Sécurisation des services

Visiocommunication Professionnelle

1. Les enjeux partagés avec nos clients et nos partenaires

1.1. Choix de notre partenaire d'hébergement

UBIQT a choisi les partenaires les plus exigeants pour ce qui concerne la sécurisation et la qualité de ses services afin d'assurer à ses clients un taux de disponibilité et une qualité du service optimum.

1.2. Maitrise des services délégués

Les services managés pour nos clients sont un de leurs actifs important qui servent souvent de vitrine de leur image aux effets de résonance multiples de l'Internet : bons et parfois mauvais. Nous avons compris la nécessité pour nos clients de continuer à maitriser la qualité de leurs services confiés à nos équipes. UBIQT et ses partenaires intègrent plusieurs niveaux de contrôles périodiques pour maintenir à niveau ces exigences:

- UBIQT met en place des audits de sécurité récurrents sur ses services et assiste régulièrement ses clients à des revues en commun avec ses clients ;
- UBIQT assure la gestion des changements de son portefeuille de services hébergés pour ses clients, pilote les modifications des versions des services en production et fait le travail préparatif en amont avec les partenaires de nos clients pour anticiper les procédures de retour arrière nécessaires à ces modifications en production ;

1.3. Les applications critiques au cœur de notre stratégie

UBIQT a pour ambition d'apporter aux entreprises, des services et systèmes de communication innovants pour répondre à leurs besoins critiques pour leur fonctionnement.

- Nous vous accompagnons, tout au long du cycle de vie de vos projets : diagnostic et définitions des besoins, conception, déploiement, exploitation, préconisations en termes d'évolutivité ;
- Nous mettons en œuvre des solutions qui sont personnalisées et réalisées, totalement ou en partie sur mesure ;

1.4. Nos valeurs

Expertise unique pour accroître votre performance

Votre activité repose désormais en grande partie sur la qualité de votre infrastructure de communication. Nous pouvons vous aider à transformer cette infrastructure pour que capital humain, processus et technologies forment un tout cohérent au service de vos intérêts. Nous contribuons à la mise en place de solutions de communication vitales pour toutes les entreprises, des multinationales aux PME. Nous vous écoutons, vous et vos clients. Et nous exploitons les connaissances acquises pour perfectionner compétences et techniques. Aujourd'hui, nous mettons les meilleures pratiques à votre service, quel que soit votre secteur d'activité : de l'évaluation de la sécurité à la gestion de la transformation IP dans votre entreprise, partout dans le monde.

1.5. L'hébergement de votre service en responsabilité

- La performance de l'hébergement est maintenue à son niveau optimal grâce à un système de surveillance des applications hébergées, de la charge et des temps d'accès ;
- Une astreinte est assurée en 24/7 avec des profils techniques directement opérationnels sur vos services ;
- UBIQT met en place des procédures d'administration automatiques, afin de surveiller l'environnement et de pouvoir immédiatement intervenir dans les meilleures conditions en cas de problème matériel ou système de la machine ;

1.6. Le management d'applications au quotidien

Nos services de management d'applications portent à la fois sur l'infrastructure technique de la plate-forme (parties matérielles et logicielles) ainsi que sur le bon fonctionnement applicatif global du service. Cette expertise matérielle et applicative mise au service du client permet ainsi de :

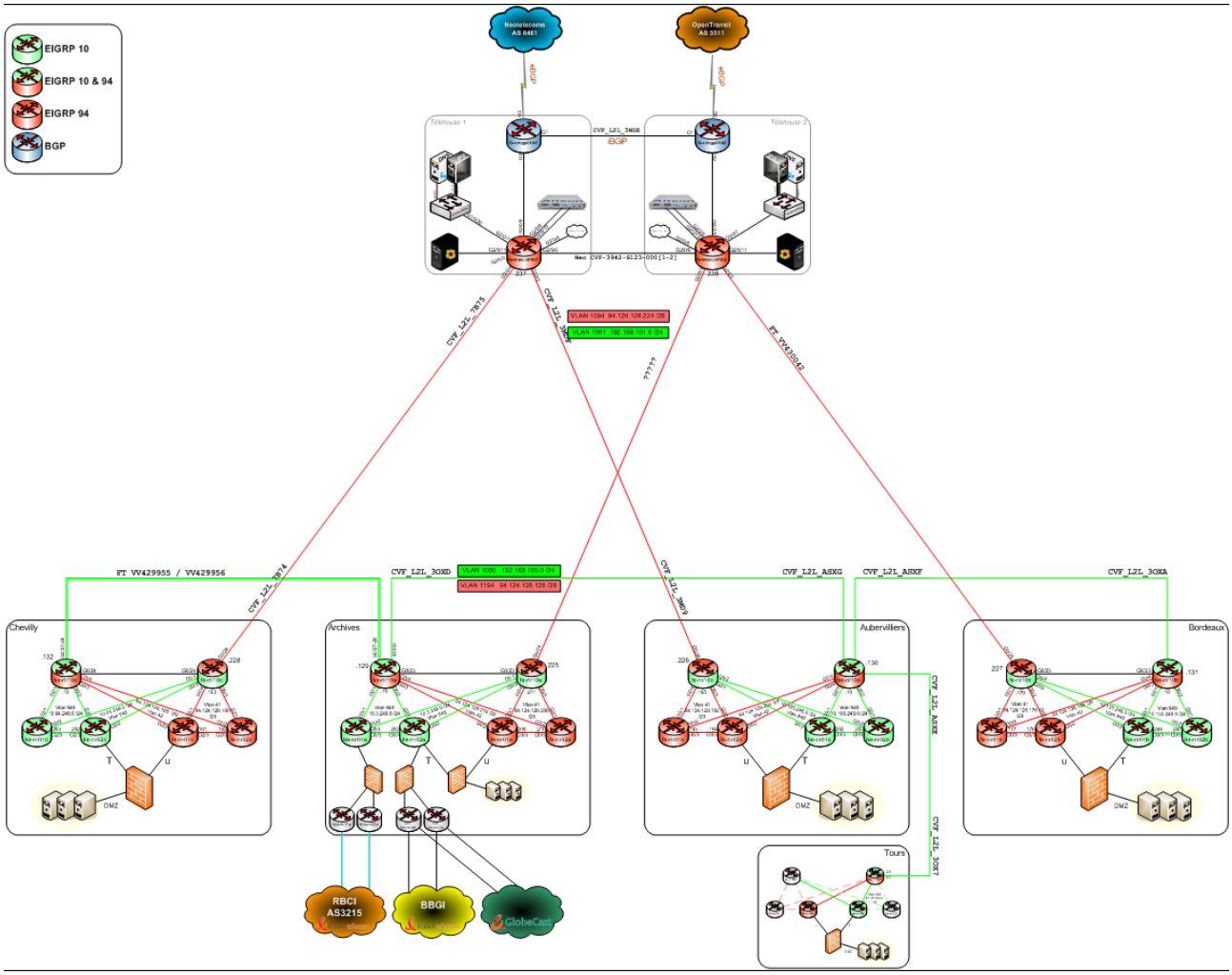
- surveiller le comportement de l'application
- réaliser la gestion de la configuration des équipements et logiciels
- réaliser une astreinte pertinente vis-à-vis du comportement des applications
- constituer une expertise en support pour les analyses des informations statistiques délivrées par le Responsable de Plateforme de Service (RPS) dans son rapport mensuel.
- réaliser et maintenir la documentation technique
- suivre et respecter les engagements pris dans le cadre du contrat SLA

