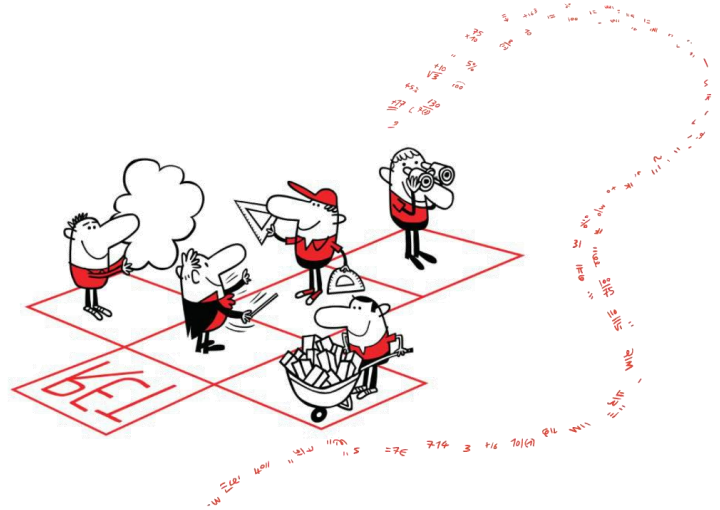
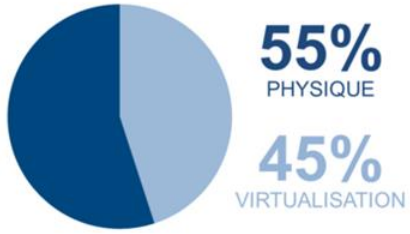


Le Cloud Interne

Stratégie Groupe L'ambition Cloud de Société Générale

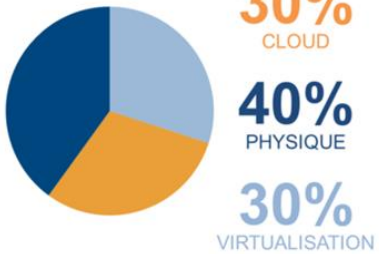
- **Pour l'hébergement d'application, SG souhaite adopter une démarche cloud hybride avec le recours au cloud interne et au cloud externe**

2014



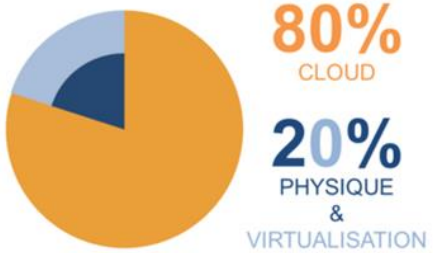
La virtualisation VM est l'offre standard

2017 *



Le Cloud Interne est l'offre standard

2020 *



80 % des OS dans le Cloud

Pour les architectures distribuées (Linux/Windows)

