Descriptif de Service - Qualité de Service
Flexible Recovery

Table des matières

1 Définitions 3
2 Objet 4
3 Présentation du Service Flexible Recovery 4
3.1 Aperçu du Service 4
3.2 Implantation géographique 5
3.3 Couverture fonctionnelle 5
3.4 Les classes de protection 5
3.5 La protection des OS, applications et bases de données 5
Mode avec agent 6
Mode hyperviseur (pour hyperviseurs Hyper-V et VMware) 6
Les bases de données 6
3.6 Période de rétention des sauvegardes 7
3.7 Restauration des données en local 7
3.8 Les mécanismes de sécurité 7
4 Les services managés 8
4.1 Descriptif des services 8
4.2 Évolutivité de la solution 9
5 Architecture du Service 9
5.1 Les espaces Cloud 9
5.2 Modes de fonctionnement du PRA 10
6 Conditions d'exécution des services 10
6.1 Mise en Service 10
6.2 Interventions du Prestataire sur les infrastructures du Client 10
6.3 Calendrier d'exécution 11
6.4 Systèmes d'exploitation supportés 11
6.5 Support 11
7 Accès au Service 12
7.1 La Console Flexible Recovery 12
7.2 Maintenance Programmée 12
7.3 Console de sauvegarde 12
8 Tests de PRA 13
8.1 Principes 13
8.2 Tests de secours informatique 13
8.3 Rapport de test de secours informatique 13
8.4 Tests de reconnexion 14
9 Activation du PRA en réel 14
9.1 Principe Général 14
9.2 Activation du PRA 15
9.3 Plage d'activation du PRA 15
9.4 Exécution technique du PRA 15

9.5 Adaptation de la politique de sauvegarde ... 15
9.6 Contexte d'une cyber-attaque ... 16
10 Le PRA à la demande ... 17
10.1 Principe du PRA à la demande ... 17
10.2 Reconnexion des sites Client ... 17
10.3 Estimation du RTO (délai de mise à disposition) ... 17
10.4 Estimation du tarif de PRA à la demande ... 18
11 Le retour à la situation nominale ... 18
11.1 Le périmètre des systèmes actifs dans le PRA ... 18
11.2 Les phases du retour à la situation nominale ... 18
11.3 Restauration ou reconstitution des systèmes et données ... 19
12 La reconnexion à l'environnement PRA ... 19
12.1 La reconnexion via Internet (Option) ... 19
12.2 La reconnexion via MPLS Orange (Option) ... 20
12.3 La reconnexion via MPLS tiers (Option) ... 20
12.4 La reconnexion via SD-WAN ... 21
12.5 La reconnexion des utilisateurs en mobilité (option) ... 21
13 SLA ... 22
13.1 Respect des RTO ... 22
13.2 Respect des RPO ... 22
13.3 Réponse sur incident critique ... 22
13.4 Tests de PRA ... 23
13.5 Performances ... 23
13.6 Disponibilité de l'infrastructure en cas d'activation du PRA ... 23
14 Prestations complémentaires ... 23
14.1 Expertise et Conseil ... 23
14.2 Assistance technique ... 24
14.3 Tarif des prestations ... 24
14.4 Processus de commande ... 24
15 Conditions de prix ... 25
15.1 Prix ... 25
15.2 Révision de prix ... 25
16 Réversibilité ... 25

1 Définitions

En complément des définitions des Conditions Générales et des Conditions Spécifiques Cloud du Prestataire, les définitions suivantes s'appliquent à ce document Descriptif de Service – Qualité de Service.

Agent de Backup : agent mis à la disposition du Client afin de lui permettre notamment de sauvegarder régulièrement ses fichiers de manière chiffrée, de les stocker dans le Cloud, d'y accéder et de les restaurer en cas de besoin.

Agent de sauvegarde ou **Agent** : logiciel installé dans le serveur à protéger.

Appliances : application matérielle conçu pour exécuter un logiciel destiné à fournir une ressource informatique distincte.

Chiffrage AES 128/256 : algorithme de chiffrement symétrique (nommé Advanced Encryption Standard) avec des clefs de 128 et 256 bits.

Clef de chiffrement ou **Clef** : algorithme permettant de chiffrer à la source les données en mode sauvegarde et de les déchiffrer lors de l'opération de restauration pour un PRA.

Console Flexible Recovery : interface d'administration de la solution Flexible Recovery.

Conteneur : espace de stockage d'objets qui peuvent stocker les objets et des métadonnées associées.

Garantie de Temps d'Intervention (ou **GTI**) désigne le Temps d'Intervention sur lequel Le Prestataire s'engage pour répondre à un ticket d'incident, en fonction du niveau de support souscrit.

Heures Ouvrées (ou **HO**) désigne les Jours Ouvrés de 8 heures à 18 heures, horaire française. Toutes les autres plages horaires sont appelées **Heures Non Ouvrées** (ou **HNO**).

Incident désigne un événement non planifié qui provoque une Interruption ou une dégradation du Service.

Interruption désigne la ou les période(s) pendant laquelle un incident provoque un dysfonctionnement significatif du Service concernée affectant le Client.

NAS SSD : (Network Attached Storage) Serveur de stockage avec disques SSD. Serveur de stockage portable connectable au réseau local et pouvant servir au chargement initial des données Client dans le cloud Flexible Engine et pouvant également servir dans un mécanisme de retour arrière vers le site nominal de production du Client.

PRA désigne le Plan de Reprise d'Activité informatique.

Prestataire : désigne l'entité du groupe Orange mentionnée au bon de commande

RCA (Remote Cloud Access) est un boitier fournit qui permet de relier par Internet un site du Client à son environnement de secours dans le Cloud Flexible Engine.

RPO (Recovery Point Objective) désigne la durée maximum d'enregistrement des données qu'il est acceptable de perdre pour le Client à la suite du sinistre ou indisponibilité sur le site couvert par le PRA.

RTO (Recovery Time Objective) désigne la durée maximale d'interruption admissible pendant lequel une ressource informatique peut ne pas être fonctionnelle à la suite d'une interruption majeure de service.

Service désigne le service Flexible Recovery

Serveur : dispositif informatique matériel ou logiciel qui offre des services, à un ou plusieurs utilisateurs du Client. Dans le cadre du service Flexible Recovery, ce terme s'applique à un serveur (physique ou virtuel), à un poste de travail (PC ou ordinateur portable).

Temps d'Intervention désigne le temps qui s'écoule entre l'ouverture d'un ticket et la notification au Client de sa prise en charge par Le Prestataire, dont on retire les périodes pendant lesquelles les engagements du Prestataire ne s'appliquent pas.

Test de redémarrage : opération consistant à vérifier la récupération des données sauvegardées et le redémarrage du serveur dans le Cloud.

Site de secours : espace dans le Cloud Flexible Engine servant d'espace de redémarrage de l'infrastructure IT du Client

Système d'Exploitation (ou **OS** pour Operating System) désigne un ensemble de programmes central d'un appareil informatique qui sert d'interface entre le matériel et les logiciels applicatifs

VM (Virtual Machine) : machine virtuelle.

2 Objet

Le présent document Descriptif de Service – Qualité de Service a pour objet de définir le Service Flexible Recovery et les conditions dans lesquelles il est fourni avec les engagements de service, en application des Conditions Générales et des Conditions Spécifiques Cloud du Prestataire.

3 Présentation du Service Flexible Recovery

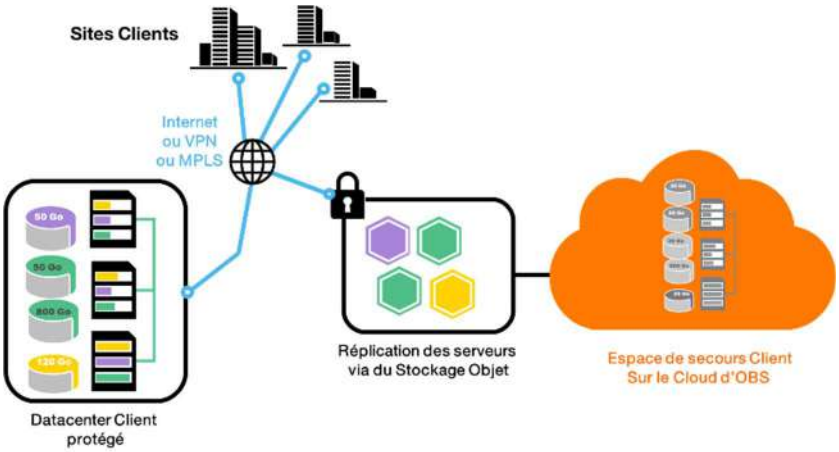
3.1 Aperçu du Service

Le Service Flexible Recovery s'appuie sur :

- L'utilisation du Cloud public Flexible Engine d'Orange Business, pour la sauvegarde des données, les tests de redémarrage et l'activation du Plan de Reprise d'Activité.
- Une offre complète de services qui inclut la sauvegarde des données, le maintien opérationnel de la solution de secours, la surveillance des sauvegardes et le pilotage de l'ensemble du projet, afin de garantir son efficacité et l'activation du PRA en cas de besoin.