2. La sécurisation de vos services

2.1. Configuration réseau et télécom

2.1.1 Réseau d'accès mutualisé

UBIQT gère elle-même ses liens de raccordement entre ses sites a travers ses parteinaires. L'architecture est entièrement redondée pour maintenir la continuité du service en cas d'incident sur un lien ou sur un équipement backbone. Ce réseau est Gigabit et multi opérateurs.



2.1.2 Les accès opérateurs présents

UBIQT a travers ses prestataires dispose de son propre AS (AS12807) avec la gestion de son plan d'adressage. Il est raccordé aux opérateurs Open transit (AS5511) et Néo Télécom (AS8218) par des liens 1 Gbps.

2.1.3 Bande passante accessible

UBIQT dispose d'une réserve de plusieurs centaines de Mbps disponible pour des besoins client. Nous avons la capacité de faire évoluer notre infrastructure en cas de besoin client. Il est possible de limiter la bande passante utilisée par les services en fonction de l'adresse IP publique et du port utilisé si besoin.

2.2. Qualité de l'environnement de la salle technique

2.2.1 Sites

Les sites utilisés pour l'hébergement de nos plates-formes de services sont les suivants :

- Site Aubervilliers,
- Site Chevilly,

Seules les équipes d'exploitation ont un accès permanent sur site 24h/24 7j/7. En cas de besoin une demande d'accès temporaire doit être demandée avec un délai de prévenance de 48h ouvrées. Les 2 sites retenus sont certifiés non inondable, non sismique et très faible niveau de risque SEVESO.

2.2.2 Alimentation électrique

Le site d'Aubervilliers est alimenté par 2 arrivées électriques de 15 000 volts délivrés par EDF. Les équipements hébergés sont alimentés par 2 chaînes de 400kVA. Le site est équipé d'un groupe électrogène d'une autonomie de 150 heures. Le site de Chevilly est alimenté par 2 arrivées électriques de 20 000 volts délivrés par EDF. Les équipements hébergés sont alimentés par 2 chaînes de 800kVA. Le site est équipé d'un groupe électrogène d'une autonomie de 72 heures. Sur chacun des sites, les baies disposent de 2 équipements PDU raccordés chacun sur une arrivée électrique différente disposant de son propre disjoncteur

2.2.3 Climatisation

Site d'Aubervilliers

- La climatisation de la salle d'hébergement est réalisée par 2 unités de climatisation sur réseau d'eau et 2 unités détente directe. L'utilisation de 2 unités suffit à refroidir la salle. La puissance des climatiseurs est de 400kw.
- L'hydrométrie de la salle est gérée par les unités de climatisation. La température en salle est de 21°C + /- 1,5°C, l'hygrométrie est entre 50 +/- 5 %.

Site de Chevilly

- La climatisation des salles d'hébergement est assurée par un ensemble d'unité de climatisation à détente directe et dispose d'une redondance de n+20%.
- Le dispositif de climatisation dispose d'une brumisation automatique des aérocondenseurs au-delà de 40°C pour assurer le fonctionnement nominal de la climatisation lors de canicule.
- La température et le taux d'humidité (hygrométrie) des salles sont mesurées en continu. la Température en salle est de 20°C + /- 1°C, l'hygrométrie est située entre 50 +/- 5 %.

2.2.4 Sécurité anti-incendie

Site d'Aubervilliers

- La salle d'hébergement est protégée contre l'incendie par un système de détection au niveau du faux plafond et du faux plancher et d'un système d'extinction automatique. Le gaz utilisé est un gaz neutre pour étouffer un feu naissant.
- Les alarmes sont remontées au PC sécurité du site et au NOC (network Opérating Center)

Site de Chevilly

- La salle informatique est protégée contre l'incendie par un système de détection et d'extinction automatique. La détection est placée aussi bien en faux-plancher qu'en ambiance. L'extinction

automatique a lieu lorsqu'il y a une double détection. La technologie choisie est l'utilisation d'un gaz neutre pour étouffer un feu naissant.

- Les alarmes incendie sont raccordées sur une centrale de supervision installée dans la salle technique différenciée des salles machines. Un report des alarmes ''feu'' et ''dérangement'' est réalisé vers le poste de sécurité du pôle de supervision.

2.2.5 Sécurité anti-intrusion

Chaque site dispose de son propre système de détection anti-intrusion avec remontée des alertes aux centres de supervisions. Sur chacun des sites, le processus d'accès aux salles d'hébergement comprend :

- un gardiennage sur place 24 heures/24 et 7 jours/7 ;
- une liste des personnes habilitées par le client à accéder à ses équipements ;
- un contrôle de l'identité des personnes par le gardien ;
- une main courante des entrées-sorties des personnes.
- Le parcours d'accès aux équipements est
- contrôlé par badge ;
- vidéo-surveillé en continu et les enregistrements des images sont stockés pour être vus le cas échéant (40 jours glissants)

2.3. Equipements réseau et sécurité

2.3.1 Les pare-feux

Les flux traversant la plate-forme et les réseaux virtuels (VLAN) qui la composent sont analysés et filtrés par une paire de pare-feu. Ces pare-feu sont les garants du respect de la matrice de flux implémentée pour répondre au bon fonctionnement de la plate-forme. Afin de garantir une sécurité optimale, la configuration appliquée est du type « tout trafic non expressément autorisé est rejeté ».

Les pare-feux installés sont doublés et fonctionnent en mode actif/passif : à un instant « t », seul un pare-feu est réellement actif. Il filtre les flux des différentes zones et échange avec le pare-feu passif les informations sur les sessions actives. En cas de défaillance du pare-feu actif, l'ensemble des flux est repris en charge par le second qui devient de fait le nouveau pare-feu actif. Le basculement s'effectue en quelques secondes, sans perte des sessions utilisateurs ni dégradation de performances : Le dimensionnement de la plate-forme et des équipements est prévu pour fonctionner aux performances nominales avec un seul équipement pare-feu en production.

