Plan de Continuité d'Activité (PCA) SAAS
SM 17 605
Ed 5

Confidentialité		
Note	**Confidentialité**	**Niveau (à cocher)**
1	Document public	X
2	Document restreint à la société	
3	Document restreint à un groupe de personnes	
4	Document confidentiel restreint aux personnes concernées	

Suivi des versions				
Date	**Versions**	**Auteur(s)**	**Validé (V) / Approuvé (A) par**	**Motif de la version**
27/12/2017	Ed. 1	SV	DSI	Version originale
17/07/2020	Ed. 2	SV	Comité de Sécurité	Ajout du paragraphe 5
25/06/2021	Ed. 3	SV	Comité de Sécurité	Revue
24/06/2022	Ed. 4	SV	Comité de Sécurité	Revue
23/06/2023	Ed. 5	FGB	Comité de Sécurité	Ajout chapitre 2

Sommaire

1 - Objet

Ce document a pour but de présenter la politique visant à favoriser la continuité de l'activité (PCA) de la société Invoke, ci-après nommée « la Société », en cas de sinistres, dommages ou mauvais fonctionnement de son Système d'Information (SI) et tout particulièrement de ses services hébergés.

Ce document décrit les différents éléments critiques constitutifs du réseau interne et externe à la Société ainsi que les procédures mises en place pour réduire les temps de coupure de service pouvant impacter les clients de la société.

2 - Organisation

Les tests de continuité d'activité sont pratiqués à minima une fois par an. Le résultat est formalisé sous forme de compte rendu incluant des propositions de pistes de progrès. Ce rapport est présenté en revue de Direction afin de valider les actions à engager.

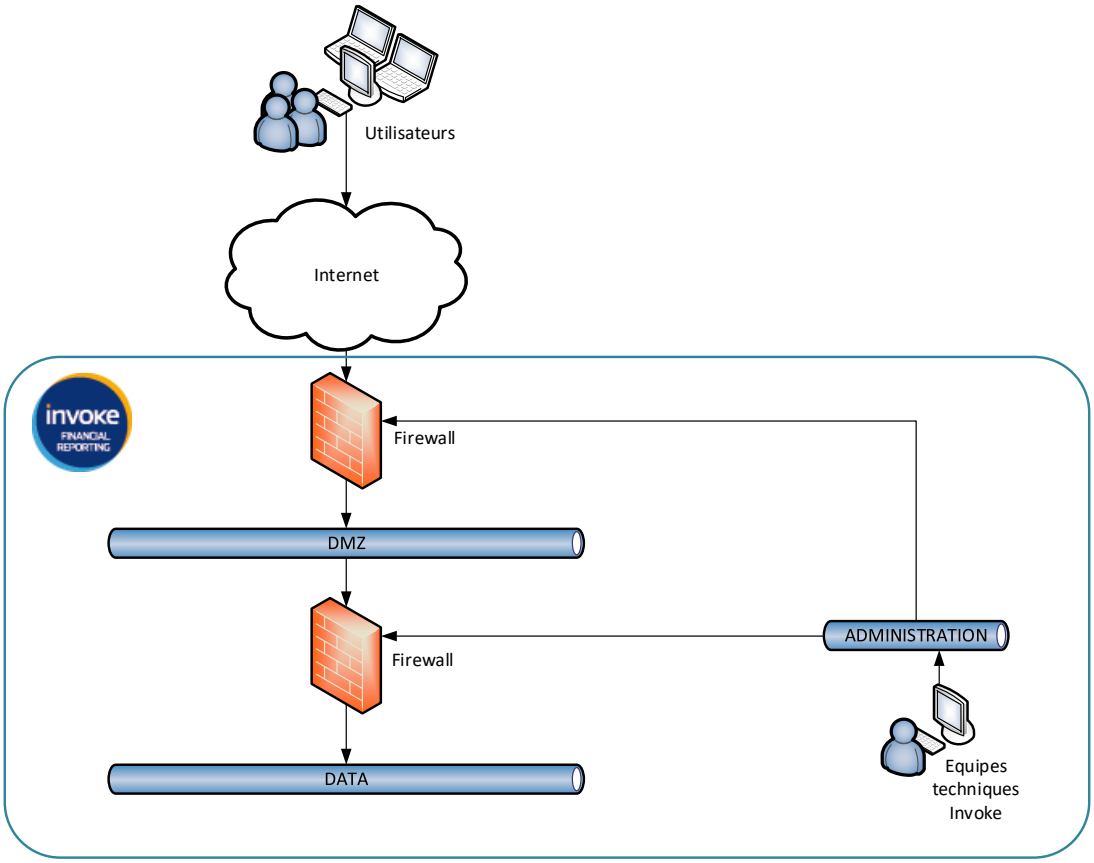
Les moyens de travail à distance des utilisateurs s'étant démocratisés, le PCA est centré sur la disponibilité des ressources IT supportant les services avec engagements proposés aux Clients de la Société.