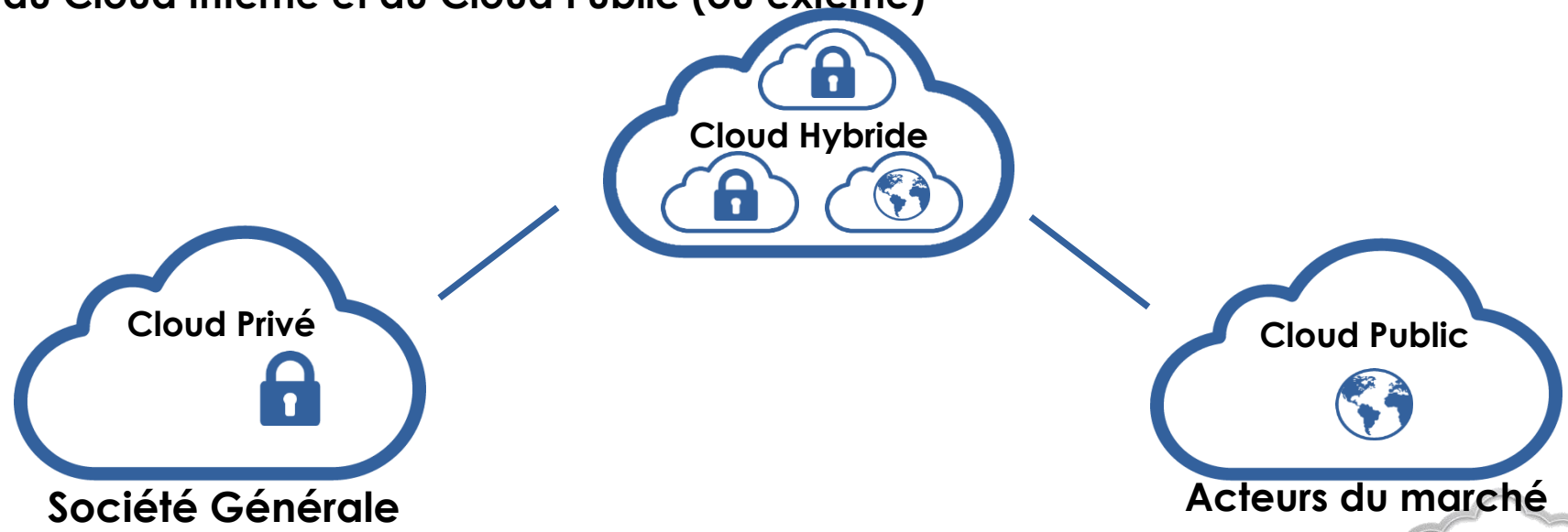
- En 2016, l'usage de cloud externe est restreint à quelques pilotes, pour un déploiement d'offre en 2017

** Cloud Interne et Externe*

Le Cloud
Modèles d'adoption

- **L'adoption du Cloud se fait en partenariat avec les DSI au sein de programmes de transformation avec des objectifs communs pour livrer plus vite et mieux :**
  - DevOpsByITIM pour iTIM
  - SOFA pour BSC

- **Pour l'hébergement d'application, SG souhaite adopter une démarche cloud hybride avec le recours au Cloud Interne et au Cloud Public (ou externe)**



Le Cloud

Les apports du Cloud pour les applications « systèmes distribués »

Pour toute nouvelle application, s'orienter vers une conception **Cloud Native en utilisant les socles Digital Client et Agence, permettra de tirer bénéfice du Cloud**

Self-Service

Capacité à commander des ressources standardisées à partir d'une interface Web ou via API

Élasticité / Robustesse

Ressources à la demande
Auto-scalling: s'adapter en temps réel
Auto-healing : l'infrastructure de « répare » d'elle-même
Mutualisation des ressources

Paiement à l'usage

- Infrastructure facturée sur la base des ressources réellement utilisées, lorsqu'elles sont utilisées
- Incitation à déployer un code plus performant => gain immédiat

Le Cloud

Réseau très haut débit

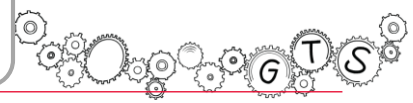
Interconnexions avec des lignes à très haut débit

