Le Cloud, nouveau challenge de la Continuité d'Activité :

quelle est la vision et l'expérience d'Orange Business Services pour réussir ces projets ?

Sommaire

Elaboré par The Duquesne Group en partenariat avec Orange Business Services.

#1 Introduction

Le point de départ de la Continuité d'Activité est les activités métier d'une entreprise. Si leurs moyens sous-jacents sont frappés par un sinistre, ces activités – la véritable raison d'être de l'entreprise - peuvent être profondément perturbées, voire interrompues.

Le management de la Continuité d'Activité prend en compte l'ensemble des moyens – techniques et non techniques – nécessaires pour les activités prioritaires des métiers. Sa finalité est de protéger, continuer voire reprendre ces activités, quelque soit la nature du sinistre et les moyens affectés.

Cependant, le système d'information occupe un rôle de plus en plus central dans les entreprises. C'est pourquoi depuis des années tant de DSI ont mis en place des mesures souvent couteuses – sites de reprise en propre, contrats de secours, etc - pour pallier à une défaillance majeure, voire un désastre affectant leur data center.

Et puis la révolution du Cloud est arrivée. A notre avis, ce nouveau paradigme représente un challenge crucial pour la Continuité d'Activité.

Pourtant, il est courant de penser que le cloud intègre nativement la continuité d'activité, ce qui relègue souvent ce sujet crucial en second plan. La question revient de temps en temps quand les services d'un grand acteur sont coupés ou fortement perturbés par la tombée de la foudre ou un incident technique majeur. En 2018, tous les grands clouds « hyperscale » ont subi des interruptions importantes, très pénalisantes pour leurs clients mais rarement d'une grande dangerosité.

Cela étant dit, il faut admettre que des événements très rares - mais à impact très lourd - finissent par arriver. Un jour ou l'autre, en France ou ailleurs, un data center Cloud sera gravement sinistré - pour des raisons naturelles, techniques ou humaines - mettant en péril les activités métier de ses clients. C'est un peu comme la grande crue centennale de la Seine : la question n'est pas « si » mais « quand ».

Cependant, le tableau n'est pas tout en noir. Grâce aux progrès technologiques, des solutions de continuité et de reprise bien adaptées aux environnements cloud sont maintenant disponibles.

La vocation de ce livre blanc est d'analyser ce nouveau challenge du Cloud pour la Continuité d'Activité, prenant pleinement en compte la grande diversité des besoins des entreprises en la matière.

Pour rendre notre analyse la plus concrète possible, nous avons choisi de l'élaborer en partenariat avec Orange Business Services. Nous avons partagé nos visions du marché, utilisé ses solutions et certaines références à titre d'exemple.

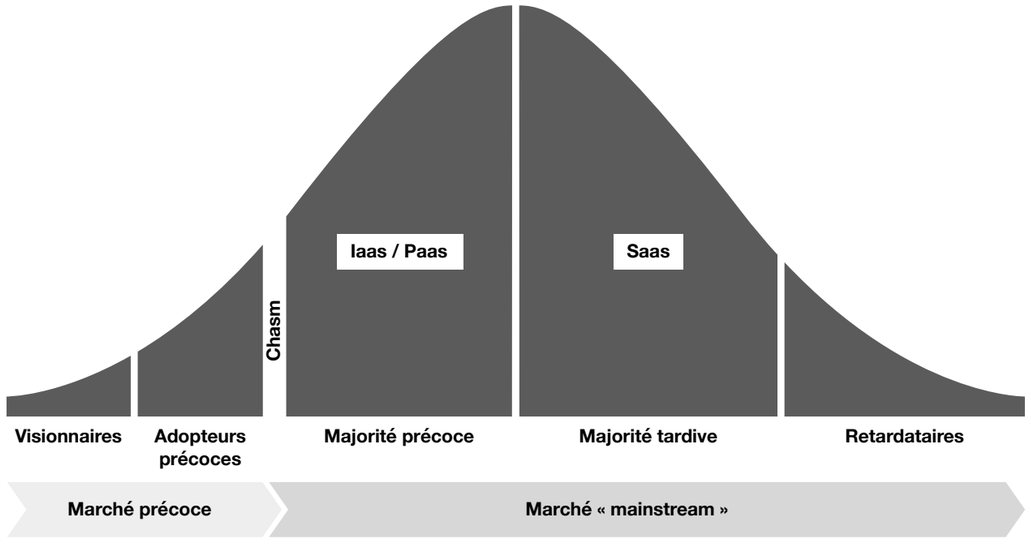
Néanmoins, ce livre blanc reflète fidèlement notre vision indépendante d'une problématique d'entreprise primordiale : la continuité des activités métier à l'époque du cloud.

#2 Évolution du marché Cloud : l'exigence de continuité

Avec autant d'organisations utilisatrices revendiquant une stratégie « Cloud First », ainsi que des transformations de pouvoir et d'influence du côté des fournisseurs, il est clair que le cloud est passé dans le « mainstream » du marché. Comme toujours dans les marchés technologiques, cette maturation se traduit par des changements dans les attentes des clients.

Pour mieux comprendre cette transition, nous positionnons ci-dessous le cloud (IaaS/PaaS) sur la courbe classique du « cycle de vie de l'adoption des technologies » de Geoffrey Moore.

Cloud sur le « technology adoption lifecycle curve »



Avant de tirer des conclusions pour notre analyse, il convient de préciser deux points :

- Dans « Cloud » (IaaS/Paas), nous incluons « public » et « privé ». Contrairement aux prévisions de nombreux experts, le cloud privé a fait preuve d'une ténacité considérable et continue de progresser avec une croissance à deux chiffres.

- L'adoption du cloud par de nombreux utilisateurs « mainstream » n'implique pas que leurs applications s'exécutent principalement dans le cloud. Diane Greene, anciennement responsable Google Cloud Platform, estime qu'environ 10% des traitements d'entreprise se font en cloud public. IBM donne une estimation de 20%, à la fois public et privé. Le paradigme cloud a conquis les esprits, mais il représente toujours une part modeste, mais croissante, de l'informatique d'entreprise.

Revenons maintenant à notre analyse du passage du cloud (IaaS/PaaS) dans le marché « mainstream ». Le cycle de vie de l'adaptation des technologies est une courbe en cloche normale divisée en cinq phases définies par types de clients : visionnaires, adopteurs précoces, majorité précoce, majorité tardive et retardataires. Le moment le plus critique du cycle est la difficile transition (le « chasm ») entre les adopteurs précoces et la majorité précoce, car les attentes sont très différentes.

• Les adopteurs précoces sont généralement motivés par des qualités techniques, tolèrent des failles inévitables d'une nouvelle technologie et sont focalisés étroitement sur leur problème spécifique. Dans les premières années du cloud, il n'est pas surprenant que les développeurs - souvent mais pas toujours dans les start-ups - aient impulsé son adoption.

• Les attentes des clients « mainstream » de la majorité précoce sont plus pragmatiques que techniques, axées sur « qu'est-ce que cela signifie pour mon entreprise ? » Parmi leurs préoccupations, citons (entre autres) l'intégration avec l'existant, les services nécessaires, la sécurité et la conformité, la facilité de management et, bien sûr, la résilience et la continuité de fonctionnement. Dans le cas du cloud, ce sont des problématiques du niveau DSI.

À notre avis, la continuité des applications dites « critiques » pour les activités prioritaires des métiers fait partie des exigences les plus importantes. Or ces applications sont de plus en plus déployées dans des environnements cloud. De ce fait, les entreprises ne peuvent plus se contenter des niveaux de disponibilité théoriques (comme dans la plupart des SLAs des clouds publics). En cas de sinistre, l'entreprise a impérativement besoin de pouvoir rétablir ces applications sous des délais et dans des conditions acceptables pour ces métiers.

Résultat : à mesure que les services cloud se développent, l'exigence de continuité pour les applications critiques de l'entreprise s'accélère.

Dans ce domaine, Orange Business Services (OBS) a fait preuve de prescience, en investissant dans un portefeuille de solutions avec des partenaires technologiques de premier plan, afin de répondre aux différentes exigences de ses clients pour la continuité des services cloud.

Pour établir le contexte de ces solutions, nous évoquons d'abord quelques fondamentaux du management de la continuité d'activité.

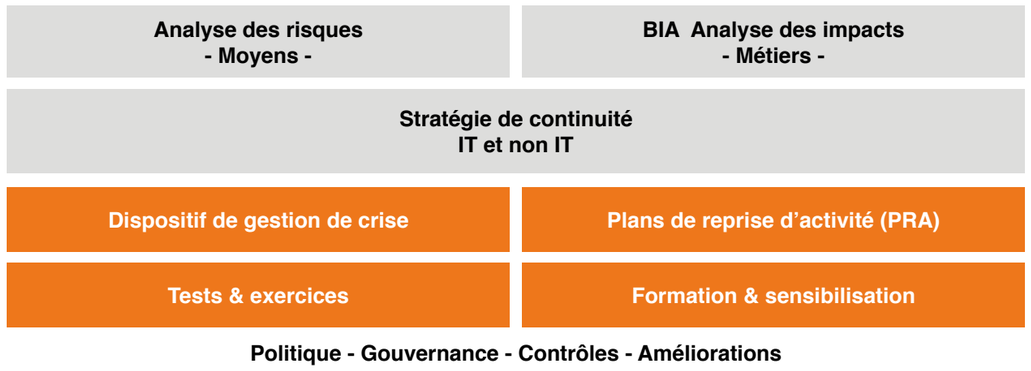
« Évolution du marché Cloud : l'exigence de continuité

- Le cloud est passé dans le « mainstream » du marché IT.
- Les applications « critiques » pour les métiers sont de plus en plus déployées dans les environnements cloud.
- En cas de sinistre, la DSI doit pouvoir les rétablir sous des délais et dans des conditions acceptables par les métiers.
- A mesure que les services cloud se développent, l'exigence de continuité pour les applications critiques de l'entreprise s'accélère

#3 ISO 22301 : le cadre général pour la Continuité d'Activité

ISO22301, la référence normative internationale en la matière, définit la « continuité d'activité » comme suit : la « capacité de l'organisation à poursuivre la fourniture de produits ou la prestation de services à des niveaux acceptables et préalablement définis après un incident perturbateur. »

En effet, la finalité de la norme est la continuité des activités métiers d'une organisation. Ces activités s'appuient sur les moyens à la fois techniques (services cloud, applications …) et non techniques (RH, bureaux…). Si ces moyens sont frappés par un sinistre (« un incident perturbateur », dans le langage de la norme), les activités essentielles des métiers peuvent être perturbées, voire interrompues.



