Business

Annexe technique au Descriptif de Service Managed Applications – Plan de Reprise d'Activé managé sur Cloud Avenue

Table des matières

1.Définitions

En complément des définitions des Conditions Générales et des Conditions Spécifiques Intégration Maintenance et Prestations associées, les définitions spécifiques suivantes s'appliquent à ce Descriptif de Service.

DFS désigne un système de fichiers en mode distribué porté les systèmes Windows Server.

DNS désigne un service qui permet de transcrire un nom de machine ou de service en adresse IP unique

DRP, Disaster Recovery Plan en anglais, ou **PRA**, Plan de Reprise d'Activité en Français, désigne le plan de mise en œuvre de reprise après sinistre ou un plan de reprise après sinistre informatique.

Environnement désigne un espace privé virtuel de ressources sur le IaaS auquel seuls les Utilisateurs authentifiés par login et mot de passe peuvent avoir accès. Les actions de création, destruction, modification, listage de ces ressources et des fonctionnalités associées sont limitées à ces seuls Utilisateurs.

Environnement d'Administration Client désigne l'environnement dans lequel est hébergé le Service du Client (build et déploiement). Les actions de création, destruction, modification, listage des ressources et des Fonctionnalités associées sont limitées au Prestataire.

Environnement Client désigne l'environnement dans lequel sont déployés les conteneurs du Client. Les actions de création, destruction, modification, listage des ressources et des fonctionnalités associées sont attribuées au Prestataire et au Client. Le Client peut utiliser ce tenant pour exécuter des applications et utiliser des fonctionnalités IaaS.

NFS désigne un système de fichiers en réseau essentiellement utilisé par les systèmes Linux

RACI désigne la définition des responsabilités entre le Client et le Prestataire. R = Responsable, A = Autorité redevable, C= Consulté, I = Informé.

RPO désigne la quantité maximale de données qu'une entreprise peut perdre, c'est donc l'intervalle de temps entre la dernière sauvegarde valide d'un client et un incident.

RTO désigne la durée maximale pendant laquelle un système, un serveur ou un réseau est hors de service suite à une défaillance matérielle ou logicielle.

SVM désigne le Storage Virtuelle Machine de NetApp qui héberge le système de fichiers en réseau dans un Cluster NetApp. Cette fonctionnalité permet de partitionner le Cluster en plusieurs sous-entités de stockage qui seront perçues comme indépendantes et unique pour chacun des clients.

Tenant désigne un espace privé virtuel de ressources sur le IaaS auquel seuls les Utilisateurs authentifiés par login et mot de passe peuvent avoir accès. Les actions de création, destruction, modification, listage de ces ressources et des Fonctionnalités associées sont limitées à ces seuls Utilisateurs. Pour les IaaS en technologie VMware, le Tenant est également appelé « Organisation ».

Tenant Managé désigne le Tenant dans lequel est hébergé le Service du Client. Les actions de création, destruction, modification, listage des ressources et des Fonctionnalités associées sont limitées au Prestataire.

Token désigne l'unité d'œuvre utilisée pour exprimer les prix applicables aux changements demandés par le Client, tels qu'indiqués dans la Fiche Tarifaire.

WLS désigne les équipes Wan Lan Services qui sont intégrées dans Cloud Avenue qui est pris en charge de la configuration, la maintenance et le cycle de vie des composants réseaux et sécurités de l'infrastructure.

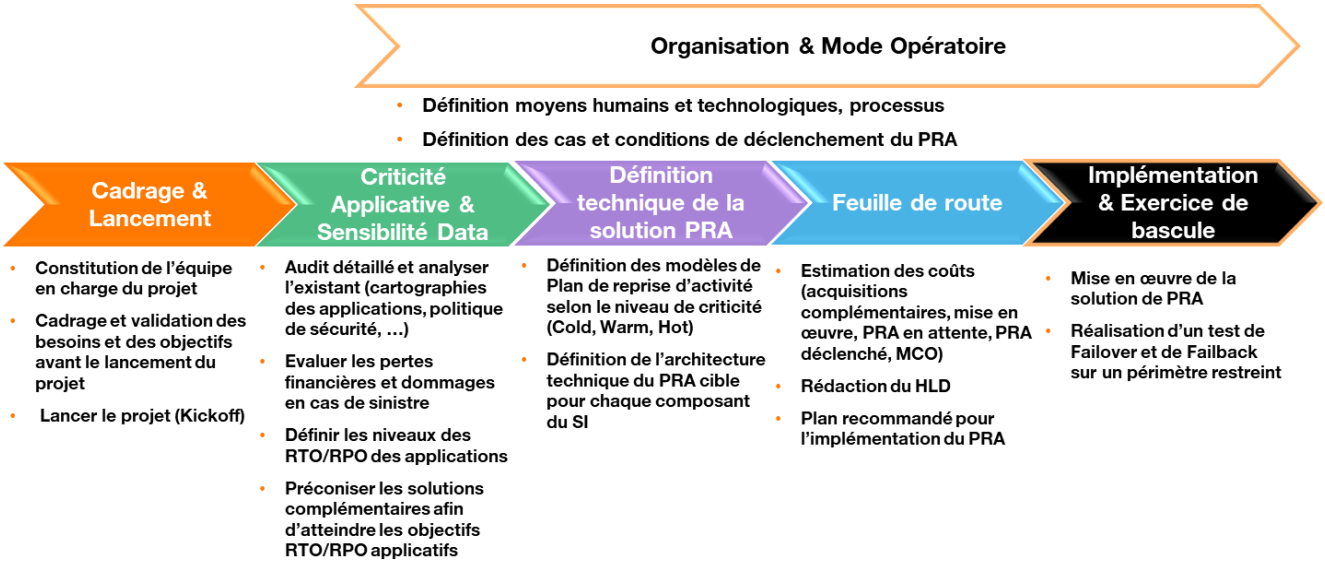
2.Objet

Le présent descriptif de service a pour objet de définir les conditions dans lesquelles le Prestataire fournit le service « Managed DRP » (pour Managed Disaster Recovery Plan) ou « PRA Managé » (pour Plan de Reprise d'Activité Managé), ci-après le « Service », au Client. Dans la suite nous ferons référence uniquement au « PRA Managé ».
Le présent descriptif est rattaché au document « Managed Applications – Descriptif de Service ».

3.Méthodologie

Nous préconisons la démarche suivante d'accompagnement à la mise en œuvre d'un Plan de Reprise d'Activité selon les 5 étapes suivantes :

1. Phase initiale de **Cadrage** pendant laquelle nos équipes (*Prestataire et souscripteur)* valident ensemble le périmètre global, définissent la gouvernance associée ainsi que le planning et les modalités des livrables attendus avant le **lancement** de la mission. Les phases de réalisation pour définir le PRA Managé et son implémentation adaptée au contexte IT et aux enjeux stratégiques, réglementaires et de sécurité sont :
2. Étude de la **Criticité Métier Applicative** en plusieurs entretiens auprès des personnes clés IT / Métiers de l'entreprise à la suite de la réception de l'inventaire applicatif/IT pour compléter l'inventaire et valider les criticités et RTO/RPO associés.
3. **Définition technique de la solution PRA** incluant la présentation du scénario cible des infrastructures, applications et Data à sécuriser, mais également du contexte, des contraintes et des exigences
4. **Feuille de route** associée (macro-budgets RUN & BUILD et architecture HLD) au meilleur choix de solution PRA avec planning d'exécution.
5. **Implémentation & Exercice de bascule** pour mettre en œuvre les solutions validées par l'Adhérent et réaliser des simulations de basculement.



