RUSSIE CLOUD IAAS

Etude des prérequis

***Prérequis et Ecosystèmes CLOUD de la Russie***

RESG/GTS/IBF/APS

Version 0.7 du 09/11/2017

Etat : Evaluation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Historique des versions | | | | | |
| **Version** | **Date** | **Auteur** | **Statut** | **Validation** | **Numéro de page** |
| **0.1** | 09/10/2017 | Amine ELOUALID ELALAOUI | Création |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Historique des updates | | | |
| **Version** | **Date** | **Type de l’update** | **Numéro de page** |
| **0.1** | 09/10/2017 | Création de document |  |
| **0.7** | 09/11/17 | Urbanisation réseau schéma d’urbanisation du réseau,  VCenter de Mangement en Russie (phase projet) | 10,11,17,18 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

| **Département** | **Destinataire** | **Fonction** |
| --- | --- | --- |
| RESG/GTS/IBF/APS |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Table des matières

[Objectif : 4](#_Toc498078758)

[L’infrastructure existante : 4](#_Toc498078759)

[Réseau 4](#_Toc498078760)

[Cloud 4](#_Toc498078761)

[Datacenter 4](#_Toc498078762)

[Écosystème 4](#_Toc498078763)

[Le design cible : 4](#_Toc498078764)

[Cibles : 4](#_Toc498078765)

[Le catalogue de service : 6](#_Toc498078766)

[Les prérequis : 9](#_Toc498078767)

[Les prérequis Réseau 9](#_Toc498078768)

[Réseau du CLOUD : 10](#_Toc498078769)

[Urbanisation Réseau : 10](#_Toc498078770)

[Les prérequis Sécurité 11](#_Toc498078771)

[Les prérequis Cloud 11](#_Toc498078772)

[VRO 11](#_Toc498078773)

[VRA 12](#_Toc498078774)

[DNS 12](#_Toc498078775)

[Marley 13](#_Toc498078776)

[AD 13](#_Toc498078777)

[Netmap 14](#_Toc498078778)

[Template et Post Install cloud : 14](#_Toc498078779)

[Stockage 15](#_Toc498078780)

[Trigrammes : 18](#_Toc498078781)

[Taxation : 18](#_Toc498078782)

[Notification : 19](#_Toc498078783)

[Sauvegarde : 19](#_Toc498078784)

[Scénario création d’une VM cloud Russie. 19](#_Toc498078785)

[Conclusion 20](#_Toc498078786)

# Objectif :

L’objectif de ce document est de définir l’architecture high level de l’instance cloud IAAS en Russie, et d’exposer les prérequis nécessaires pour la mettre en place.

# L’infrastructure existante :

## Réseau

Un réseau non SGNA sur les sites de la ROSBANK.

## Cloud

Une infrastructure VMware Vsphere dédiée pour la virtualisation traditionnelle.

Pas du cloud.

## Datacenter

Deux sites distants (20 KM entre les deux DC)

## Écosystème

L’écosystème existant ne sera pas utilisé dans le cloud de la Russie.

Pour le cadre du projet du cloud IAAS de la Russie, l’objectif est d’utiliser le même écosystème standard du cloud de GTS.

# Le design cible :

La cible pour le Cloud de la Russie est de créer un CLOUD IAAS sur deux Datacenters en Russie, pour déployer des VMs de test, développement et de la production.

Les services proposés par le cloud de la Russie seront les mêmes que ceux proposés par le CLOUD GTS avec une livraison progressive des services (voir chapitre catalogue de service) pour avoir une idée sur les services de la première version et ensuite la vision de la solution à terme.

La cloud IAAS en Russie va offrir la possibilité de créer des VMs dans la région de la Russie avec deux availability zones, chaque AZ est composée d’un DC.