Trois composants de type « étude amont » se trouvent en haut du schéma :

- **Le BIA** (Business Impact Analysis en anglais) est, comme l'écrit Emmanuel Besluau expert français de référence en la matière, « au cœur des démarches modernes de management de la continuité. Il porte sur les activités métiers de l'entreprise et permet de répondre à des questions comme : «quelles activités doivent être continuées ou reprises en priorité en cas de sinistre ?» ... «sous quels délais ?» ... «avec quels moyens ?» Emmanuel Besluau ajoute, « autant dire que le BIA est un point de départ essentiel. »

  Deux exigences métiers formulés lors du BIA, sont particulièrement importantes :
  - Durée Maximale d'Interruption Acceptable (DMIA)
  - Perte Maximale de Données tolérable

  On entend dire parfois que les métiers exigent une continuité totale pour l'ensemble de leurs activités. Or, cette affirmation est fausse. Les niveaux d'exigence des organisations et de leurs métiers sont différents. Par ailleurs, il y a toujours une hiérarchie de priorités temporelles dans les activités, même si la tendance aujourd'hui va vers des DMIAs de plus en plus courtes.

En cloud, le point de départ reste les exigences métiers de continuité

> Pris ensemble, ces deux exigences métiers – durée maximale d'interruption acceptable et perte maximale de données tolérable - expriment à la fois la vision du métier de la « criticité » d'une activité et leurs exigences pour sa poursuite ou reprise en cas de sinistre. Ils sont au cœur de la problématique de choix des solutions de continuité en cloud. On y revient.

- **L'Appréciation des Risques** porte sur les moyens (IT, RH, bureaux, …) sur lesquels ces activités s'appuient. Elle permet d'identifier, d'analyser et d'évaluer de manière systématique les risques auxquels sont exposés les moyens et de déterminer les scénarios de sinistre à prendre en compte. Cependant, il est dans les règles de l'art (et aussi souvent parmi les exigences des régulateurs) de toujours prendre en compte les scénarios de « choc extrême » tels que la perte du siège ou une coupure longue du système d'information. Par ailleurs, cette appréciation est aussi l'occasion de voir si l'on ne pourrait pas réduire a priori les conséquences des sinistres.

- **La Stratégie de Continuité** est une étape cruciale. Selon la norme, « la détermination et le choix d'une stratégie doivent être basés sur les conclusions de l'analyse d'impacts sur l'activité et de l'appréciation du risque. » Plusieurs combinatoires de solutions pour la continuité ou la reprise des activités prioritaires sont peut-être possibles, plusieurs critères d'évaluation (techniques, économiques, organisationnels…) peuvent entrer en ligne de compte, mais il faut décider ! Le plus souvent, la décision finale relève de la Direction Générale.

Sur la base de sa stratégie de continuité, l'organisation peut passer à l'élaboration, la documentation et la mise en œuvre des mesures « opérationnelles » dont la vocation est d'assurer qu'elle pourra faire face aux divers sinistres le moment venu.

- **Le Dispositif de Gestion de Crise** a pour première vocation de maintenir la capacité de décision de l'organisation dans une situation de fonctionnement anormal. Le point central du dispositif est la cellule de crise dont la composition dépend de la structure de l'organisation et de la nature et gravité du sinistre. Elle se met en place rapidement pour « prendre les choses en main » en matière de décision, gestion de priorités et communication. Elle lance et suit les PRA préparés et prend en charge l'imprévu.

- **Les Plans de Reprise des Activités (PRA)** préparés d'avance constituent une sorte de « boite à outils » pour la cellule de crise, lancés en fonction des circonstances pour poursuivre ou reprendre les activités métier prioritaires et rétablir ou fournir des moyens (IT, bureaux, RH, …) nécessaires. La plupart des PRA-IT s'appuient sur des outils techniques mis en place, notamment ceux ayant pour vocation de protéger les données - par exemple en les répliquant sur un site de secours ne partageant pas de risques conjoints - et de rétablir les services et les applications pour les activités prioritaires des métiers.

Le Cloud pour un site de secours

> Le recours au cloud comme « site de secours » présente de nombreux avantages. La mise en place et gestion d'un site de secours physique est une option lourde et couteuse, notamment en matière d'investissement (CapEx) pour des moyens qui sont peu utilisés. Un site de secours en cloud tire profit de la mutualisation des ressources et permet de payer que les ressources réellement consommées (OpEx).

- **Formation & Sensibilisation** sont des exigences fondamentales de la norme. Elle attache beaucoup d'importance aux compétences des personnes chargées de l'ensemble des mesures du PCA. Outre les formations aux outils techniques, des formations certifiantes ISO 22301 peuvent être envisagées. Même si l'entreprise ne vise pas une véritable certification, la certification de quelques acteurs clés du management de la continuité est un gage de sérieux. Par ailleurs, la norme exige une sensibilisation régulière de tous les personnels, notamment à leur propre rôle en cas de sinistre.

  Quand un sinistre arrive, l'efficacité du PCA dépendra en grande partie de la compétence et de la bonne préparation des personnes qui doivent y faire face.

- **Les Tests** des mesures du PCA figurent parmi les exigences fondamentales de la norme. Il est quasi certain qu'un PCA qui n'est pas testé régulièrement et, par voie de conséquence non tenu à jour, va se révéler comme défaillant quand le sinistre arrive.

Deux précisions de la norme sont particulièrement pertinentes. Elle exige des tests qui : « cumulés au fil du temps… valident l'ensemble de ses dispositions en matière de continuité d'activité » et « minimisent le risque de perturbation des opérations »

L'avantage du Cloud pour les tests

Un avantage majeur des solutions modernes de reprise en cloud est de faciliter les tests. La plupart des outils PRA en cloud permettent l'exécution des tests plus fréquents, avec des ressources spécifiques payées à l'usage (OpEx) et surtout sans perturber les opérations. On y revient dans le chapitre suivant.

En bas du schéma, nous trouvons d'autres exigences de la norme – Politique de Continuité d'Activité, Gouvernance, Contrôles et Amélioration Continue – qui permettent de s'assurer (au-delà de simples tests des mesures en place) que le PCA puisse rester efficace dans la durée, évoluer en ligne avec les besoins de l'organisation et s'améliorer en permanence.

Maintenant, en s'appuyant sur les bonnes pratiques éprouvées de la norme, nous sommes prêts à rentrer dans le vif de notre sujet et aborder la problématique du choix des solutions de continuité et reprise dans le cloud.

ISO 22301 : le cadre général pour la Continuité d'Activité

- La finalité d'ISO 22301 - référence normative pour tout PCA (Plan de Continuité d'Activité) - est la continuité des activités métier d'une organisation
- Le BIA permet de répondre à des questions comme : « quelles activités métier doivent être continuées ou reprises en priorité en cas de sinistre ? » … « sous quels délais ? » … « avec quels moyens ? »
- Deux exigences métier cruciales sont formulées lors du BIA : la durée maximale d'interruption acceptable et la perte maximale de données tolérable.
- Dans le volet IT d'un PCA, le cloud comme « site de secours » présente de nombreux avantages : la mutualisation des ressources, le paiement à l'usage (OpEx), etc.

#4 Comment choisir sa solution de continuité et reprise dans le cloud ?

Pour la DSI, le choix d'une solution de continuité et reprise (et aussi le choix du fournisseur ou prestataire) est souvent complexe, parce qu'il doit prendre en compte de nombreux facteurs.

Avant d'aborder des critères de choix, rappelons que le choix d'une « solution PRA » se situe dans la partie « aval » des travaux PCA selon la norme ISO 22301. Nous prenons ici l'hypothèse qu'un minimum de réflexion « amont » a été faite en préalable au moins sur la partie IT, notamment en matière de BIA et de Stratégie de Continuité. Selon la taille et la structure des organisations, cette réflexion n'est pas forcément complètement structurée, mais il faut au moins une vision claire sur les exigences des métiers qui sont au cœur de toute démarche de continuité d'activité.

Sous cette hypothèse, nous mettrons en exergue quelques critères majeurs permettant de structurer la problématique. A titre d'exemple, nous évoquerons aussi certaines offres d'Orange Business Services mais la logique de choix reste valable quel que soit le fournisseur.