Le modèle à suivre :

- Le Prestataire construit et maintient le descriptif du plan de reprise d'activité sur la partie technique et la partie organisationnelle lié à ses équipes.
- Le Client est responsable de demander le déclenchement du PRA en cas de sinistre
- Le Prestataire est responsable de renseigner et de maintenir le descriptif du PRA concernant la partie organisationnelle de ses équipes (point de contact, personne autorisé à demander le déclenchement du PRA, etc…)
- La réplication synchrone / asynchrone est surveillée en temps réel

- Un test de reprise est planifié annuellement en HO par défaut. La périodicité et la plage horaire du test de PRA peut être adaptée sur devis au besoin du client. Le test de PRA peut être complet ou partiel en fonction de l'architecture et des contraintes du client.
- Le Prestataire s'engage sur la garantie de bon fonctionnement du Plan de Reprise d'Activité (PRA) uniquement dans le cas où un test annuel complet a été réalisé sur l'ensemble du périmètre de l'infrastructure couverte. En conséquence, tout test réalisé sur un périmètre partiel ou restreint ne saurait être considéré comme représentatif du bon fonctionnement global du PRA et ne peut engager la responsabilité du Prestataire quant à la garantie du service.
- L'architecture réseaux de la cible du PRA Managé pourra être construite selon deux modèles en fonction des plateformes et solutions choisies :
    - Réseaux cible identique et isolé de la source
    - Réseaux cible pouvant communiquer avec la source et :
        - Modification des paramètres IP lors d'une reprise (automatisé par certaines solutions)
        - Construction d'une cible synchronisée avec des paramètres IP différents dans le cadre d'une solution de continuité d'activité. (Actif / Actif)

4.Présentation du Service

Dans le cadre du service de PRA Managé, nous assurons la gestion du plan de reprise d'activité selon le niveau de "Managed Applications" souscrit sur une infrastructure Cloud Public IaaS (plateformes d'hébergement supportées) de la liste ci-dessous.

- Cloud Avenue Val de Rueil
- Cloud Avenue Chartres

Sur les plateformes d'hébergement supportées, nous intervenons sur les offres suivantes :

- Serveurs virtuels selon les modalités de management des applications
- Serveurs BMS (Baremetal Server) dès lors que les ressources sont disponibles ou souscrites sur les multiples zones et Datacenter de l'offre Cloud Avenue
- Liens réseaux d'interconnexions externes :
    - Business VPN, pour son accostage, la création des règles de routage en nominal et de secours, sa diffusion au sein des zones clientes de Cloud Avenue
        - Deux variantes : MPLS en zone de Colocation et le BVPN qui arrive directement sur la T0 en zone cliente. Ces deux niveaux d'accostages sont sous la responsabilité des équipes du Prestataire.
    - VPN IPSec pour sa génération des clefs de configuration, son accostage, la création des règles de routage en nominal et de secours, sa diffusion au sein des zones clientes de Cloud Avenue.
- Données hébergées sur tout espace de stockage à condition que les espaces de stockage sur le site distant aient été souscrits au niveau de l'infrastructure.

Les services mutualisés d'infrastructure fournis par Cloud Avenue (NSX-T, Load Balancer, CyberArk ou Maserpam, Proxy, SMTP CAV, Console d'administration, …) disposent déjà de dispositifs de continuité et de reprise d'activité et ne font pas l'objet du service décrit dans ce document.

La responsabilité du Client inclut la gestion de ses applications, la vérification de leur bon fonctionnement selon le niveau de "Managed Applications" souscrit, la contractualisation des liens réseaux opérateurs auprès de ses fournisseurs de services, des licences applicatives (Middleware pour la synchronisation – haute tolérance logicielle ou matérielle et des supports éditeurs en-cours de validité).

5.Schéma de principe

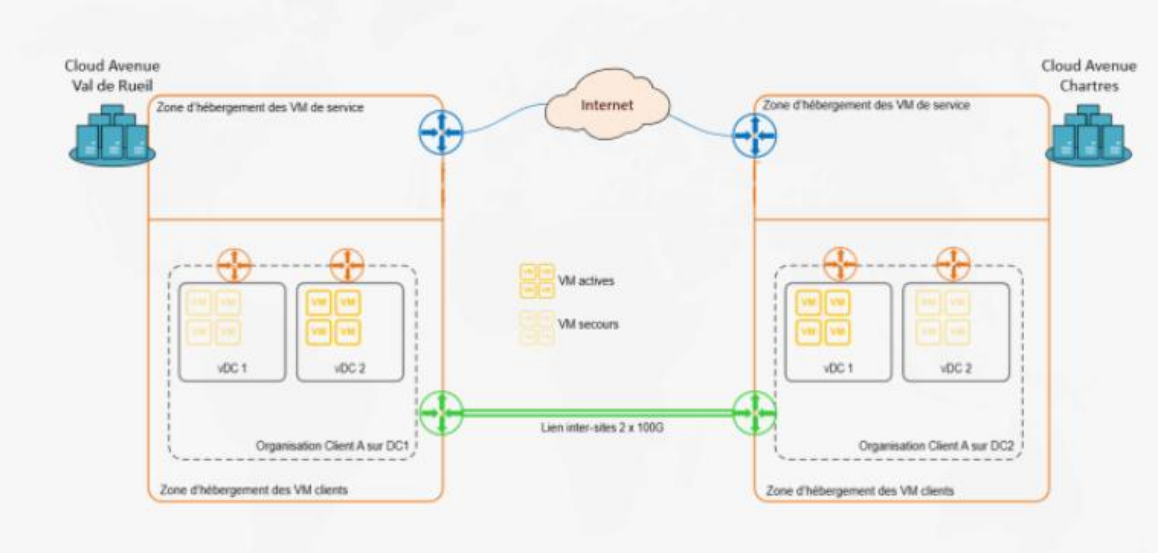
Le service Managed PRA est un service managé par les équipes du Prestataire qui s'appuie sur la fonctionnalité DRaaS (Disaster Recovery as A Service) de VMware permettant à nos clients de répliquer des machines virtuelles VMware entre 2 salles ou de sites de Cloud Avenue.

Ce service managé s'appuie sur le logiciel vCloud Director Availability (vCDA) de VMware, disponible en standard dans le portail vCloud Director de Cloud Avenue.

Plusieurs cas d'usage du Plan de Reprise sur Incidents sont acceptés via l'usage du produit VCDA qui permet de prendre en charge les bascules de machines virtuelles entre le site de Val De Rueil Normandie 1 vers Val de Rueil Normandie 2 et de Val de Rueil vers Chartres. La souscription de deux organisations virtuelles Cloud Avenue sur chacun des sites reste un prérequis technique et fonctionnel comme représenté sur le schéma ci-dessous.

- Entre 2 vDC d'une même organisation
- Entre 2 organisations situées sur le même site
- Entre 2 organisations situées sur 2 sites différents

Ici entre Cloud Avenue de Val de Rueil et Chartres



6.Prérequis

Les conditions préalables pour accéder au service « PRA Managé » sont :

- La souscription à l'offre IaaS Cloud Avenue - Dual Room ou Dual Site
- La souscription à un service managé minimum (Managed OS)
- La souscription au service de réplication (VCDA) pour les serveurs virtuels de Cloud Avenue.

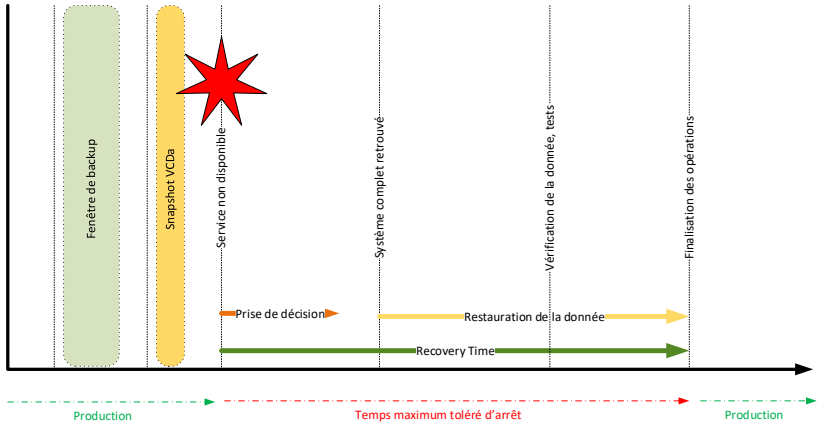
Tous les prérequis liés aux niveaux de "Managed Applications" doivent être souscrits pour l'exécution du service "PRA Managé".