2.3.2 Load balancer / reverse proxy

Afin de garantir une disponibilité maximale de nos services managés, un mécanisme de répartition de charge est implémenté au sein de l'infrastructure mutualisée. Ce système repose sur l'utilisation de deux serveurs LVS à haute disponibilité spécialisés dans la gestion du trafic et fonctionnant dans un mode actif/passif.

- fonctionnalité de répartition de charge (« load-balancing »)

- chaque service est identifié par une adresse IP virtuelle (publiée dans les DNS et utilisée pour accéder au service),
- des serveurs sont regroupés dans des « fermes » : Ensemble machines rendant le même service,
- les LVS assurent la répartition de l'ensemble des connexions arrivant sur l'adresse IP virtuelle vers les serveurs situés dans les « fermes ».

Deux protocoles sont gérés : TCP, UDP

Trois méthodes de routage peuvent être implémentées :

- Via du NAT (Network Address Translation) [méthode utilisée par défaut par UBIQT]
- Via IP Tunneling
- Via Direct Routing

Divers algorithmes de répartition sont disponibles :

- Round-Robin: Dans cette configuration, la répartition fonctionne de manière cyclique, sans se préoccuper de la charge des serveurs. La première requête sera affectée au 1er serveur, la seconde au second serveur, ainsi de suite en boucle.
- Weighted Round-Robin: Même technique que l'algorithme précédent, en ayant la possibilité d'attribuer des poids aux serveurs.
- Least-Connection : Le load-balancer possède une table des connections actives. Il renverra toute nouvelle requête au serveur possédant le moins de connexions actives, dynamiquement.
- Weighted Least-Connection : Même technique que l'algorithme précédent, en ayant la possibilité d'attribuer des poids aux serveurs. [méthode utilisée par défaut par UBIQT]
- Locality-Based Least-Connection : Le load balancer choisit un serveur réel dans un groupe en fonction de l'adresse IP de destination. Il est utilisé dans les clusters de cache.
- Locality-Based Least-Connection with Replication : Même technique que l'algorithme précédent, avec une fonctionnalité supplémentaire : si tous les serveurs du groupe sont surchargés ou indisponibles, il choisit un serveur dans un autre groupe pour l'affecter au 1er groupe de serveurs.
- Destination Hashing : Affecte la requête arrivant à un serveur d'un groupe fixé dans une table de hashage, en fonction de l'adresse IP de destination.
- Source Hashing : Affecte la requête à un serveur réel en fonction de l'adresse source round robin.

Le répartiteur de charge assure également le monitoring des nœuds de la ferme de manière à détecter les éventuelles pannes et ne répartir les requêtes que sur les machines opérationnelles. La persistance de session peut si besoin être assurée par le biais du LVS (l'adresse IP source). Une fonctionnalité de reverse-proxy peut être implémentée. Cette fonctionnalité n'est pas prise en compte dans cette proposition. Cette prestation ferait l'objet d'une proposition complémentaire.

2.3.3 Commutation Ethernet

Un groupe de 2 commutateurs assurent à la fois :

- la commutation Ethernet (carte de commutation),
- la segmentation en VLANs,
- matériel : Un ensemble de commutateurs Cisco de type Catalyst 2960G

2.3.4 Cache

Les caches utilisés sont des BlueCoat ProxySG 8100. Caractéristiques techniques :

- Protocole gérer en mode proxy : HTTP, HTTPS, CIFS, SSL, FTP, MAPI, P2P, SOCKS, AOL IM, Yahoo IM, Microsoft IM, MMS, RTSP, QuickTime, TCP-Tunnel
- Accélérateur SSL
- Capacité de traitement : 3000 req/s – 350 Mbps

Ces équipements permettent d'accélérer le temps de réponse des différents sites en prenant à leur charge la délivrance du contenu statique et ainsi allègent le débit réseau vers la plateforme mais aussi la charge des serveurs qui ont moins de requêtes à traiter.

Le temps pendant lequel la page est « cachée » par cet équipement peut être positionné par type de fichier (jpg, html, gif ….)

2.3.5 Maintenance des équipements réseau et sécurité

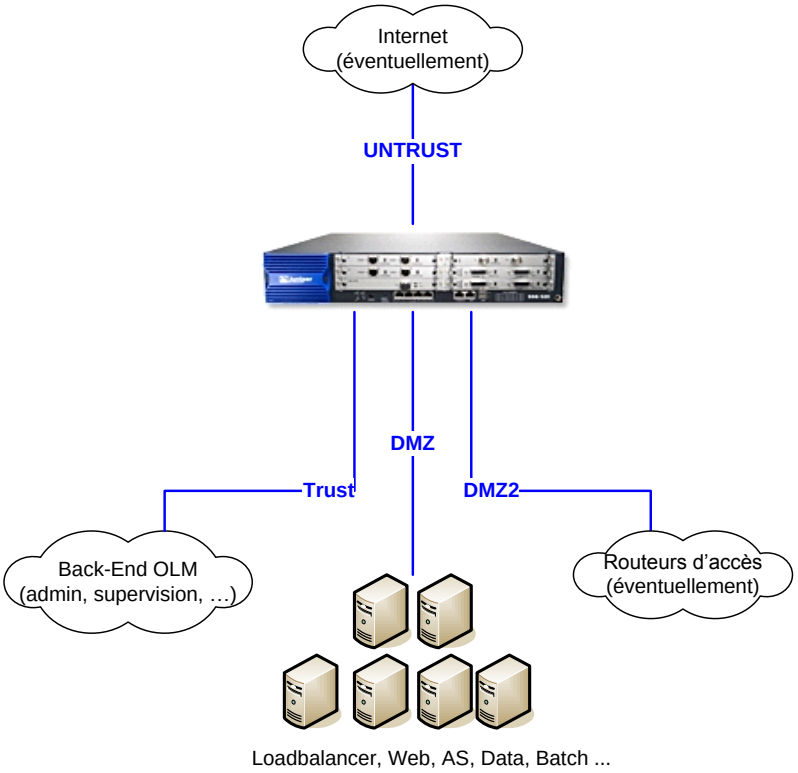
Tous les équipements réseaux font l'objet d'un contrat de maintenance

- J+1 jour ouvré sur la partie matériel
- 24/7 sur la partie logicielle

Pour tous les équipements, UBIQT dispose de matériel en spare.