## Cibles :

Consiste à :

* Utilisation du VRA/VRO centrale de paris, pour piloter les ressources déployées en Russie.
* Déploiement de réseaux SGNA (Réseaux de management et réseaux clients)
* Étendre l’écosystème utilisé par le cloud de GTS vers les infrastructures de la Russie (DNSonDemand, Marley…).
* Création des clusters des ressources de calcul et stockage sur les deux Datacenters de la Russie.
* Création d’un cluster de Mangement sur les deux Datacenters de la Russie.
* Création d’un réseau étendu entre les deux sites de la Russie.
* Utilisation du réseau de la filiale de la ROSBANK pour le management de la plate-forme cloud de la Russie.
* Création d’un CLOUD-IAAS pour héberger les plate formes TEST, DEV, et prêt pour héberger la plate-forme de la production.
* La mise en place des prérequis nécessaires pour ce design (voir chapitre prérequis).

Avantages :

* Bénéficier des nouveaux services déployés à Paris.
* Maîtrise parfaite du service cloud déployé sur le portail du cloud de la Russie.
* Utilisation du même écosystème du cloud de GTS ; à terme la gestion des MAJ et des modifications dans les APIs de l’écosystème est assurée par l’équipe CLOUD de GTS.
* Simplification de l’exploitation et du support.
* VRA/VRO gérés par l’équipe CLOUD de GTS.
* Déploiement d’un réseau SGNA.
* Suivi des standards de GTS.

Inconvénients :

* Création des comptes de service pour l’équipe cloud pour le pilotage des ressources localisées à Moscow.
* Gestion des ouvertures des flux entre paris et Russie (PAX)
* Nécessite d’intégrer l’écosystème GTS (DoD,Marley,AD,…) avec les infrastructures de la Russie.

Ci-dessous le schéma de la cible résumé :

SCHEMA

# Le catalogue de service :

Ci-dessous le catalogue de service V0 souhaité dans une première itération :

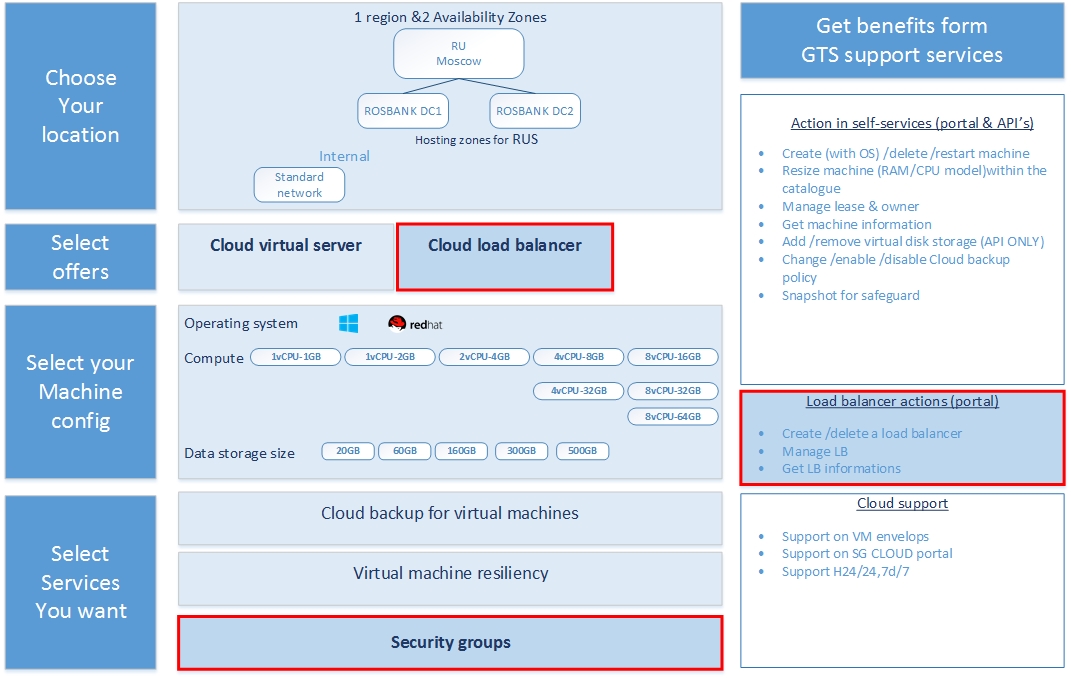
SCHEMA

Première itération :