Le Service est constitué par :

- Un agent installé sur les serveurs du Client permettant l'exécution des tâches de sauvegarde, pour l'envoi des données chiffrées via la connexion réseau du Client.
- Un abonnement mensuel qui permet l'accès par le Client à un espace de sauvegarde externe et mutualisé dans le Cloud d'Orange Business. La capacité de cet espace de sauvegarde est déterminée lors de la souscription du Service et peut être modifié selon les besoins.
- Un accès à une console permettant : de monitorer les sauvegardes et les tests (redémarrage et PRA) et d'avoir une vue de synthèse du fonctionnement de tous les composants du PRA.
- D'options complémentaires payantes lors de la souscription : boitier RCA, NAS SSD, etc.



3.2 Implantation géographique

Le Service est accessible aux Utilisateurs localisés en France métropolitaine et en DOM-TOM.

Il est opéré sur des Plateformes localisées en France.

3.3 Couverture fonctionnelle

Flexible Recovery protège aussi bien des infrastructures traditionnelles dans les locaux des entreprises que des infrastructures Cloud (public ou privé).

Infrastructure traditionnelle sur site (On Prem)	Infrastructure de type Cloud

• VMWare
• Hyper-V
• Autres hyperviseurs
• Serveurs physiques
	• Cloud Public
	  ○ Flexible Engine, AWS, OVH, Azure, …
	• Cloud privé ou privatif
	  ○ Cloud Avenue, OpenStack, OVH…

3.4 Les classes de protection

Il existe 3 classes de protection :

Serveurs en protection PRA	Serveurs en backup avec tests de redémarrage dans le Cloud	Serveurs en backup simple (sans test de redémarrage)
La classe PRA : il s'agit de serveurs qui sont testés régulièrement (par défaut tous les 6 mois) dans un cadre de test de secours informatique complet qui a objectif principal de vérifier le bon fonctionnement des serveurs et Appliances en périmètre PRA Ce test de secours informatique pouvant intégrer des tests réseaux et des tests de reconnexion des utilisateurs au site de secours.	La classe Backup avec Tests : les sauvegardes des serveurs de cette classe sont testées automatiquement tous les 6 mois (par défaut) dans le Cloud Flexible Engine. Les différents services des serveurs sont scannés afin de valider leur bon fonctionnement. En option et sur devis, pour les serveurs dans cette classe, des tests de secours informatique complets peuvent être réalisés.	La classe sauvegarde externalisée : il s'agit de serveurs dont la sauvegarde est externalisée dans le Cloud Flexible Engine.

3.5 La protection des OS, applications et bases de données

Flexible Recovery permet de couvrir un périmètre hétérogène d'environnement qui peut contenir :

- Des serveurs physiques.
- Des VM dans des environnements où le Client gère son hyperviseur.
- Des VM pour lesquels le Client n'a pas accès à l'hyperviseur (par exemple dans le Cloud public).

Il existe deux approches différentes :

- Mode Hyperviseur : La sauvegarde se fait via les mécanismes de l'hyperviseur (VMware ou Hyper-V)
- Mode avec Agent : Un agent de sauvegarde est déployé dans chaque serveur

Mode Hyperviseur	Mode avec Agent
Un agent est installé sur une VM de l'hôte (ou plusieurs suivant le nombre de serveurs à sauvegarder) et va servir à toutes les sauvegardes de l'hôte. C'est une solution de sauvegarde centralisée, les VMs n'ont pas d'agent installé et elles n'ont pas besoin d'être allumées pour être sauvegardée. Cette solution fonctionne en parcourant les fichiers pour déterminer les changements qui ont été effectués depuis la précédente sauvegarde.	Un agent (un exécutable) est installé sur chaque serveur (physique ou virtuel) pour assurer la sauvegarde. Le serveur doit être allumé lors de la sauvegarde et il doit se faire sur une plage horaire précise. Dans la réalité, plusieurs exécutables (et services) sont installés sur chaque serveur.

Mode avec agent

Deux types d'agent peuvent coexister dans un même serveur :

Les agents dit Standard au niveau de l'OS qui permettent de réaliser une sauvegarde en mode image Les OS serveur supportés sont : • Pour Microsoft Windows: Windows Server 2012 à 2022 ainsi que Windows 8/10/11. • Pour Linux : les principales distributions qui sont en mode support (Debian, CentOS, Ubuntu, Suse Entreprise, RHEL, Oracle Linux, …)	Les agents dit dédiés au niveau d'une application Sur Windows Server, il existe un agent dédié pour : • SQL server (versions 2012 à 2019) • MS Exchange (versions 2016 à 2019)

Mode hyperviseur (pour hyperviseurs Hyper-V et VMware)

Une VM Windows (ou plusieurs suivant le nombre de serveurs à sauvegarder) est installée dans l'hôte à protéger avec un agent spécifique à l'hyperviseur (Hyper-V ou VMware). Les VM sont alors sauvegardées via des mécanismes natifs de l'hyperviseur.

Le mode de sauvegarde hyperviseur permet de prendre en compte des VM avec des OS ne disposant plus de la maintenance de l'éditeur (par exemple Windows Server 2003, 2008, CentOS 6/7, …) ou qui sont spécifiques (Appliance de sécurité, autre distribution).

Les bases de données

Pour les sauvegardes des bases de données, le principe général est d'avoir une sauvegarde de la base de données plus une sauvegarde des dumps :

- Pour les bases MS SQL Server, un agent spécifique permet d'appliquer des scénarios de sauvegarde prédéfinis :
  - Sauvegarde incrémentale quotidienne avec une sauvegarde différentielle à une fréquence souhaitée par le Client (RPO) en fonction de la capacité de la bande passante (facteur limitant).
- Pour les bases Oracle, deux solutions sont possibles suivant les mécanismes mis en œuvre par le Client :
  - Soit les mécanismes d'image des machines hôtes (VSS, cliché),
  - Soit les mécanismes internes d'Oracle (RMAN par exemple) pour sauvegarder les logs.
- Pour les bases Linux, suivant les bases de données, des scénarios à base d'image de volume disque et de sauvegarde régulière des fichiers de logs/ dumps de base sont générés.

3.6 Période de rétention des sauvegardes

Lors de la souscription, le Client choisit une période de rétention des sauvegardes (en standard 7 jours/14 jours/30 jours). Cette période de rétention permet d'estimer le besoin d'espace de stockage des sauvegardes.

Il est ensuite possible d'adapter par serveur cette durée de rétention et cette modification peut avoir un impact sur le besoin d'espace de stockage des sauvegardes.

3.7 Restauration des données en local

Quelle que soit la classe de protection utilisée, le Client a la possibilité, soit en direct via une console de sauvegarde, soit via une demande au support, de restaurer en local les données sauvegardées.

Par défaut, et quel que soit le mode de sauvegarde, la granularité de restauration est au fichier unitaire.

3.8 Les mécanismes de sécurité

Les mécanismes de sécurité mis en œuvre sur Flexible Recovery s'appuient sur les éléments suivants :

- Le chiffrement des données de sauvegarde (en AES 128 ou 256) avec des clefs de chiffrement détenues par le Client.
- Le transfert des données vers le stockage Flexible Engine est sécurisé par du TLS 1.2.
- L'isolation des environnements de sauvegarde dans le Flexible Engine via des conteneurs de sauvegarde dédiés.
- Une redondance des données de sauvegarde native via les mécanismes du Cloud public Flexible Engine, les données de stockage S3 sur Flexible Engine sont répliqués sur les 3 datacenters (AZ) en France.
- Le service Objet Storage,service de Cloud public Flexible Engine, hébergé dans les Datacenters certifiés (ISO27001, HDS, ISAE3402, PCI-DSS, …).

4 Les services managés

4.1 Descriptif des services

Flexible Recovery est une solution entièrement managée avec Maintien en Conditions Opérationnelles (MCO) de la solution.

Elle intègre des tests réguliers de restauration dans le Cloud pour les classes de protection PRA et backup avec tests, ajustés à la classe de protection choisie (par défaut semestriels).

Ces services managés accompagnent le Client à chaque étape du projet.

Lors de la mise en œuvre :

Cette étape intègre :

- Une phase de conception et de lancement de projet avec :
  - L'élaboration des stratégies de sauvegarde de données, notamment afin de garantir le respect des RTO/RPO dans un contexte de protection PRA
  - L'intégration des composants d'architecture Client dans la modélisation de votre infrastructure en base de données
  - La préparation des éléments nécessaires aux tests de secours informatique (:serveur rebond, boitier RCA de connectivité (option), la fourniture d'un NAS SSD pour le chargement des données (option), ainsi qu'aux tests de reconnexion avec la mise en œuvre du lien VPN Galerie (option)
- Une phase de déploiement de la solution avec :
  - La création des espaces Cloud
  - L'installation des logiciels de sauvegarde et leur paramétrage pour les serveurs
  - L'installation des sauvegardes et leur paramétrage pour les serveurs
  - La création des éléments du projet en base de données
  - La rédaction des procédures PRA ajustée à votre environnement technique et humain
  - Le transfert de compétences vers les équipes du Client
  - Le premier test du PRA (test de secours informatique initial)

En fonctionnement nominal :

Les équipes Flexible Recovery administrent et exploitent la solution afin de garantir un fonctionnement efficace. (Maintenance et mises à jour des composants Flexible Recovery ; surveillance de la solution ; résolution des problèmes ; support aux utilisateurs ; adaptation du périmètre du projet en liaison avec les équipes Client afin de suivre l'évolution du SI ; organisation des tests de restauration des VM et des tests de PRA suivant la fréquence définie avec le Client.)