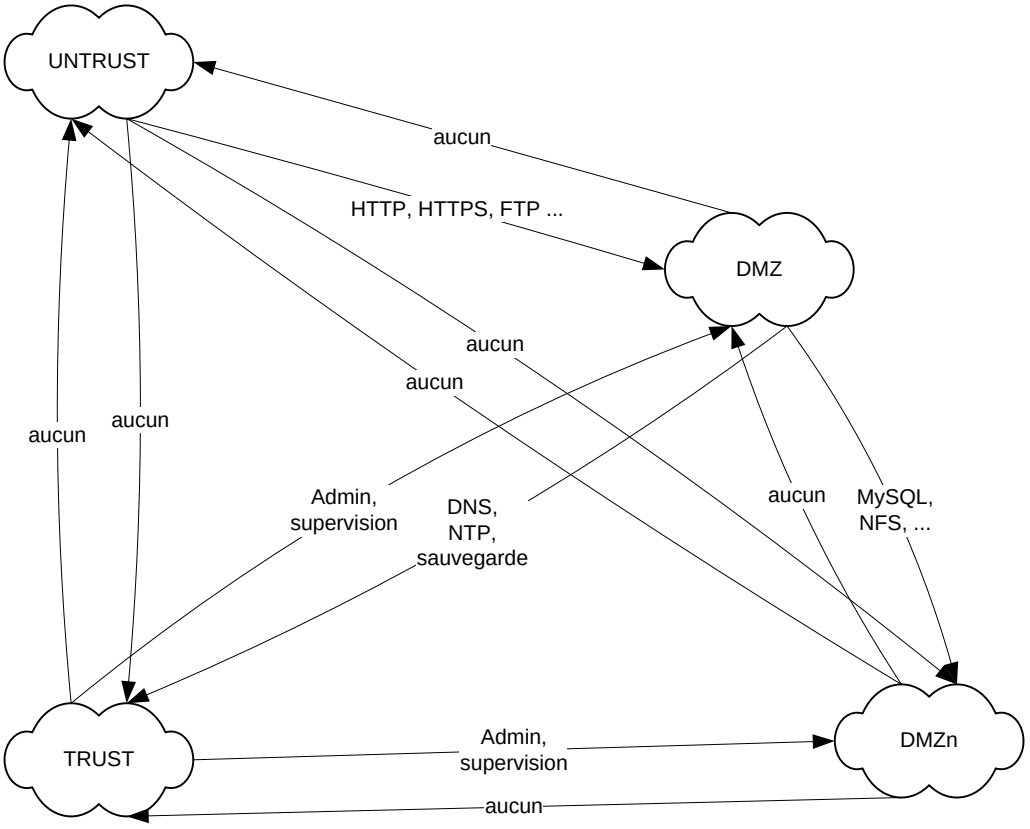
2.4. Sécurité des applicatifs

La ferme de services UBIQT est protégée par un couple de pare-feu en mode haute disponibilité (HA) actif/passif avec échange de la table des sessions. Ces pare-feu, véritables policiers de la plate-forme, régulent les accès entre les serveurs de la plateforme et les systèmes externes, les utilisateurs et contributeurs externes, les entités d'administration de UBIQT.


Internet
(éventuellement)
UNTRUST
DMZ
Trust
DMZ2
Back-End OLM
(admin, supervision, …)
Routeurs d'accès
(éventuellement)
Loadbalancer, Web, AS, Data, Batch ...

Les zones physiques d'un pare-feu de ferme :

- zone « TRUST » : la zone de confiance qui relie la ferme UBIQT au backend UBIQT
- zone « UNTRUST » : la zone non protégée du pare-feu de ferme, contient lorsque nécessaire peut contenir un raccordement à un accès public de type Internet
- zone « DMZ » : le compartiment principal de la ferme, ne contient que des serveurs du service concerné, en l'occurrence les serveurs d'application
- zone « DMZn » : les n DMZ supplémentaires de la ferme, peut contenir des accès de type routeur client



Détection d'intrusion : exemple à plusieurs niveaux de protection

A l'intérieur des différentes zones physiques, les différentes zones fonctionnelles de la plate-forme sont cloisonnées en VLANs. Les flux inter-VLANs sont intégralement analysés et filtrées par les pare-feu et/ou les châssis de commutation : Aucun flux entre ces zones ne peut passer sans avoir été autorisé sur ces équipements.

Cependant, la sécurité ne se limite pas à cette couche. En effet, au niveau du front-end de UBIQT et de sses partenaires, une sécurité logique a été mise en place grâce aux équipements IDS. Il s'agit d'un équipement en coupure de notre alimentation réseau internet, pare-feu réseau et applicatif transparent (ne disposant pas d'interfaces IP donc non vulnérable aux attaques IP) équipé d'un logiciel de détection et blocage d'intrusion.

Cet équipement constitue un premier niveau de filtrage qui évite l'inondation de trafics malsains dans notre architecture réseau. Il déjoue les scans de port, les floods et autres pré-attaques ou attaques réseau.

Il bloque également, au plus haut niveau de notre réseau les URL malicieuses générés par vers ou virus extérieurs. De surcroît, ce pare-feu nous permet d'opérer, en cas d'urgence, un filtrage général sur l'ensemble de nos fermes sans devoir intervenir unitairement sur chaque pare-feu. Il dispose également d'un module de sécurisation applicative permettant de vérifier l'exactitude de l'ensemble des transactions par rapport à la grammaire des protocoles employés. Cette technologie permet ainsi de s'affranchir des attaques de type applicatif (débordement de tampon, identification des versions installées…).

Un second IDS est positionné en port mirroring mais ne dispose pas non plus d'interface IP. Contrairement au premier, il n'est pas en coupure de l'accès internet mais en port-mirroring (un switch lui fait une copie de tout trafic entrant/sortant sur internet). De ce fait, il détecte, alerte, mais ne bloque pas les anomalies. Le logiciel Prélude installé sur cette sonde nous donne donc une vision sur ce que le premier IDS ne voit et donc ne bloque pas. Ses logs sont régulièrement étudiés. Ils permettent notamment d'écrire de nouvelles règles de filtrage des URL malicieuses.

Dans le cadre de la veille sécurité incluse au titre de l'hébergement, les versions logicielles des différents composants de la plate-forme (OS, pare-feu, …), sont maintenus à jour quotidiennement afin de prévenir toute faille susceptible de représenter une menace pour la plate-forme.