A ces prérequis de base s'ajoutent les prérequis liés aux rubriques suivantes.

La fonctionnalité VCDA constitue un prérequis fourni par Cloud Avenue. La licence VCDA ainsi que les ressources d'infrastructure associées sont portées par l'offre Cloud Avenue et ne sont pas incluses dans les Unités d'Œuvre du service "PRA Managé" du test annuel est lissé sur l'année.

6.1 Mécanisme de réplication des serveurs virtuels

La réplication des machines virtuelles entre deux VDC distant est assurée via VCDA (vCloud Director Availability), qui permet la duplication des données des machines virtuelles entre deux salles ou datacenters, selon une politique de RPO définie. La politique de réplication détermine la fréquence et la durée de conservation des réplicas de la machine source vers le Datacenter ou la salle distante.



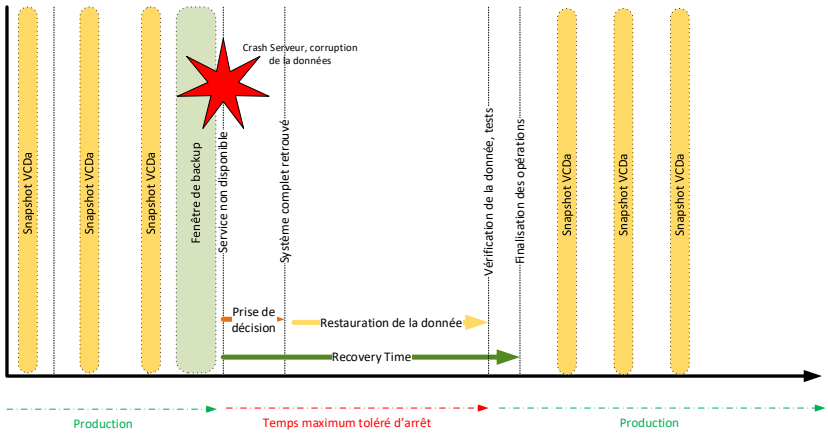
Voici le détail non contractuel des politiques de réplication disponibles sur Cloud Avenue :

Politique	RPO	Rétention
Bronze	24h	uniquement le dernier réplica
Silver	6h	uniquement le dernier réplica
Silver +	6H	un réplica conservé 24h
Gold	1h	uniquement le dernier réplica
Gold +	1h	3 réplicas conservés sur 3 jours
Platinum	5mn	uniquement le dernier réplica
Platinum +	5min	7 réplicas conservés sur 7 jours

Ainsi il est nécessaire de comprendre que le mécanisme de synchronisation VCDA au maximum passe sur chacune des machines virtuelles toutes les 5 minutes (politique de synchronisation Platinum) pour mettre à jour les données et stockage locaux après la dernière synchronisation « success »et ne conserve donc que les 7 derniers réplicas sur les 7 derniers jours glissant.
Donc pour une politique de RPO Bronze nous avons un snapshot toutes les 24h et donc une perte potentielle de 1 jours de données.

Si la demande du client et de récupérer toutes ses données métier dans un intervalle de compris entre 4h et 1h, alors le mécanisme de réplication Gold et Platinum est nécessaire.

Le niveau de RPO souscrit doit être cohérent avec la classe de stockage associée. En conséquence, un RPO de niveau Platinum ne peut être garanti que si les données sont hébergées sur une infrastructure de stockage de classe équivalente (Platinum).



Ici sur cette représentation, nous pouvons identifier 3 Snapshots correspondant à la politique Gold + ainsi que le passage de la dernière sauvegarde. Le temps d'indisponibilité est donc plus court et la perte des données est aussi plus faible.

6.2 Mécanisme de réplication des serveurs physiques (BMS)

Pour les serveurs physiques, des serveurs BMS supplémentaires, provisionnés en attente, sont utilisés pour la reprise. La mise à disposition de ces serveurs est un prérequis au PRA managé.

La réplication des données s'effectue via :

- La sauvegarde des espaces disques locaux
- Le mécanisme de réplication du stockage réseau
- En option : Le mécanisme de réplication des Middleware

6.2.1 Mécanisme de réplication du stockage réseau

Les espaces de stockage réseaux tel que le stockage NetApp CIFS et NFS peuvent être couverts par l'option « dual site répliqué » ; qui doit être contractualisée dans l'offre Cloud Avenue par le client et implémenté par les équipes opérationnelles pour être couvert par l'offre Service Managed PRA.
La réplication est suivie par les équipes du Prestataire et la bascule des accès stockages CIFS de NetApp et les stockage réseaux NFS NetApp sont opérées par les équipes de Managed Services lors du déclenchement du PRA.

La bascule de la SVM n'est pas automatique entre les Datacenter de Val de Rueil vers Chartres et/ou inversement. Les équipes techniques du Prestataire doivent intervenir pour opérer la configuration et permettre la bascule de la ressources Active vers Passive d'un Datacenter à l'autre.

6.3 La bascule du réseau

La bascule est surtout liée à la déclaration des réseaux qui ne peut pas être déclarée sur les 2 Datacenters en même temps.
La bascule du réseau d'un Datacenter vers l'autre est un point impactant à prendre en compte lors de l'étude et de la mise en œuvre du plan de reprise d'activité.

- Le Managed PRA implique la gestion du réseau T0 & T1 par les équipes du Prestataire
- Un segment IP bascule complètement d'un site source vers le site distant, le site source est alors inactif ce qui rend inopérant les IPs et son segment IP durant toute la bascule du site source.
- Le site distant récupère le segment IP ainsi que toutes les adresse IP qui deviennent alors actives sur ce site distant

6.3.1 Premier cas réseau, pare-feu géré par le client

Le client est responsable de la gestion, la création et la suppression de ses règles de gestion et de flux de ses machines virtuelles, cependant la route par défaut sur les pares-feux doit rester la Edge Gateway T1 au sein du VDC client qui est la seule route qui permet de communiquer vers sur la T0 du Prestataire nécessaire pour les réplications des machines virtuelles dans l'offre Managed PRA ; la modification de cette route rend inopérant notre activité de Managed Service et nous empêche d'activer la bascule entre les VDC source et de destination ainsi que les réplications des machines virtuelles entre les VDC client.

Les équipes du Prestataire effectuent une première configuration des pares-feux du client pour y inscrire la configuration Dual Site nécessaire pour la bascule du Managed PRA avant que le client puisse en reprendre la main et déclarer ses règles de routages et autres flux de sécurités pour ses machines virtuelles.
Ainsi, les équipes du Prestataire sont embarquées dès la création du VDC client dans le plan de bascule pour gérer et configurer les routes et réseaux T1 & T0 du client d'un Datacenter à l'autre.

6.3.2 Second cas réseau, T1 et pares-feux gérés par les équipes réseaux du Prestataire

Les équipes techniques du Prestataire disposent de la main sur la configuration et la propagation des routes et segment réseau, il est plus aisé d'opérer la bascule des machines virtuelles et de diffuser le réseau source vers le Datacenter distant.

- La déclaration des réseaux sur le site distant est à évaluer par les équipes techniques lors de la création du VDC client
- Le temps de bascule est variable en fonction de la complexité réseau du client, cette charge sera établie lors de l'étude de l'environnement en Avant-Vente.
- Les contraintes fonctionnelles et techniques seront incluses dans l'étude.

