aruba.it

Aruba – Solutions Cloud

Sécurité physique, Continuité de service et Reprise après sinistre

14.04.2023

SOMMAIRE

1 HOUSING DES SYSTÈMES ET SÉCURITÉ INFORMATIQUE

En Italie, tous les systèmes de traitement utilisés pour la fourniture des services Cloud du Groupe Aruba se trouvent dans les deux data centers d'Arezzo IT1 et IT2, situés respectivement Via Gobetti 96 et Via Ramelli 8, et les data centers IT3 DCA et DCB de Ponte San Pietro (BG) situés à Via San Clemente 53.

Figure 1 – Data Center IT1

Figure 2 – Data Center IT2

Figure 3 – Campus IT3

En plus des data centers italiens, le Groupe Aruba s'appuie, pour la fourniture des services Cloud, sur un réseau international d'infrastructures, qui lui appartiennent ou qui appartiennent à des partenaires qualifiés et en particulier :

- Data center CZ1, situé à Ktiš en République tchèque et qui appartient au réseau international des data centers propriété de l'Organisation.
- Data center FR1, situé à Paris en France et qui appartient au réseau des data centers partenaires.
- Data center DE1, situé à Francfort en Allemagne et qui appartient au réseau des data centers partenaires.

- Data center UK1, situé à Londres au Royaume-Uni et qui appartient au réseau des data centers partenaires.
- Data center PL1, situé à Varsovie en Pologne et qui appartient au réseau des data centers partenaires.

Figure 4 – Réseau international de data center des services Cloud

Pour satisfaire les rigoureuses normes de qualité, tous les data centers possèdent la certification ISO 9001.

Nous illustrerons dans le paragraphe suivant les principales mesures de sécurité physique adoptées.

1.1 Description des mesures de sécurité physique

Les data centers possèdent la certification ISO 27001 et les principales mesures destinées à garantir la sécurité physique des structures sont mises en œuvre dans ces derniers.

1.1.1 Tier 4*/Rating 4

Les data centers IT1, IT3 DCA et DCB du Groupe Aruba sont conformes au niveau maximal (Rating 4) parmi ceux prévus par la norme ANSI TIA 942-B-2017. Ce résultat, qui indique la capacité d'éviter des interruptions des services même en cas de pannes graves (fault-tolerance), a été obtenu grâce à une série de dispositifs de conception et d'exécution ayant concerné tous les aspects du data center : choix du site, aspects architecturaux, sécurité physique, système anti-incendie, installation électrique, installation mécanique et réseau de données.

Un data center de Rating 4 (former Tier 4) possède des composants redondants toujours actifs, en plus de multiples parcours d'alimentation et de refroidissement des hardwares.

Les data centers sont structurés pour supporter une panne partout dans l'installation sans provoquer de downtime et sont protégés contre les évènements physiques dont les catastrophes naturelles (ex : incendie, inondation, tremblement de terre, etc.).

1.1.2 ISO/IEC 22237

Les data centers IT3 DCA et DCB du Groupe Aruba sont certifiés ISO/IEC 22237, la norme internationale de référence pour l'ensemble du cycle de vie du data center, de la conception stratégique à la construction et à la mise en service, conformément aux réglementations ANSI/TIA 942 (norme américaine) et EN 50600 (norme européenne). La norme, intitulée « Data centre facilities and infrastructures », est composée de sept parties : General concepts, Building construction, Power distribution, Environmental control, Telecommunications cabling infrastructure, Security systems et Management and operational information.

1.1.3 Surveillance 24 heures sur 24

Tous les data centers sont surveillés par une équipe technique 24 heures sur 24, 365 jours par an.

Les data centers partenaires sont également gérés à distance par une équipe technique de la Control Room du Groupe Aruba.

En plus de la supervision locale, les data centers propriétaires disposent d'un BMS (Building Management System) capable d'alerter en temps réel des événements significatifs et permettant à des techniciens de gérer à distance toutes les installations.

1.1.4 Contrôle des accès physiques

L'accès aux bâtiments n'est possible qu'à ceux qui en ont un besoin effectif, après s'être enregistré à la réception, et l'accès aux locaux techniques n'est autorisé qu'au personnel autorisé, après identification avec un badge et un code PIN.

Pour les data centers propriétaires, le système de gestion des accès prévoit la possibilité d'activer ou de désactiver chaque carte en fonction des zones, des heures et d'autres paramètres, de manière à garantir une sécurité maximale des environnements ainsi que la fluidité nécessaire des accès.

Certains data centers partenaires, comme FR1, DE1 et UK1, disposent d'un système de contrôle biométrique des accès.

1.1.5 Système anti-intrusion

Tous les data centers disposent de grilles, de vitres et de portes blindées, de portails motorisés (anti-intrusion passifs) et des systèmes TVCC et VMD (anti-intrusion actifs) sont installés.

De plus, dans toutes les zones des data centers propriétaires, des détecteurs de mouvement capables de détecter la présence de personnes sont installés ; dans les zones sensibles (Salles des données, Power Center, entrepôts) se trouvent également des capteurs qui détectent l'ouverture des portes.

1.1.6 Système anti-incendie, anti-inondation et bâtiments parasismiques

Les data centers sont tous conformes à la réglementation antisismique. De plus, il existe des systèmes automatiques de détection et d'extinction d'incendie avec des gaz inertes, inoffensifs pour les personnes et les systèmes informatiques et des systèmes de détection d'inondation avec des capteurs répartis à tous les étages des bâtiments.

Les bâtiments sont également situés dans des zones basses et en position surélevée par rapport à la campagne.