Résumé des moyens en œuvres

- Déni de service
- IDS en tête de réseau
- Protection par les pare-feu de ferme
- Protection par application d'un traffic shaping
- Scan
- Blocage des tentatives de découverte réseau par les pare-feu de ferme
- Spoofing
- Outil dédié permettant de détecter le spoofing au sein des fermes
- Signalement et blocage des tentatives de spoofing externes à la ferme par les pare-feu de ferme
- Virus/Ver
- IPS applicative en tête de réseau
- Passerelle mail sécurisée avec AntiSpam et AntiVirus
- Poste utilisateur sécurisé : AntiSpyware,AntiVirus, FW personnel
- Backdoors
- IDS applicative en tête de réseau
- Analyseur de protocole alertant en tête de réseau
- Audits externes réguliers de la visibilité d'UBIQT – online multimedia depuis l'extérieur
- Faiblesse des mots de passe : Usage d'une passerelle sécurisée de connexion, Audit permanent des mots de passe (crackage)

UBIQT à travers ses partenaires dispose donc:

- en standard, des certificats auto-signés pour la pré-production,
- en option, la fourniture et la gestion de certificats serveur SSL de 128 bits, un pour chaque URL à sécuriser.

2.5. Sauvegarde des données

La sauvegarde des serveurs est assurée par le logiciel Arkeia. L'ensemble de la robotique associée à l'architecture de sauvegarde est entièrement dédiée à la zone d'hébergement : Il n'y a aucun lien entre cet environnement de sauvegarde et celui utilisé pour les applications internes du système d'information de UBIQT. En standard, UBIQT et ses partenaires prévoit :

- une sauvegarde totale toutes les semaines, avec rétention pendant 30 jours,
- une sauvegarde incrémentale quotidienne, avec rétention pendant 30 jours,
- un archivage du sous ensemble nécessaire 1 fois par mois; conservé pendant 1 an

La sauvegarde des données est de type "Disk to Disk to Tape", toutes les semaines nous effectuons une sauvegarde totale sur disque puis quotidiennement une sauvegarde incrémentale, ces sauvegardes ont une rétention de 30 jours. Une fois par mois les données sont archivées sur bandes avec une rétention de 1 an. La sauvegarde "disk to disk" est assurée par le logiciel Arkeia et des baies de disques SATA alors que la sauvegarde "disk to tape" est assurée par le logiciel Legato Networker et des librairies Overland. Pour des raisons de performances notre sauvegarde sur disque s'effectue sur site et la sauvegarde mensuelle sur bande hors site, mais nous disposons de plateformes de sauvegarde sur disque dans plusieurs datacenter et rien ne nous empêche d'effectuer des sauvegardes sur disque hors site.

Les sauvegardes sont contrôlées par notre plateforme de supervision, plusieurs tests sont effectués, vérification de la création des bandes, vérification des sauvegardes mensuelles, vérification des taches de sauvegardes en cours, surveillances des librairies. Un Intranet met à disposition du RTS (Responsable Technique de services) et du RPS (Responsable de plateforme de services) des rapports quotidiens. Nous utilisons l'outil SystemImager pour créer des images systèmes qui nous permettent de restaurer la totalité d'un système en cas de crash d'un serveur.

2.5.1 Alerte danger système d'interruption du service

En dehors du processus interne de gestion des crises, nécessaire au respect des engagements de service, la prestation de service client inclut une procédure d'escalade pour informer nos clients lors d'incident grave (bloquant ou majeur) et définir alors avec lui le plan d'actions adéquat. Ce processus de crise est déclenché lorsque les délais de traitement d'un incident bloquant ou majeur risquent de dépasser les engagements contractuels pris par UBIQT.

La procédure est déclenchée :

- soit à l'initiative de UBIQT,
- soit à l'initiative de nos clients; qui prennent alors contact avec l'interlocuteur désigné dans la liste des interlocuteurs en escalade, mentionnée dans Plan d'Assurance Qualité; cet interlocuteur qualifie la demande Client avant de déclencher la procédure d'escalade.

Lors du déploiement de l'Application, le Responsable Plateforme de Services (RPS) définit avec La Poste les conditions d'application de la gestion des escalades. Il définit notamment avec le client pour chaque type d'incident, bloquant ou majeur, les noms, coordonnées et critères d'appel des différents managers et directeurs à alerter côté client en cas d'incident. Ces informations sont consignées dans le Plan d'Assurance Qualité.

Lorsque la procédure d'escalade est déclenchée, le Responsable Plateforme de Services (RPS) devient, en période d'heures ouvrables, l'interlocuteur privilégié de La Poste pour la résolution de cet incident. Il vérifie

que la procédure d'escalade est bien respectée et coordonne l'ensemble des actions nécessaires pour corriger le dysfonctionnement.

Les alertes remontées sont traitées de la façon suivante :

- les équipes du Service Exploitation exécutent les instructions de travail adéquates et, en cas de nécessité, font appel aux équipes d'administration en heures ouvrées ou aux équipes d'astreinte en heures non ouvrées.
- le Service Exploitation assure le traitement global de l'incident, avec l'assistance le cas échéant des équipes d'administration et du Responsable Plateforme de Services (RPS), du diagnostic détaillé à la mise en œuvre des actions correctives et du contrôle du bon fonctionnement des sites.
- l'ensemble des actions menées est consigné dans l'outil de suivi du Service Exploitation.

Le Responsable Plateforme de Services (RPS) analyse les incidents majeurs ou bloquants. Son analyse porte plus particulièrement sur la détermination des causes de ces incidents et il s'appuie sur la compétence des experts de UBIQT et de ses partenaires pour établir ce diagnostic ; il peut proposer le cas échéant des prestations d'audit complémentaires sur la plate-forme ou sur l'application pour affiner son analyse.

Cette analyse lui permet de proposer des mesures correctives qui peuvent être, selon le cas, l'adaptation des procédures définies entre UBIQT et ses clients, l'évolution de la plate-forme ou des préconisations pour le développement du service.

2.6. Exploitabilité du service

2.6.1 La surveillance des infrastructures techniques et des services

Dans le cadre de son offre de services managés, UBIQT met en œuvre, pour chaque équipement dont il a la responsabilité, un environnement adapté de supervision et de gestion des alertes. Cet environnement répond à l'objectif essentiel d'alerter les équipes de supervision UBIQT des cas de dysfonctionnement afin que ces dernières puissent déclencher les vérifications et les actions prévues dans ce type de situation.

monitoring interne

L'environnement technique de supervision UBIQT repose sur la solution Hobbit. L'outil Hobbit représente le pivot central de supervision dans le sens où c'est à partir de ce dernier que sont émises les alertes à destination des équipes de supervision. Hobbit permet d'effectuer deux types de supervision, selon les possibilités des équipements :

- supervision active : Les équipements sont sollicités à intervalle régulier et la réponse à ces sollicitations est analysée. Le résultat de cette analyse conduit à l'émission ou non d'une alarme de supervision,
- supervision passive : UBIQT installe sur les équipements compatibles (i.e disposant d'un système d'exploitation accessible et paramétrable) un agent local Hobbit. Ce dernier vérifie régulièrement un certain nombre de paramètres sur le système et les émet en direction des consoles de supervision.