Nous commençons avec trois critères majeurs :

- **La « criticité » des applications et des données à protéger**

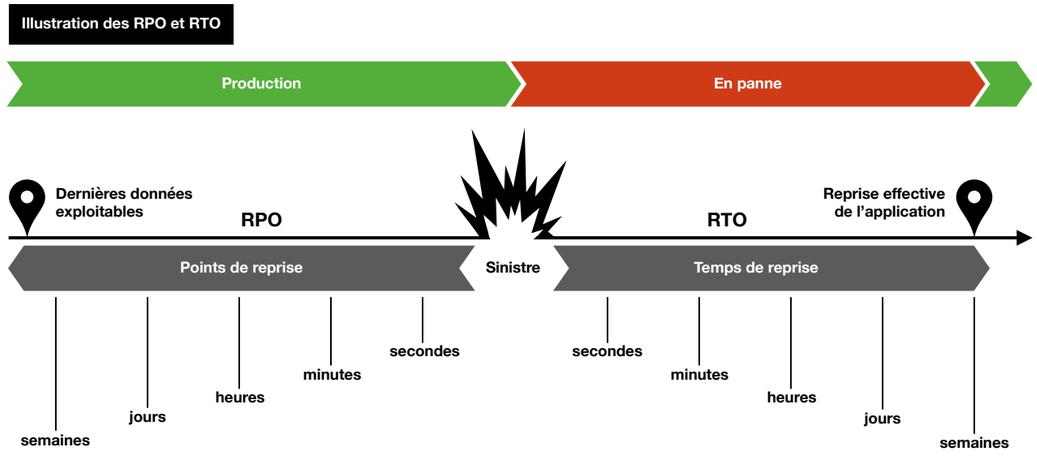
  Ce critère est de loin le plus structurant. Rappelons que la finalité d'un PCA est de protéger, poursuivre ou reprendre les activités métiers prioritaires en cas d'interruption ou de sinistre. Lors du BIA, deux exigences métiers sont identifiées pour chaque activité prioritaire :

  - Durée Maximale d'Interruption Acceptable (DMIA)
  - Perte Maximale de Données tolérable

  Durant les travaux sur la Stratégie de Continuité, ces exigences sont confrontées aux réalités techniques et budgétaires pour d'éventuels ajustements ou validations. Sur la base des exigences métiers finalisées, l'entreprise peut les traduire en deux paramètres techniques :

  - Recovery Time Objective (RTO)
  - Recovery Point Objective (RPO)

  Ils sont présentés sur le schéma ci-dessous :



Selon ISO 22301, le RPO - ou en français « point de récupération des données » - correspond au « point à partir duquel les informations utilisées par une activité doivent être restaurées afin de permettre son fonctionnement à la reprise. » La signification du RPO est généralement assez claire pour tous, parce que sa valeur est fonction des dernières données utilisables pour la reprise suite à un sinistre.

En revanche, une certaine confusion demeure sur la véritable signification du RTO. Sur le schéma ci-dessus, la représentation du RTO est en ligne avec ISO 22301 qui le définit comme « la durée après un incident durant laquelle… une activité doit être reprise, ou des ressources (pour l'activité) doivent être rétablies. » Le RTO (qui est bien un objectif voire un engagement mais jamais une certitude) démarre donc avec l'incident (ou sa détection) et court jusqu'au rétablissement des applications critiques pour les métiers.

La capacité de respecter un RTO fixé dépend de plusieurs facteurs, non seulement de l'outil de reprise (par exemple celui de Zerto, partenaire technologique d'Orange Business Services, dont les performances intrinsèques se chiffrent en minutes) mais aussi des procédures et dispositifs organisationnels en place pour gérer un sinistre. Dans ce contexte, le « RTO éditeur » annoncé pour l'outil n'est que l'un des composants – souvent le plus court - du RTO global :

- Suite à la détection d'un sinistre, le RTO fixé doit tenir compte des temps d'escalade, d'analyse et de décision. La survenance d'un incident même majeur n'implique pas forcément une bascule. Si le temps d'arrêt pour réparation est acceptable en fonction des circonstances, l'entreprise peut décider de ne pas basculer.
- Si la décision de basculer est prise, le « RTO éditeur » commence avec l'activation de l'outil et se termine (en général) avec le rétablissement des VMs sur le secours.
- Ensuite, il faut activer les VMs et rétablir l'application, sans oublier de vérifier la cohérence applicative et la bascule du réseau pour les accès utilisateurs.

De plus, le retour en service de l'application n'implique pas le redémarrage immédiat des activités métiers, ce qui explique pourquoi la norme précise que le RTO fixé doit être inférieur au DMIA. Avec l'appui de la DSI, les métiers doivent effectuer des contrôles fonctionnels, analyser l'impact d'une éventuelle perte des données et le cas échéant faire des travaux de rattrapage avant de pouvoir redémarrer leurs activités.

Malgré ces bémols sur le RTO, la « criticité » des applications et des données (RTO, RPO) nous permet d'établir une typologie structurante (dans le tableau ci-dessous) pour le choix du type de solution de continuité et/ou de reprise.

Niveau	Nature de la solution	RTO et RPO pour les métiers	Solutions Orange Business Services et outils techniques partenaires
0 - Froid	Sauvegardes des données (ou copies) sorties hors du site de l'entreprise	RTO : non défini RPO : fonction de la dernière sauvegarde utilisable	Flexible Recovery d'Orange Business Services avec l'outil partenaire Veeam Repository as a Service
1 - Tiède	Préparatifs en place pour reconstruire rapidement l'environnement SI sur le secours et redémarrer à partir des sauvegardes	RTO défini, non nul RPO : fonction de la dernière sauvegarde utilisable	Solution partenaire Nuabee d'Orange Business Services
2 – Chaud	Environnement de protection à jour sur le secours (réplication continue des données) avec VMs prêtes à être rétablies	RTO et RPO définis mais non nul	Flexible Recovery Advanced d'Orange Business Services (prochainement disponible) avec l'outil partenaire Zerto IT Resilence Platform
3 – HD	Haute Disponibilité (HD) : 2 sites actifs synchrones (donc proches à < 40km)	RTO et RPO à zéro (en principe), avec bascule des utilisateurs transparente, mais risques conjoints de distance en cas de sinistre régional	Cloud privé dédié ou virtuel d'Orange Business Services avec un catalogue de solutions logicielles telles que SQL Server Always On de Microsoft
4 – Vital	HD sur 2 sites actifs proches PLUS reprise chaude sur un 3ème site passif à >100 km	- RTO et RPO à zéro (en principe) avec bascule des utilisateurs transparente pour les 2 sites HD actifs - RTO et RPO définis mais non nul pour le 3ème site passif secours	Flexible Resilience d'Orange Business Services : Projet client Orange Business Services avec un catalogue de solutions logicielles telles que SQL Server AlwaysOn de Microsoft PLUS Zerto IT Resilience Platform

Cette typologie – fondée sur la « criticité » des applications et des données à protéger – nous permet d'identifier déjà les catégories de solutions PRA à étudier.

- **La capacité de la solution à faciliter les tests**

Ce critère est aussi très important, parce que des bonnes campagnes de tests apportent à l'entreprise l'assurance qu'en cas de sinistre son dispositif de protection fonctionnera comme prévu. Ce sont des tests qui permettent de déceler et de corriger d'éventuelles incohérences entre le site nominal et le site de secours (par exemple, suite à la mise en production d'une nouvelle application) ou encore de vérifier l'efficacité des procédures et les compétences de tous les acteurs en situation de sinistre.

Les technologies les plus récentes permettent de tirer des avantages majeurs de la virtualisation et du cloud. Ces technologies créent en effet, dans le cloud, un 'bac à sable' dédié aux tests. La production continue ainsi son cours en parallèle des tests et n'est pas impactée. La protection, même, n'est pas impactée. Si un sinistre intervenait, alors que des tests étaient en cours, le RPO et le RTO n'en seraient pas pour autant dégradés.

Par ailleurs le périmètre de bascule peut être aisément délimité, tant pour les tests que pour les bascules réelles. Ceci présente d'autres avantages considérables, notamment si la protection ne couvre qu'une partie du SI. Il devient en effet ainsi possible de gérer le test de bascule d'un périmètre restreint, sans impacter ni la production, ni la protection et en impliquant des équipes également restreintes. Les tests peuvent ainsi être fractionnés, multipliés et menés en heures ouvrées donc plus fréquents et aussi plus formateurs puisqu'ils peuvent impliquer tous les acteurs.

Enfin, avec le paiement à l'usage (OpEx), les solutions de continuité en cloud apportent un avantage économique substantiel. Les ressources utilisées dans le cloud ne sont en effet facturées que lorsqu'elles sont sollicitées, c'est-à-dire lors des tests et des bascules réelles. Et cette facturation peut se faire au prix catalogue des plates-formes de cloud.

- **Les services d'accompagnement**

Les besoins des clients pour les services d'accompagnement autour du choix, de la mise en place voire du management des solutions PRA sont variables, en fonction de leur taille, leur organisation, leur SI existant et surtout des compétences dont ils disposent.

Dans les solutions de type reprise, le socle de l'offre Orange Business Services est la mise à disposition d'une solution de protection avec un outil et une plateforme de reprise, avec tarification à la VM. Ce type d'offre simple et « sur étagère » correspond bien aux besoins d'une partie importante de ses clients, surtout des grands groupes.