Qualité

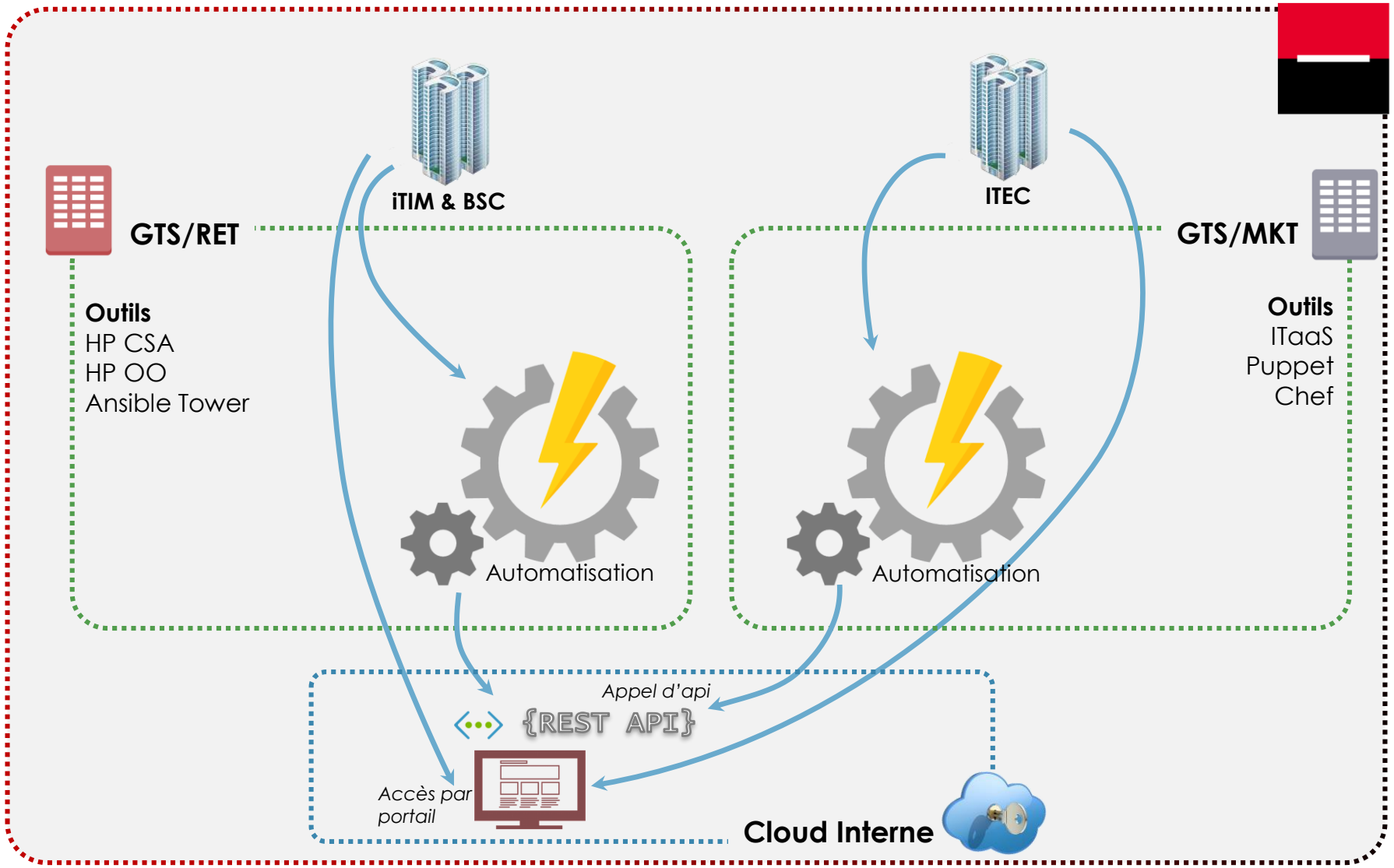
- Idempotence : capacité à reconstruire une application/service à tout moment à l'identique
- Systématisation des tests
- Automatisation des tests dès que possible

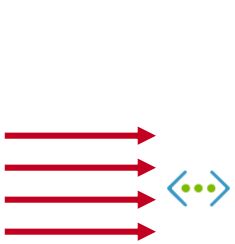
Pilotage des ressources

- Un pilotage centré sur l'application
- Prise en charge du cycle de vie complet de nos applications, dont le déploiement