* Création de la région de la Russie avec les deux zones d’availability (zone DC1 & zone DC2)
* Création des VMs Standard en COMPUTE et STORAGE.
* Création des VMS dans les zones standard dans les environnements de TST,DEV,UAT,PRD
* Proposition des Templates standard GTS Redhat 7.2, Windows 2012.
* Proposition du service de la sauvegarde des VMs dans l’environnement de production.
* Proposition de la réplication des VMs de la production.

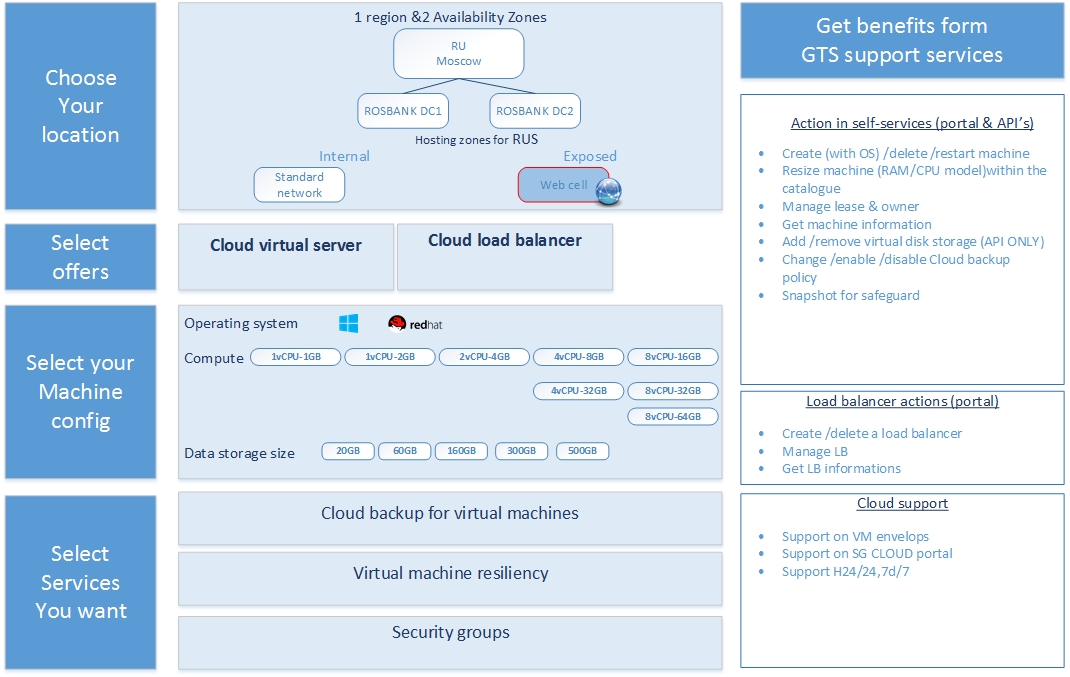
Ci-dessous le catalogue de service V1 souhaité dans une deuxième itération :

* Ajout de la fonctionnalité de load balancer, consommée par le portail cloud.
* Ajout du service de Security groups.



Ci-dessous le catalogue de service V2 souhaité dans une troisième itération :

* Ajout de la zone Webcell .



Des workshops techniques pourront être mis en place sur les points spécifiques qui pourraient apparaître lors de la phase de projet.

Perspective du catalogue de service V3 est d’ajouter la zone DMZ.

# Les prérequis :

Le chapitre suivant va nous présenter les composants qui constituent les prérequis nécessaires pour monter le cloud IAAS de la Russie et ils vont nous aider pour la mise en place d’un plan d’action clair.