En revanche, d'autres clients (notamment des PME et des ETI mais non seulement) peuvent avoir besoin de plus d'accompagnement. C'est pourquoi Orange Business Services propose (d'ailleurs comme certains concurrents) une large palette de services à la carte, au choix du client en fonction de ses besoins. Ils sont présentés de manière synthétique dans le tableau ci-dessous :

Etude	Configuration	Tests	Mise à jour	Bascule	Bascule arrière
Identifier les activités métiers prioritaires, déterminer leurs exigences de continuité, identifier leurs moyens sous-jacents (BIA)	Déployer les outils de protection sur le site nominal	Organiser le(s) test(s)	Ajuster la configuration pour corriger les écarts (réactif)	Assurer l'organisation pour pouvoir basculer l'activité	Tester le bon fonctionnement de la plate-forme nominale
Evaluer la criticité des applications et des données pour ces activités métier (BIA)	Configurer l'environnement de reprise sur le secours	Tester le bon déroulement du PRA	Revoir /réviser les processus pour la MAJ conjointe du SI et du PRA (proactif)	Définir les procédures (décideurs / acteurs / actions)	Organiser la bascule arrière
Identifier les composants SI nécessaires à ces applications	Configurer l'environnement de test sur le secours	Déterminer les écueils au redémarrage des applications	Mettre à jour le PRA au gré de l'évolution du SI (proactif)	Mettre en place une organisation 24/24, 365/365	Relancer les serveurs et les applications
Choisir le niveau de protection désiré pour ces composants SI	Configurer les liaisons réseaux nécessaires	Vérifier la cohérence applicative		Le moment venu, basculer : -Relancer les serveurs et les applications -Vérifier le bon fonctionnement et la cohérence applicative	Vérifier le bon fonctionnement et la cohérence applicative
Qualifier la (les) solution(s) technique(s)	Configurer la protection des applications	Comparer les résultats aux RPO et RTO définis			
	Initier la réplication des données	Analyser les causes des écarts			

Le tableau résume les services d'accompagnement proposés par Orange Business Services pour ses offres de type reprise sur un site de secours en cloud. Cependant, nous avons aussi identifié, dans notre typologie, des solutions de type Haute Disponibilité (HD). Pour être clair, il faut préciser que ces solutions HD se font généralement dans le cadre des projets plus larges - de déploiement, migration voire développement d'applications.

En tout cas et de matière générale, la capacité du prestataire à fournir des services qui répondent aux besoins du client est un critère majeur dans le choix d'une solution PRA.

- **D'autres critères à prendre en compte**

Comme nous avons écrit plus haut, le choix d'une solution PRA doit prendre en compte de nombreux facteurs. Jusqu'ici nous avons mis en exergue trois critères majeurs pour optimiser le choix : la « criticité » des applications et les données à protéger, la capacité à faciliter les tests, et les services d'accompagnement.

Bien entendu, d'autres facteurs entrent en ligne de compte. Citons par exemple :

- **L'environnement technique Cloud (VMware, OpenStack, AWS, Azure…)**

Auparavant ce facteur était incontournable. Cependant, la tendance claire des outils techniques de continuité et de reprise est de devenir « cloud agnostique ». D'ailleurs, de plus en plus de prestataires – dont Orange Business Services - se positionnent aussi comme « multi-cloud », un changement que nous évoquerons plus loin.

- **L'existant informatique sur site client**

Les solutions PRA discutées dans ce livre blanc sont pertinentes pour des architectures standard x86. Or, de nombreux clients utilisent aussi des systèmes dits « legacy » (mainframes, IBM i, UNIX propriétaires. Dans un contexte DRaaS, il faut donc combiner une solution PRA standard avec des solutions spécifiques pour ces systèmes.

- **Une volonté d'éviter la dépendance sur un seul fournisseur cloud public**

Certains clients exigent que le secours de leurs applications dans un cloud soit dans un cloud d'un autre fournisseur, soit pour éviter le « verrouillage » soit pour se prémunir contre une défaillance majeure frappant plusieurs plateformes du même fournisseur. Un exemple de ce type de défaillance est la célèbre panne AWS de 2017 dans la région US-EAST-1, qui a interrompu le service de toutes les AZ (« Availability Zones ») de la région.

- **La localisation géographique**

Pour des raisons réglementaires ou simplement prudentielles, certaines entreprises exigent que le data center du cloud en secours soit localisé dans leur propre pays, notamment (pas uniquement) dans le secteur Finance. Dans le cas des clients européens, une localisation dans un autre pays de l'Union Européenne est parfois acceptable.

Dans le chapitre qui suit, nous présenterons quelques exemples des clients d'Orange Business Services qui illustrent bien cette logique de choix.

Comment choisir sa solution de continuité et reprise dans le cloud ?

- Deux paramètres techniques sont définis sur la base des exigences métiers :
  - RTO : temps entre le début d'un sinistre et la reprise effective de l'application
  - RPO : fonction des dernières données utilisables pour la reprise suite à un sinistre.

- 1er critère majeur : la « criticité » (RTO et RPO) des applications et des données. Sur la base de ce critère structurant, les solutions reposant sur différentes technologies sont classées de la façon suivante : Froid, Tiède, Chaud, HD (Haute Disponibilité) et Vital (HD + reprise chaude).

- 2ème critère majeur : la capacité de faciliter les tests de reprise en cloud, avec paiement en OpEx et sans impact sur la production en cours.

- 3ème critère majeur : les services d'accompagnement « à la carte » autour du choix, de la mise en place voire du management de la solution.

- Autres critères pertinents selon les cas : la localisation géographique, les environnements techniques, la volonté de ne pas dépendre d'un seul fournisseur, etc.

#5 Orange Business Services, ses clients et les réponses à leurs projets

Dans ce chapitre, nous passons en revue quelques cas de clients qui ont trouvé la réponse à leurs attentes avec OBS en matière de continuité d'activité dans le cloud. Il s'agit de clients réels mais, avec son souci habituel de discrétion, Orange Business Services nous a demandé de les présenter de manière anonyme.

Les exemples seront présentés en ligne avec la logique exposée dans le chapitre précédent : en séquence ascendante de « criticité » des applications et des données à protéger pour les métiers, tout en évoquant d'autres facteurs qui ont joué dans les choix des clients.

- **Un bailleur social : niveau 0 de criticité « Froid »**

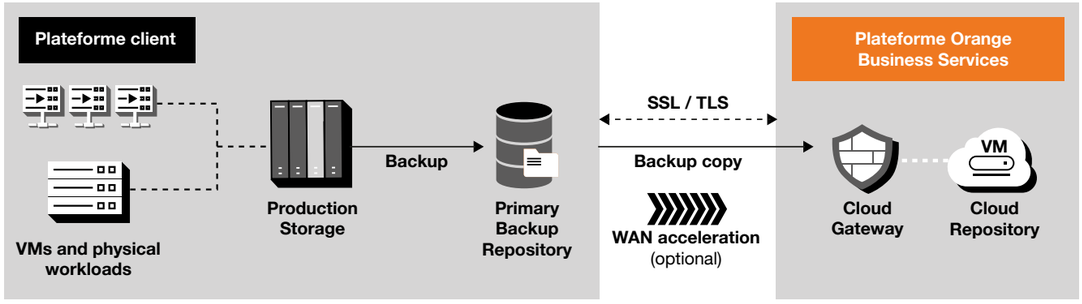
  « Sortir les sauvegardes » - ou plus précisément des copies - est une règle d'or de la continuité d'activité. C'est le niveau de protection le plus élémentaire. Une organisation qui a perdu ses serveurs suite à un « choc extrême » peut éventuellement reconstruire son système d'information. Mais si elle a perdu définitivement ses données, c'est l'espoir qui est perdu.

  Ici nous prenons l'exemple d'un acteur du logement social qui a souhaité externaliser ses sauvegardes pour s'assurer un premier niveau de sécurité. Son activité de bailleur social est de développer l'offre de logements sociaux mais aussi d'offrir une réelle qualité de service aux locataires. Il devenait alors primordial pour lui de minimiser la perte de données provenant de ses locataires.

  Pour ce client, Orange Business Services a mis en place le volet backup dans le cloud de Flexible Recovery, en s'appuyant sur les outils « Repository as a Service » et « Cloud Connect » de son partenaire Veeam, un leader technologique incontournable en matière de gestion des sauvegardes.

  L'architecture générale de la solution est présentée sur le schéma qui suit :

Architecture générale d'une solution de back up basée sur Veeam d'Orange Business Services



  Ce client avait déjà en place une solution de sauvegarde Veeam backup sur son site de production et était déjà habitué à l'expérience Veeam ne nécessitant pas d'apprentissage complémentaire de la solution. Flexible Recovery - s'appuyant sur d'autres outils Veeam - a permis d'étendre l'infrastructure existante de sauvegarde au cloud et ainsi mettre les données à l'abri, dans un data center hautement sécurisé d'Orange Business Services.

- **Une délégation de service public : niveau 1 de criticité « Tiède »**

Beaucoup de PME et ETI ne peuvent pas se contenter des sauvegardes hors site. Elles souhaitent se doter d'une véritable solution PRA, en dépit d'expertises informatiques restreinte et d'un cadre budgétaire serré. Dans ce contexte, une solution PRA « tiède » peut offrir un bon rapport coût /risque.