L'abonnement mensuel aux services couvre :

- La mise à disposition des licences des agents de Backup intégrant les mises à jour des nouvelles versions (versions mineures et majeures),
- La consommation de stockage de l'espace Cloud
- La surveillance des sauvegardes externalisées dans le Cloud
- Pour les serveurs en classe de protection backup avec tests, la réalisation des tests automatiques de redémarrage des serveurs et la production du rapport de test unitaire
- Pour les serveurs en classe de protection PRA, la restauration des données avec :
  - Le redémarrage des serveurs et l'activation des plateformes de secours afin de permettre aux équipes Client de faire des tests de bon fonctionnement des applications
  - La production des comptes-rendus de tests, accompagnés des éventuelles actions correctrices nécessaires
- Le support à l'utilisation de la solution Flexible Recovery.

Activation en mode secours :

Cette prestation fait l'objet d'une présentation détaillée aux chapitres 9 et 10 du présent descriptif de services. Elle est réalisée au forfait pour les VM en classe de protection PRA et selon les dispositions de la proposition technique et commerciale ou fait l'objet d'une assistance technique au temps passé pour les VM en classe de protection Sauvegarde avec tests.

4.2 Évolutivité de la solution

Flexible Recovery est une offre évolutive qui permet :

- D'inscrire de nouveaux serveurs dans le périmètre et de définir leur classe de protection.
- De changer la classe de protection d'un serveur.
- De supprimer des serveurs et d'archiver les données.
- De faire évoluer les serveurs existants.
- L'ajout, la modification ou la suppression d'un disque.
- Le changement d'OS, …

Le prix de ces évolutions peut être défini et prévu dans la proposition initiale et/ou donner lieu à un devis complémentaire suivant les évolutions demandées.

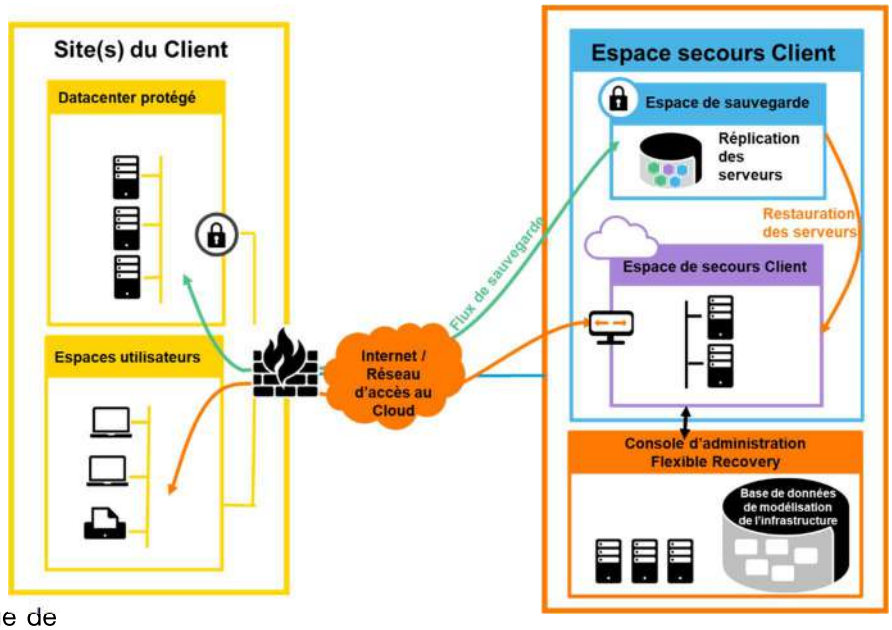
5 Architecture du Service

5.1 Les espaces Cloud

Dans un contexte de protection PRA, un environnement dédié est créé dans le dans le Cloud public Flexible Engine.

Cet environnement dédié se compose de :

- Un **Espace de sauvegarde** organisé avec des conteneurs (stockage objet) spécifiques à chaque Client.
- Un **Espace de secours** dédié à la restauration des serveurs Client pour la mise en œuvre technique du PRA.
- Une **Console Flexible Recovery** permet de disposer de la modélisation des SI Clients et des outils d'administration.



L'**Espace de sauvegarde** est une image de l'ensemble des systèmes et des données du périmètre du PRA obtenue par sauvegarde et de façon régulière (c'est le point de récupération des données, correspondant au RPO par serveur). Il est construit sur une capacité de stockage dédiée aux opérations de sauvegarde.

L'**Espace de secours** est vide jusqu'à son activation lorsque survient un sinistre ou qu'un test de PRA est réalisés. Il est activé en restaurant l'image de l'ensemble des systèmes et des données stockés dans l'Espace de sauvegarde.

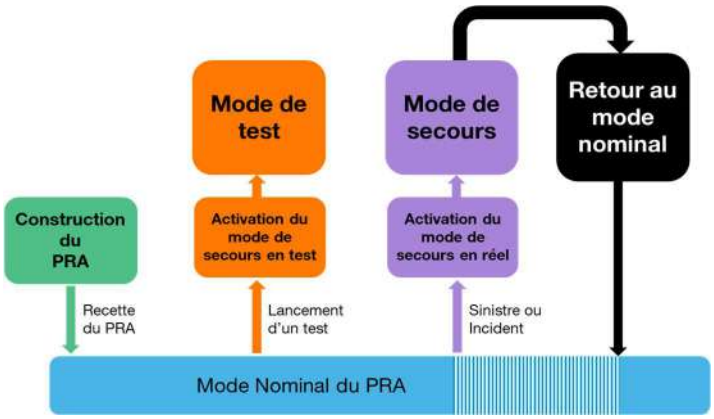
5.2 Modes de fonctionnement du PRA

Le Plan de Reprise d'Activité se décline en deux modes de fonctionnement :

- Fonctionnement en mode nominal
- Fonctionnement dans l'espace Cloud de secours

Ces modes sont complétés par des transitions qui permettent de formaliser les phases :

- De création ou de révision du PRA.
- D'activation du PRA lors des tests.
- D'activation du PRA en cas de de sinistre.
- De retour à la situation nominale après que l'espace protégé original est à nouveau opérationnel.



6 Conditions d'exécution des services

6.1 Mise en Service

À date de réception de la Commande du Client, le Prestataire nomme un interlocuteur qui prend contact avec le Client :

- Le Prestataire s'engage à désigner un chef de projet et à le rendre disponible pour une réunion de préparation de la Mise en Service.
    - Cette réunion téléphonique sera organisée par le chef de projet sous 10 (dix) jours ouvrés maximum pour présentation des prochaines étapes de la Mise en Service.
- Le Prestataire s'engage à participer sous 15 (quinze) jours ouvrés maximum à une première réunion projet (pour la collecte détaillée des données techniques du Client sur la préparation du Service et pour la définition d'un planning de déploiement), sous réserve de disponibilité du Gestionnaire Client sur cette période.

Lorsque le Service ne nécessite pas d'intégration spécifique, Le Prestataire s'engage à assurer la Mise en Service sous 3 (trois) mois, sous réserve de disponibilité du Gestionnaire Client sur cette période et d'une capacité connectivité adéquate.

L'ensemble des acteurs du projet ont accès à un espace documentaire partagé expliquant les différentes étapes du projet et un espace d'échange (compte-rendu réunion, messagerie directe, …).

6.2 Interventions du Prestataire sur les infrastructures du Client

Afin de pouvoir paramétrer ou tester les sauvegardes de données, le Client autorise le Prestataire à effectuer si nécessaire certaines opérations techniques sur chacun des serveurs dont les données doivent être protégées.

Le but de ces interventions est d'installer, de paramétrer et de tester les agents de sauvegarde de données.

Le Client s'engage à :

- Être présent (physiquement ou en mode connecté) lors de toute intervention du Prestataire sur son infrastructure.
- Veiller à la conservation en lieu sûr du mot de passe donnant accès à la Clé de chiffrement. Le Client est informé que, sans ce mot de passe et en cas de perte de données,

    - La récupération des sauvegardes est impossible,
    - Le rechargement de la totalité des données de sauvegarde du Client est nécessaire et pourra donner lieu à facturation du Prestataire au temps passé.
- Veiller à disposer d'une connexion au réseau Internet opérationnelle et de débit suffisant, sans laquelle la sauvegarde de données ne peut être garantie.
- Mettre en œuvre dans les meilleurs délais les préconisations du Prestataire du ressort du Client et nécessaires à l'ajustement des services, par suite d'incidents de sauvegarde ou tests de PRA.
    - Au bout de 3 relances infructueuses du Prestataire avec absence de tout retour du Client, les serveurs impliqués seront sortis temporairement du périmètre de protection et seront réintégrés dès la mise en œuvre des préconisations par le Client.
- Ne pas modifier les agents et logiciels fournis par le Prestataire de quelque façon que ce soit, ni les intégrer dans quelque autre programme que ce soit.
- Consulter régulièrement les rapports de sauvegarde (logs) générés par les agents de sauvegarde.