En cas de sinistre, la cellule de crise décisionnelle en l'instance du Comité de Sécurité est constituée. Celle-ci regroupe notamment les fonctions de Direction Générale, Direction des Systèmes d'Information et Responsable de la Sécurité Des Systèmes d'Information. La cellule mobilisera selon les besoins des fonctions plus opérationnelles et/ou transverses comme le service communication ou juridique. La cellule de crise décisionnelle assure la traçabilité des actions et des décisions prises.

En fonction du sinistre, une cellule opérationnelle sera constituée avec les ressources idoines strictement nécessaires à la poursuite de l'activité afin d'assurer les efforts dans le temps et le maintien des services non touchés.

3 - Présentation générale du réseau

L'infrastructure réseau utilisée dans le cadre de la fourniture des services hébergés de la Société est divisée en plusieurs zones. Les communications entre ces différentes zones sont régies par des firewalls permettant d'assurer l'isolation des différents serveurs et équipements intervenant dans la fourniture des services proposés aux clients.



Le réseau servant à l'hébergement est divisé en 4 zones distinctes isolées les unes des autres par des firewalls permettant de filtrer les services exposés :

- Le réseau WAN servant à l'interconnexion des infrastructures avec l'extérieur et plus généralement, Internet.
- Le réseau DMZ (démilitarisé) qui est le seul réseau accessible par le WAN sur lequel se trouvent les serveurs frontaux distribuant les applications hébergées.
- Le réseau DATA hébergeant les serveurs de bases de données utilisés par les applications hébergées.
- Le réseau ADMINISTRATION regroupant les serveurs permettant l'administration des solutions hébergées et accessible des seules équipes de la Société.

Celle-ci dispose de ses propres infrastructures afin de fournir le service d'hébergement des solutions proposées. Les datacenters ainsi que les équipements les constituant sont la propriété exclusive de la société et sont opérés et maintenus par ses équipes, sans recours à des tiers.

4 - Chaine critique

L'ensemble des éléments intervenant dans la fourniture des services SAAS de la société sont identifiés comme faisant partie de la chaine critique d'exploitation. Cette chaine impose une supervision renforcée et propose une résilience élevée afin de parer à toute défaillance. L'architecture est donc développée dans un souci de proposer la meilleure disponibilité possible.

Les éléments constitutifs de cette chaine critique sont les suivants :

- Datacenters
- Alimentation électrique
- Climatisation
- Risques environnementaux
- Réseaux
- Serveurs
- Stockage des données
- Sauvegardes des données

5 - Sécurisation de la chaine critique

5.1 - Supervision

L'ensemble des éléments constitutifs du Système d'Information de la société est monitoré en temps réel afin de veiller à son bon fonctionnement. Les éléments monitorés incluent notamment :

- L'alimentation des baies de serveurs
- La température ambiante des salles
- Les systèmes de climatisations
- L'état physique des serveurs (état des disques, de la mémoire, erreurs CPU, …)
- L'état logique des serveurs (connectivité, état des services, …) et de leurs consommations (CPU, mémoire, disque et réseau)
- Les équipements réseau (fonctionnement, état des ports, connectivité, …)

Toute anomalie détectée est remontée immédiatement à l'équipe en charge de la supervision et donne lieu à l'ouverture et au suivi de l'incident constaté via l'outil de gestion des incidents interne à la société.