La supervision active disponible offre au niveau réseau (OSI 3 & 4) les possibilités de tests suivants :

- ping ICMP,
- ping TCP.

Ces tests permettent de déclencher des alarmes au niveau applicatif en cas de non réponse ou cas de dépassement d'un seuil préalablement défini : HTTP, HTTPS, DNS, FTP, IMAP, LDAP, POP, SMTP, RADIUS.

Ces tests permettent, de façon complémentaire, de réaliser une transaction (établissement de la connexion, échange de données, clôture de la connexion) liée au protocole utilisé et donc de déclencher des alarmes lorsque le résultat de la transaction n'est pas conforme au résultat attendu.

Exemple simple : un test HTTP doit renvoyer un code HTTP en 2xx ou 3xx. Dans le cas contraire, une alarme est émise. Il est possible d'affiner ce test en décrivant les données attendues dans la réponse HTTP, la taille des données attendues, les délais de réponse, etc.

La supervision passive offre les possibilités de tests suivants :

- présence de processus,
- taux de mémoire utilisée,
- taux de d'espace swap utilisé,
- taux de remplissage des systèmes de fichiers,
- charge moyenne CPU.

Chaque test est associé à un seuil défini lors de la mise en place de l'outil. Si ce seuil est dépassé, une alarme est émise.

La mise en œuvre de la supervision vise à définir pour chaque équipement pris en charge par UBIQT, les tests à réaliser par le biais de la supervision active, les valeurs « normales » attendues en réponse à ces tests ainsi que les seuils de déclenchement d'alerte. UBIQT préconise de limiter le nombre de test de supervision effectués sur chaque équipement à :

- un test de niveau réseau (permettant de s'assurer de la vitalité de l'équipement),
- un test de niveau applicatif pour chaque fonction rendue (permettant de s'assurer du bon fonctionnement du composant).

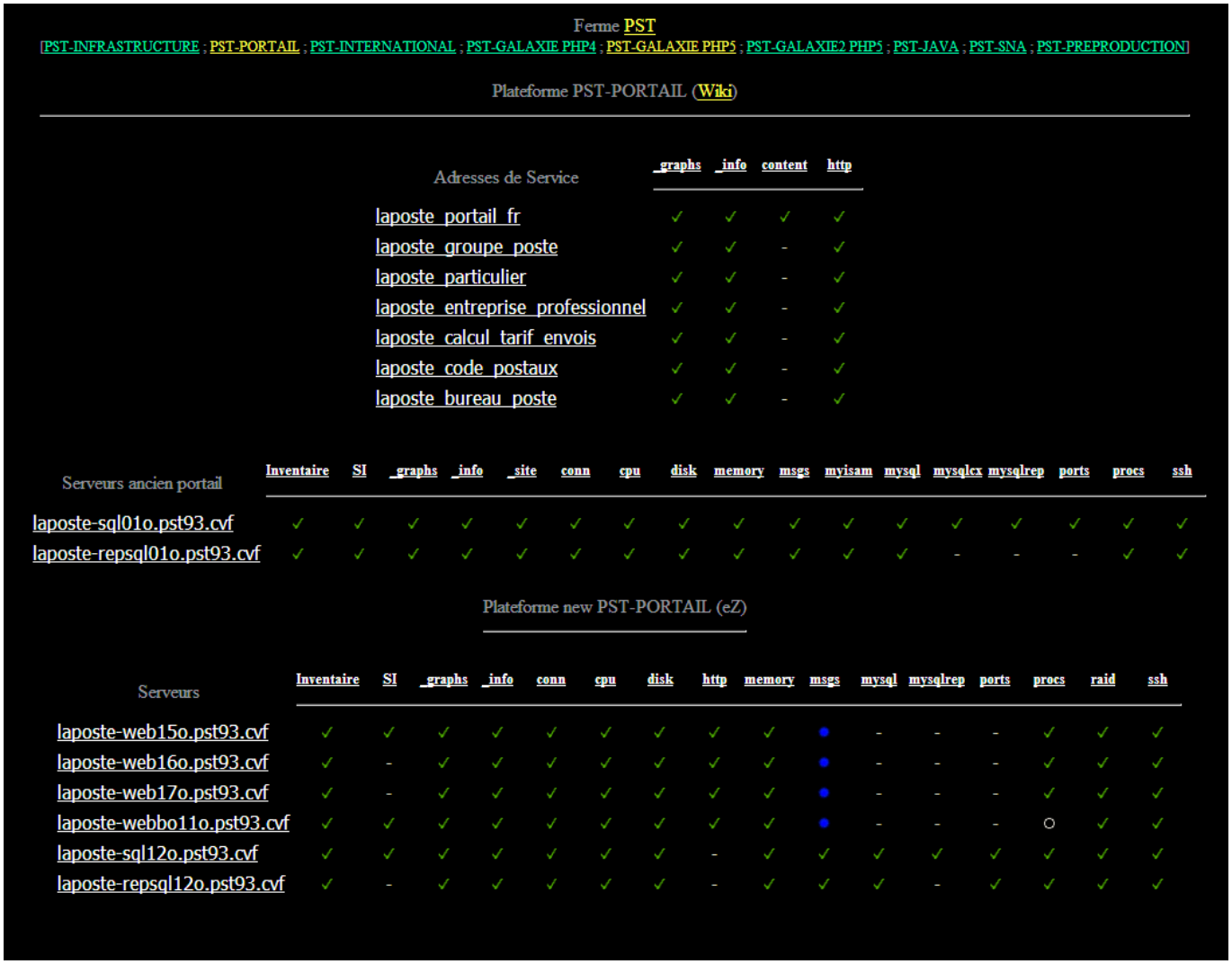
Ces règles visent à éviter les cascades d'alarme en cas d'incident et à ne pas surcharger inutilement l'équipement par des sollicitations ayant un même objectif.

La phase de mise en œuvre est également l'étape au cours de laquelle UBIQT rédige les instructions de travail associées à chaque donnée de supervision. Ces instructions de travail sont un élément important de la supervision car elles définissent :

- la corrélation à effectuer vis à vis d'éventuelles autres alarmes remontées dans la même période,
- la liste des vérifications techniques à effectuer sur l'environnement hébergé,
- la liste des actions à mener pour résoudre l'incident.