6.3 Calendrier d'exécution

Si un calendrier d'exécution est défini dans la Proposition et/ou la Commande, les Parties s'engagent à le respecter. Toute évolution du calendrier devra faire l'objet d'un accord préalable entre les Parties.

Cependant, tout retard / décalage de planning qui ne serait pas causé par le Prestataire sera répercuté aux frais du Client sur le calendrier d'exécution des services et le Prestataire ne saurait être responsable de l'éventuel décalage et/ou retard par rapport au planning prévu dans la Commande.

En cas de retard / décalage de planning en raison d'un retard ou d'une omission du Client, le Prestataire pourra facturer au Client le temps passé pour la mise en service infructueuse.

6.4 Systèmes d'exploitation supportés

Le Client est tenu informé par le Prestataire des systèmes d'exploitation que ce dernier supporte dans sa solution de restauration dans le Cloud. Le Client s'engage à garder ses serveurs équipés avec des versions récentes des systèmes d'exploitation supportés par la solution de PRA Flexible Recovery.

Cette liste est disponible dans la Console Flexible Recovery.

6.5 Support

Un accueil téléphonique en Heures Ouvrées est mis à la disposition du Client.

Le Service est soumis à des frais de mise en œuvre et à une redevance mensuelle définies dans la Proposition Technique et Commerciale annexée au Contrat. La Proposition Technique et commerciale précise également les coûts d'évolution du périmètre et de prestations complémentaires (activation du PRA en mode secours).

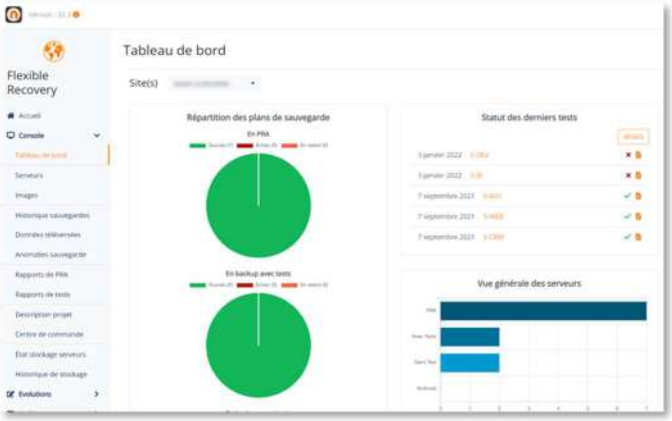
Objet	Détail
Support Langue : Français ○ Par courriel : support.orange@nuabee.fr ○ Par téléphone : +0 805 690 963 (prix d'un appel local)	Disponibilité ○ Du lundi au vendredi (jours ouvrés du calendrier français métropolitain) ○ Heures ouvrées : 9h00-12h30 et 14h-18h Délai de réponse aux questions • Minimum 75% des questions répondues en moins de 24h pendant les jours ouvrés • Maximum 25% des questions restantes répondues entre 24h et 5j. Procédure d'escalade : Le Prestataire s'engage à communiquer au lancement du projet un contact pour escalade en cas de dysfonctionnement dans la prise en charge de l'assistance du Client sur le Service.

7 Accès au Service

7.1 La Console Flexible Recovery

Flexible Recovery dispose d'une console qui permet au Client d'avoir une synthèse du fonctionnement de tous les composants de la solution de PRA et de Backup.

La Console Flexible Recovery donne une vision complète des services avec notamment :



- Une synthèse des plans de sauvegarde et des niveaux de protection souscrits par serveurs
- La modélisation des infrastructures de secours (gabarit des serveurs, disques, réseau, ordre de redémarrage des serveurs et composants)
- Le suivi et un historique de la consommation d'espace disque par serveur et par type de stockage
- Les rapports de tests de restauration et de PRA effectués
- Un espace documentaire (procédure de sauvegardes et restauration, procédures de gestion de crise…).

Cette Console est accessible à l'adresse suivante : https://flexible-recovery.nuabee.com/.
Le paramétrage de la double authentification est fortement recommandé.

7.2 Maintenance Programmée

La maintenance programmée porte sur les mises à jour correctives, et ou mises à niveau de la Console.

Une information est alors affichée dans la Console Flexible Recovery.

7.3 Console de sauvegarde

L'accès à une console de sauvegarde, permettant au Client, la restaurations de serveurs ou de fichiers en autonomie est disponible sur demande.
Le paramétrage de la double authentification est fortement recommandé.

8 Tests de PRA

8.1 Principes

Les tests de PRA couvrent deux aspects complémentaires :

- Le test de secours informatique qui a pour objectif principal de
  - Vérifier le bon fonctionnement des serveurs et Appliances en périmètre PRA
  - Vérifier la gestion des dépendances entre serveurs
  - Vérifier la connectivité WAN et le paramétrage du boitier en cas d'utilisation du boitier RCA

- Le test de reconnexion qui a pour objectif principal de :
  - Vérifier la bascule du réseau de production
  - Tester la reconnexion mobilité (VPN SSL, …)

8.2 Tests de secours informatique

Le test de secours informatique est, par défaut, semestriel et sa date définie entre les parties. Il se déroule en HO et consiste à redémarrer dans l'espace de secours du Client dans le Cloud

- L'ensemble des serveurs du périmètre du PRA,
- Les éventuelles Appliances du périmètre du PRA,
- En cas d'utilisation du boitier RCA, le VPN de reconnexion du (des) site(s) utilisateur(s) au site de secours dans le Cloud.

Le test de secours informatique porte sur :

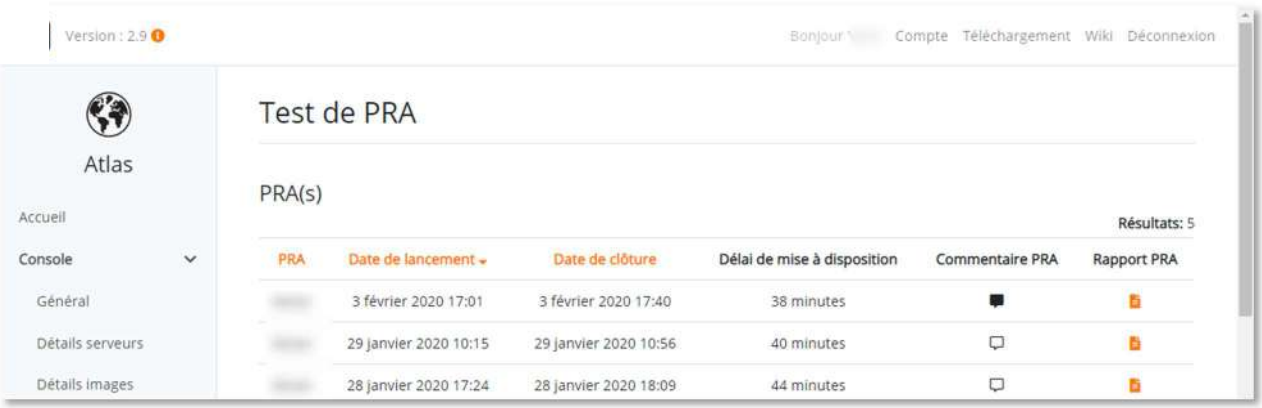
- Les automatismes et les procédures de restaurations et de redémarrage,
- Le bon fonctionnement du réseau LAN et des serveurs redémarrés.

Le Client a la responsabilité de faire le test sur chaque serveur et chaque application et d'indiquer ses tests dans la page de test de la Console Flexible Recovery.

Ce test est aussi l'occasion de constater d'éventuelles variations du périmètre du PRA et d'étudier s'il convient d'effectuer la modification des procédures associées.

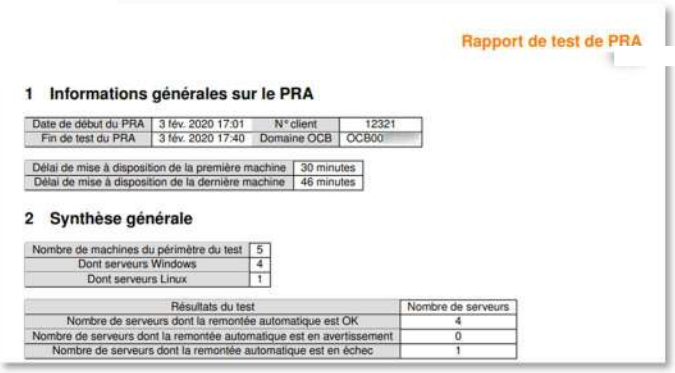
8.3 Rapport de test de secours informatique

À chaque test, un rapport de test est généré et est stocké dans la Console Flexible Recovery. Il intègre les commentaires des tests Client sur chaque serveur/application.