5.2 - Datacenters

La Société dispose de deux datacenters indépendants reliés entre eux par plusieurs fibres optiques permettant une synchronisation en temps réel des données. Ces deux datacenters sont utilisés conjointement en répartition de charge. Ce mode de fonctionnement permet de vérifier le bon fonctionnement de chaque salle à tout instant.

En cas de défaillance de l'un des deux datacenters, l'intégralité de la charge peut être reprise par celui restant. En effet, les ressources utilisées sont définies de manière à ne pas utiliser plus de 50 % de la puissance totale de production que peut fournir chaque datacenter. En cas de bascule de la totalité de la charge d'un datacenter à l'autre, les ressources nécessaires à cette opération sont donc toujours disponibles.

Des tests de bascule complète de charge sont réalisés de manière annuelle afin de valider le bon fonctionnement de l'ensemble.

L'accès aux salles hébergeant les serveurs de la Société n'est autorisé qu'aux seules équipes de la DSI et est contrôlé par clé et badge d'accès nominatif.

Enfin, ces datacenters sont surveillés en permanence par une société de télésurveillance qui fait intervenir systématiquement une équipe de sécurité en cas de déclenchement d'alarme (intrusion, incendie, …).

5.3 - Alimentation électrique

Chaque baie de serveurs dispose de deux circuits électriques ondulés. Cette double alimentation permet d'intervenir sur le réseau électrique de la salle sans interruption de service pour les équipements. Elle permet également une redondance complète de la chaine électrique en cas de défaillance sur un équipement ou une alimentation. Enfin, l'alimentation ondulée permet de prévenir les défauts et fluctuations du courant délivré aux serveurs et équipements.

Le principal datacenter de la Société est équipé d'un groupe électrogène permettant d'alimenter le bâtiment ainsi que les serveurs de ce site pendant 24 heures à pleine charge dans le cas où l'alimentation électrique ne pourrait être assurée. Son démarrage est automatique et permet l'alimentation normale des infrastructures quelques secondes après la détection d'une perte d'alimentation. Durant ces quelques secondes, l'alimentation en courant de l'infrastructure est assurée par les onduleurs en place. Ce groupe électrogène est testé tous les deux mois afin de vérifier son bon fonctionnement. Il est également couvert pas un service de dépannage 24/24 7/7.

5.4 - Climatisation

Chaque salle serveur dispose de deux systèmes de climatisation indépendants. Ces systèmes fonctionnent en actif/actif ou actif/passif suivant la salle et permettent de maintenir une température constante et contrôlée.

Ces systèmes de climatisations sont couverts pas un contrat de maintenance et font l'objet d'un contrôle régulier. Tout défaut de température est immédiatement remonté à l'équipe de supervision via les équipements de monitoring pour action immédiate.

5.5 - Risques environnementaux

Les datacenters de la Société sont situés hors de zones à risques (inondations, séismes, …).

En cas de détection d'un feu dans l'un ou l'autre des datacenters, une alerte à destination de la télésurveillance est immédiatement émise. De plus, le principal datacenter est équipé d'un système de détection et d'extinction automatisé de feu.

Ces systèmes font l'objet d'un contrôle régulier de leur fonctionnement. De plus, tout défaut est immédiatement remonté à l'équipe en charge de la supervision.

