v. 2 décembre 2012

Extrait de
Plan de Continuation d'Activité
Octopuce

Introduction

Octopuce est un hébergeur d'infrastructures web, opérateur Internet indépendant, et fournisseur d'infogérance pour ses clients.

Une garantie de qualité de service et de redondance est proposée à nos clients, qui dépend du type de contrat qui leur est propre.

Ce document énumère les problèmes que nous avons identifiés comme dépassant le service habituellement fourni par Octopuce à ses clients, afin de garantir la meilleure qualité de service en cas de problème majeur, et ceci dans tous les aspects de la chaîne de production d'Octopuce : matériel, puissance de calcul, données, réseau, support.

Chaque question posée verra sa *potentialité* et son *impact* mesurée entre 1 et 5. La profondeur de la réponse apportée sera bien entendu proportionnelle à ces 2 facteurs, qui représentent la *gravité* d'une situation.

Chaque question sera accompagnée de la réponse à apporter, des personnes responsables et de la communication vers le client proposée dans ce cas. Si besoin, un dispositif de retour à la normale sera décrit.

Niveaux de qualité de service

Chaque client dispose d'un niveau de qualité de service garantie, dont les caractéristiques sont les suivantes :

niveau 1 :

- Le client dispose d'un seul serveur capable de fournir le service.

- La sauvegarde de ses données est effectuée sur le même site toutes les nuits, avec conservation de 7 images quotidiennes, pour pouvoir remonter rapidement (montage réseau) le service en cas de panne matérielle ou de perte de données. Une sauvegarde sur un site distant est aussi en place, qui nécessite d'être restaurée pour rendre le service à nouveau opérationnel

niveau 2 :

- Le client dispose de 2 serveurs physiques distincts (à double adduction edf & réseau) capables de fournir le service. Ces 2 serveurs sont situés dans 2 baies distinctes du même datacenter, aucun SPOF local n'est présent.

- Les backups distants disposent de plusieurs images et peuvent être remontés rapidement (montage réseau)

niveau 3 :

- Le client dispose de plus de 2 serveurs physiques distincts capables de fournir le service, ces serveurs sont situés sur au moins 2 sites distincts. Aucun SPOF global n'est présent. La bascule inter site peut être effectuée manuellement ou automatiquement selon la criticité des transations de l'application concernée.

Services non pris en compte dans ce document

Ce document ne prend pas en compte les questions répondues au quotidien et en situation normale par Octopuce. Voici un résumé ni exhaustif ni détaillé de ces situations et ressources allouées :

- L'accès à Internet dans les locaux d'Octopuce où nous assurons le service de support en journée est redondé

- Existance d'une personne d'astreinte 24/7/365 recevant les alertes Nagios par SMS, disposant à tout moment d'un ordinateur avec accès à Internet, d'un accès au VPN d'Octopuce permettant l'accès aux LANs d'administration, de l'accès à la copie distante de l'Octomanager (intranet d'Octopuce), des contacts 24/7 des NOC dans les datacenters où nous disposons d'équipements réseau ou hébergemenet.

- Double supervision par Nagios des services : supervision interne complète (tous les services, logiciels, systèmes d'exploitation et matériels) et supervision externe des services réseaux (depuis un opérateur tiers, ping, http etc.). Chaque service réseau étant supervisé séparémment en IPv4 et IPv6

- Tout système d'exploitation infogéré par Octopuce est installé sur un espace disque à redondandance de données RAID 1, 5, 6 ou 10, permettant de se prémunir contre toute panne de disque dur HDD ou SSD. Aucune exception.

- Nos routeurs BGP (en bordure du réseau d'opérateur indépendant qu'est Octopuce) sont redondants sur leurs transits et situés dans des baies distinctes. Aucun routeur n'a une mesure de bande passante au 95e centile supérieur à 50% de sa capacité réseau.

- Nous ne sommes présents que dans des datacenters disposant d'une redondance totale (double adduction réseau, edf, onduleurs, groupe électrogène, climatisation) et d'une sécurité physique suffisante (présence humaine 24/7, accès biométrique, caméra)

- Nous disposons, dans chaque baie de serveur, d'une machine de secours non utilisée et non branchée, nous permettant de remonter toute partie d'infrastructure en panne matérielle dans les plus brefs délais.