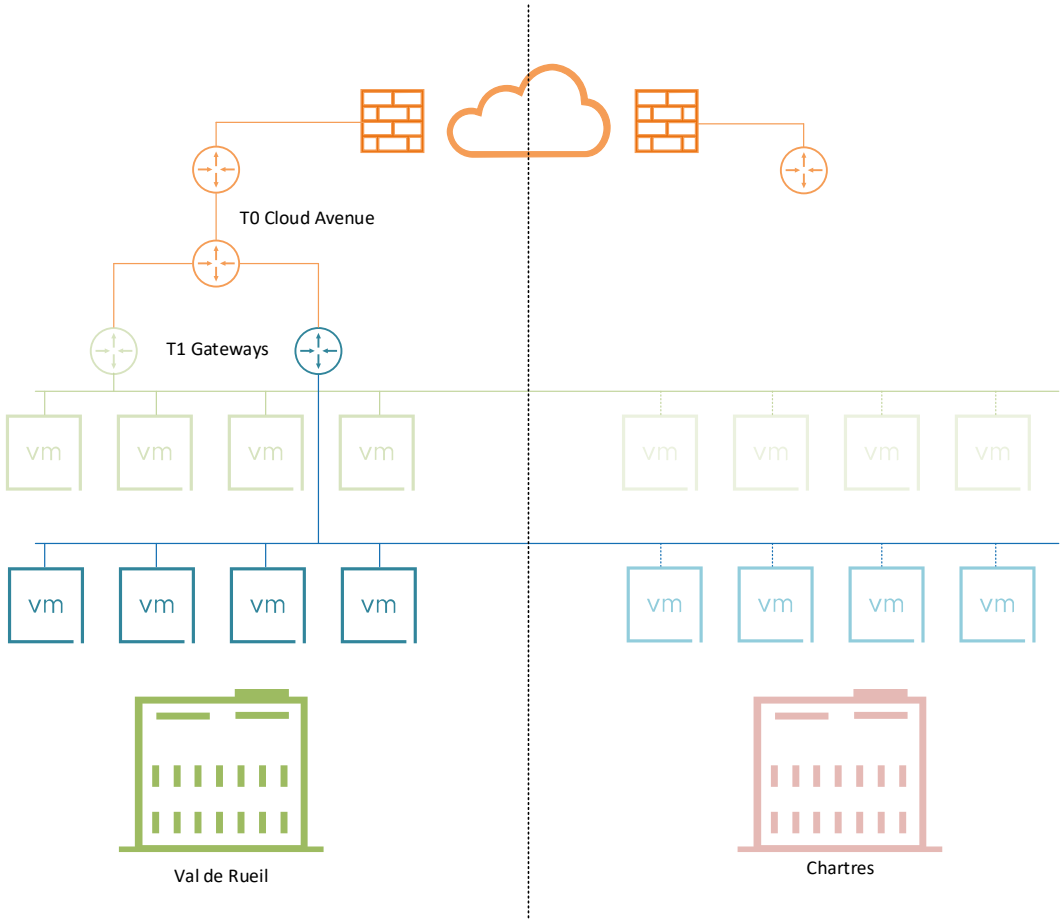


Figure 1 - VDC Nominal avant bascule

6.3.3 Bascule complète du Tenant client

La bascule complète des machines virtuelles vers le Datacenter distant est effectuée par l'arrêt des machines sources (via une défaillance ou un acte manuel des équipes techniques du Prestataire) et le démarrage des machines distantes sur le site de destination.

Les machines virtuelles sont accostées sur la T1 Gateway du VDC distant qui dispose de toutes les règles de flux et de routage pour permettre une communication identique à l'origine.

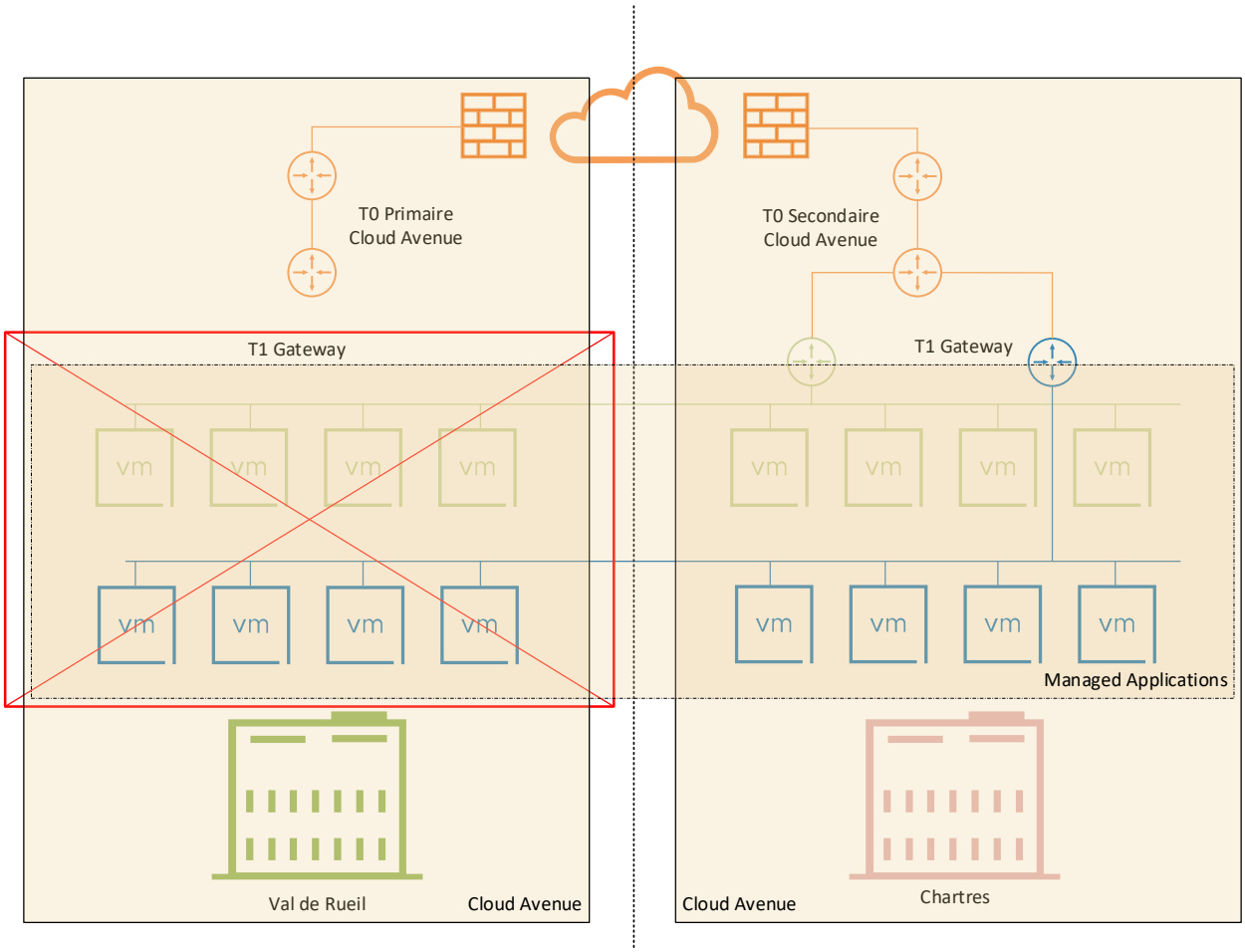


Figure 2 - Bascule du Tenant client

Sur le schéma ci-dessus, nous avons donc les machines virtuelles et les T1 Gateway qui sont actives pour recevoir et accorder les communications sur le site distant. Le service est toujours apporté au client et utilisateurs avec un minimum de perte de données ou d'interruption de service.

6.4 Eléments spécifiques à prendre en compte

Le Plan de Reprise d'Activité est un service important pour permettre à nos clients une reprise de leur activité plus rapidement que la restauration d'un service pour les Core business.

Un Service Active Directory par exemple est nativement redondé dans sa conception et propose la réplication de tous les jetons d'authentification, changement de mot de passe, historique des changements, inscription/suppression de comptes et machines dans un environnement de production. Nos abaques en production imposent le déploiement de deux contrôleurs de domaine pour la redondance du service.

Dans le cadre d'un plan de Reprise d'Activité, nous conseillons de déployer un troisième contrôleur de domaine sur le VDC distant et d'y apporter une continuité réseau entre les deux segments réseaux afin de garantir les synchronisations de l'Active Directory. La présence d'un troisième Domain Controller sur le site distant permet de garantir la bascule, l'accostage des machines répliquées en toute transparence sans coupure de service d'authentification.

Certains moteurs de bases de données permettent une reprise d'activité plus simplement et rapidement par l'ajout du service ou de la fonctionnalité Cluster (mise en place de nœuds actif/passif notamment). C'est le cas par exemple d'Oracle, SQL AlwaysOn et MariaDB (Master/slave).