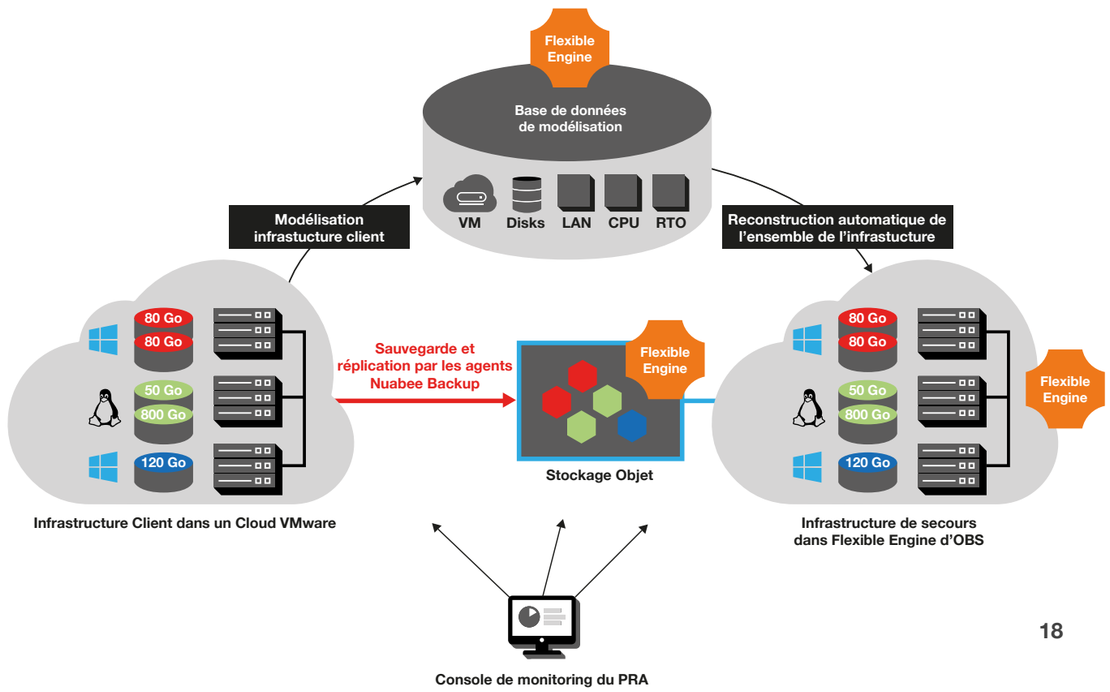
Le client que nous évoquons ici est une délégation de service public de taille intermédiaire, chargée d'enregistrer et mettre en œuvre des demandes de blocage (particuliers et entreprises) des démarchages commerciaux téléphoniques. Le client peut supporter une interruption de plusieurs heures du système d'information et la perte d'une journée de données. Néanmoins, il faut toujours pouvoir assurer la continuité d'un service public ! C'est pourquoi nous mettons ce cas dans la catégorie « tiède » de criticité et de reprise. Mais d'autres critères évoqués dans le chapitre 4 ont aussi été pris en compte.

Le système d'information s'appuie sur un cloud dédié VMware vCenter chez OVH en France, hébergeant environ 35 VMs Linux (Debian) sur 3 hyperviseurs ESXi. Orange Business Services a proposé la solution de son partenaire Nuabee avec le site nominal toujours chez OVH et le secours sur Flexible Engine, sa plateforme OpenStack. Pour expliquer la logique du choix final, en complément des critères de criticité, nous citons le RSSI de cette entreprise :

« Quand il a été statué qu'un PRA était nécessaire, s'est posée la question de l'opérateur. Afin de garantir que nous ne serions pas vulnérables en cas de défaut de l'opérateur initial, nous avons décidé de trouver un opérateur alternatif, qu'il devait répondre à des critères de qualité compatibles avec le statut de délégataire de service public, et devait héberger les données en France. L'autre choix était de conserver un environnement VMware vCenter ou d'opter pour un environnement différent. La mise en œuvre d'un PRA sur une infrastructure identique est plus simple mais nous rend vulnérable à un défaut ou une attaque visant cette plateforme. Notre décision a été d'aller vers une solution différente…. ».

Le schéma ci-dessous présente l'architecture générale de la solution retenue :

Architecture générale de la solution Nuabee, partenaire d'Orange Business Services



Les principes de fonctionnement sont clairement indiqués sur le schéma. Gardons toutefois à l'esprit que dans le cas de ce client, la solution PRA est entièrement managée par Nuabee, c'est à dire, mise en œuvre, tests, surveillance des réplications, bascule le cas échéant sur le secours et retour sur le nominal.

- Mise en œuvre

  - L'infrastructure du client du site nominal est modélisée dans une base de données dans le cloud Flexible Engine (OpenStack) d'Orange Business Services
  - Un « tenant » vide est réservé dans Flexible Engine pour accueillir le site de secours en cas de sinistre ou pour les tests
  - Des agents Nuabee sont installés dans les VMs Linux ou Windows du site nominal
  - Une copie complète des données est transmise à Flexible Engine et gardée sous forme de « stockage objet ». Ce point est clé : le stockage objet des données coûte environ 10 à 20 fois moins cher que le stockage bloc traditionnel.

- Fonctionnement courant

  - Une ou deux fois par jour, les agents transmettent les données associées aux VMs protégées (seulement les blocs qui ont changés depuis la dernière fois) du site nominal au stockage objet de Flexible Engine.
  - En cas de changement dans l'infrastructure : par exemple l'ajout d'une VM à protéger : un agent doit être installé sur cette VM et la base de données de modélisation mise à jour
  - Pour les tests : les VMs protégées sont reconstruites automatiquement à partir de la base de modélisation, dans un espace prévu sur le secours et testées avec un snapshot des données. Ainsi, les tests de PRA se font sans perturber ni la Production ni la protection de la Production.

- En cas de sinistre

  - Le RTO (dans ce cas 4H) commence à courir à partir du signalement de l'incident par le client
  - Compte tenu de son très faible coût, la reconstruction automatique de l'infrastructure peut être lancée sur le secours, sans attendre une éventuelle bascule : rétablissement des VMs (avec des agents) et création des blocs des données à partir des sauvegardes en stockage objet.
  - Si la décision s'impose, la Production est basculée sur le secours.
  - Puis les accès réseaux sont basculés et les applications sont rétablies
  - Après avoir statué sur la question de rattrapage des données éventuellement perdues, les métiers peuvent recommencer leurs activités sur le secours.

- Retour sur le nominal : il s'appuie sur les mêmes mécanismes, dans un moment bien plus calme que la situation du sinistre qui a nécessité une bascule sur le secours.

Avec ses automatismes qui tirent parti du cloud (OpenStack) et du stockage objet, Nuabee se distingue par sa facilité d'utilisation, un bon rapport coût/risque et sa capacité à gérer des configurations de systèmes d'informations très variées. Avec la solution de son partenaire Nuabee, Orange Business Services peut donc proposer une réponse bien ciblée sur les attentes d'un grand nombre de PME et même d'ETI.

- **Une agence européenne de haute technologie : niveau 2 de criticité « Chaud »**

Restant dans notre logique de « criticité » ascendante des applications et des données dans le cloud, nous abordons maintenant le niveau de criticité « chaud ». Dans cette catégorie, nous mettons des solutions PRA qui maintiennent un environnement de protection à jour – grâce à la réplication continue des données – avec les VMs prêtes à être rétablies sur le secours.

Le client que nous avons choisi ici est une agence intergouvernementale coordonnant les projets spatiaux menés en commun par une vingtaine de pays européens. Dotée d'un budget de 5.720 millions d'euros en 2019, l'agence emploie environ 2.250 personnes et comprend une dizaine d'établissements répartis dans les différents pays contributeurs, ayant chacun un domaine d'intervention bien précis.

Cette référence est si connue que nous dérogeons à notre règle d'anonymat pour inviter les lecteurs connectés à découvrir une vidéo de deux minutes dans laquelle le client explique son choix de cloud privés et son besoin d'une solution PRA sûre et performante (voir la vidéo).

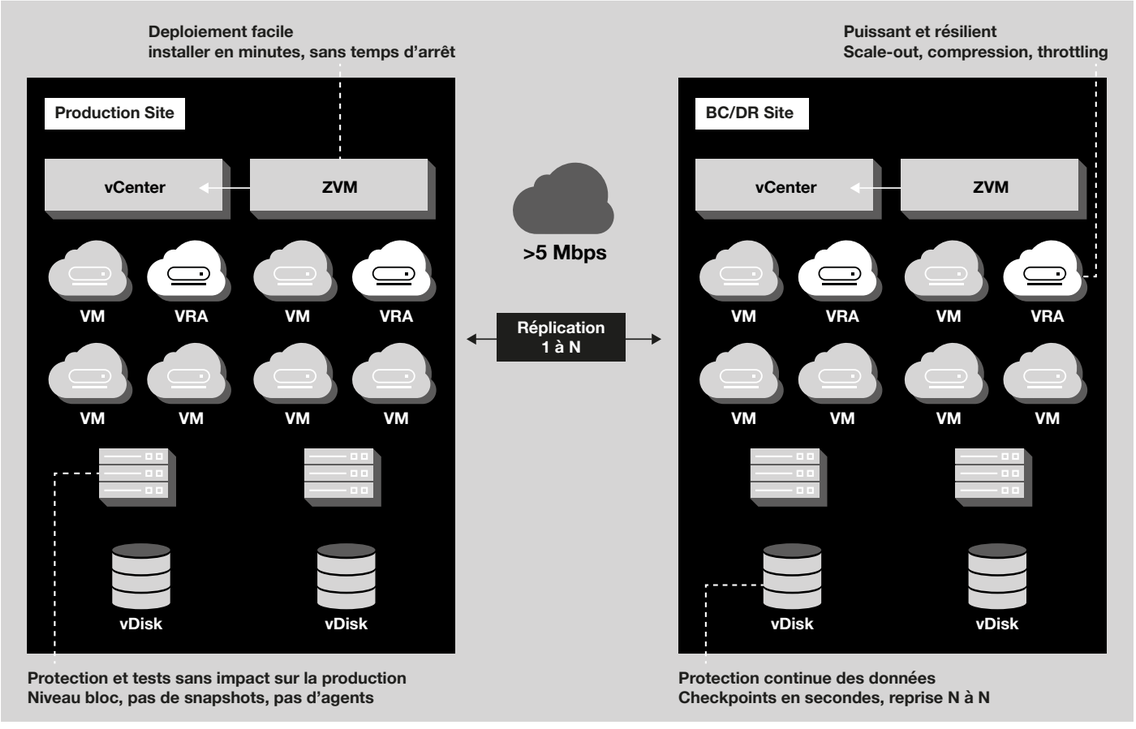
Outre le caractère critique des applications et des données dans les deux cloud privés en Italie et en Allemagne, le critère de facilitation des tests était crucial pour ce client.