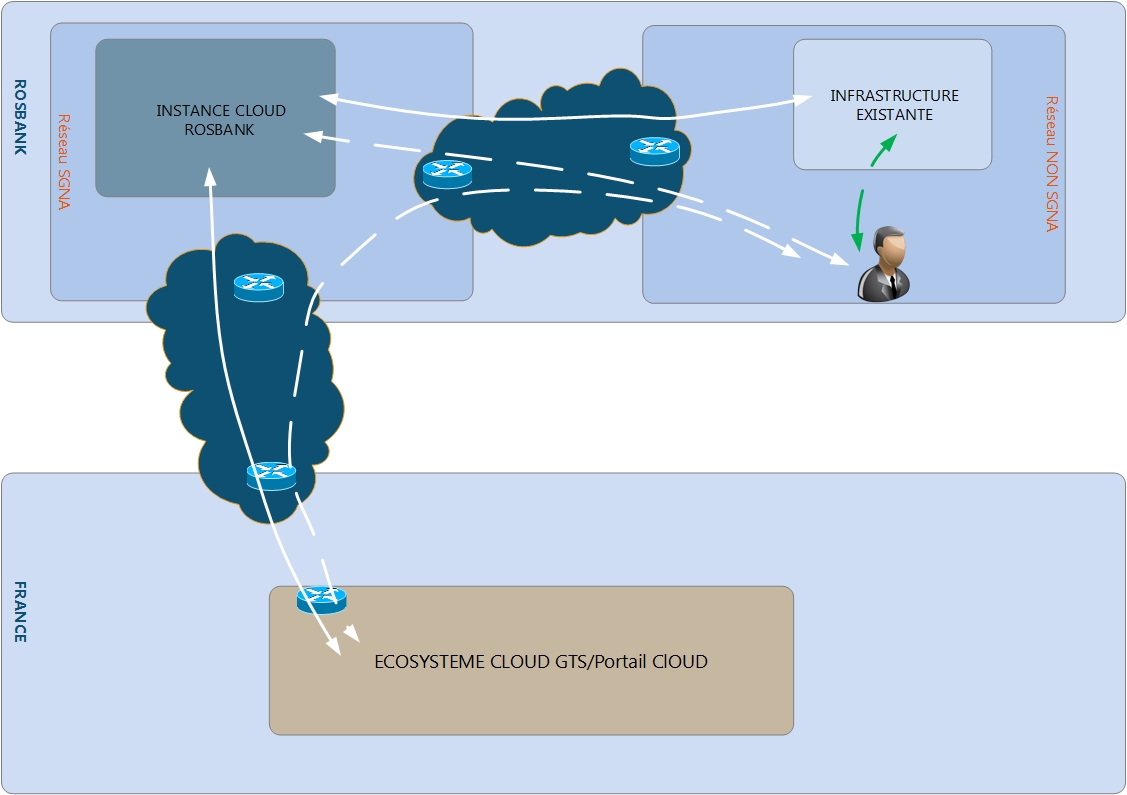
## Les prérequis Réseau

**Cible**

La mise en place du cloud IAAS de la Russie va nécessiter :

* La création du réseau SGNA pour le Cloud sur les sites ROSBANK.
* L’ouverture des flux entre le réseau SGNA de la ROSBANK et l’ECOSYSTEME du CLOUD de GTS.
* L’existant de flux entre le réseau SGNA et le réseau non SGNA dans les sites de la ROSBANK.