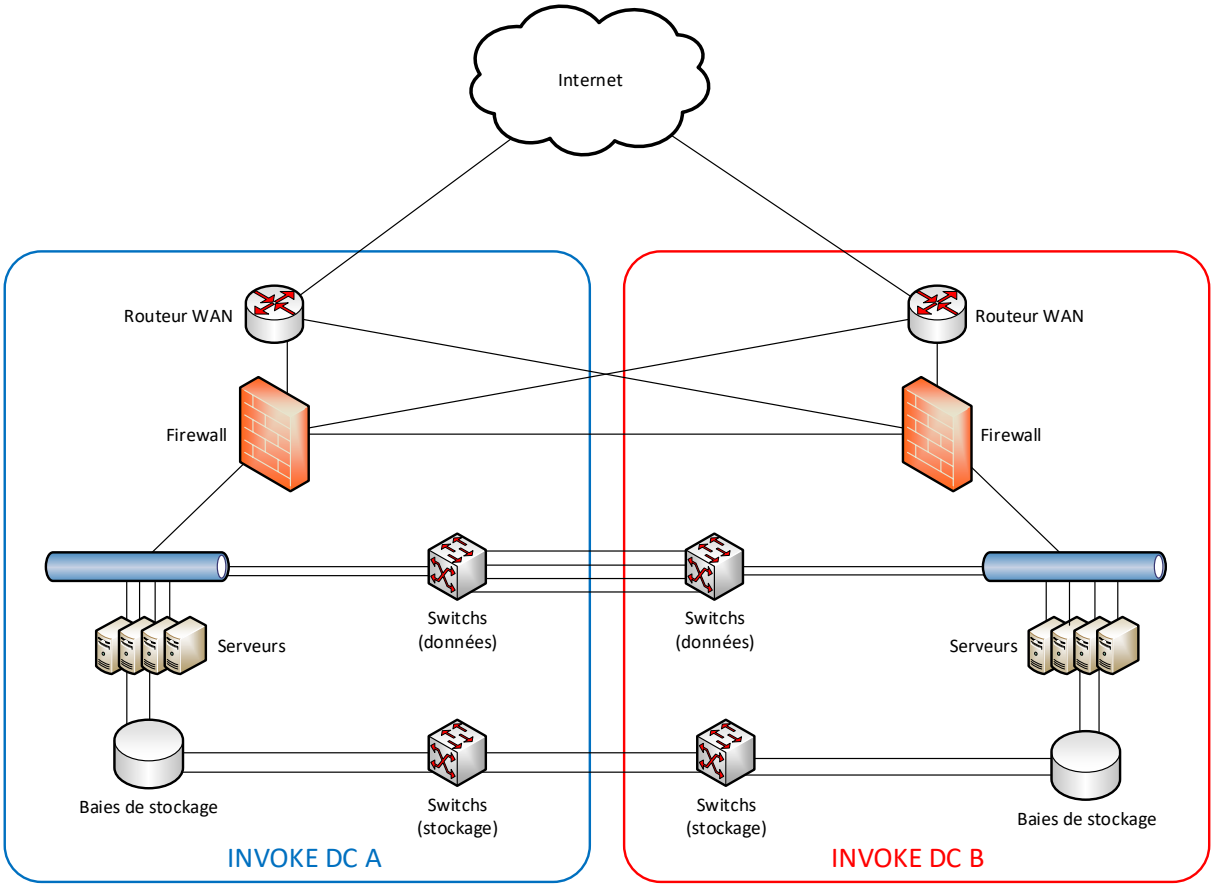
5.6 - Réseaux

Les réseaux en œuvre dans les datacenters de la Société sont tous redondés afin de fournir la disponibilité maximale pour les différents services proposés. Ces réseaux transitent via des fibres optiques dédiées entre les deux datancenters.

Ces réseaux sont entièrement redondés, tant au niveaux des liaisons (6 fibres optiques en propre) que par les équipements (switchs, firewalls, fabriques, …). Cette redondance permet la maintenance ou la défaillance de plusieurs équipements ou liens sans interruption de service.

Ces réseaux sont de deux natures :

- Réseaux de données servant à la communication entre les serveurs.
- Réseaux de stockage servant à la communication entre les baies de stockage et les serveurs.