En effet, l'agence disposait déjà d'une solution PRA mais elle ne pouvait être testée qu'en mode « tout ou rien ». Il n'était pas possible de la tester uniquement sur une partie des charges de travail, sans affecter toutes les autres. La solution existante n'a donc pas été testée fréquemment et un réel doute a pesé sur son efficacité. Il était crucial pour l'agence de pouvoir tester son PRA sans perturber sa production, tout en augmentant la flexibilité et la granularité des tests.

Pour répondre à ces attentes, Orange Business Services a proposé et mis en œuvre un PRA, qui s'appuie sur l'outil partenaire Zerto IT Resilence Platform. Du fait que les applications et les données des deux cloud (VMware) sont totalement disjointes, ce PRA a été mis en place dans une configuration « active-passive croisée » avec chacun des deux sites servant comme secours pour l'autre.

L'architecture générale du PRA avec Zerto IT Resilience Platform est présentée sur le schéma qui suit :

Architecture générale de la solution Zerto IT Resilience Platform



Le schéma présente l'architecture de l'outil pour les environnements cloud VMware. Sans entrer dans le détail, on remarque deux composants clés : le ZVM et le VRA. Selon Zerto :

- Le ZVM (Zerto Virtual Manager) se connecte directement à la console de gestion virtuelle (telle que le VCenter de VMware), offrant ainsi une visibilité sur l'ensemble de l'infrastructure. ZVM est le centre névralgique de la solution, gérant la réplication de l'ensemble du domaine VSphere.
- Le VRA (Virtual Replication Appliance) est un module logiciel déployé automatiquement sur les hôtes physiques. Le VRA réplique en continu les données à partir de machines virtuelles sélectionnées par l'utilisateur, en les compressant et en les envoyant au site distant via des liaisons WAN.

Plusieurs points forts techniques de l'outil sont clairement indiqués sur le schéma qui nous a été fourni par Zerto, un leader mondial reconnu en matière de reprise chaude en cloud. Nul besoin de les rappeler ici.

Cependant, nous pouvons recenser quelques avantages pertinents de la solution mise en œuvre par Orange Business Services pour l'agence :

- Simplicité et souplesse pour les tests : il s'agit d'une exigence majeure de ce client et de beaucoup d'autres.
- Facilité de mise en œuvre et d'utilisation : ce point est largement reconnu dans le marché et fortement appréciée par les clients.
- Services d'accompagnement : Orange Business Services a assuré non seulement la mise en place de l'outil mais reste responsable pour les tests et, le cas échéant, la bascule sur le secours.
- Tarification OpEx : Après des frais de mise en œuvre, la solution est tarifiée sous forme d'un coût mensuel, ajusté en fonction du nombre de machines virtuelles protégées, pour couvrir la protection.

Pour conclure, il convient de préciser qu'OBS ne se limite pas à la configuration de PRA de type cloud privé – privé, comme dans cet exemple. Avec Flexible Computing Advanced, Flexible Computing Premium et Flexible Engine, Orange Business Services possède également de nombreuses références, en France, en Europe et en Asie-Pacifique, avec des configurations cloud public - public.

Par ailleurs, Orange Business Services va lancer également une offre de « Disaster Recovery As a Service » appelée Flexible Recovery Advanced. Cette offre répondra aux attentes du marché en termes de PRA d'un cloud privé vers un cloud public : sans modification du cloud privé, sans avoir à investir dans un cloud de reprise, avec un accompagnement du client et avec un paiement à l'usage qui lui permet de sensiblement optimiser ses coûts.

- **Un groupe paramédical international : niveau 3 de criticité « HD »**

Au-delà de la reprise chaude, certaines entreprises et grandes organisations sont encore plus exigeantes sur la disponibilité de leurs applications et données dans le cloud. Elles demandent une continuité de service sans aucune interruption, que ce soit pour gérer un sinistre affectant un data center, pour réparer dans deux heures une défaillance technique ou encore pour un besoin prévisible de la Production, par exemple pour monter la nouvelle version d'un logiciel.

Suivant notre typologie par « criticité », nous mettons dans cette catégorie des solutions Haute Disponibilité (HD) avec 2 sites actifs synchrones, donc nécessairement proches à < 40 km. Avec en principe un RTO et RPO à zéro, elles permettent une bascule transparente des utilisateurs d'un site à l'autre, sous réserve d'un sinistre régional.

L'exemple client que nous évoquons ici est une entreprise du secteur paramédical, qui regroupe en modèle coopératif de près de 1400 magasins spécialisés, en France et à l'étranger. Outre ses expertises techniques, la qualité d'accueil et le service personnalisé au client en magasin sont au cœur de la proposition de valeur de la marque. Le fonctionnement des magasins adhérents dépend de l'application métier principale. L'indisponibilité de cette application dégraderait forcément « l'expérience client » que le groupe souhaite fournir.

Par ailleurs, en tant qu'entreprise d'un secteur paramédical, elle traite et conserve des flux très importants des données sensibles, telles que les scans des ordonnances et cartes mutuelles, les devis, les factures émises...

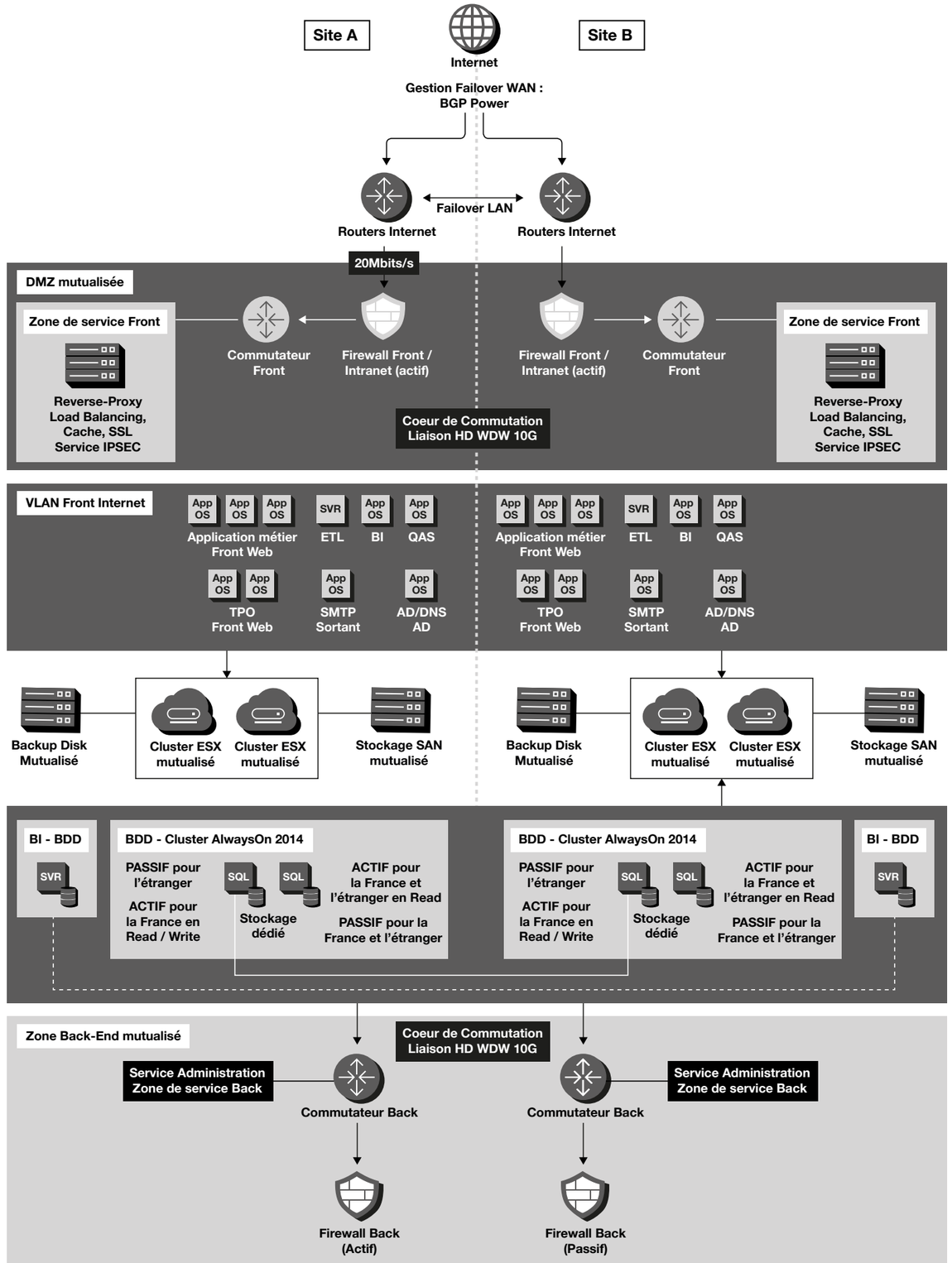
Par voie de conséquence, ce groupe ne peut tolérer aucune interruption de service ni perte de données. Nous considérons donc que ses exigences de continuité la situent au niveau 3 de « criticité » - la Haute Disponibilité (HD).