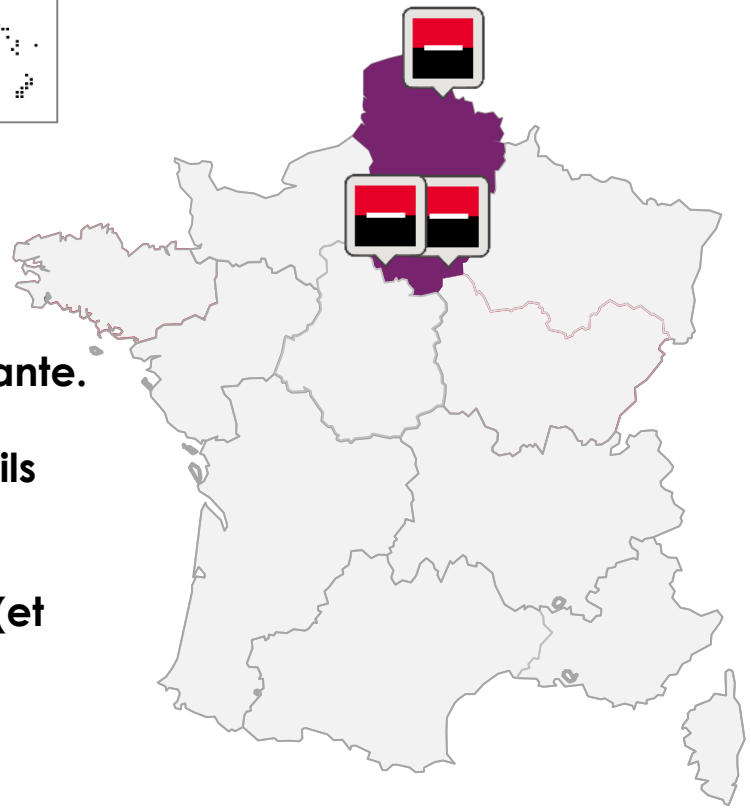
« Big Picture » Générale





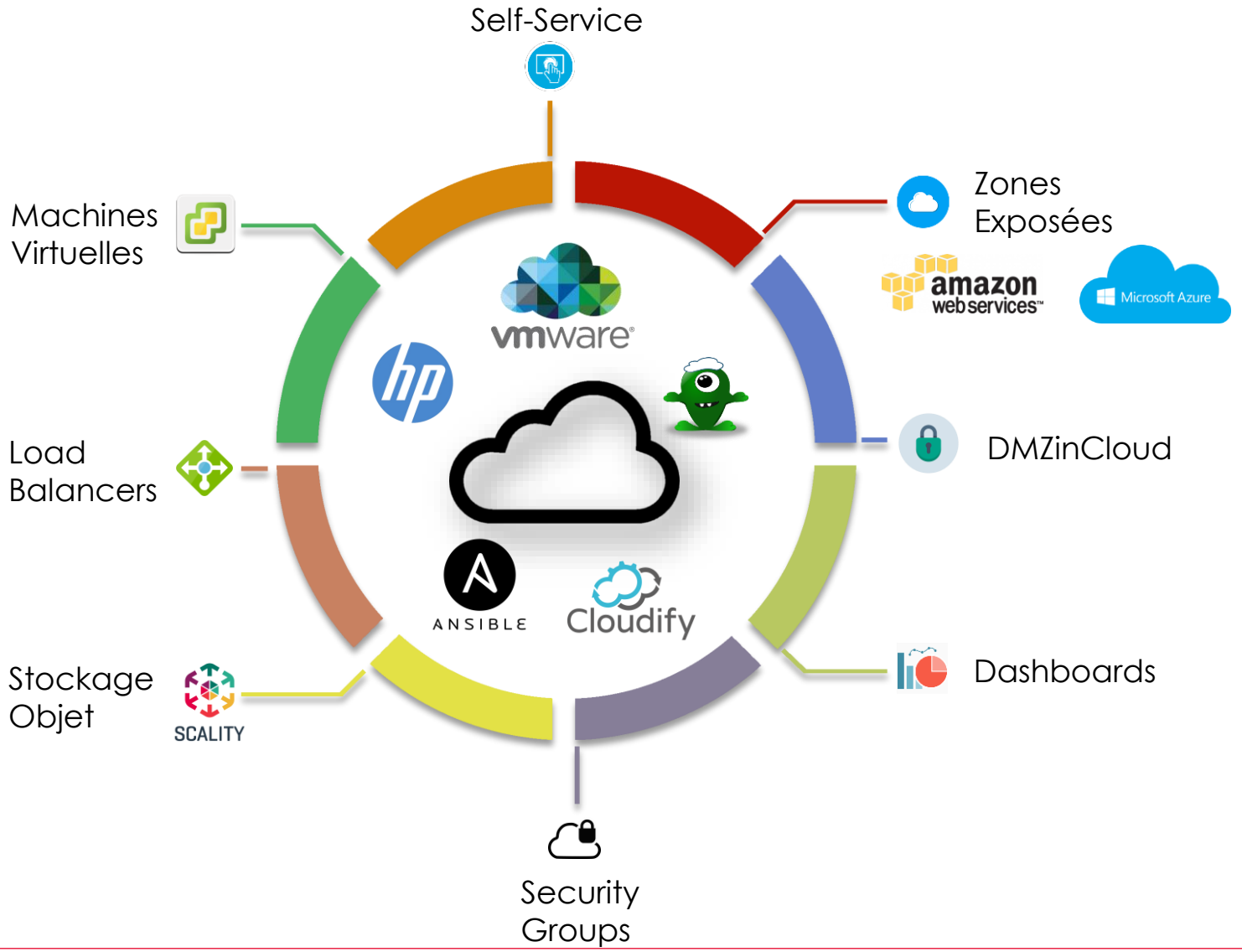
L'offre Cloud Interne – SG Cloud Regions & Availability Zones (AZ)