Ce rapport de test de secours informatique indique :

- Le délai de mise à disposition du premier serveur.
- Le délai de mise à disposition du dernier serveur.
- La synthèse générale.
- Puis, sur les pages suivantes, le détail pour chaque serveur.



Rapport de test de PRA

1 Informations générales sur le PRA

Date de début du PRA	3 fév. 2020 17:01	N° client	12321
Fin de test du PRA	3 fév. 2020 17:40	Domaine OCB	OCB00

Délai de mise à disposition de la première machine	30 minutes
Délai de mise à disposition de la dernière machine	46 minutes

2 Synthèse générale

Nombre de machines du périmètre du test	5
Dont serveurs Windows	4
Dont serveurs Linux	1

Résultats du test	Nombre de serveurs
Nombre de serveurs dont la remontée automatique est OK	4
Nombre de serveurs dont la remontée automatique est en avertissement	0
Nombre de serveurs dont la remontée automatique est en échec	1

À la suite de chaque test de secours informatique, il est défini dans ce rapport les éventuelles actions à mener.

8.4 Tests de reconnexion

La fréquence du test de reconnexion est dépendant de l'architecture du Client et est une extension demandée par le Client lors de la planification d'un test de secours informatique standard.

Par défaut, il se déroule le même jour que le test de secours informatique.

Il consiste à vérifier la bascule du réseau de production du Client en cas d'activation d'un PRA et, suivant le périmètre du projet, de tester les mécanismes de reconnexion en mobilité (VPN SSL, …).

Il se déroule en HO et si l'architecture du Client impose un test en HNO, un devis sera établi préalablement par le Prestataire.

9 Activation du PRA en réel

9.1 Principe Général

Lorsqu'un Client identifie le besoin d'une bascule en mode secours, le Client contacte l'équipe Flexible Recovery aux moyens des éléments décrits dans la Console Flexible Recovery.

- Pour des raisons de sécurité, un responsable de l'équipe Flexible Recovery rappelle une des personnes du Client habilitées à déclencher un PRA (cette liste est présente dans la Console Flexible Recovery).

Il est défini lors de cet échange s'il s'agit :

- D'une mise en alerte pour un éventuel déclenchement ultérieur.
- D'une bascule immédiate en secours. Il sera également précisé le périmètre à activer (complet ou partiel)

Dès la confirmation reçue (via un SMS ou un mail), il est procédé à l'activation du PRA via la procédure technique de lancement du PRA.

Une procédure détaillée décrit les mécanismes d'activation d'un PRA en réel.

9.2 Activation du PRA

Le lanceur de PRA est une fonction dédiée aux équipes de Flexible Recovery qui permet de lancer automatiquement le PRA du Client et d'en suivre son exécution pas à pas.

Le Client dispose dans la Console Flexible Recovery d'un suivi de la progression de son PRA.

Ce lanceur permet de définir si le PRA à lancer est total ou partiel, et dans ce dernier cas de définir les serveurs à lancer.

9.3 Plage d'activation du PRA

En standard la plage d'activation du PRA est en Heures Ouvrées : 8h-18h

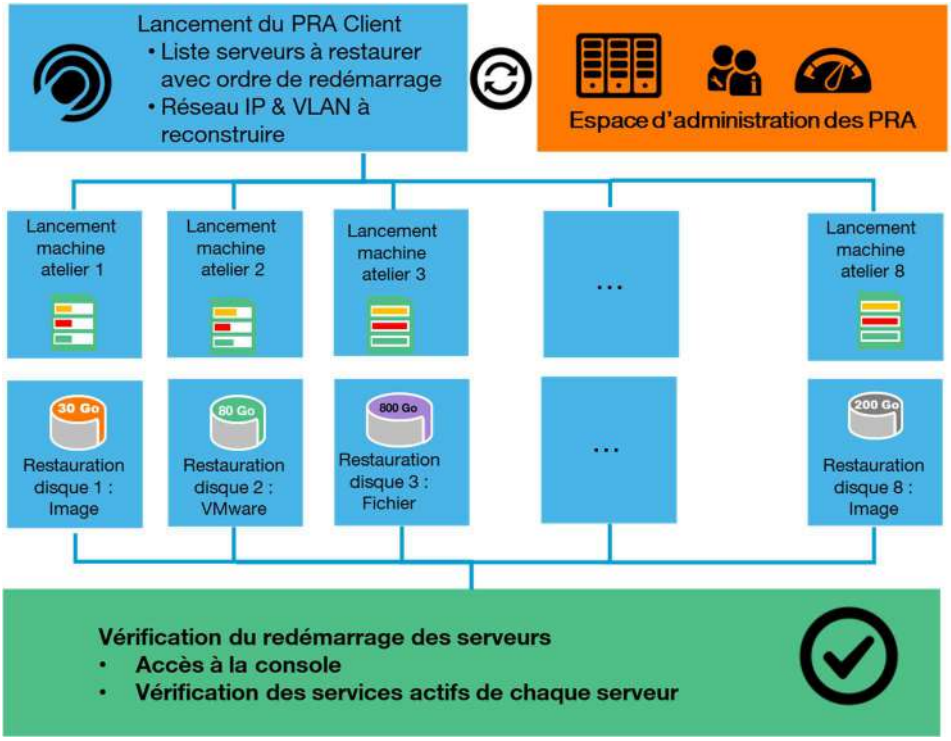
Sur option payante, la plage d'activation de PRA en mode secours peut se faire en 24/7/365.

9.4 Exécution technique du PRA

Lors de l'exécution technique du PRA, cela lance une restauration en parallèle de l'ensemble de disques des VM du périmètre du PRA.

Les disques étant restaurés, les serveurs sont relancés

- Dans l'ordre qui a été défini par le Client (dépendances des serveurs en amont et aval).
- Avec le gabarit du serveur (CPU/RAM) indiqué dans la Console.
- Chacun des serveurs est analysé pour en vérifier son fonctionnement et un rapport est généré dynamiquement dans la Console.



9.5 Adaptation de la politique de sauvegarde

Lors de la l'activation du PRA à la suite d'un sinistre, la plateforme de secours doit d'être sauvegardée. Dans ce cadre la politique de sauvegarde du système d'information peut ou doit être adaptée.

Elle le peut lorsque le Client, qui ne dispose plus de son système de sauvegarde locale, souhaite :

- Augmenter la durée de rétention des sauvegardes,
- Augmenter la fréquence des sauvegardes,
- Disposer de plusieurs solutions de sauvegarde différentes.
- Sauvegarder sur un autre région Cloud, voire sur un autre fournisseur de stockage objet.

Elle le doit, lorsque les mécanismes de sauvegarde du site nominal n'existent pas à l'identique dans le cloud de secours. Par exemple, lorsque la sauvegarde de serveurs ou VM du site nominal s'effectue via les mécanismes natifs de l'hyperviseur (VMware ou Hyper-V)

9.6 Contexte d'une cyber-attaque

Spécificités d'un scénario de crise cyber

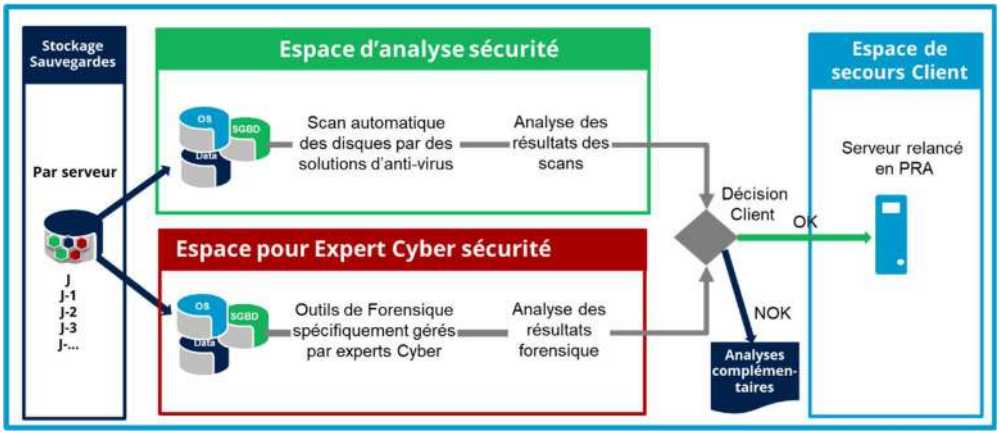
En comparaison à d'autres scénarios de crise, les crises cyber ont des caractéristiques propres qu'il est important d'appréhender :

- Une double temporalité, avec des impacts immédiats et une remédiation longue pouvant s'étendre sur plusieurs semaines, voire plusieurs mois.
- Une incertitude concernant le périmètre de la compromission.
- Une absence d'unicité de lieu de réalisation, qui sous-entend une potentielle propagation à d'autres organisations/entreprises en raison de l'interconnexion des SI.
- Une menace pouvant s'adapter aux mesures d'endiguement et de remédiation.
- Une complexité pour comprendre les objectifs de l'attaquant et attribuer l'origine de l'attaque.