Le équipements réseau utilisés dans le cadre de la fourniture des services hébergés sont divisés de la sorte :

- **Routeurs WAN** : deux routeurs principaux (actif/passif) assurant la connexion avec l'extérieur. La défaillance d'une liaison entraine la bascule automatique du trafic vers le second routeur en quelques secondes.
- **Firewalls** : cluster de firewalls (actif/passif) assurant l'isolation entre les différents réseaux. La défaillance d'un nœud actif entraine la bascule immédiate et sans perte de connexion sur le nœud restant.
- **Swicths de données** : clusters de swicths assurant la communication entre les serveurs et entre les datacenters. La perte d'un équipement est sans conséquence du fait de la redondance complète des liaisons entre les serveurs et les switchs.
- **Switchs de stockage** : fabriques assurant la communication entre les baies de stockage et les serveurs. La perte d'un équipement est sans conséquence du fait de la redondance complète des liaisons entre les serveurs, les baies de stockage et les switchs.

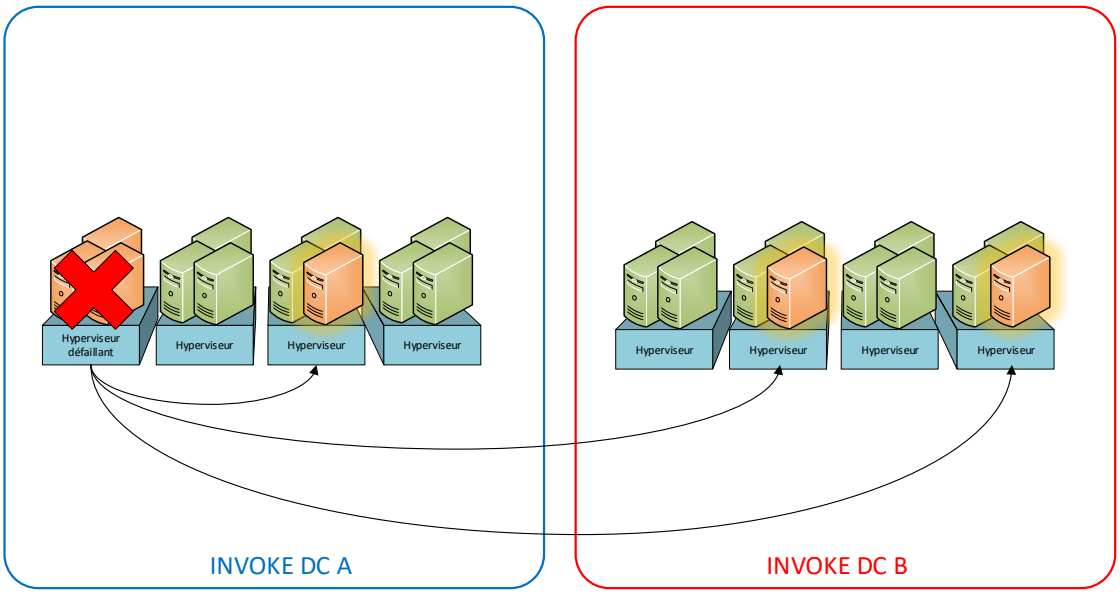
L'ensemble de ces réseaux est monitoré en permanence et toute anomalie ou perte de lien est immédiatement signalée à l'équipe en charge de la supervision.

5.7 - Serveurs

Les serveurs utilisés dans le cadre de l'hébergement des solutions de la Société reposent sur des machines virtuelles. Cette technologie permet d'assurer un haut niveau de disponibilité.

En effet, ces machines virtuelles ne sont pas attachées à un hôte physique et peuvent être déplacées sur d'autres serveurs situés ou non dans le même datacenter. Ces opérations de déplacement peuvent être effectuées « à chaud », sans interruption de service pour les utilisateurs finaux.

De plus, un système de haute disponibilité est implémenté et permet de redémarrer automatiquement un serveur virtuel sur un autre hôte (dans le cas d'une défaillance d'un hôte de virtualisation ou de la perte d'une salle serveurs par exemple). Bien que l'équipe en charge de la supervision soit alertée de la survenance d'une anomalie, cette sécurité ne demande aucune intervention humaine.