- **Paris : 2 Datacenters**
  - Tigery
  - Marcoussis
- **Nord : 1 Datacenter**
  - Seclin



- **Le SG Cloud est disponible sur plusieurs implantation. Ces implantation sont composées de Régions et de zones de disponibilités (AZ).**
- **Chaque Région est une zone géographique séparée et complétement indépendante.**
- **Une Région est composée d'au moins une à plusieurs zones isolées avec des profils de risques différents, nommé Availability Zone (AZ)**
- **Le SG Cloud fournit différents services et mécanismes de résilience dans chaque (et entre) Région et AZ pour fournir :**
  - Cross-Regions Disaster Recovery
  - Intra-Region Disaster Recovery (quand la region a plusieurs AZ)

L'offre Cloud Interne – IaaS*



* *Infrastructure as a Service*

L'offre Cloud Interne – IaaS*

- **La plateforme Cloud Interne est certifié D3 I1 C2 P2**
- **Hébergement de Virtual Machines (VM)**
  - 18 tailles de VM (jusque 12 vCPU et 128 Gb de RAM) avec 9 offres de taille de stockage
  - 2 types OS : Windows & Linux Redhat
- **Hébergement de Load Balancers**
  - Les loadbalancers permettent de d'effectuer une répartition de charge de niveau 4 (L4) des applications.
  - L'équilibreur de charge classique achemine le trafic sur la base des informations du niveau de l'application ou du réseau et est idéal pour un équilibrage de charge simple du trafic sur plusieurs instances, lorsqu'une haute disponibilité, une mise à l'échelle automatique et une sécurité robustes sont requis.
- **Tagging de VM**
  - Le tagging permet d'ajouter des informations pour catégoriser les ressources que vous positionnez dans le Cloud Interne en y affectant un couple de clef / valeur.
  - Ces tags, sont interrogeable par API ce qui permet d'obtenir par exemple la liste des ressources qui ont un tag particuliers
  - L'offre de service sur le Cloud interne permet de positionner 10 Tags par VM.

** Infrastructure as a Service*

L'offre Cloud Interne – IaaS*

- **Backup des VM sur le Cloud Interne**
  - La sauvegarde de la VM est proposé sur le Cloud Interne pour la PROD, mais n'est pas obligatoire. Le back up est répliqué sur une autre région.
  - L'offre de sauvegarde avec TSM (offre RET) est également disponible pour les VMs positionnées sur le Cloud Interne.
  - La politique de back up peut etre choisie à la création de la machine virtuelle et peut être changé, tout comme la back up peut être activé / désactivé à n'importe quel moment.
  - Les politiques de back up sont basées sur leurs fréquences, rétention et heure de démarrage. (Quotidienne, rétention de 31j, démarrage à 2 AM ou 4 AM).
  - La restauration peut se faire pour la totalité des VMs ou pour des fichiers spécifiques, cette opération est réalisée par GTS.