6.4.1 Ce qui est intéressant d'inclure dans un PRA :

Il est très intéressant d'inclure dans un Managed Service PRA les services dont les fonctions support ont une faible activité en mémoire et une plus grande inertie sur le système de fichiers.

- Un Filer Windows Server qui ne repose pas sur la fonctionnalité **DFS** ou DFS-R
- Les Web Server, qui par définition est très souvent statique
- Une base de données mono serveur, qui ne propose pas la haute disponibilité
- Les machines ou services qui écrivent directement sur disque et ont peu de threads en mémoire
- Les machines dont le temps de restauration est supérieur au **RTO**

Plus le taux de changement des données sur les disques de la machine virtuelle est élevé, et plus la fenêtre de réplication est éloignée et moins le service de plan de reprise est préconisé.
A l'inverse, un faible taux de changement des données permet d'inclure la machine virtuelle dans le plan de reprise d'activité pour bénéficier d'un RPO très faible.

6.4.2 Les services difficilement supportés par le Managed PRA

Certains services nécessaires au fonctionnement des architectures de nos clients ne sont pas les mieux secourus par le Managed PRA. Nous pouvons par exemple citer les composants suivants :

- Active Directory
- SQL Server
- MariaDB/MySQL
- Oracle
- PostgresSQL

VCDA permet uniquement de répliquer la configuration système et la configuration Middleware, mais ne peut pas servir de socle fiable pour la réplication de la base de données.
Les logs transactionnels et fichiers de sauvegarde de Base de données sont inclus dans le mécanisme de réplication, mais une restauration complète des données sera nécessaire en cas de PRA (PointInTimeRecovery possible).

NOTA : une base de données très transactionnelle occasionne une grande quantité de fichiers modifiés. De surcroit si cette base est de gros volume, le temps de synchro VCDA pourra être élevé. Il est nécessaire d'adapter la politique VCDA choisie afin qu'elle soit ajustée pour atteindre le RTO désiré.

La mise en place des synchronisations de VCDA est à effectuer VM par VM afin de ne pas de peupler les Datastores par la réplication de toutes les VM en un point de destination sur le même temps de réplication.

Par ailleurs, l'outil limite le volume de réplication à des clichés instantanée jusqu'à 1To pour ne pas saturer les environnements de stockage en lecture et écriture pendant la réplication.

De plus il est plus aisé de ne pas inclure toutes les machines virtuelles dans un seul batch de synchronisation, car en cas de problématique de synchronisation sur l'une des machines virtuelles, tout le batch est alors en échec.

Un job de synchronisation par machine est plus aisé pour relancer la synchronisation sans relancer toutes les machines et dégrader les performances globales des datastore source et cible.

6.5 Mécanisme de réplication des Middleware - optionnel

Managed Applications propose, dans le cadre de la gestion du Managed PRA des Middleware, de s'appuyer sur les sauvegardes des bases de données vers les espaces disques locaux et/ou du stockage réseau.

A cela nous pouvons ajouter selon les Middleware la mise en place des mécanismes de réplication améliorant le processus de PRA :

- Base de données :
  Voici une liste non contractuelle des mécanismes possible liés au PRA des bases de données (cf. annexe contractuelle « Managed Database ») :

Type de Base	Mécanisme natif	RPO avec le mécanisme de réplication de la base de données
PostgreSQL	PostgreSQL Streaming réplication	~0
MySQL	MySQL réplication	~0
Microsoft SQL Server	Cluster Always On Availability Group	~0 ~0 minute
Oracle	Oracle Dataguard (PRA) DBVisit	~0 1 minute
MongoDB	MongoDB réplication	~0

L'usage des options PRA est une option intéressante mais avec l'ajout de la fonctionnalité Haute Tolérance de panne pour les moteurs de base de données apporte une plus grande continuité dans la reprise d'activité et réduit à pratiquement un Downtime à 0 seconde, cependant cela nécessite obligatoirement 2 nœuds actifs/actifs ou actif/passif répartis sur 2 sites distincts.

Le temps d'indisponibilité du service sera réduit au plus strict minimum du temps de bascule d'un nœud à un autre et de la remise en ligne ou de la montée de la ressource par le moteur.

La souscription de l'option Managed PRA ne garantit pas la non-corruption des bases de données en cas de bascule. Ainsi Il est plus pertinent de mettre en place une haute tolérance dans le service natif que souscrire à l'offre Managed PRA, car le temps de bascule entre les ressources hébergées par le service natif est plus rapide et moins consommateur en ressources passive que le nombre de synchronisation sur le stockage distant, ou le temps de restauration des fichiers de sauvegarde. Par ailleurs, les services qui travaillent en priorité en mémoire ne peuvent pas être répliqués en dynamique ou correctement pris en charge par le mécanisme de synchronisation qui ne peut dupliquer que la data sur le stockage de l'hyperviseur.

- Autres Middleware :
  La réplication des Middleware est incluse dans la réplication des VM via l'outil VCDA. Si besoins spécifiques, des sauvegardes "Fichiers" peuvent être mises en place.

Ci-dessous, un exemple non-contractuel de Middleware pris en charge.

Middleware	Distribution
Serveur web	▪ Apache server ▪ NGINX server ▪ IIS server
Serveur Proxy	▪ Squid server ▪ HaProxy server
Serveur d'application	▪ Tomcat server ▪ Microsoft IIS + ASP.NET ▪ PHP server ▪ SOLR server ▪ Web server + PHP server
DDI	▪ DNS server standalone ▪ DHCP server standalone
Serveur de fichiers	▪ Samba server ▪ Microsoft File server ▪ Microsoft DFS server ▪ ProFTPD server
Gestion des opérations de fabrication (MOM)	▪ Kafka ▪ Zookeeper ▪ RabbitMQ
Transfert de fichiers managé	▪ CFT Managé (cf. description ci-jointe)

6.6 Sauvegarde

Pour assurer le service, il y a 2 types de sauvegarde que l'on peut mettre en place en plus des réplications :

- Sauvegarde de VM (sans agent) réalisée par l'outil Netbackup et donc qui attrape la machine virtuelle depuis l'infrastructure sous-jacente.
- Sauvegarde de VM et fichiers (avec agent) via l'outil Netbackup (optionnel) et qui lui permet d'obtenir une granularité des sauvegardes et restaurations.

Pour assurer le rétablissement du service en cas de problèmes majeurs et sévères, nous préconisons à minima une sauvegarde avec 6 jours de rétention. Les sauvegardes sont réalisées selon les politiques choisies et l'exploitation de la sauvegarde est assurée selon le niveau de support souscrit. Ces sauvegardes sont effectuées via l'outil NetBackup directement via l'infrastructure VMware ou via un agent a positionner dans la machine virtuelle.

Une durée de rétention différente peut être choisie selon la disponibilité du backup de l'infrastructure Cloud hébergeant le service.

Voici les politiques de sauvegardes possibles (cette liste est non exhaustive et est détaillée dans l'annexe contractuelle Cloud Avenue correspondante) :

Nom de la politique	Description
D6	Sauvegarde quotidienne (sauf les dimanches et 1er lundi du mois), avec 6 jours de rétention
D6A	Sauvegarde quotidienne (sauf les dimanches et 1er lundi du mois) entre 18:00 et 22:00, avec 6 jours de rétention
D6B	Sauvegarde quotidienne (sauf les dimanches et 1er lundi du mois) entre 22:00 et 02:00, avec 6 jours de rétention