Pour répondre aux attentes de ce client, Orange Business Services a mis en place une solution d'hébergement dans le cloud avec les caractéristiques fondamentales suivantes :

- Déploiement sur deux plateformes cloud managées Active-Active en région Parisienne
- Haute disponibilité de la solution 24/7
- Pas d'interruption de service : bascule transparente des utilisateurs d'un site à l'autre en cas de besoin
- Pas de perte de données en cas de sinistre sur un data center
- Services à valeurs ajoutés en complément des services de management

Afin de rentrer un peu plus dans le concret, l'architecture de la solution - sur les deux sites A et B - est présentée sur le schéma qui suit :

Architecture générale de Haute Disponibilité « Always On » d'Orange Business Services



Nous n'entendons pas décortiquer dans le détail cette architecture quelque peu complexe, mais tout simplement souligner quelques aspects techniques majeurs.

Tout d'abord, vers le bas du schéma nous voyons la clef de voute de la solution HD – un cluster Microsoft SQL Server AlwaysOn réparti sur les deux data centers avec deux nœuds par site. En cas de sinistre, la BD AlwaysOn permet une bascule immédiate sur un autre nœud.

Compte tenu du rôle crucial du cluster AlwaysOn pour le fonctionnement en HD entre les deux sites, le contrat entre Orange Business Services et le client prévoit un RTO de 1 heure (à titre d'exception) en cas de défaillance au niveau du cluster BD réparti entre les deux sites.

Dans cet exemple, le client a choisi une certaine spécialisation des back-end BD des deux sites entre France et Etranger (dont les DOM-TOM). Une transaction de consultation (80% des volumes) peut utiliser de manière indifférente les deux sites. En revanche, les mises à jour France sont normalement traitées sur le back-end du site A et celles de l'Etranger sur le site B. Cependant, les mises à jour effectuées sont immédiatement envoyées par « log shipping » d'un site à l'autre pour synchroniser les bases de données.

Ensuite, en montant dans le schéma, nous voyons que tous les équipements sont redondés entre les deux sites et, dans la zone « VLAN Front Internet », les mêmes applications sont déployées des deux côtés, sans oublier Active Directory qui est un logiciel incontournable dans des environnements Microsoft.

Enfin, en haut du schéma, nous voyons des équipements de « load balancing » qui assurent à la fois la répartition de charges et la bascule transparente des utilisateurs d'un data center à l'autre, en cas de sinistre.

En résumé, avec cette solution HD AlwaysOn, Orange Business Services a pu répondre à la demande de ce groupe paramédical pour une continuité de service ininterrompu … qu'il juge comme indispensable pour la qualité de « l'expérience client » qu'il tenait à fournir dans tous les magasins adhérents de la marque partout dans le monde.

- **Une banque française : niveau 4 de criticité « Vital »**

Pour terminer ce chapitre sur des exemples clients, nous abordons maintenant le niveau de criticité « Vital ».

Si les solutions de Haute Disponibilité discutées précédemment - avec deux systèmes proches (<40 km) en Actif-Actif - apportent généralement une bonne assurance de continuité de service ininterrompu, elles restent néanmoins exposées à un risque de sinistre régional. Dans des secteurs tels que la Finance ou encore certains échelons de l'administration publique, ce n'est pas acceptable.

Dans la catégorie la plus exigeante de notre typologie par criticité, nous mettons des configurations HD sur 2 sites actifs proches, avec en plus la reprise chaude sur un 3ème site passif, à >100 km, qui ne partage pas de risques conjoints avec les deux premiers sites.

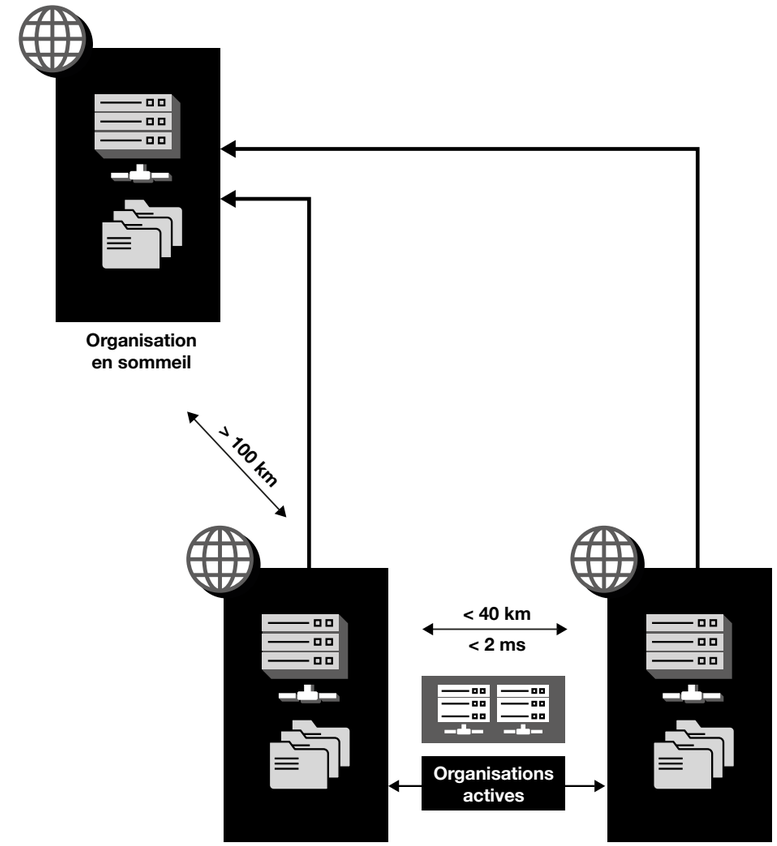
Ici nous prenons comme exemple une banque française implantée sur tout le territoire nationale avec 17 000 points de contacts, au service de plus de 10 millions de particuliers mais aussi des entreprises, des professionnels, des acteurs de l'économie sociale et du secteur public local. Pour des raisons à la fois prudentielles et réglementaires, elle a choisi en 2014 – dans le cadre de son programme déjà engagé de rénovation de ses infrastructures IT - de mettre en place une architecture de clouds privés accompagnée des solutions de continuité et reprise, selon le modèle « Vital ».

Cette mission a été confiée à Orange Business Services qui a mis en place pour cette banque trois clouds privés - avec 2 sites en Actif-Actif proches et un 3ème site de reprise passif à >100 km – en s'appuyant sur des technologies VMware, Cisco, EMC² et VCE.

Ce projet innovant en cloud privé a été tarifié à l'époque en CapEx. Mais depuis peu, Orange Business Services a lancé une offre avec une architecture générale similaire - aussi au niveau Vital - en cloud public. Parmi les avantages de cette nouvelle offre - nommée Flexible Resilience – est la tarification en « Full OpEx ». Après des frais d'installation en cloud public d'Orange Business Services, l'offre est tarifiée à l'usage, en fonction du nombre de VMs.

Elle est présentée sur le schéma qui suit :

Architecture générale de Flexible Resilience d'Orange Business Services



Par rapport au schéma, nous soulignons simplement deux points :

- L'architecture HD des systèmes proches actifs ressemble fortement à celle présenté dans la section HD précédente.
- La reprise chaude des deux sites actifs vers le 3ème site passif, à >100 km, est assurée par la technologie Zerto.

Avec cette nouvelle offre, Orange Business Services peut proposer une réponse très ciblée aux clients qui souhaitent profiter des avantages du cloud public et une tarification en OpEx, tout en étant extrêmement exigeante sur la continuité des leurs applications et données dans le cloud.

Orange Business Services, ses clients et les réponses à leurs projets

- **Exemple criticité « Froid » :** Mise en place du volet backup dans le cloud avec **Flexible Recovery**, en s'appuyant sur les technologies Veeam

- **Exemple criticité « Tiède » :** mise en place et management du plan de reprise par le partenaire d'Orange Business Service, **Nuabee**, avec site nominal chez OVH et secours chez **Flexible Engine** d'OBS.

- **Exemple criticité « Chaud » :** mise en place et management d'une solution de reprise (Actif-Passif croisée) entre deux clouds privés en Allemagne et Italie, s'appuyant sur les technologies Zerto. Une offre similaire **Flexible Recovery Advanced** - entre cloud privé et cloud public **VMware** – sera prochainement disponible.

- **Exemple criticité « HD » :** mise en place et management d'une solution avec deux sites Actif-Actif de **Flexible Computing Premium**, s'appuyant notamment sur la technologie SQL Server AlwaysOn de Microsoft

- **Exemple criticité « Vital » :** mise en place (en CapEx) d'une configuration avec trois clouds privés - 2 sites Actif-Actif proches et un 3ème site Passif de reprise chaude à >100 km – en s'appuyant sur des technologies VMware, Cisco, EMC² et VCE. Depuis peu, une offre similaire Flexible Resilience – avec les clouds publics d'OBS et facturée en OpEX - est disponible.

- Orange Business Services est en capacité d'accompagner ses clients dans leur projet de continuité d'activité dans le cloud en répondant aux besoins très variés des entreprises, des PME jusqu'aux grand groupes, en France comme à l'international.

#6 Les nouveaux challenges des environnements multi-cloud

Depuis trois ans, Orange Business Services a élaboré avec des partenaires technologiques de premier plan un large portefeuille de solutions de continuité et de reprise dans le cloud. Comme nous l'avons vu, ce portefeuille lui a permis de répondre aux besoins très variés de ses clients, des PME jusqu'aux grands groupes, en France comme à l'international.

Cependant, le marché n'a de cesse d'évoluer et de nouveaux challenges apparaissent. Dans ce chapitre nous évoquerons les nouvelles perspectives qui s'ouvrent avec l'émergence du « multi-cloud ».

- **Le Multi-cloud : la nouvelle réalité du marché**

Selon les idées reçues d'il y a deux ou trois ans, la plupart des utilisateurs externaliserait leur SI en tout ou partie dans un seul grand cloud public, avec seulement quelques « hyperscalers » dominant l'ensemble du marché.