Étapes optionnelles

Lors d'une crise cyber, des actions complémentaires peuvent être engagées avant la réouverture des applications aux utilisateurs :

- Exécution de scan anti-virus sur les disques et les VM
- Exécution d'outils d'investigation numérique (forensique) sur les disques et les VM



Nota : Ces actions sont optionnelles et ne rentrent pas dans le calcul du délai de RTO par serveur.

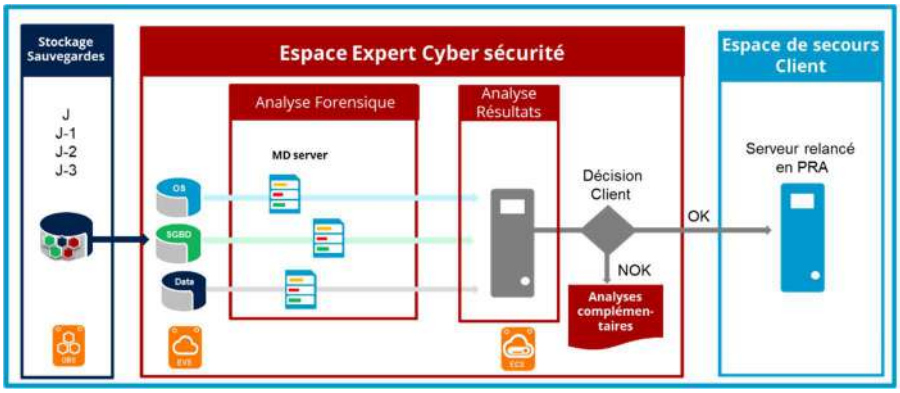
Étape supplémentaire d'analyse d'outils de forensique

Le Client peut faire appel à son prestataire ou à Orange Cyber Defense pour exécuter des outils d'investigation numériques.

Le principe est de mettre à la disposition du prestataire un environnement Cloud dédié sur lequel le prestataire pourra :

- Installer ses propres outils de forensique sur des VM de l'environnement
- Demander pour analyse, la restauration de VM dans toute la profondeur des sauvegardes disponibles
- Exécuter ses tests soit sur des disques, soit sur des VM actives

Le prestataire est en autonomie pour faire ses actions via des accès administrateurs à un environnement Cloud Flexible Engine isolé.



10 Le PRA à la demande

Pour les serveurs en classe de protection « **backup avec tests de redémarrage** dans le Cloud », le Client peut demander de réaliser :

- Sur devis : un test de PRA informatique.
- En prestation au temps passé : une assistance pour la bascule en mode PRA pour couvrir un sinistre qui rendrait le système d'information inopérant.

Cette option n'est disponible que pour les serveurs déjà protégés en mode **Sauvegarde avec tests.**

10.1 Principe du PRA à la demande

L'espace de secours est créé et activé à la demande du Client :

- Pour réaliser un test (notamment à la demande d'un client, d'un assureur ou d'une autorité de contrôle).
- Pour répondre à un sinistre ou une cyber-attaque qui rendraient le système d'information inopérant.

10.2 Reconnexion des sites Client

¨Pour la reconnexion des sites Client à l'environnement Cloud, un boitier (RCA) peut être fourni (voir le chapitre 12). Le RCA pallie la défaillance des services DNS et DHCP qui ont été détruits dans le sinistre.

10.3 Estimation du RTO (délai de mise à disposition)

Le RTO correspond à la durée de redémarrage la plus longue des serveurs protégés en sauvegarde avec tests.

Contrairement à la classe de protection PRA, le RTO n'est pas garanti dans ce mode de secours à la demande.

10.4 Estimation du tarif de PRA à la demande

Le prix de cette bascule en mode secours est composé :

- D'une prestation d'activation du mode secours
  - Sur devis (test) ou au temps passé (en cas de sinistre)
- D'une prestation de fonctionnement de l'espace de secours
  - Qui donne lieu à une redevance quotidienne basée sur les ressources de cloud consommées (VM, disques, trafic réseau…).
  - Ce prix donne lieu à un devis dans un contexte de test ou d'un détail de consommation des ressources dans un contexte de bascule en mode secours.

11 Le retour à la situation nominale

Le retour à la situation nominale consiste à la remise en service de l'infrastructure informatique telle qu'elle existait avant sinistre. Mais elle peut aussi être l'occasion de modifications pour prendre en compte le nouveau contexte lié au sinistre, comme :

- La nature du sinistre (cyber-attaque, incendie, terrorisme…),
- La portée du sinistre sur l'infrastructure informatique (destruction logique, destruction physique partielle ou totale),
- La portée du sinistre sur les métiers de l'entreprise (destruction des moyens de productions, réorientation de l'activité…).

11.1 Le périmètre des systèmes actifs dans le PRA

Lors de la bascule en PRA, après vérification du bon fonctionnement des serveurs dans le périmètre du PRA, le Client exploite cette infrastructure dans l'espace cloud PRA, pour produire les services dont il a besoin.

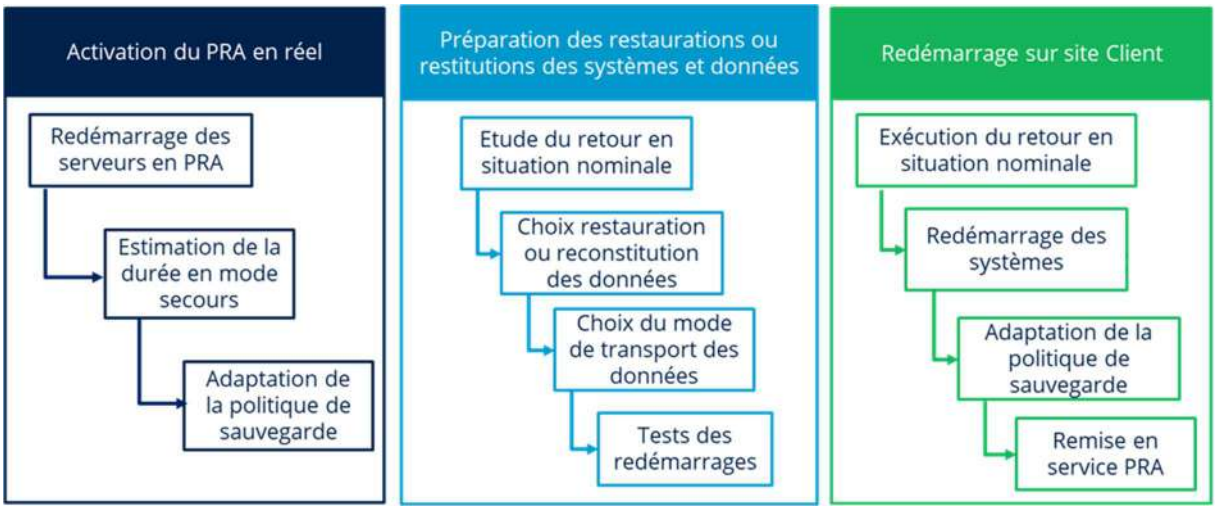
L'exploitation du système d'information dans le PRA ne se déroule pas obligatoirement dans des conditions identiques à l'exploitation dans la situation nominale.

- Certaines composantes du système d'information peuvent être indisponibles, car ne faisant pas partie du plan de secours.
- Certains serveurs en classe de protection « Serveurs en backup avec tests de redémarrage dans le cloud » devront peut-être redémarrés en mode secours à la demande en fonction de la durée estimée de traitement du sinistre.

11.2 Les phases du retour à la situation nominale

Partant de l'exploitation du PRA en réel, le retour à la situation nominale se déroule en 2 étapes complémentaires :

- La préparation des restaurations ou restitutions des systèmes et données,
- Le redémarrage des systèmes sur la nouvelle infrastructure nominale, en y intégrant les données.



Le mode de sauvegarde initial est un facteur qui influe fortement sur les solutions techniques et le processus de la restauration ou restitution des systèmes et données et le redémarrage sur site du Client.

11.3 Restauration ou reconstitution des systèmes et données

Pour le retour en situation nominale (c'est-à-dire dans l'infrastructure du Client), il existe deux solutions :

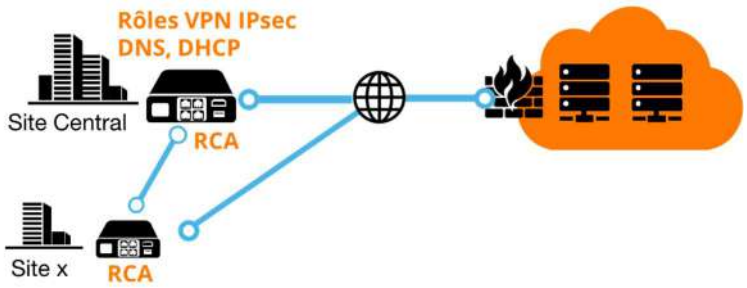
La restauration des données	La reconstitution des données
Elle utilise directement les agents de sauvegarde, à partir des sauvegardes réalisées pendant la période de bascule en PRA. La restauration prend la forme des sauvegardes élaborées pendant le fonctionnement du PRA en réel dans le cloud. Elles sont disponibles dans le Cloud, au format logique du logiciel de sauvegarde utilisé.	La reconstitution prend la forme de disques virtuels « prêts à l'emploi ». Ils sont destinés à être attachés par le Client sur les machines virtuelles dans sa nouvelle infrastructure nominale virtualisée. Ces disques virtuels sont élaborés à partir des sauvegardes réalisées pendant le fonctionnement du PRA en réel dans le cloud. Leur format est adapté en fonction de l'hyperviseur cible (format de disque virtuel compatible VMDK, VHD ou QCOW2). Flexible Recovery utilise un Atelier de reconstitution pour offrir ces disques virtuels prêts à l'emploi. Cet atelier utilise les mêmes technologies qui permettent au Prestataire d'offrir le PRA dans le cloud pour tout système, quelle que soit son origine physique ou virtuelle.

