management de la sécurité de l'information

ISO 9001

Management de la qualité

ISO 50001

Systèmes de management de l'énergie

02

Architecture redondante.

Pour assurer la continuité du service.

Nous avons mis en place une architecture 100 % redondante afin que la panne d'un composant n'entraîne aucune conséquence sur le fonctionnement normal de la plateforme et des services.

Nœuds de calcul.

Chaque hôte dispose de **deux alimentations électriques**, connectées chacune à un segment électrique différent du CTD. Tous les équipements qui composent l'infrastructure disposent d'au moins **deux connexions réseau en haute disponibilité** (LAG). De plus, chaque connexion réseau a son propre commutateur, si bien qu'une panne d'un commutateur n'entraîne aucune interruption de service. La **mémoire RAM** des hôtes est de type **ECC**, ce qui garantit une protection contre la corruption des données et d'éventuelles pannes.

Nos CTD sont également équipés d'**hyperviseurs en N x 1,25**. L'espace disponible est ainsi suffisant pour faire face à une panne de 25 % d'entre eux. En cas de panne d'un hyperviseur, les serveurs qu'il héberge sont automatiquement démarrés sur d'autres hyperviseurs.

Stockage.

Nous offrons un stockage en haute disponibilité qui combine une mise en grappe de baies et une réplication synchrone pour assurer un basculement transparent. Avec ce système de stockage redondant, nous garantissons :

- Une protection accrue contre les pannes matérielles, du réseau ou des installations.
- Une élimination des temps d'arrêt et de la gestion des changements.
- Une mise à niveau du matériel et des logiciels sans interruption de service.

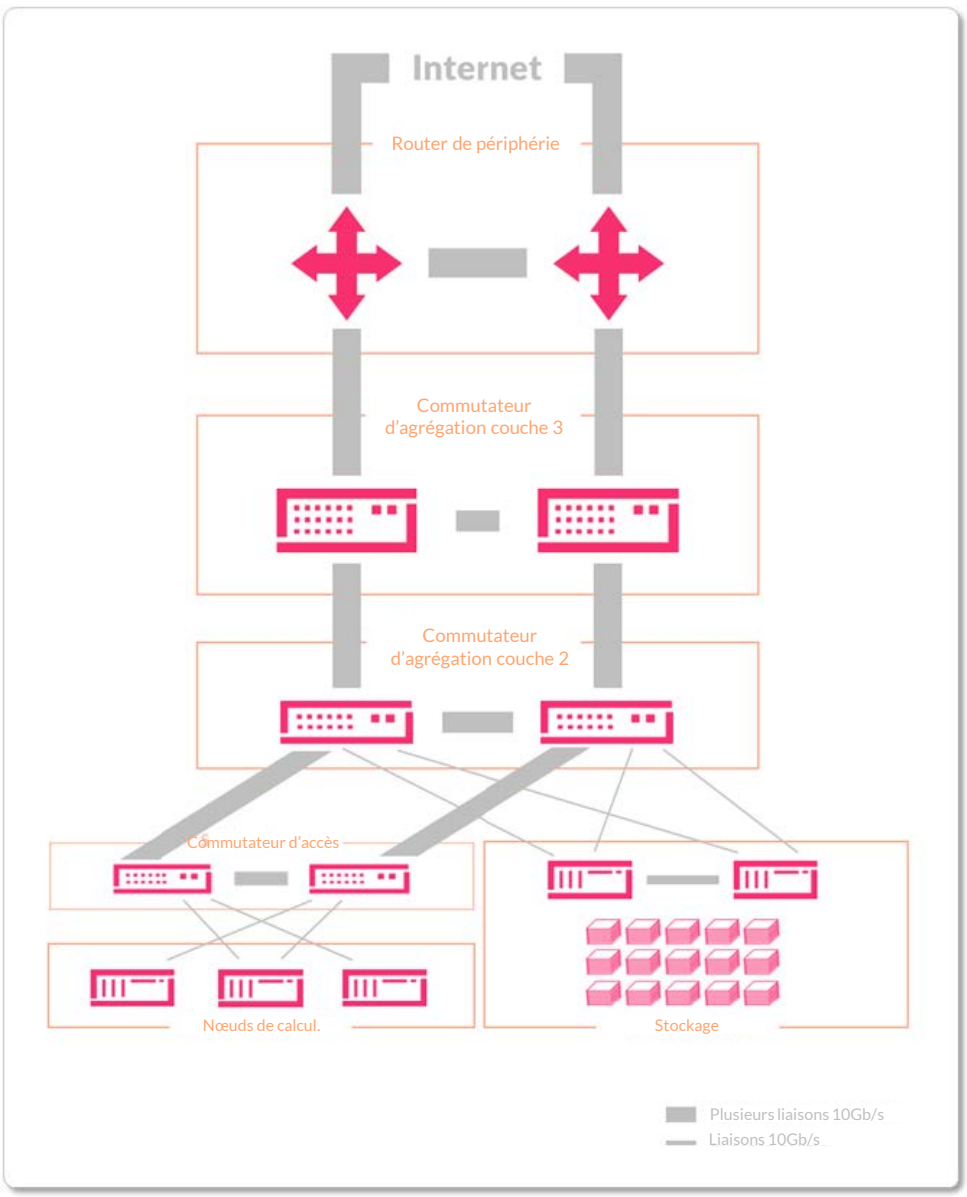
Réseau de données.