UBIQT peut définir les Instructions de Travail à dérouler lors de la détection d'un incident par la chaîne de supervision.

exemple de présentation des indicateurs



Ferme PST

[PST-INFRASTRUCTURE ; PST-PORTAIL ; PST-INTERNATIONAL ; PST-GALAXIE PHP4 ; PST-GALAXIE PHP5 ; PST-GALAXIE2 PHP5 ; PST-JAVA ; PST-SNA ; PST-PREPRODUCTION]

Plateforme PST-PORTAIL (Wiki)

Adresses de Service	_graphs	_info	content	http
laposte_portail_fr	✓	✓	✓	✓
laposte_groupe_poste	✓	✓	-	✓
laposte_particulier	✓	✓	-	✓
laposte_entreprise_professionnel	✓	✓	-	✓
laposte_calcul_tarif_envois	✓	✓	-	✓
laposte_code_postaux	✓	✓	-	✓
laposte_bureau_poste	✓	✓	-	✓

Serveurs ancien portail	Inventaire	SI	_graphs	_info	_site	conn	cpu	disk	memory	msgs	myisam	mysql	mysqlcx	mysqlrep	ports	procs	ssh
laposte-sql01o.pst93.cvf	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
laposte-repsql01o.pst93.cvf	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	-	-	✓	✓

Plateforme new PST-PORTAIL (eZ)

Serveurs	Inventaire	SI	_graphs	_info	conn	cpu	disk	http	memory	msgs	mysql	mysqlrep	ports	procs	raid	ssh
laposte-web15o.pst93.cvf	✓	✓	✓	✓	✓	✓	✓	✓	✓	●	-	-	-	✓	✓	✓
laposte-web16o.pst93.cvf	✓	-	✓	✓	✓	✓	✓	✓	✓	●	-	-	-	✓	✓	✓
laposte-web17o.pst93.cvf	✓	-	✓	✓	✓	✓	✓	✓	✓	●	-	-	-	✓	✓	✓
laposte-webbo11o.pst93.cvf	✓	✓	✓	✓	✓	✓	✓	✓	✓	●	-	-	-	○	✓	✓
laposte-sql12o.pst93.cvf	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	✓	✓
laposte-repsql12o.pst93.cvf	✓	-	✓	✓	✓	✓	✓	-	✓	✓	✓	-	✓	✓	✓	✓

monitoring externe

UBIQT peut proposer des outils de supervision et d'analyse des applications externes en partenariat avec tiers de confiance (exemple IP-Label). Les sondes statistiques installées par nos partenaires sur divers backbones permettent de tester les pages web des applications client. Les sondes simulent une connexion Internet toutes les 5 minutes (connexion à la plate-forme) ou toutes les 15 ou 60 minutes (consultation de page web).

- Les indicateurs remontés par les sondes permettent de mesurer en temps réel le temps de réponse et la disponibilité des applications :
- observations « réseau »,
- contrôle de l'accessibilité d'une adresse IP,
- disponibilité - test toutes les 5 mn,
- routage principal sur une période choisie (heure, jour, semaine),
- temps de réponse depuis un ou plusieurs points du backbone,
- observations « web »,

- temps de chargement d'une page web,
- test toutes les 15 mn,
- performance du jour, de la semaine et du mois,
- temps de chargement (connexion, dns, 1er octet, page complète),
- observation selon scénario,
- solution simulant la visite de plusieurs pages au sein d'une même application, avec ou sans authentification.

2.7. Processus d'exploitation récurrents

2.7.1 Méthodologie et Qualité des services suivant ITIL

En proposant une compilation des bonnes pratiques en matière de processus informatiques, ITIL v2 a connu le succès. ITIL v3 élargit la réflexion et propose une vision basée sur les services rendus à l'entreprise. La v3 préconise donc de maitriser le cycle de vie des services, de l'étude de l'opportunité jusqu'à la suppression du service. Les quatre processus principaux d'ITIL v3, sur lesquels s'appuie UBIQT afin de délivrer une meilleure qualité de service, sont :

- **le Service Design :** Ce processus détermine comment concevoir un service pour qu'il soit implémentable : définition de l'architecture, développement de la solution, métriques et résultats attendues. Ce processus permet notamment de définir le SLA.
- **le Service Transition :** Ce processus décrit la gestion des changements, des mises en production et des configurations. Leur mise en place permet de tester et vérifier les livrables avant toute mise en production.
- **le Service Opération :** Il concerne les activités quotidiennes. Ce processus décrit la gestion des incidents, la gestion des problèmes, la gestion des événements, la gestion des demandes et la gestion des accès.
- **le Continual Service Improvement :** Ce processus porte sur l'ensemble du cycle de vie. Il a pour objectif de vérifier que le niveau de service est réalisé grâce à la mise en place d'un système de reporting et de KPI.

2.7.2 Gestion des incidents

La supervision des plates-formes de services est assurée par les équipes de UBIQT qui traitent 24h/24 et 7j/7 les éventuelles alarmes et interviennent soit directement, soit en prévenant le collaborateur d'astreinte si besoin est (notamment en heures non ouvrées – HNO). La supervision s'effectue au travers :

- des valeurs de fonctionnement prélevées par SNMP ou en simulant certains modes de fonctionnement,
- d'une console de remontée d'alarme,
- d'un accès à l'outil de ticketing UBIQT : Outil centralisé de gestion des tickets d'incidents permettant notamment de :
- gérer des tickets pour chaque incident,
- créer une base de connaissances sur les incidents et solutions associées,

- gérer des FAQ,
- gérer les escalades,
- guider les exploitants lors des procédures d'escalade en fonction de scénarios prédéfinis et du niveau de gravité des incidents.
- d'un accès à la base documentaire des Instructions de Travail,
- d'un accès au réseau d'administration.

Les équipements sont sollicités toutes les 5 minutes par la supervision active. Les équipements qui bénéficient de la supervision passive effectuent un test toutes les 5 minutes et renvoient le résultat de ce test au serveur central de supervision. Lorsqu'un test de supervision remonte une alarme, celle-ci est présentée sur la console des équipes de supervision. L'alarme indique, outre le test en erreur et l'équipement incriminé, le nombre d'occurrences consécutives et l'instruction de travail à appliquer. Le traitement de l'alarme est réalisé à la deuxième occurrence consécutive. L'intervention débute alors par la saisie d'un ticket d'incident puis, selon la période horaire, se poursuit soit par le déroulement de l'instruction de travail associée à l'alarme, soit par l'activation des équipes d'astreinte.

2.7.3 L'administration et la surveillance des accès télécoms

La supervision des équipements réseaux est assurée par le logiciel Nagios. Il réalise également l'alerting à destination des équipes de supervision en fonction de paramètre définie par UBIQT. Les fonctionnalités du module de surveillance de Nagios sont :

- surveillance des services réseaux (SNMP,PING,HA...) des équipements interne/clients mutualisés et dédiés
- surveillance des ressources des équipements (charge processeur, utilisation des mémoires, bande passante, etc.)
- parallélisassions de la vérification des services
- utilisation d'une hiérarchie du réseau en utilisant des hôtes parents permettant la détection et la distinction entre les hôtes qui sont à l'arrêt de ceux qui sont injoignables

Les fonctionnalités du module d'Analyse de Nagios sont :

- les événements des équipements réseaux sont notifiés au format syslog
- le trafic de toute interface réseau est graphe. Les données sont collectées toutes les 5 minutes et stockées dans une base RRD propre à l'interface.