- **Réplication des VM entre différentes zones de disponibilité (AZ)**
  - Asynchrone entre différentes régions (1h)
  - Disponible pour les environnements de PROD uniquement
    - Local RTO (redémarrage automatique après un problème sur local host) : <10min
    - Local RPO (cluster) : 0min
    - Distant RTO (failover de l'infrastructure Cloud vers le site DR) : 4h
    - Distant RPO (1h réplication asynchrone vers le site DR) : 60 min

** Infrastructure as a Service*

CLOUD SERVICE CATALOG

Services to implement during SG Cloud evolution v1
Services already delivered during v1

1 Select offers

- Cloud virtual machine
- Cloud load balancer
- Object storage offer: Standard; Storage synchronous replication

2 Choose your OS

- Standard OS: Windows; redhat
- Custom OS: GTS Signed; Unsigned (Sandbox VM only)

3 Size your machine

Standard sizing

- Compute: Micro; Small; Medium; Large; X-Large
- Data storage size: 20 GB; 60 GB; 160 GB; 300 GB; 500 GB; 750 GB; 1 TB; 1.5 TB dev only; 2 TB dev only
  System storage: Linux 24 GB – Win2008: 40 GB – Win2012: 60 GB

4 Select services you want

Virtual machine hosting zones

- Internal: Standard zone; DMZ zone
- Exposed: Web cell; Cloud cell

Cloud backup for virtual machines

Security groups (specific for each AZ & not for replicated machines)

5 Select service level

- Virtual machine resiliency: Standard; Asynchronous replication Greater Paris - North
- Virtual machine performance: Standard; CPU guaranteed; High I/O

6 Get benefits from GTS support services

Available sites (regions & AZ)

- North
- Greater Paris: AZ eur-fr-paris-1; New AZ eur-fr-paris-2

Action in self-services (portal & API's)

- Create (with OS) / delete / restart machine
- Resize machine (RAM/CPU model) within the catalogue
- Manage lease & owner
- Get machine information
- Add / remove virtual disk storage *(API only)*
- Change/enable/disable Cloud backup policy
- Create / delete a load balancer
- Manage LB: health checks & backend servers
- Snapshot for safeguard
- Instances tagging
- Access segregation for PROD
- Stop virtual machine to not pay compute

Business services

- D3 I1 C2 P2 certified
- Pay per use billing (per hour)
- Consumption quotas
- Online dashboards

Cloud support

- Support on VM envelops & SG Cloud portal
- Support H24/24 , 7d/7 with on-duty during non business hours