Nous disposons de plusieurs circuits 10G auprès de différents fournisseurs. Ainsi, un problème chez un fournisseur n'a aucune conséquence pour la connectivité.

L'agrégation de liens multichâssis constitue l'épine dorsale du réseau au sein du CTD. Elle garantit à la fois **redondance et évolutivité** tout en évitant la formation de boucles.

Chaque centre de données dispose d'une paire de routeurs de bordure qui facilitent la connexion à Internet et aux autres centres. Viennent ensuite les commutateurs d'agrégation de couche 3, les commutateurs de couche 2 et, enfin, les commutateurs d'accès, auxquels sont connectés les nœuds de calcul.

Tous les commutateurs logiques sont appariés pour garantir la redondance et connectés à l'ensemble des appareils par l'intermédiaire d'une agrégation de liens multichâssis, composée d'au moins 2 connexions 10G ou 40G. Cette typologie permet d'**éviter le risque de formation de boucles au niveau de la couche 2**.



03

Sécurité périmétrique.

Sécurité périmétrique et anti-DDoS.

L'infrastructure est équipée de systèmes anti-DDoS qui préviennent et filtrent les attaques par déni de service afin de garantir la disponibilité permanente des serveurs.

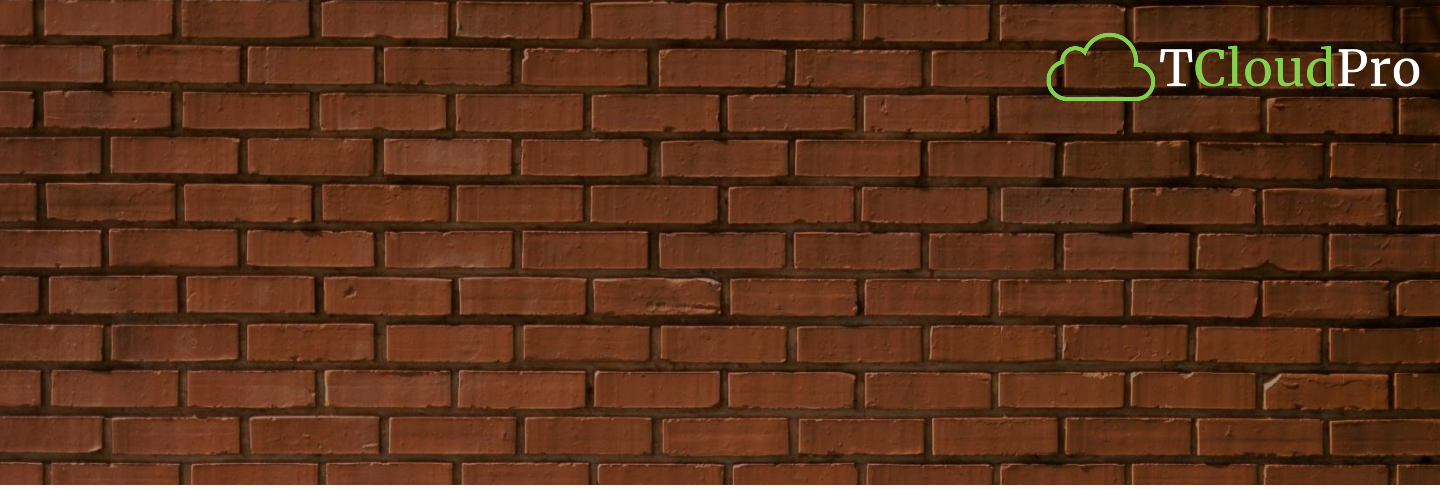
Notre système anti-DDoS est structuré en plusieurs lignes de filtrage et de détection qui permettent de passer au crible et de différencier les petites attaques (quelques centaines de Mb/s) des autres attaques de milliers de Gb/s.

IDS/IPS.

Un système logiciel de détection d'intrusion (IDS) permet de détecter les accès non autorisés à l'infrastructure. Il agit en évaluant l'intrusion au moment où elle se produit et génère une alarme. L'IDS est accompagné d'un système de prévention d'intrusion (IPS) qui suit en permanence et de manière proactive le trafic réseau suspect ou inhabituel.