La solution Nagios dispose d'une interface web permettant de connaitre l'état du réseau en temps réel, de voir les notifications en cours, l'historique des problèmes ainsi que les fichiers de log des équipements. Cette solution nous permet aussi de réaliser une sauvegarde automatique de toutes les configurations des équipements avec versionning tous les 24h. L'infrastructure réseau et télécom d'UBIQT est entièrement redondé ce qui permet en cas de perte d'un élément (équipements ou liaisons) de maintenir les services de nos clients.

2.8. La gestion de la capacité de production

2.8.1 Relation avec nos clients

UBIQT propose à ses clients des pools de responsables technique de service (RTS) dédiés par application. Ces RTS prennent en charge toutes les activités liées au bon fonctionnement et gestion proactive du service. En se basant sur des seuils prédéfinis (moindre que les seuils remontant des alarmes au niveau de la supervision), les RTS ont alors le recul nécessaire pour diagnostiquer un problème pouvant survenir dans un avenir plus ou moins proche et cela leur permet de conseiller La Poste sur les actions palliatives à mettre en oeuvre en fonction des niveaux de responsabilités. Certains indicateurs sont définis dès la phase de déploiement du service pour La Poste. Toutefois les éléments surveillés pro-activement sont enrichis tout au long de la vie de l'application. Car c'est en suivant au jour le jour que les RTS prennent connaissance de l'application et de son comportement. Ainsi quotidiennement, un bilan technique d'exploitation de la plate-forme rendant le service est réalisé par les RTS. Le Bilan d'exploitation couvre les aspects suivants détaillés par la suite :

- applicatif – critique,
- applicatif – non critique,
- hébergement – sauvegarde,
- hébergement – indicateurs techniques,
- hébergement – Système,
- hébergement – base de données,
- hébergement – veille vulnérabilité.

Tous les bilans quotidiens sont archivés par les RTS. Ces bilans techniques d'exploitation sont la propriété de UBIQT et ne sont pas transmis à La Poste. Certains éléments peuvent toutefois être intégrés au Compte Rendu Mensuel Exploitation (CRME) fourni dans le cadre de la prestation RPS (Responsable Plateforme de Service).

2.8.2 contrôles applicatifs

Les RTS testent certaines fonctions du site, par un contrôle visuel des différentes pages et fonctionnalités de l'application qui doivent apparaître. Ces contrôles applicatifs peuvent être

- un test d'URL simple,
- un test d'URL contenant un traitement de données (passage de commande …),
- la vérification des journaux de logs applicatifs :
- les RTS reçoivent tous les matins un mail contenant les erreurs éventuelles de l'application,
- cette vérification est basée sur des mots clefs contenus dans les fichiers de logs de l'application que La Poste aura réalisée.
- les mails « Error Logs » sont archivés,
- la disponibilité du site :
- une vérification auprès des outils internes de supervision est réalisée,
- les copies d'écran de la disponibilité sont intégrées dans le CRME.

2.8.3 contrôle du bon déroulement de la sauvegarde

Lors du bilan technique quotidien, les RTS vérifient que les sauvegardes se sont déroulées comme prévues sur l'ensemble des serveurs à sauvegarder par l'intermédiaire d'un outil interne (Site portail de sauvegarde). Dans le cas où une procédure de sauvegarde ne s'est pas déroulée, les RTS demandent alors aux exploitants la relance de la sauvegarde pour le serveur impacté.

2.8.4 vérification des indicateurs techniques

Les RTS effectuent une collecte des indicateurs techniques de la plate-forme comme :

- l'accessibilité des serveurs (ICMP, TSE ou SSH),
- l'état du matériel : Suivant le type de matériel, l'outil indique l'état physique des processeurs, des ventilateurs, des alimentations, des cartes mémoires
- la charge CPU des serveurs,
- la charge mémoire des serveurs,
- le taux d'utilisation des disques : Pour chacun des disques, l'outil remonte l'occupation globale des disques ainsi que des répertoires critiques,
- l'état des disques montés en RAID indiquant si le mode de mirroring utilisé fonctionne correctement
- le nombre de sessions sur les serveurs,
- l'état physique des baies de disques externes éventuelles,
- la présence des processus nécessaires au bon fonctionnement de chacun des serveurs et des outils d'administrations,
- le temps de réponses des requêtes applicatives (définies avec La Poste).
- autres données diverses comme la date du dernier reboot des serveurs, la version des logiciels, la date de dernière application de patch …

La plupart de ces indicateurs techniques sont collectés et conservés sous forme de graphique MRTG sur l'ensemble de la journée de la veille. Les administrateurs effectuent une corrélation de ces différents indicateurs techniques afin de déterminer leur cohérence et ainsi de façon proactive déterminer si la plate-forme peut avoir un comportement amenant à des incidents. (par exemple une fuite au niveau de la mémoire qui ne se libère pas)

2.8.5 veille vulnérabilité

UBIQT met en place des moyens de détection des incidents pour toutes les attaques estimées possibles même si elles paraissent improbables. Le fonctionnement de cette veille sécurité est le suivant :

- les logiciels utilisés par l'application de nos clients sont référencés dans une base de données. Les informations telles que le nom du logiciel, sa version, son éditeur sont également enregistrées dans cette base,
- une veille est réalisée quotidiennement (en jour ouvrables) pour suivre l'ensemble des alertes de sécurité. Si une alerte de sécurité concerne un des éléments de la plate-forme de nos clients, l'alerte sera enregistrée et traitée. La veille se base sur :
- les informations des sites spécialisés (CERT, CERTA, PacketStorm, Security Focus),
- les compétences internes,

- des fournisseurs d'informations privés.
- une analyse manuelle plus fine est nécessaire pour déterminer la criticité des alertes par rapport à chaque projet UBIQT.
- selon la gravité des failles détectées, plusieurs procédures peuvent être mises en place:
- correctif non urgent : Décision en collaboration avec nos clients du processus et des délais d'application,
- correctif urgent : Si notre client a formellement communiqué son autorisation, application immédiate,
- en cas de problème menaçant l'intégrité des données, possibilité d'isoler les serveurs incriminés ou la plate-forme complète.
- reporting vers nos clients (par le RPS) pour les alertes jugées impactantes.