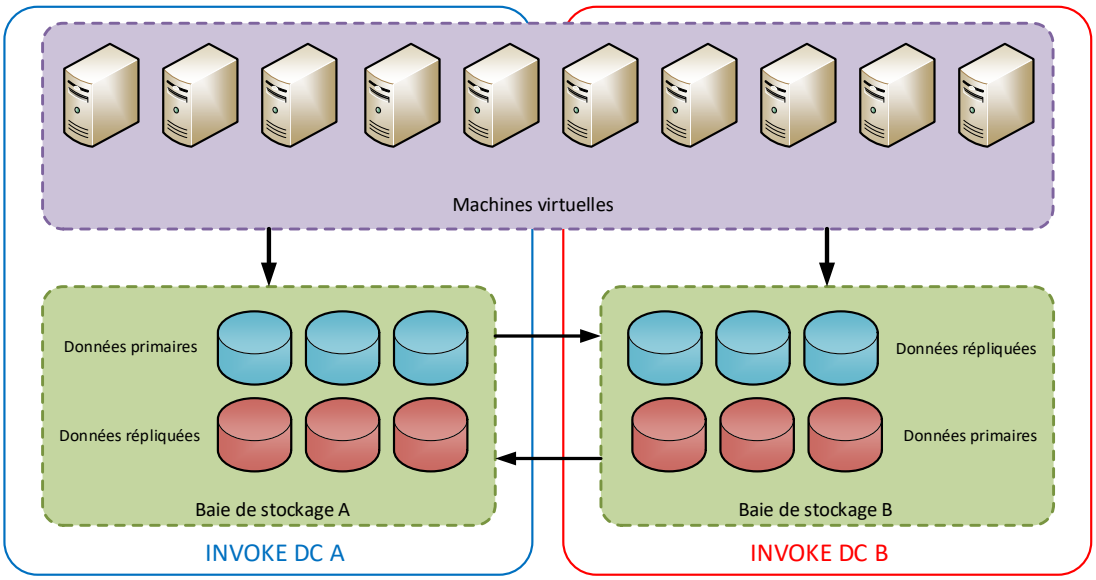
5.8 - Stockage des données

Le stockage des données des serveurs et applications utilisées dans le cadre de l'hébergement proposé par la Société est réalisé sur des baies de stockage sécurisées.

Deux baies de stockage sont utilisées pour cette tâche et sont réparties dans les deux datacenters de la société. Ces baies disposent d'un ensemble de disques redondés ainsi que de disques de secours prêts à être intégrés instantanément dans le système de stockage en cas de défaillance d'un ou plusieurs disques actifs.

Toute défaillance détectée sur ce système de stockage est automatiquement remontée dans les outils de supervision et entraine la réaction immédiate des équipes techniques.

De plus, ces deux baies sont répliquées entre elles de manière synchrone afin de disposer d'une copie exacte et complète des données à tout moment. Ce mécanisme permet la perte d'une baie sans aucune incidence sur les services en cours de fonctionnement. En cas de défaillance, les volumes de données sont automatiquement et instantanément mis de nouveau à disposition pour les services d'hébergement sur la baie encore en fonction.



Ce système de stockage, primordial pour le fonctionnement des services hébergés, est couvert par une maintenance « Mission critique 4 heures 24/24 7/7 » auprès de son fabriquant.

5.9 - Sauvegarde des données

Les données relatives aux services hébergés sont stockées dans des bases de données. Ces bases de données sont vérifiées et sauvegardées dans leur intégralité quotidiennement puis transférées vers des serveurs de sauvegarde dédiés à cette tâche.

Les sauvegardes sont ainsi répliquées sur deux serveurs distincts présents dans chacun des deux datacenters et sont conservées sur une période minimale de dix jours glissants.

Le processus de sauvegarde est monitoré et toute anomalie est automatiquement remontée à l'équipe en charge de la supervision pour action.

6 - Objectifs de disponibilité

Les éléments présentés précédemment permettent de répondre aux exigences métier suivantes :

Durée d'Interruption Maximale Autorisée (DIMA ou RTO)	**4 heures**
Perte de Données Maximale Autorisée (PDMA ou RPO)	**24 heures**