L'offre Cloud Interne – Iaas*

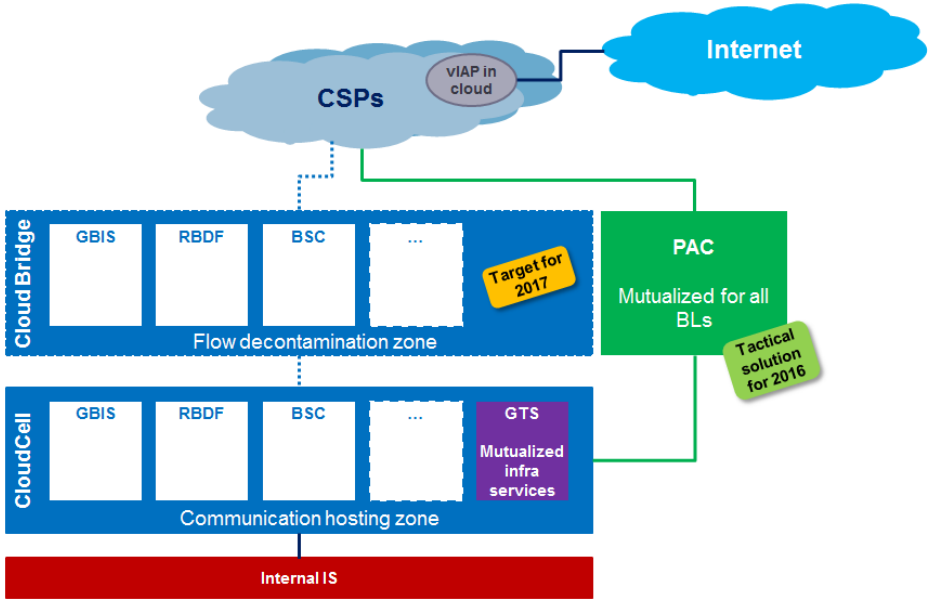
- **Security Group**
  - Les Security Group représente un moyen de cloisonner els applications en maitrisant les flux. On peut comparer cela un FireWall applicatif.
  - Au sein du Cloud Interne, ils permettent de créer des groupes et d'y associer des VMS. Sur ces groupes peut être appliqué un filtrage par écrire de règles (ce ne sont pas des ouvertures de routes réseau). Ces règles sont à la main des DSI
- **Une offre de Stockage Objet basé sur Scality.**
  - Cette offre expose des api du service AWS S3 directemetn consommable par els projet des DSI.
  - L'infrastructure est répartie entre la région Paris et Nord.
- **Des CloudCell pour déployer chez AWS des applications**
  - Exposé sur les CSP, avec des DMZ par DSI afin de déployer les composants nécessaires à l'hébergement dans le Cloud Public
  - Zones en travaux concernant les résiliences (Région Paris / Nord)
  - Consommés par ITIM et BSC pour des projets de déploiements chez AWS (Exemple : NGIM)
- **Des vWebCell pour exposer les application sur internet**
  - Une zone exposée sur internet avec l'agilité du Cloud Interne.
  - Chaque DSI dispose d'une vWebCell avec des DMZ qui lui sont propres pour pouvoir déployer ses applications avec une exposition directe aux clients

** Infrastructure as a Service*

L'offre Cloud Interne – Les zones exposées CloudCell et vWebCell

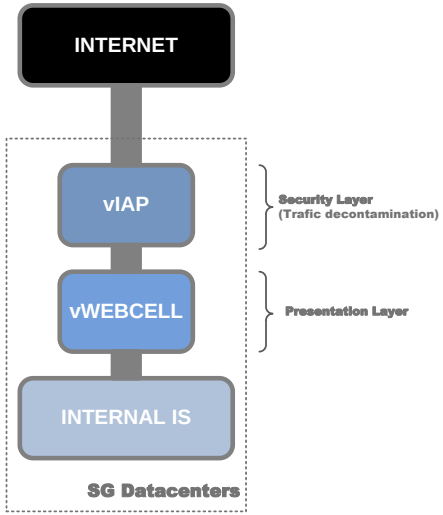
La CloudCell

- Il s'agit d'une zone sécurisée, situé entre le SI Interne et les Cloud Service Provider (CSP), hébergée à la Société Générale.
- Il y a une CloudCell par Business Line, composée de plusieurs DMZ chacune.



La vWebCell

- Jusqu'à maintenant le hosting d'applications exposées sur Internet était fournis au travers d'une infrastructure dédiée nommé WebCell qui est protégé d'Internet par une plateforme de sécurité (Internet Access Point).
- Pour accroitre l'agilité des business Line, dans le cadre du projet Cloud Evolution, une nouvelle infrastructure composée d'un vIAP et d'une vWebCell est en construction