Les systèmes IDS et IPS ne peuvent pas arrêter les attaques à eux seuls et ont donc besoin d'outils complémentaires, comme les pare-feux, pour les aider dans le processus de blocage.

TSIFi 6 rue de Porstrein , Port de commerce 29200 Brest 02 90 91 45 74 contact@tsifi.com www.tsifi.com



Filtrage et blocage à l’aide de pare-feux périmétriques.

Les pare-feux périmétriques analysent en permanence le trafic qui arrive jusqu’au CTD et bloquent le trafic manifestement malveillant avant qu’il n’y entre. En parallèle, ils vérifient également le volume de trafic que chaque machine reçoit, ce qui permet de contrôler le trafic reçu par chaque serveur et de détecter d’éventuelles attaques DDoS.

04

SSD et NVMe.

Disques SSD haut de gamme.

Afin de garantir la plus haute disponibilité, nous utilisons uniquement des disques SSD de la plus haute qualité sur protocole NVMe (baies 100 % Flash).

L'utilisation de ce type de disques d'entreprise vise plusieurs objectifs :

Rendement optimum constant.

Grâce à l'utilisation de baies 100 % Flash, nous visons à offrir des performances excellentes et constantes, quelle que soit la charge de travail du disque ou son degré d'occupation.

Protection des données.

Le système 100 % Flash fournit une couche supplémentaire de protection des données de manière intégrée. La réplication synchrone, le cryptage intégré, la protection WORM ou l'authentification multifactorielle ne sont que quelques-uns des avantages de nos baies de stockage qui permettent de maintenir les données critiques disponibles, protégées et sécurisées.