12 La reconnexion à l'environnement PRA

12.1 La reconnexion via Internet (Option)

Afin de pouvoir tester la reconnexion depuis un site en mode test (ou en réel), un boitier (RCA) peut être fourni permettant de relier par Internet les sites Client à l'environnement Cloud de secours via un tunnel IPsec.

L'offre de service intègre la **fourniture de (ou des) mini-serveur RCA avec les fonctions de services DHCP et DNS** qui seront installées sur le(s) site(s) en cas de test ou d'activation du PRA.

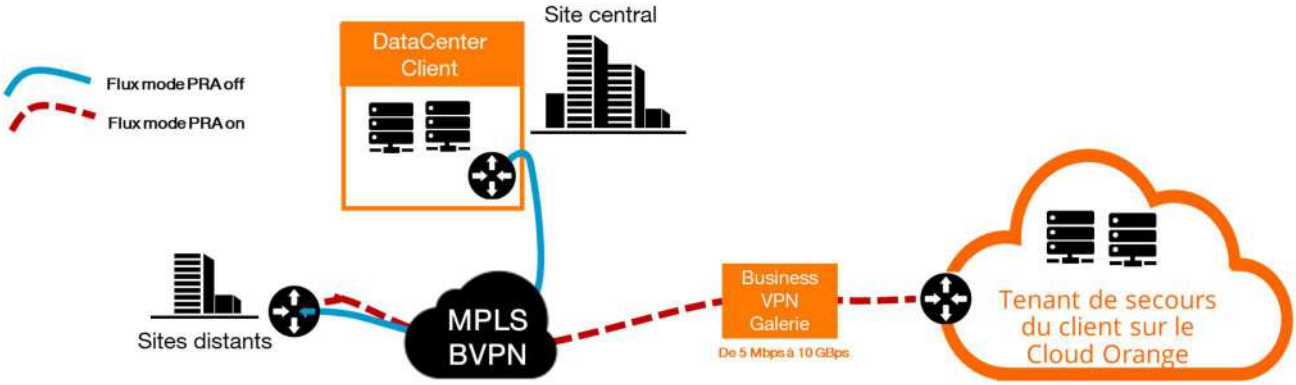


Un sinistre à l'origine de l'activation du PRA détruirait les services DHCP et DNS nécessaires au fonctionnement des postes de travail et imprimantes installés sur les différents sites de l'entreprise.

Le service DNS doit être installé à proximité des machines qui en sont clientes pour offrir de bonnes performances. Le RCA pallie la défaillance des services DNS et DHCP qui ont été détruits dans le sinistre.

12.2 La reconnexion via MPLS Orange (Option)

Dans le contexte d'un MPLS Orange (offre BVPN), en mode secours réel, via la solution Orange VPN Galerie, l'ensemble des flux des sites sont reroutés vers l'espace de secours dans le Cloud du Prestataire.

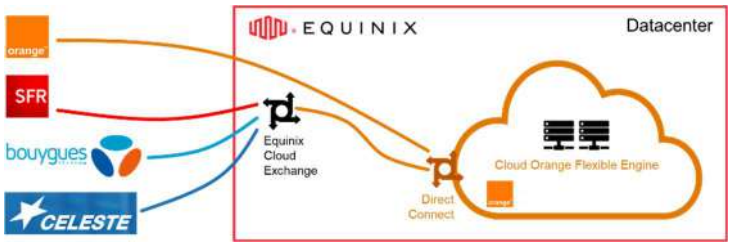


Cette solution intègre des mécanismes de bascule automatique via :

- La mise en place de routage BGP en cœur de réseau avec poids de routes différentes :
  - Accès Nominal MPLS > Accès Secours MPLS > Accès via VPN Galerie
- Depuis le Client, de procédures de redirection des flux sur condition réseau.

12.3 La reconnexion via MPLS tiers (Option)

Tout MPLS devant s'interconnecter au cloud Flexible Engine dans le cadre de l'offre Flexible Recovery doit pouvoir s'interconnecter à Equinix Cloud Exchange.

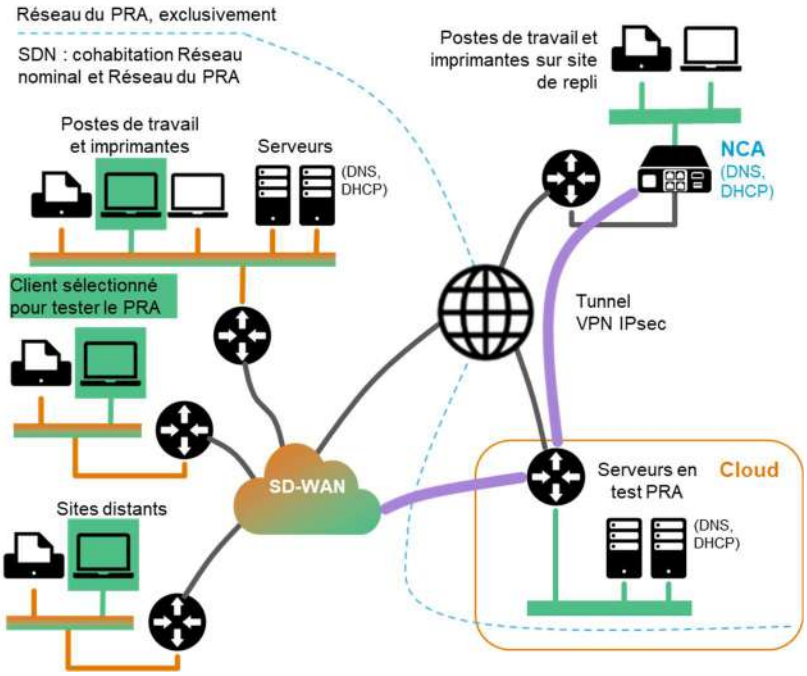


En sus, le Client est responsable de l'implémentation du routage approprié vers le PRA dans le MPLS lors du déclenchement de celui-ci.

12.4 La reconnexion via SD-WAN

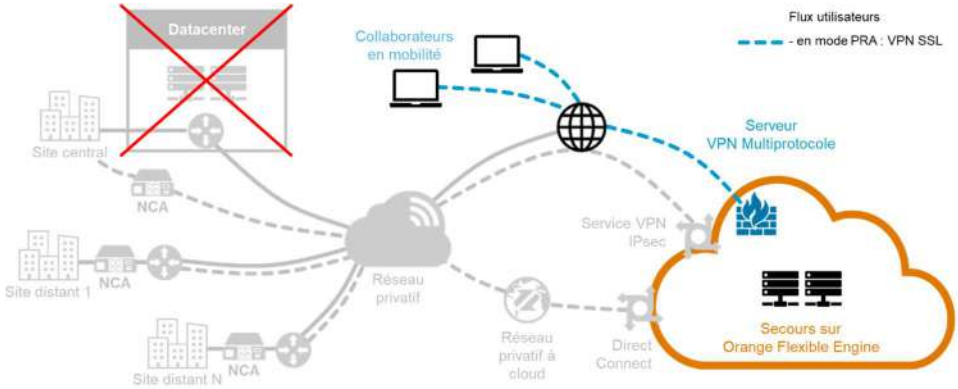
De multiples solutions de SD-WAN sont aujourd'hui déployées chez les clients, chaque solution doit être considérée de manière individuelle.

Le Client est responsable de la gestion / provisionnement des licences dans le produit de SD-WAN lié à l'utilisation / exploitation du site de PRA dans Flexible Engine.



12.5 La reconnexion des utilisateurs en mobilité (option)

L'offre de PRA dispose d'une option de reconnexion des utilisateurs via un serveur VPN adossé au réseau de PRA, permettant aux utilisateurs de se reconnecter au cloud malgré l'absence de l'Appliance de sécurité qui assurait normalement la connexion aux serveurs.



Le serveur VPN Multi-protocole (open-source) fonctionne :

- Sur tous type d'appareils numériques (Tablette, mobile, …)
- Avec plusieurs protocoles : L2TP / IPSEC (natif Windows)

13 SLA

13.1 Respect des RTO

Le RTO par serveur est défini initialement au travers du questionnaire de qualification rempli par le Client.

Ce RTO dépend des informations fournies par le Client, notamment sur la taille des disques des serveurs qui est un des éléments clefs du RTO d'un serveur.