Mais nous constatons aujourd'hui que les choses ne se sont pas passées ainsi. Si certaines entreprises ont opté pour une démarche « all in » avec un seul grand fournisseur de cloud, la plupart – comme le démontrent de nombreuses études - utilisent plusieurs partenaires et s'attendent à en utiliser davantage à l'avenir. En effet, les hyperscalers se sont développées rapidement mais ils travaillent de plus en plus en partenariat avec toutes sortes d'acteurs. De plus, un écosystème dynamique de logiciels et de services qui s'affirment comme « cloud agnostiques », prend forme.

- **Orange Business Services adopte une stratégie de services multi-cloud**

Ayant pris pleinement la mesure de cette nouvelle réalité du marché, OBS a annoncé le 18 septembre 2018 son ambition de devenir un leader mondial des services multi-cloud. « Orange Business Services fait le choix d'être agnostique en matière de technologies cloud », se positionnant à la fois comme intégrateur et opérateur dans un environnement multi-cloud, qu'il s'agisse de cloud public ou privé.

Rien de tout cela ne suggère qu'OBS arrêtera d'investir dans ses propres infrastructures clouds VMware et OpenStack, qui sont des actifs stratégiques pour un acteur de services multi-cloud. En revanche, cela signifie clairement qu'OBS est en capacité de fournir des services également autour des clouds d'autres acteurs. OBS a ainsi signé des accords avec des hyperscalers tels qu'AWS et Microsoft et a déjà certifié certains de ses ingénieurs avec Google.

Le virage multi-cloud d'Orange Business Services change radicalement la donne pour son activité de solutions de continuité d'activité dans le cloud. Auparavant focalisée essentiellement sur ses propres plateformes, son « marché adressable » s'élargi encore plus. D'autant que de nombreux clients actuels des clouds d'OBS utilisent aussi des plateformes d'autres fournisseurs. Ainsi les clients qui le souhaitent peuvent déjà s'appuyer sur les expertises d'OBS pour la mise en place (voire le management) de solutions de continuité dans une démarche d'ensemble pour leurs environnements multi-cloud.

- **Trois challenges majeurs**

Pour capitaliser sur cette opportunité pour mieux servir les clients, Orange Business Services doit relever de nombreux défis. Ici nous nous contenterons d'en évoquer trois.

- **Développer les compétences techniques : hyperscalers et plateformes open source**

Pour une entreprise de grande technicité comme Orange Business Services, la maîtrise technique complète des environnements dans lesquels ses équipes vont travailler est un préalable incontournable.

OBS a déjà formé un bon nombre d'ingénieurs sur les technologies de Microsoft Azure, AWS et Google Cloud Platform. C'est un bon début. Cependant, les hyperscalers sont des environnements très riches qui évoluent vite, et ces investissements en compétences techniques sont à poursuivre dans la durée.

Dans le domaine des solutions PRA, les partenaires technologiques d'OBS sont (plus ou moins) cloud agnostiques. Dans le cas des applications « classiques », le travail de mise en œuvre sera similaire à ce qu'OBS fait déjà dans des clouds VMware et OpenStack, moyennant un complément d'expertise spécifique. En revanche, si l'application fait appel à des services avancés et propriétaires de l'hyperscaler (par exemple le « serverless »), le travail sera plus complexe. La simple réplication des VMs (comme fait Zerto) sur un autre cloud ne suffira pas, parce que ces services devraient également être prévus et configurés en sommeil sur le secours.

De plus, il faut aussi prendre en compte les expertises nécessaires pour les clients qui utilisent des plateformes Open Source comme Cloud Foundry ou OpenShift, sans oublier le duo Kubernetes-Docker (containeurs) qui a été choisi par de nombreux grands groupes. Ces logiciels ajoutent bien entendu une autre couche de complexité pour la mise en œuvre des solutions de continuité et de reprise.

Les programmes de formations des ingénieurs d'Orange Business Services vont être chargés !

- **Se préparer à l'avènement du « Edge Computing »**

Si le paradigme cloud est clairement entré dans le « mainstream » du marché, un nouveau modèle – plus décentralisé mais complémentaire – est en train d'émerger, ce qu'on appelle « Edge Computing ». On ne peut pas toujours tout faire dans un cloud centralisé. Le fond du problème est tout simplement la vitesse de la lumière ! De nouvelles catégories d'applications – telles que les systèmes s'appuyant sur l'IoT (Internet of Things) ou encore la réalité augmentée – nécessitent des temps de latence réseau très courts, incompatibles avec un traitement dans un grand cloud public à quelques centaines de kilomètres. Il faut mettre l'intelligence au plus près du point de capture des données.

Là encore la continuité de service sera une nécessité vitale, aussi bien pour les grandes infrastructures connectées (villes, autoroutes, réseaux électriques…) que pour les entreprises dans des secteurs tels que l'Industrie et la Commerce de détail.

OBS a investi depuis des années dans le domaine des objets connectés et, de plus, exploite des grands réseaux capillaires de télécommunications. Avec certains opérateurs confrères comme Telefónica et AT&T Business, Orange Business Services est plutôt bien positionné pour profiter de cette évolution, à condition d'intégrer la continuité de service (et bien sûr la sécurité) dans ces nouveaux systèmes « Edge » dès la conception.

- **Faire valoir ses atouts et se différencier avec la continuité d'activité**

Orange Business Services n'a pas encore la notoriété qu'elle mériterait d'avoir sur le marché de l'IT, en France ou à l'international. Mais avec son virage vers les services multi-cloud, cette dernière a pris la décision qui s'impose, même si ce marché est déjà encombré et qu'il faut de la différenciation.

Cependant, OBS a fait preuve de préscience en développant des compétences distinctives dans le domaine de la continuité dans le cloud, avec un portefeuille de solutions pour répondre à cette exigence majeure des clients « mainstream » bien avant l'arrivée du multi-cloud.

Certes, OBS a d'autres pistes de différenciation potentielles à poursuivre, mais à notre avis le moment est venu de faire valoir cet atout distinctif sur le marché.

Les nouveaux challenges des environnements multi-cloud

- Le « Multi-cloud » est la nouvelle réalité du marché, à la fois en terme de choix d'un grand nombre d'utilisateurs mais aussi du côté des stratégies des fournisseurs de services cloud
- En choisissant d'être « agnostique en matière de technologies cloud », se positionnant comme « intégrateur et opérateur » multi-cloud, « qu'il s'agisse de cloud public ou privé », Orange Business Services a pris la décision qui s'impose.
- OBS continue à investir dans ses propres infrastructures clouds mais est aussi en capacité de fournir des services autour des clouds d'autres acteurs.
- 1er challenge : poursuivre le développement des compétences techniques (hyperscalers et plateformes open source)
- 2ème challenge : se préparer à l'avènement du « Edge Computing »
- 3ème challenge : faire valoir ses atouts et se différencier, notamment avec la continuité d'activité

#7 Conclusion

Le 3 juillet 2018, Orange Business Services et Zerto ont remporté le Trophée du « Meilleur cas client cloud » décerné par l'Eurocloud France. Ce trophée a été attribué pour une solution de continuité et reprise d'activité (PRA) mise en place pour l'Agence Spatiale Européenne (ESA) entre deux clouds privés en Italie et en Allemagne.

Cette victoire illustre, d'une part, l'importance croissante de la continuité dans l'univers du cloud et, d'autre part, un début de reconnaissance par le marché des compétences distinctives d'OBS en la matière.

De par sa culture d'opérateur d'infrastructures critiques, la continuité et la reprise en cas de défaillance ou sinistre sont des sujets naturels pour OBS, à l'instar des opérateurs d'électricité, de gaz ou encore de transports. La vie économique et la vie de tout le monde s'appuient sur ces infrastructures et leurs services. Il n'est donc guère surprenant qu'OBS ait abordé le marché du cloud avec la même culture de fiabilité, moyennant des investissements considérables au fil des dernières années.

Avec des partenaires technologiques de premier plan, OBS a élaboré et porté au marché un large portefeuille de solutions de continuité en cloud, dont la plupart sont des offres industrialisées (« sur étagère »). Son ambition est de répondre aux besoins très variés des entreprises, des PME jusqu'aux grand groupes, en France comme à l'international.

Pour sa part, Orange Business Services se met au service de ses clients afin qu'ils trouvent les bonnes réponses pour leurs projets face à une problématique d'entreprise primordiale : la continuité des activités métier à l'époque du cloud.

#8 A propos

Duquesne Group est un cabinet français d'analyse et de conseil en organisation et technologies de l'information. Ses associés sont des professionnels très expérimentés, issus de grands cabinets internatioaux de conseil aux entreprises ou d'étude des marchés technologiques. Ils réunissent un haut niveau technique et une bonne culture métier et partagent des valeurs professionnelles d'indépendance, de service au client et d'engagement civique.

Leurs principaux domaines d'expertise sont la continuité d'activité, la sécurité de l'information et les technologies digitales de l'univers du cloud.

Leurs analyses et retours d'expérience sont disponibles en libre accès sur les sites www.DuquesneGroup.com (français) et www.DuquesneAdvisory.com (anglais). De plus, les associés ont publié des articles dans la presse économique et informatique et l'un d'eux est auteur de l'ouvrage de référence en matière de continuité d'activité dans le monde francophone.

Par ailleurs, Duquesne Group est aussi un organisme de formation. En partenariat avec le certificateur international PECB, le cabinet dispense des formations certifiantes :

- ISO 22301 : Continuité d'Activité
- ISO 27001 : Sécurité de l'Information
- ISO 31000 : Management du risque

De culture franco-américaine, le cabinet est basé à Paris et travaille, en France et à l'international, pour des clients de toutes tailles et secteurs.