1.1.7 Systèmes de climatisation redondants

Le système de climatisation des salles de données et des installations technologiques est réalisé avec des modules multiples redondants garantissant le bon fonctionnement, même s'il y a plusieurs pannes simultanées.

Le système de climatisation est protégé par UPS avec des batteries et des générateurs électriques d'urgence afin de garantir la continuité du service.

1.1.8 Alimentation et redondance des Power Centers

Le Groupe Aruba utilise pour ses propres services exclusivement des serveurs et des appareils munis d'une double alimentation. À la sortie de chaque Power Center se trouvent des dispositifs STS (Static Transfer Switch) capables dans tous les cas de garantir la continuité de l'alimentation électrique des deux lignes présentes, garantissant ainsi le fonctionnement des serveurs et des appareils qui ne disposent pas de double alimentateur.

L'alimentation fournie aux serveurs est complètement redondante grâce à deux Power Centers séparés. Chaque Power Center possède la capacité d'alimenter toutes les salles de données présentes dans les data centers propriétaires, même à pleine charge, et est équipé de systèmes UPS à double conversion et à haute efficacité énergétique (redondance de type 2N+1 pour IT1, IT2 et IT3 et de type 2N pour CZ1).

Les systèmes d'alimentation des data centers partenaires sont eux aussi complètement redondants et équipés de systèmes UPS à double conversion.

Pour plus de détails concernant les caractéristiques techniques des data centers, veuillez-vous reporter à la page internet : « Nos data centers ».

2 CONTINUITÉ DE SERVICE ET REPRISE APRÈS SINISTRE

2.1 Introduction

L'objectif de ce chapitre est de décrire la procédure de Reprise après sinistre et de Continuité de service mise en œuvre pour en garantir l'application pour les services Cloud du Groupe Aruba.

L'activité de toutes les entreprises et les activités connexes dépendent strictement de la disponibilité des structures et des ressources dédiées aux processus d'assistance. En règle générale, l'impact résultant d'une indisponibilité du service s'accroit de manière exponentielle lorsque l'interruption perdure, et il est possible de compromettre en peu de temps et de manière définitive la capacité de fonctionner de l'entreprise.

Pour garantir la continuité des Processus d'activité, il est extrêmement important de protéger toutes les ressources qui contribuent à la fourniture des services les plus critiques : informations, personnes et infrastructures, technologies, réseaux de communication, etc.

Le Groupe Aruba a décidé d'adopter un programme de gestion de Continuité de service d'entreprise pour analyser et gérer les impacts sur le fonctionnement face à certains scénarios catastrophes et identifier à la suite les solutions de recovery pour soutenir la continuité opérationnelle.

Ces solutions entrainent la reprise des services essentiels d'un point de vue aussi bien organisationnel que logistique ou informatique.

2.2 Plan de Continuité de service

Le Plan de Continuité de Service (appelé ci-dessous par abréviation « PCS ») ou « Plan de Continuité Opérationnelle » est l'ensemble des normes et des procédures qui – en préfigurant un ou plusieurs scénarios d'indisponibilité capables d'interrompre le fonctionnement normal de n'importe quel système organisé – définit les responsabilités, détermine les activités et fournit les instruments pour gérer l'interruption et amener le système à un état de fonctionnement opérationnel suffisant.

Le PCS a pour objectif de garantir le rétablissement des processus critiques dans des délais tolérables et prédéterminés pour chaque processus.

Tout l'environnement de production relatif aux services Cloud est protégé par le PCS d'entreprise, avec des tests de Continuité de service sur l'infrastructure programmés chaque année.

Ce Plan possède la fonction de guider le Groupe Aruba dans la gestion et la médiation des éventuels risques identifiés en appliquant la méthode de « Gestion du Risque pour la Sécurité des Informations », décrite de manière détaillée dans le chapitre spécifique.

De plus, le PCS définit et liste les actions à entreprendre avant, pendant et après une condition d'urgence pour garantir la continuité du service. Il fournit des indications et, si possible, des instructions étape par étape destinées à garantir la continuité des services critiques du Groupe Aruba même en cas d'évènements indésirés pouvant provoquer l'arrêt prolongé des systèmes informatiques.

2.3 Reprise après sinistre

L'environnement Cloud est composé d'une infrastructure multi-datacenters, dont les services sont interconnectés par un réseau IPSEC à bande et protection élevée.

Chaque data center fournit de nombreux types de services, dont :

- Cloud Computing
- Jelastic Cloud
- Data Base as a Service
- Virtual Private Cloud – VPC
- Cloud Object Storage
- Domain Center
- Cloud Monitoring
- Cloud Backup

De plus, chaque data center présente une structure formée par les machines de base suivantes :

- Domain Controller
- Équilibreur LVS
- Front-End
- WCF (Webservice Microsoft)
- Provisioning
- Comptabilité pour la facturation
- Database
- Hypervisor hosts
- Cloud Storage hosts
- Cloud Monitoring hosts
- Cloud Private hosts
- Cloud backup hosts

La structure étant pensée pour être multi-datacenters, celle-ci est nativement prédisposée à la Reprise après sinistre car tous les data centers sont indépendants d'un point de vue logique.

Il est important de souligner que les machines virtualisées des Clients ne sont pas soumises à une Reprise après sinistre géographique car tous les instruments nécessaires pour construire sur mesure les systèmes et les procédures de Reprise après sinistre sont fournis au Client.

HISTORIQUE DES VERSIONS

VERSION 1.1 DU 14/04/2023	***NATURE DES CHANGEMENTS : Inséré : Certification ISO/IEC 22237 et Campus IT3 avec référence à DCA et DCB ; mise à jour de la liste des services Cloud.***
VERSION 1.0 DU 01/01/2022	***NATURE DES CHANGEMENTS : Première édition***