05

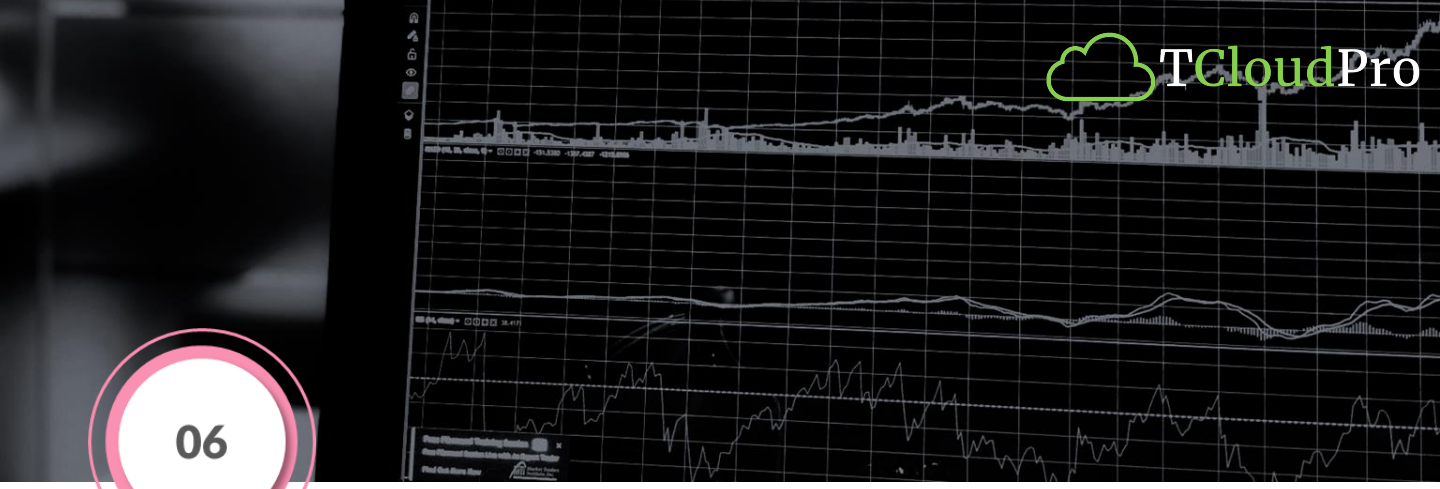
Authentification et cryptage.

Double authentification.

L'accès au portail a été renforcé avec la possibilité de mettre en place une double authentification (2FA) par le biais d'un jeton d'accès généré sur un appareil mobile. Ce jeton consiste en un numéro à six chiffres que l'utilisateur doit fournir en plus de son nom d'utilisateur et de son mot de passe pour accéder aux services.

Protection des données.

Le cryptage est un **processus de codage des informations**. Il convertit les informations d'origine (texte en clair) sous une autre forme (texte chiffré ou crypté) que seules les parties autorisées peuvent déchiffrer. Les services utilisent différents systèmes de codage et de cryptage pour la gestion et le transfert des informations, ce qui constitue une couche supplémentaire de protection contre d'éventuels piratages.

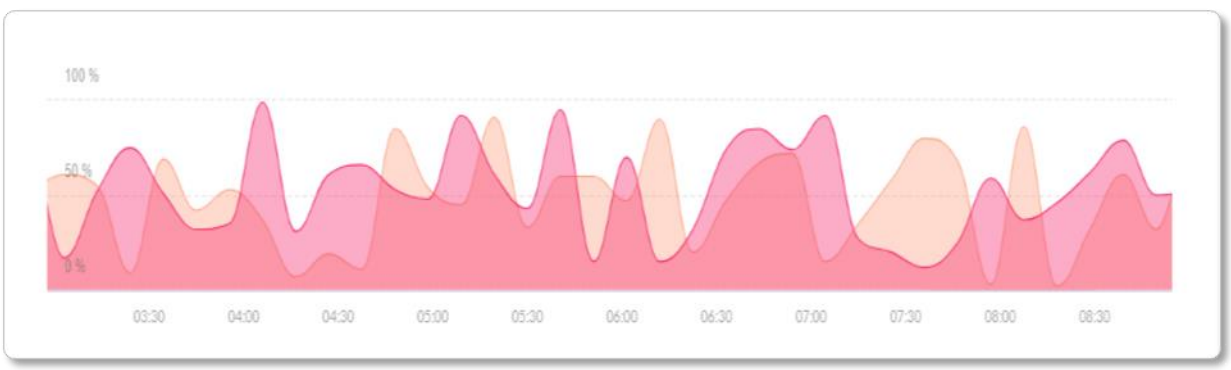


06

Surveillance 24/7.