- Perte ou fuite de données confidentielles : La sécurité d'Octopuce a fait sa réputation, notamment en terme de confidentialité et de non pénétration (ne comprenant pas les problèmes applicatifs du client). Les clients disposant de données confidentielles sont systématiquement installés sur un partition entièrement chiffrés avec le système LUKS, utilisant la couche cryptographique du noyau Linux. Les sauvegarde de ces clients utilisent le logiciel de sauvegarde incrémentale cryptographique duplicity.

- Les documentations internes d'Octopuce sont disponibles :

    * sur l'intranet d'Octopuce (panel.octopuce.fr) où l'on trouve l'ensemble des serveurs, leurs site, adressage, configuration et graphiques divers, ainsi que les contacts email et sms de chaque client.

    * sur notre outil de gestion de projets (projets.octopuce.fr) où l'on trouve les procedures générales d'administration, et les infrastructures spécifiques par client.

Ces documentations sont répliquées quotidiennement sur notre infrastructure de supervision secondaire dans un datacenter et sur le réseau IP du groupe Iliad, indépendant d'Octopuce.

Contenu de chaque chapitre

Chaque chapitre abordera un problème précis traité par la PCA.

Chaque problème comprendra les sections suivantes :

Problème: description du problème, détection, cas exclus de ce processus etc.

Réponse: réponse apportée par cette PCA

Responsable: personne responsable du traitement du problème

Escalade: action entreprise en cas de non réponse ou de délai de traitement supérieur à la normale.

Point de vigilance [mois-année]: défaut potentiel ou avéré sur lequel une action interne est à envisager pour éviter la non applicabilité de la réponse.

Voici donc les différentes situations prises en compte dans notre PCA à ce jour :

Attaque DDOS

Nous avons prévu les 2 types d'attaques DDOS classiquements traitées :

Problème: attaque DDOS par saturation des routeurs (de nombreux petits paquets)

Nos routeurs étant protégés contre ce type d'attaque, c'est l'infrastructure client qu'il faut protéger dans ce cas. En cas de dépassement d'un certain nombre de PPS (variable dans le temps) le routeur nous alerte d'une attaque potentielle.

Réponse : Nous procédons à l'installation, au cas par cas, et le temps de l'attaque, de règles de pare-feu sur l'infrastructure client, pour ignorer les paquets d'attaque.

Problème: attaque DDOS par remplissage (saturation des débits sur nos liens de transit)

Notre supervision externe détectera une telle saturation, constatant une perte importante de paquets sur l'arrivée de notre réseau.

Réponse: Octopuce étant opérateur indépendant, nous contrôlons nos annonces BGP sur l'Internet. La mise en place de routes dites BlackHole[1] par RTBH est prévu dans la fiche wiki "routage bgp"[2] de notre Intranet. Le client attaqué sera donc indisponible le temps du DDOS, mais sans impact sur les autres infrastructures.

Les autres attaques (syn flood, aspiration de site, password dictionnary, hash collision etc.) n'ont pas d'impact critique sur nos infrastructures et sont généralement traitées au cas par cas avec nos clients.

Responsable: Adminsys d'astreinte

Escalade: si pas de traitement du problème dans l'heure, escalade automatique de la supervision vers la direction d'Octopuce

Panne électrique ou climatisation sur un site

Problème: En cas de panne électrique ou de climatisation sur un site, notre supervision externe le détectera

- soit par l'accès aux sondes thermiques du site concerné

- soit par l'absence de ping des infrastructures du site concerné

Notez que ce cas n'est qualifié que lorsque la température dépasse le seuil de fonctionnement, ou que la panne électrique entraine le défaut de certaines infrastructures, soit par non relai des alimentations double, soit par échec de la bascule du STS.

Réponse:

Dans les 2 cas, les clients de niveau 1 sont ignorés. Si la température dépasse le seuil de fonctionnement prévu, les serveurs concernés seront éteints.

Les clients web de niveau 2 sont basculés au niveau DNS sur une page web d'annonce spécifique à ces derniers, située sur un autre site.

Les clients de niveau 3 sont basculés sur leur infrastructure secondaire, soit manuellement (via la personne d'astreinte) soit automatiquement (avec vérification de la personne d'astreinte).