D6C	Sauvegarde quotidienne (sauf les dimanches et 1er lundi du mois) entre 02:00 et 06:00, avec 6 jours de rétention
D7	Sauvegarde quotidienne (du lundi au dimanche), avec 7 jours de rétention
D14	Sauvegarde quotidienne (lundi au dimanche de 18:00 à 06:00), avec 14 jours de rétention
D30	Sauvegarde quotidienne (sauf les dimanches et 1er lundi du mois), avec 30 jours de rétention
D30NQ	Sauvegarde quotidienne sans mise au repos (sauf les dimanches et 1er lundi du mois), avec 30 jours de conservation
D60	Sauvegarde quotidienne (sauf les dimanches et 1er lundi du mois), avec 60 jours de rétention
W4	Sauvegarde hebdomadaire chaque 1er dimanche de chaque semaine, avec 4 semaines de rétention
M3	Sauvegarde mensuelle chaque 1er lundi du mois, avec 3 mois de rétention
M12	Sauvegarde mensuelle chaque 1er lundi du mois, avec 12 mois de rétention
XD6	Sauvegarde quotidienne (sauf dimanche & 1er lundi du mois) + Réplication avec 6 jours de rétention sur les 2 sites (Val de Reuil et Chartres)
XD6A	Sauvegarde quotidienne (sauf dimanche & 1er lundi du mois) entre 18:00 et 22:00 + Réplication avec 6 jours de rétention sur les 2 sites (Val de Reuil et Chartres)
XD6B	Sauvegarde quotidienne (sauf dimanche & 1er lundi du mois) entre 22:00 et 02:00 + Réplication avec 6 jours de rétention sur les 2 sites (Val de Reuil et Chartres)
XD6C	Sauvegarde quotidienne (sauf dimanche & 1er lundi du mois) entre 02:00 et 06:00 + Réplication avec 6 jours de rétention sur les 2 sites (Val de Reuil et Chartres)
XD7	Sauvegarde quotidienne (du lundi au dimanche) + Réplication avec 7 jours de rétention sur les 2 sites (Val de Reuil et Chartres)
XD30	Sauvegarde quotidienne (sauf dimanche & 1er lundi du mois) + Réplication avec 30 jours de rétention sur les 2 sites (Val de Reuil et Chartres)
XD6O	Sauvegarde quotidienne (sauf dimanche & 1er lundi du mois) + Réplication avec 60 jours de rétention sur les 2 sites (Val de Reuil et Chartres)
XW4	Sauvegarde hebdomadaire chaque 1er dimanche de chaque semaine + Réplication avec 4 semaines de rétention sur les 2 sites (Val de Reuil et Chartres)
XM3	Sauvegarde mensuelle chaque 1er lundi du mois + Réplication avec 3 mois de rétention sur les 2 sites (Val de Reuil et Chartres)
XM12	Sauvegarde mensuelle chaque 1er lundi du mois + Réplication avec 12 mois de rétention sur les 2 sites (Val de Reuil et Chartres)

En fonction de l'horaire de réplication des machines virtuelles, il peut être intéressant de réinjecter par ailleurs les données sauvegardées fraichement retenues par l'outil NetBackup. Si la dernière synchronisation VCDA est passée avec succès après le dernier travail de sauvegarde NetBackup, la réinjection des données sauvegardées n'est pas nécessaire ou judicieuse.

Les sauvegardes sont à réinjecter dans le plan de PRA. Mais si le PRA est en Dual Room, alors les backups doivent rester sur le site original. Si le client souscrit à l'option Dual Site, alors les backups doivent être croisés.

6.7 Redondance des liens réseaux d'interconnexions externes

Afin de pouvoir garantir un accès en tout temps aux machines exportées par le Managed PRA, il est nécessaire que le client souscrive à des points d'accès externe à la plateforme. Ces points d'accès externe sont des liens d'interconnexions et doivent être redondants afin d'assurer une continuité d'accès, de supervision pour respecter les délais de remise en ligne des services.

Les liens réseaux d'interconnexions externes compatibles avec l'offre Managed PRA sont les suivants :

- Business VPN
- VPN IPSec
- MPLS opérateur

Seuls les liens ayant une terminaison dans les plateformes d'hébergement supportées sont intégrables à ce service de PRA managé, arrivant donc sur les T0 de Cloud Avenue et/ou étant gérés par les T1 du client.

Dans tous les cas ces liens doivent être redondés c'est-à-dire qu'un deuxième lien « passif » est mis en place à l'activation du service. Ce lien est configuré et sera activé manuellement par les équipes techniques dès la sollicitation des équipes du Prestataire, par le Responsable Client ou par la soumission d'un ticket par le Client via son portail d'incidents. Une validation fonctionnelle et technique en amont est nécessaire pour éviter toute corruption des données, bagotage des liens, erreurs de configurations réseaux et sécurités, routage des liens et écrasements & pertes de données pour les utilisateurs et services métier.

6.8 Supervision

La supervision des services managés est intégrée au niveau de l'offre « Managed Applications » souscrite. Elle constitue un outil essentiel pour la prise de décision lors du déclenchement du PRA. Ce service perdure dans la continuité avant, pendant et après la bascule du Tenant client.

6.9 Dépendances

Les prérequis pour pouvoir garantir l'intégrité de la solution lors d'un PRA sont :

- La bonne exécution des différentes réplications ("VCDA")
- La bonne exécution des différentes sauvegardes ("NetBackup")
- L'intégrité des données présentes dans ces sauvegardes

7.Exécution du PRA

7.1 Déclenchement du PRA

Le déclenchement intervient à la suite d'une détection d'indisponibilité, par le biais des alertes de supervision ou des remontées du Client. Le Client, après consultation avec le Prestataire, décide de lancer le plan de reprise.

Une matrice d'escalade est disponible auprès du Service Delivery Manager qui détaille les modalités de déclenchements du Managed PRA entre le Prestataire, et le Client.
En fonction du niveau de service souscrit, le client pourra contacter le Service Delivery Manager en heure ouvrée ou le service support en heure non-ouvrée qui déclenchera et exécutera les procédures et les actions techniques par les équipes d'exploitation.

Les actions techniques sont décrites, dans les documents d'exploitation utilisés par les équipes du Prestataire, lors de la phase de conception du service PRA souscrit. Un plan complet et détaillé est alors mis en œuvre conjointement avec le client et en accord avec les équipes techniques du projet ; afin de garantir l'ordonnancement, les actes techniques, les temps nécessaires et les équipes à mobiliser. Ce chronogramme est à la charge du Chef du Projet en concertation avec les équipes techniques, des plans de continuité souscrit par le client mais aussi en fonction du volume de machines et leur fonction dans le plan de reprise.

7.2 Test du plan de reprise total

Les prérequis nécessaires pour pouvoir prétendre à un plan de reprise Total maitrisé et fonctionnel sont de respecter les points suivants :

- La contractualisation de l'offre Managed PRA, Managed OS ainsi que des éléments Virtual Datacenter Customer sur la salle ou le site distant
- Identification des liens et interconnexions nécessaires à la connectivité pour la reprise du service (pare-feu et ses règles, routeurs et leurs tables de routage, switch d'interconnexion)

- Identification des composants d'infrastructures nécessaires pour la remise en ligne des éléments fondamentaux du client (Virtual Datacenter Customer, serveurs physiques pour les bases de données Oracle)
- Identification de la chaine de contact et des outils à solliciter pour la bascule, le pilotage et assurer le suivi de la reprise du service
- Identification des personnes habilitées pour déclencher, initier les scripts et changements de configurations, piloter la bascule et opérer la reprise du service
- Etablir les critères de succès du plan de reprise, le temps pendant lequel il peut vivre, et l'organisation du son retour à l'état initial.

Le responsable client peut être amené à établir la charge, le chronogramme, identifier les équipes nécessaires pour l'activation, les impacts du déclenchement et les modalités de retour en phase nominale ainsi que la date du test.

Le test annuel total est inclus dans l'offre Managed PRA dont son cout est lissé sur l'année civile de facturation.

Le test annuel est à effectuer en heure ouvrée durant lesquelles les équipes techniques sont disponibles pour opérer les actions et corrections nécessaires.

Le test annuel de Managed PRA ne peut pas être activé par les équipes d'astreinte d'infrastructure ou de celles de Managed Services.

7.3 Chronogramme générique – Prestataire/Client.

Afin d'aider nos clients, la chefferie de projet ainsi que les exploitants, il est important que certains points soient mis en œuvre et validés en amont pour la bonne exécution du plan souscrit comme :

- le chronogramme soit préétabli
- Les outils soient identifiés pour l'exécution du plan de reprise d'activité
- Le client nous confirme les services vitaux
- Les services supports et les services annexes ou connexes aux services rendus aux utilisateurs finaux soient pleinement identifiés, que cela soit en respect du métier
- Que la capacité des infrastructures soit identifiée et conforme aux exigences techniques et fonctionnelles du Prestataire et du client.