SG Cloud Service Levels

Cloud VM resiliency service levels

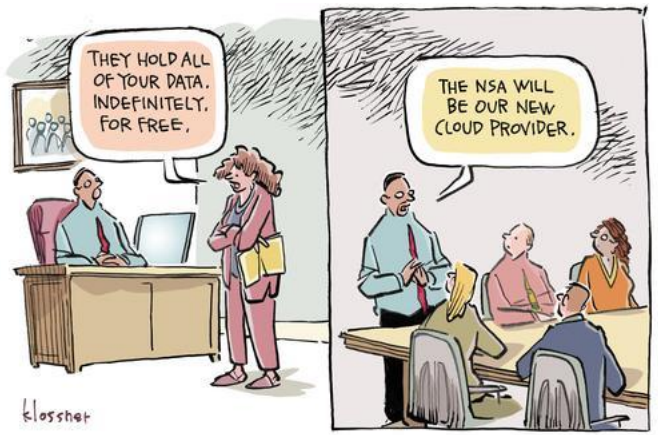
Region / Availability zones	❑ Region North (Availability zone : Seclin 2) ❑ Region IDF (Availability zone : Marcoussis)
Resiliency Service Levels	❑ **STANDARD VM** *Deployed on a 1 single AZ, local cluster resiliency, no distant replication* ○ **Local RTO** (automatic restart after a local host failure) : **<10min** ○ **Local RPO** (cluster) **: 0min** ❑ **REPLICATED VM** *Standard VM + asynchronous distant replication to a different Region/AZ* ○ **Available only for PRD** environment (+ UAT for RET ITIM and BSC) ○ **Local RTO** (automatic restart after a local host failure) : **<10min** ○ **Local RPO** (cluster) **: 0min** ○ **Distant RTO** (failover of the Cloud infrastructure to the DR site) : **4h** ○ **Distant RPO** (1h asynchronous replication to the DR site) : **60 min**
Disaster recovery & DR Exercises	❑ **Disaster Recovery Plan** ○ Available only for replicated VMs ○ Bidirectional (Seclin 2 → Marcoussis, or Marcoussis → Seclin 2) ○ Service switching only for global GTS DR plan and managed by GTS ○ Extended vlan : same IP address for the replicated VM ○ Different MAC address ❑ **DR Exercise** : GLOBAL

Cloud VM Performance service levels

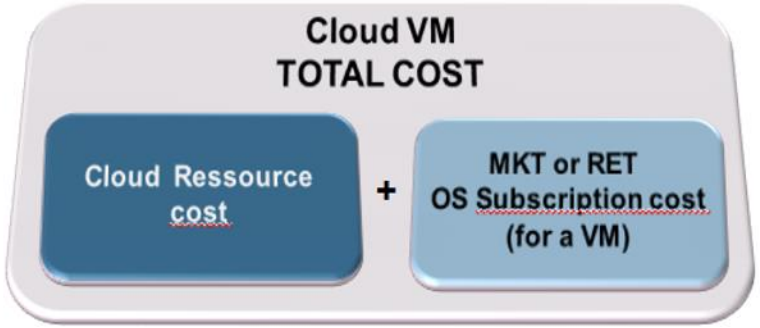
Configuration / performance	❑ Network : 1 Gbs/VM ❑ Max vCPU = 8 (and 2.4Ghz per vcpu) ❑ Max Memory = 64 Gb ❑ Max Storage = 1 To ❑ IOPS : 1 IOPS/Gb

Cloud support service levels

Cloud Support	❑ Support on VM envelop ❑ Support on SG Cloud portal ❑ Support H24/24, 7d/7 with on duty during non business hours



Les coûts de l'offre RET



+ option : Cloud backup
Tarif : 2€ / Gb / year

Unit : In Cloud VSPEC A calculated unit depending on the size of the VM (cpu, ram, disk) and the resiliency (standard VM / replicated VM)	
2017 Tarif	**24€ / VSPEC / year** (0.066€ / VSPEC / day)
underlying costs & services	All Cloud VM costs & services up to the VM envelop - Cloud infrastructure (including storage) - Cloud team support & services
Billing rule	Standard VM : see Cloud VSPEC pricing catalog Replicated VM : 2x VPEC size of the standard VM

Unit : Per VM OS subscription	
2017 Tarif	**1173€ / year / VM OS**
underlying costs & services	OS costs & services (inside the VM envelop) - OS licences and administration costs - Monitoring
Billing rule	Standard VM : 1x VM OS subscription Replicated VM : 2x VM OS subscription