Dans tous les cas, un appel téléphonique et l'ouverture d'un ticket de support auprès des reponsables du datacenter correspondant est effectué

---

1 Exemple de routage BlackHole chez Hurricane Electric https://www.he.net/adm/blackhole.html
exemple chez un autre de nos transitaires : https://apps.db.ripe.net/whois/lookup/ripe/aut-num/AS29075.html

2 https://projets.octopuce.fr/projects/admin/wiki/TransitInternet

Responsable: Adminsys d'astreinte

Escalade: si pas de traitement du problème dans l'heure, escalade automatique (par la supervision) vers la direction d'Octopuce

Retour à la normale : En cas de retour à la normale, la bascule des clients de niveau 2 est automatique, celle des clients de niveau 3 est automatique ou manuelle, au cas par cas (selon le type de transactions concernées)

Point de vigilance [2012-12] : s'assurer du contrôle par notre équipe des entrées DNS A des domaines concernées par les niveaux 2 et 3. Soit via nos DNS (primary/secondary/tertiary) soit via l'accès à des infrastructures tierces décrites dans la page wiki des infrastructures clientes concernées.

Perte de données

En cas de perte de données "normale" à savoir si un client ou un défaut matériel provoque la perte de données client, les sauvegardes standard sur site sont mises en oeuvre. Leur supervision étant assurée, ce cas est traité par le support habituel d'Octopuce.

Cependant, en cas de perte majeure de données, le processus suivant est prévu.

Problème: On appelle perte majeure toute perte de données consistant en **à la fois** les données du client (serveur de production) **et** les sauvegardes locales de ce dernier.

Réponse:

Les clients de niveau 1 sont restaurés en derniers si d'autres clients sont concernés

Les données des clients de niveau 1 sont restaurées et la machine relancée ensuite

Les données des clients de niveau 2 ou 3 sont montées directement via NFS depuis la baie de backup, et l'infrastructure relancée dans l'élan.

Un contact téléphonique ou par mail avec les clients de niveau 2 ou 3 est obligatoirement mis en oeuvre avant de relancer l'infrastructure sur sa sauvegarde.

Responsable: L'Adminsys d'astreinte, qui préviendra dès le début de la procédure la direction d'Octopuce.

Escalade: Pas d'escalade prévue (le client étant inclus dans les décisions de ce processus dès le début)

Perte majeure de matériel

Problème: On appelle perte majeure de matériel toute destruction de serveur le rendant inutilisable, concernant plus que le nombre de serveurs de secours disponible sur le site concerné par la destruction.

On note tout d'abord la faible probabilité d'une telle perte : Tout datacenter ayant des systèmes anti-incendie non destructifs, seul un incendie dans nos baies est susceptible de provoquer une telle perte.

Réponse: En cas de perte majeure de matérielle, la reprise d'activité se fait selon l'ordre suivant :

- les clients de niveau 3 puis 2 concernés par cette perte sont remis en production avant les clients de niveau 1.

- les machines de secours éventuelles d'autres sites sont déplacées sur le site endommagé pour reprendre l'activité au plus vite

- les graphiques de consommation de ressource (I/O, RAM, CPU) des machines endommagées sont analysés pour permettre une répartition optimales des machines virtuelles sur les serveurs remis en place (quitte à tasser un peu) le temps de retrouver un service normal. La virtualisation nous permet ainsi une plus rapide remontée en puissance, même si en mode dégradé pour certaines infrastructures.

- les machines virtuelles sont restaurées depuis les sauvegardes locales, soit les sauvegardes distantes sont déplacées sur le site sinistré pour restauration si les locales sont aussi endommagées.

- Une commande de matériel est immédiatement déclenchée si besoin, soit pour revenir à une situation nominale des services, soit pour revenir à une situation nominale des machines de secours.

Le contact avec les clients concernés doit être immédiat, ainsi que le contact des assurances d'Octopuce et d'eventuelles assurances clients dans le cas où le matériel lui appartiendrait.

Responsable: L'Adminsys d'astreinte, qui préviendra dès le début de la procédure la direction d'Octopuce.

Escalade: Pas d'escalade prévue (le client étant inclus dans les décisions de ce processus dès le début)