Ce document sera renseigné et mis en œuvre pour chacune des bascules et tests de Managed PRA par les équipes du Prestataire.

7.4 Déclenchement de la bascule

La bascule des VMs, est effectuée depuis la console VCDA dès l'exécution du JOB par un opérationnel du Prestataire. La création d'une vAPP (groupement de plusieurs machines virtuelles synchronisées) VCDA est nécessaire pour automatiser la restitution du service aux utilisateurs et réduire les temps d'attente entre chaque lancement de machines virtuelles.

NOTA : la vAPP est une notion strictement VCD & Vmware.
Les Avantages de la vAPP sont de permettre la configuration en lotissant les machines virtuelles, d'automatiser les arrêts et démarrages des machines virtuelles sources et de relire le job en mode inversé pour initier le démarrage du PRA.

7.5 SLA

Dans le cadre de l'offre Managed PRA nous assurons des garanties de reprise sur incidents selon les modalités souscrites par le client auprès du fournisseur.

Actions	SLA	RPO
Rétablissement des liens réseaux	Définit selon le niveau de support souscrit	N/A
Rétablissement des VM	Définit selon le niveau de support souscrit	Définit selon la politique VCDA souscrite
Rétablissement des BMS	Définit selon le niveau de support souscrit	Définit selon la politique Netbackup souscrite
Rétablissement des Middleware	Définit selon le niveau de support souscrit	• Bases de données : ~0 • Autres : Définit selon la politique Netbackup souscrite
Rétablissement des stockages partagés	Offre en développement	N/A

8.Conditions de prix

8.1 Tarification

Le service Managed PRA repose sur un modèle de facturation composé :

- d'une prestation de Build initiale ;
- d'Unités d'Œuvre (UO) récurrentes d'exploitation ;
- d'Unités d'Œuvre associées aux campagnes de test PRA ;
- de prestations ponctuelles de déclenchement réel du PRA.

8.2 Prestations de Build

Les activités de Build ne sont pas incluses dans les Unités d'Œuvre récurrentes du service Managed PRA. Elles comprennent notamment :

- l'analyse du besoin client ;
- la conception de l'architecture PRA ;
- la définition des scénarios de reprise ;
- la configuration des réplications ;
- la mise en œuvre des groupes de protection VCDA ;
- la rédaction des procédures de reprise ;
- la préparation et l'exécution du premier test de validation.

Les prestations de Build font l'objet d'un chiffrage spécifique pour chaque Client. Le chiffrage est réalisé par les équipes Avant-Vente et exprimé en homme-jours.

8.3 Prérequis Cloud Avenue

Le service Managed PRA s'appuie sur les fonctionnalités natives de réplication fournies par la plateforme Cloud Avenue.

La fonctionnalité VMware Cloud Director Availability (VCDA) constitue un prérequis à la fourniture du service.

Les éléments suivants sont fournis dans le cadre des services Cloud Avenue et ne sont pas inclus dans les UO du Managed PRA :

- licence VCDA ;
- stockage associé aux réplications ;

- ressources CPU et RAM réservées ;
- mécanismes de réplication et de bascule ;
- services d'infrastructure nécessaires à l'hébergement du PRA.

8.4 UO « Plan de Continuité d'Activité sur Cloud Avenue : opérations hors test annuel »

Cette UO couvre les activités récurrentes nécessaires au maintien en condition opérationnelle du dispositif PRA.

Elle comprend notamment :

- la vérification du rattachement des machines virtuelles aux groupes de protection VCDA ;
- la vérification de la cohérence du périmètre protégé ;
- le contrôle des prérequis nécessaires à l'exécution du PRA ;
- la vérification que les sauvegardes requises sont correctement réalisées lorsqu'elles relèvent du périmètre Managed OS ;
- le suivi opérationnel du dispositif PRA.

Cette UO ne couvre pas la réalisation des campagnes de test PRA.

La facturation est réalisée par tranche de 100 machines virtuelles protégées.

Exemple :

Nombre de VM protégées	Nombre d'UO
1 à 100 VM	1 UO
101 à 200 VM	2 UO
201 à 300 VM	3 UO

8.5 UO « Test PRA annuel »

Le service inclut une UO spécifique destinée à couvrir la réalisation d'un test PRA annuel.
Cette UO est facturée mensuellement et répartie sur douze mois.
La mensualisation couvre :

- la préparation du test ;
- la coordination des intervenants ;
- l'exécution du scénario de reprise ;
- les contrôles post-exécution ;
- la production du compte-rendu et du retour d'expérience.

Le test annuel inclus correspond à une campagne de test PRA.

8.6 Campagnes de test PRA complémentaires

Une campagne de test PRA correspond à une opération de validation réalisée sur un périmètre défini et exécutée dans le cadre d'une session planifiée.

Exemples de campagnes :

- test PRA d'un environnement de préproduction ;
- test PRA d'une application spécifique ;
- test PRA d'une machine virtuelle ;
- test PRA complet d'un environnement de production.

Chaque campagne de test constitue une prestation indépendante et donne lieu à la consommation de l'UO correspondante.

Exemple :
Si un Client réalise :

- un test de préproduction ;
- un test sur une machine virtuelle ;
- un test complet de production ;

alors trois campagnes distinctes sont réalisées et trois UO de test PRA sont consommées.

8.7 Heures Ouvrées et Heures Non Ouvrées

Les campagnes de test PRA sont généralement réalisées en Heures Non Ouvrées (HNO) afin de limiter les impacts sur les environnements de production.

Deux types d'UO peuvent être proposés :

- UO Test PRA HO ;
- UO Test PRA HNO.

Les conditions tarifaires applicables sont précisées dans le catalogue des Unités d'Œuvre.

8.8 Organisation France / Offshore

Les activités de Build ainsi que les campagnes de test PRA sont réalisées par les équipes expertes localisées en France.

À date :

- le Build est réalisé en France ;
- le premier test PRA est réalisé en France ;
- les campagnes de test PRA sont réalisées par les équipes françaises disposant des compétences nécessaires.

Afin de simplifier le modèle économique de l'offre, les UO de test PRA sont établies sur une base de coûts France, indépendamment du modèle de Run retenu pour le Client (France ou Offshore).

8.9 Déclenchement réel du PRA

Les opérations de déclenchement réel du PRA à la suite d'un sinistre ne sont pas incluses dans les UO récurrentes.

Elles font l'objet d'une facturation au temps passé conformément aux dispositions contractuelles en vigueur.

9.RACI

RACI des taches de PRA

ID	Tâches	Le Prestataire	Client
1	Définir les criticités des briques applicatives et le niveau de PRA souhaité	I – C	A – R
2	Souscrire au service	I – C	A – R
3	Déclaration des VM protégées dans VCDA	A – R	I – V
4	Prérequis – Build et Management des BMS de spare	A – R	I – V
5	Prérequis – Build de la réplication du stockage réseau	A – R	I – V
6	Prérequis – Build de la réplication des bases données - option	A – R	I – V
7	Prérequis – Build de la sauvegarde	A – R	I – V
8	Prérequis – Build de la redondance des liens réseaux d'interconnexions externes	A – R	I – V
9	Mise en place et/ou vérification de la configuration VCDA	A – R	I – V
10	Prérequis – Mise en place du reporting de sauvegarde	A – R	I – V

ID	Tâches	Le Prestataire	Client
11	Mise à jour des documents d'exploitation	A – R	I
12	Test de PRA – Déclenchement du test	I – C	A – R
13	Test de PRA – Application du test	A – R	I – C
14	Test de PRA – Vérification du bon fonctionnement applicatif du périmètre testé	I – C	A – R – V
15	En cas de PRA – Déclenchement du PRA	I – C	A – R
16	En cas de PRA – Application du PRA	A – R	I – C
17	En cas de PRA – Vérification du bon fonctionnement applicatif	I – C	A – R – V
R : Réalisateur – A : Accountable (Responsable) – C : Consulté – I : Informé – V : Valideur			

10.Support

Nous présentons ci-dessous le support spécifique que nous apportons à l'offre PRA Managé.