- Le RTO des serveurs est vérifié semestriellement lors du test de secours informatique et est disponible dans le rapport de test PRA disponible dans la Console Flexible Recovery.
- En cas de non-respect du RTO, Le Prestataire s'engage à fournir une proposition de plan d'action pour revenir au RTO initialement prévu
    - Il est convenu que si les données du serveur incriminé ont évolué entre temps (augmentation supérieure de 15% de l'espace disque utilisé), un nouveau RTO du serveur devra être arbitré.

Le Prestataire s'engage à respecter les RTO définis dans les conditions suivantes :

- Les serveurs sont remis en service dans l'ordre et avec les priorités définies au lancement du projet et accessibles dans la Console Flexible Recovery.
- Les résultats des temps de restauration unitaires des serveurs sont disponibles dans la Console Flexible Recovery.
- Les équipes du Prestataire n'ayant pas accès au système d'exploitation du serveur redémarré, les éventuelles manipulations à faire pour remonter les services qui ne redémarrent pas automatiquement seront à la charge du Client.

13.2 Respect des RPO

Le RPO par serveur est défini initialement au travers du questionnaire de qualification rempli par le Client.

Lors de la mise en œuvre du projet, le RPO est défini par serveur et par disque.

Le RPO dépend de plusieurs paramètres dont certaines ne sont pas dépendants du Prestataire, notamment :

1. La bande passante réseau WAN (Internet, MPLS, …) disponible pour réaliser la sauvegarde
2. La plage horaire disponible pour réaliser la sauvegarde
3. La capacité de l'infrastructure Client à réaliser la sauvegarde : bande passante sur le réseau local interne, capacité en IO et CPU de l'infrastructure.

En cas de non-respect du RPO d'un serveur, Le Prestataire devra proposer au Client des axes d'amélioration pour respecter les RPO qui pourront être :

- Soit à la main du Prestataire : refonte et optimisation des plans de sauvegarde, nouvelle planification, …
- Soit à la main du Client : augmentation bande passante réseau WAN, plage horaire disponible pour réaliser la sauvegarde, …

13.3 Réponse sur incident critique

Incident critique : interruption totale ou partielle non programmée du Service, notamment la console de pilotage du PRA, dans des conditions qui affectent sévèrement le fonctionnement du Service. Ces conditions ont un impact sur plusieurs Clients et requiert une action corrective immédiate 24h/24 et 7j/7.

Tout Incident « critique », c'est-à-dire ayant un impact sur les activités du Client fera l'objet (à l'issue de son rétablissement), d'un envoi par Le Prestataire auprès du Client d'un Compte Rendu d'Incident communiqué sous dix jours ouvrés.

Le Compte Rendu d'Incident devra au minimum comporter les informations suivantes :

- La date et l'heure d'apparition de l'incident
- Le niveau de gravité
- Son statut (fermé / suivi / ouvert)
- Les actions entreprises, détaillant pour chaque action, dans la mesure du possible :
  - Date / heure
  - La personne en charge de l'opération
  - Les raisons de l'intervention
  - Le résultat de l'action
  - La date prévue de correction s'il y a lieu ou de clôture

13.4 Tests de PRA

Suivant la fréquence définie dans la proposition, des tests de secours informatique sont réalisés avec le Client. Ces tests sont planifiés en commun au moins 30 jours avant la date retenue.

Les tests donnent lieu à un compte-rendu de test disponible pour le Client dans la Console Flexible Recovery.

13.5 Performances

Les temps de réponse du Service, que ce soit la durée d'exécution des sauvegardes/restaurations ou bien l'affichage des pages de la Console Flexible Recovery sont dépendants de la performance de l'accès Internet du Client (bande passante, temps de transit, erreurs…).

13.6 Disponibilité de l'infrastructure en cas d'activation du PRA

Pour la disponibilité de l'infrastructure cloud (sous-jacente à l'offre et intégrée dans l'offre Flexible Engine), se référer au document Qualité de Service de Flexible Engine et notamment au taux de disponibilité des infrastructures IaaS (https://cloud.orange-business.com/wp-content/uploads/2019/03/flexible_engine-qualite_de_service.pdf) .

(Le Taux de Disponibilité de l'infrastructure Flexible Engine sous-jacente est de 99,99% pour les services de Compute et de 99,9% pour les services de Stockage Objet.)

14 Prestations complémentaires

Il peut s'agir de prestation en amont de projet ou durant le cycle de vie de la solution Flexible Recovery (liste non exhaustive).

14.1 Expertise et Conseil

Les prestations complémentaires d'expertise et de conseil peuvent être opérées par les équipes Flexible Recovery

- *Business Impact Analysis* : identification des procédures critiques, impacts potentiels d'une interruption, objectifs de reprise, développement du plan de reprise)
- Architecture :
    - Optimisation de serveurs de l'infrastructure (e.g. structure de serveurs de fichiers)
    - …
- Rédaction de procédures de crises
- Organisation du retour arrière après activation du PRA (retour en mode nominal) : en fonction de la durée de secours dans le cloud, les mécanismes de secours peuvent être adaptés :
    - Soit par la mise en place de mécanismes inverses dès la remise en service du site nominal Client
    - Soit par le transfert de données par un moyen externe (type NAS SSD) pour rapatrier les données
    - Soit par l'optimisation des services cloud pour rester dans le modèle cloud

14.2 Assistance technique

- Prestations de support en mode secours :
    - Adaptation de la politique de sauvegarde dans le Cloud pour les modifications rendues nécessaires par la bascule en mode Cloud Flexible Engine
    - Assistance à l'adaptation des gabarits des serveurs en cas de performance dégradée de certaines applications
    - Assistance à l'identification d'incidents de production
    - Assistance sur l'état de santé des serveurs en utilisant des outils dédiés de cyber sécurité
    - Redémarrage de services non intégrés dans le périmètre de protection classe PRA (pare-feu, filtrage…)
    - Installation de nouvelles applications à partir d'images Cloud existantes
    - Transfert de sauvegardes
    - Renforcement du niveau de sécurité …
- Gestion de crises cyber : assistance aux experts cyber en remontant d'autres environnement isolés de l'environnement de secours du Client pour que ceux-ci puissent faire des investigations numériques
- Reconstruction de serveurs en dehors du périmètre PRA
- Test et relance de serveurs dans d'autres classes de protection
- Mise en œuvre d'Appliances de sécurité complémentaire
- …

14.3 Tarif des prestations

Le tarif des prestations complémentaires fait l'objet de précisions soit dans la proposition technique et commerciale envoyée au Client dans le cadre de la souscription du contrat, soit dans des devis spécifiques.

Ces prestations peuvent se faire à l'heure, à la demi-journée ou à la journée.

14.4 Processus de commande

En cas de besoin urgent de prestations complémentaires, notamment en cas de bascule en mode secours, un processus simplifié de validation de prestations pourra se faire via échange de mail.

Ceci sera complété par la validation par le Client d'un bon de commande formel rédigée par le Prestataire.

15 Conditions de prix

15.1 Prix

Le Service comporte des frais de mise en œuvre et une redevance mensuelle définis dans la Proposition technique et Commerciale. La Proposition Technique et Commerciale définit également les coûts d'évolution ou d'interventions complémentaires (ajout, retrait ou évolution de services ; activation du mode PRA en mode secours)

Sauf dispositions contraires les tests de restauration et de PRA s'effectuent en Heures Ouvrées (HO). En cas de réalisation en Heures Non Ouvrées (HNO), un complément de prix sera appliqué.

Sauf stipulations dérogatoires indiquées au Bon de Commande, l'échéancier de facturation est le suivant :

- Pour les **Frais de Mise en Service** :
  - Facturation de 40% à la commande
  - Facturation du solde à l'issu du premier test de secours informatique
- Pour la **redevance mensuelle** :
  - Facturation mensuelle, terme à échoir.
- Pour les services complémentaires (activation de PRA sur la plateforme de secours, tests en HNO…) :
  - Facturation à terme échu.

15.2 Révision de prix

Les prix font l'objet d'une révision annuelle à chaque premier jour du mois de la date anniversaire de la Date d'Effet du Contrat], par application de la formule suivante :

$P = P_{-1} * [½ (S/S_{-1}) + ½ (Eqpt/Eqpt_{-1})]$

Dans laquelle :

- **P** est le prix révisé, **P-1** est le prix en vigueur avant la date de révision,
- **S** est le dernier indice Syntec publié à la date de la révision, **S-1** est l'indice Syntec publié douze mois avant la date de révision.
- L'indice mensuel Syntec est accessible sur le site www.syntec.fr,
- **Eqpt** est l'indice mensuel de prix d'importation de produits industriels (INSEE référence 10535854) publié à la date de révision et **Eqpt-1** est l'indice mensuel publié douze mois avant la date de révision.

En cas de disparition ou de non-publication d'un de ces indices, il sera remplacé par un indice d'effet comparable.

16 Réversibilité

Au terme du Contrat, le Client pourra récupérer l'ensemble des données sauvegardées dans son Espace de Sauvegarde sous forme d'un média (disque dur externe, NAS SSD …), sur acceptation d'un devis par le Client dans les conditions visées à l'article « Réversibilité » des Conditions Spécifiques Cloud.