Plus d'indicateurs métriques pour une plus grande capacité de réponse.

Nous disposons d'un **système de surveillance et d'alerte 24/7** qui nous permet de suivre en continu l'état de l'ensemble du système, tant l'infrastructure que le reste des sous-systèmes, afin de garantir la fiabilité et la stabilité des services et de la plate-forme. Cela nous permet d'évaluer l'état et le rendement de l'ensemble du système.



Notre système de surveillance 24/7 est basé sur la collecte d'indicateurs métriques, le traitement et la visualisation de données ainsi que l'établissement de règles et d'alertes. L'objectif ultime est d'identifier d'éventuels symptômes de risque ou de dysfonctionnement avant toute panne ou temps d'arrêt.

TCloudPro

07

Sauvegarde et restauration.

La sauvegarde est une copie des données d'origine qui constitue un moyen de récupération en cas de perte. Elle est extrêmement utile pour différents événements et usages. Nous le savons et c'est pourquoi nous mettons en place différentes stratégies et différents types de sauvegardes en fonction du service.

Stratégie de sauvegarde dans le Stockage Cloud.

Le service de Stockage Cloud dispose d'une stratégie de sauvegarde prédéfinie et commune à tous les utilisateurs à un niveau granulaire et sous forme cryptée.

La **stratégie de sauvegarde** est détaillée ci-dessous :

Rétention des sauvegardes :

- Une fois par heure [5 dernières heures]
- Une fois par jour [14 derniers jours]
- Une fois par semaine [8 dernières semaines]

Par ailleurs, des **instantanés de volume VSS** sont disponibles pour restaurer des versions précédentes de fichiers et de dossiers.

Programmation d'instantanés : Tous les jours

Rétention des instantanés : 64 instantanés.

Système de récupération de données, instantané et en ligne, accessible à tout utilisateur.

TCloudPro

Répliques dans Stockage d'Archives.

Le système de stockage d'archives réplique chaque objet sur **3 disques différents situés sur 3 serveurs différents**. La stratégie établie conservera par défaut au moins une des copies dans un **centre de données différent**.

Le service Stockage d'Archives dispose également d'une fonctionnalité de versionnage qui peut être activée à tout moment à partir de l'espace utilisateur de la plateforme par nos administrateurs. De cette façon, il est possible de récupérer des versions précédentes par le biais du protocole S3.

Sauvegarde sur Remote Desktop et Serveurs.

Les services Remote Desktop et Serveurs disposent d'une stratégie de sauvegarde basée sur des instantanés de disque avec une programmation à intervalles réguliers :

- Une fois par heure [5 dernières heures]
- Une fois par jour [14 derniers jours]
- Une fois par semaine [8 dernières semaines]

En outre, nos administrateurs peuvent effectuer des sauvegardes manuelles ou mensuelles basées sur des instantanés de disque. La programmation mensuelle a une durée de rétention maximale de 24 mois.

La restauration des sauvegardes est disponible sur demande auprès de nos administrateurs.

Contrat de niveau de service (SLA).

DISPONIBILITÉ	COMPENSATION
99,99>D>=99,72	10% redevance mensuelle
99,72>D>=99,44	20% redevance mensuelle
99,44>D>=99,16	30% redevance mensuelle
D<99,16	40% redevance mensuelle

Disponibilité (D) = [(Heures par mois – Heures d'indisponibilité) / Heures par mois] x 100

N'entre pas en compte dans le calcul de la disponibilité de l'accès (SLA) :

- Causes indépendantes de notre volonté et cas de force majeure.
- Temps d'indisponibilité dus à des pannes logicielles des machines virtuelles.
- Virus et attaques informatiques entraînant l'impossibilité totale ou partielle de fournir les services.

Totem Services Informatiques Finistère

6 rue de Porstrein , Port de commerce 29200 Brest

02 90 91 45 74

contact@tsifi.com

Vos données sont en sécurité.