10.1 Gestion des changements

La gestion des changements pour le service PRA Managé s'inscrit dans le modèle commun de nos services managés. Vous disposez d'un catalogue de demandes standards présenté dans l'annexe contractuelle de l'offre PRA Managé.

Pour une demande hors catalogue, l'équipe opérationnelle évalue sa faisabilité, 2 cas de figure se présentent :

1- Demande aisément qualifiable

L'équipe opérationnelle vous fait un retour sur le nombre de Tokens nécessaire pour la réalisation et si applicable les ressources d'infrastructure nécessaires et la charge de service récurrente qui en résultent.
Après votre accord, la demande sera réalisée. Vous serez facturé :

- Le nombre de Tokens débité sur votre forfait si vous en avez souscrit un ou hors forfait,
- Les ressources d'infrastructure additionnelles selon votre contrat d'infrastructure Cloud,
- La charge de service récurrent

2- Demande à qualification spécifique
L'équipe opérationnelle vous fait un retour vous indiquant de vous rapprocher de votre contact commercial.

11.Chaine de soutien du Managed PRA

Afin d'assurer l'exécution du Plan de Reprise d'Activité dans les meilleures conditions de sécurité et de disponibilité, le service Managed PRA s'appuie sur une chaîne de soutien associant le Client, les équipes Managed Applications et, lorsque nécessaire, les équipes du Prestataire.

11.1 Principes généraux

Le déclenchement d'un PRA relève exclusivement d'une décision du Client ou de ses représentants habilités.

À réception de la demande de déclenchement, les équipes Managed Applications assurent la qualification de la demande, la coordination des intervenants et l'exécution des procédures de reprise définies lors de la phase de conception du service.

Selon le périmètre concerné et les composants techniques impliqués, les équipes Managed Applications peuvent :

- réaliser de manière autonome l'ensemble des opérations de reprise ;
- ou solliciter les équipes du Prestataire lorsque des actions relèvent de leur domaine de responsabilité (réseau, infrastructure, stockage ou services mutualisés).

11.2 Organisation de la chaîne de soutien

La chaîne de soutien s'articule autour des acteurs suivants :

11.2.1 Client

Le Client :

- décide du déclenchement du PRA ;
- valide le périmètre concerné ;
- participe aux validations fonctionnelles ;
- confirme le retour au fonctionnement nominal.

11.2.2 Équipes Managed Applications

Les équipes Managed Applications :

- assurent le pilotage opérationnel du PRA ;
- exécutent les procédures techniques de reprise ;
- coordonnent les différentes équipes contributrices ;
- assurent la communication et le suivi de l'avancement ;
- produisent le compte-rendu d'intervention et le retour d'expérience.

11.2.3 Équipes du Prestataire

Les équipes du Prestataire interviennent lorsque la reprise nécessite des actions relevant de leur responsabilité, notamment :

- l'activation ou la modification des services d'infrastructure ;
- les opérations sur les composants réseaux T0/T1 ;
- les opérations sur les services mutualisés Cloud Avenue ;
- les actions spécifiques liées au stockage ou à l'hébergement.

11.3 Déclenchement du PRA

Deux scénarios principaux sont couverts :

11.3.1 Test planifié du PRA

Le Client soumet une demande de changement conformément au catalogue de services.

Les équipes Managed Applications planifient et coordonnent l'ensemble des opérations avec les parties prenantes concernées sur la base d'un chronogramme validé.

11.3.2 Activation réelle du PRA

En cas d'incident majeur affectant tout ou partie de l'environnement de production, le Client contacte le support selon les modalités prévues au contrat.

Après validation de la décision de déclenchement, les équipes Managed Applications coordonnent les opérations de reprise et mobilisent les ressources nécessaires jusqu'au rétablissement du service.

11.4 Escalade et coordination

Les modalités détaillées d'escalade, les contacts opérationnels et les personnes habilitées à déclencher un PRA sont définis dans la matrice d'escalade associée au service.

Cette matrice est maintenue à jour par le Prestataire et revue lors des exercices annuels de PRA.

11.5 Retour d'expérience

Chaque test ou activation réelle du PRA donne lieu à :

- un bilan d'exécution ;
- l'identification des éventuels écarts ;
- la mise à jour des procédures d'exploitation ;
- la mise à jour de la documentation du PRA lorsque nécessaire.

Ce bilan est à l'initiative du Responsable Client ou Service Delivery Manager afin d'identifier les axes de progression et les canaux de communication afin de gagner en résilience.

La mise à jour de la documentation sera à la charge du Technical Design Architect qui communiquera à toutes les parties prenantes.

11.6 Vue d'ensemble du processus cible

Nous avons établi une activation du Plan de Reprise d'Activité en neuf étapes afin de garantir sa bonne exécution et un pilotage au retour nominal dans les règles de l'art.

- Détection d'incidents/anomalies majeures ou Demande d'activation du Plan de Reprise d'Activité.
- La qualification du scénario est nécessaire afin de ne pas déclencher des activations sur des faux-semblants.
- Evaluation de l'impact de la bascule ainsi que de la criticité de l'évènement.
- Décision d'activation du Plan de Reprise d'Activité
    - Nous déclenchons les étapes techniques et nous déroulons le chronogramme validé avec le client
    - Nous ne déclenchons pas le plan et nous assurons la remise en état du service défaillant par les méthodes conventionnelles (rollback déploiement, restauration configuration infrastructure/réseau/système, restauration des fichiers/serveurs déclenchement RMA, etc.)
- Mobilisation des acteurs chez le Prestataire, le co-traitant, le client
- Préparation opérationnelle
- Activation du Plan de Reprise d'Activité et bascule des ressources
- Pilotage de la période du Plan de Reprise d'Activité
- Retour au mode nominal et déclenchement d'une analyse de Retour d'Expérience pour en tirer les bénéfices et améliorations à produire.

11.7 Qualification du besoin et décision d'activation

Pour aider le client et les opérationnels dans la décision de déclenchement du Plan de Reprise d'Activité, nous afin établi un logigramme décisionnel pour qualifier le besoin. Il se décompose dans les étapes ci-après.

- Test ou cas Réel ?
- Si le cas est Réel, alors identification si c'est en **Heure Ouvrées** ou en **Heures Non-Ouvrées** (en-dehors des Horaires de Services déclarés par le client)
- Quantité de Service Impacté (Total, partiel, intermittent)
- Identification de la criticité du métier impacté (Stratégique, confidentiel, restreint, critique, haute, moyenne, faible)
- Identification de la rapidité de remise en ligne du service impacté.
- Les prérequis techniques et organisationnels sont-ils réunis pour le déclenchement du PRA ?
- Le Plan de Reprise d'Activité est-il initialement au contrat du client ?
    - Décision de contractualiser
    - Décision d'activer un PRA
- Validation par le Client et en appui avec le SDM

- Décision d’activer totalement le PRA
- Décision de reporter le PRA
- Décision d’activer partiellement le PRA.

Annexe 1 – Catalogue des demandes standard

Catalogue	Catégorie	Description	Nombre tokens
Managed PRA	Politique	Ajout de serveur dans la politique de réplication	2
		Ajout d'une politique de réplication (vApp)	2
		Modification politique de rétention (durée, catégorie, ordonnancement)	2
		Suppression de serveur dans la politique de réplication	1
	Réseau	Ajout de réseau supplémentaire	2
		Mise en place d'un routage asymétrique	2
		Suppression d'une annonce de réseau distant	1
	Communication	Demander de l'information (catégorie générale)	2
		Fournir une information au Prestataire	2
		Création de rapport personnalisé	2
	Backup	Demander un backup ou une restauration de machine	2
		Mettre à jour la politique de sauvegarde	2
		Sauvegarde complète occasionnelle / ponctuelle	1
		Modifier paramètre sauvegarde (rétention, catégorie)	2
		Restauration de données depuis le serveur source	3
		Test de restauration du serveur	3