Le résumé est dans le schéma ci-dessous :



### Réseau du CLOUD :

Pour ce point de prérequis faut :

* Créer une infrastructure réseau redondante dédiée pour le cloud multi tenant de la Russie sur les deux DCs avec un adressage SGNA.
* Assurer que le réseau pour les zones de Sécurité est tendu entre les datacenters.
* Utiliser même type des équipements que Paris, le choix de matériel. (Faut planifier un atelier pour ce sujet généralement du cisco N2K,N5K,N7K,N9K )

Le schéma ci-après présente l’objectif de ce réseau

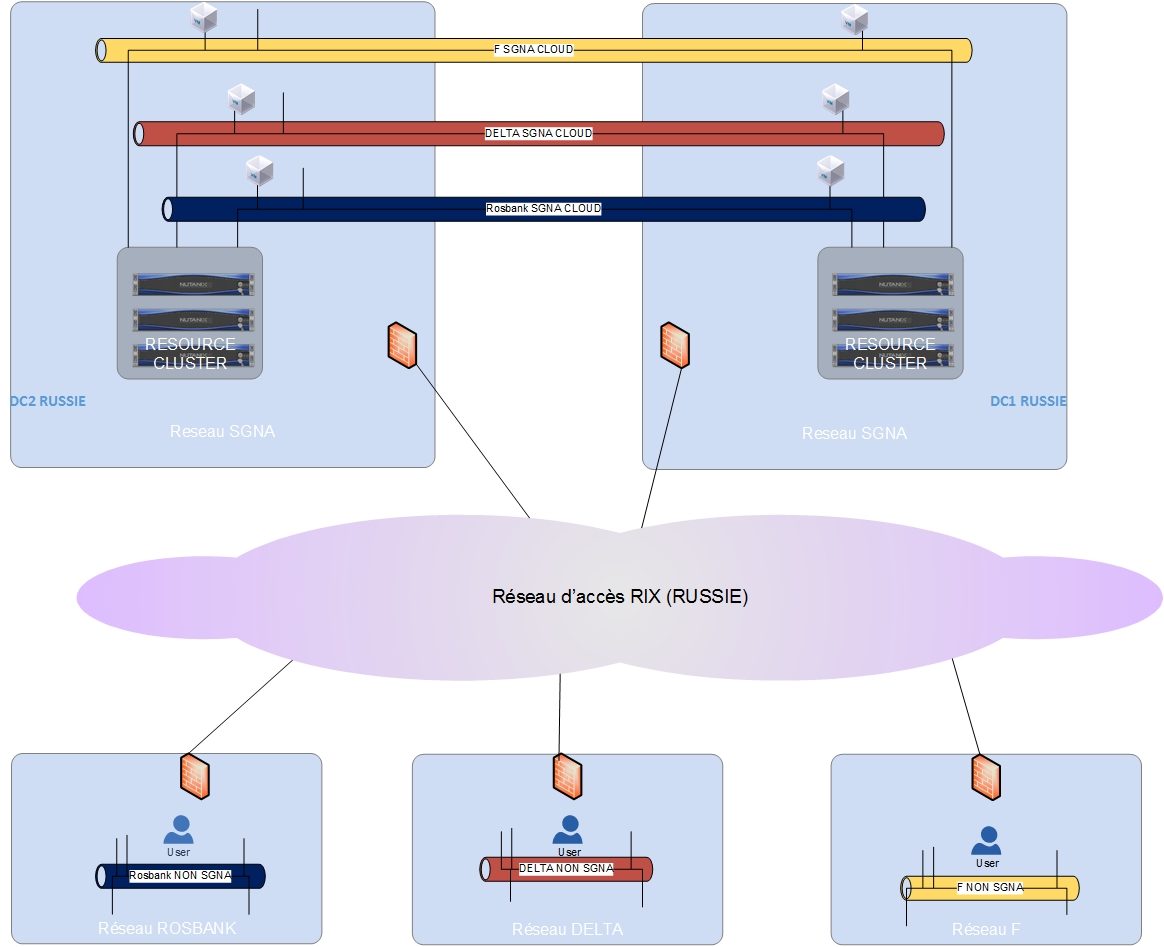
### Urbanisation Réseau :

Pour respecter l’urbanisation du réseau faut :

* Créer un réseau d’accès en Russie. (RIX Russie)
* Connecter les filiales à ce réseau d’accès.
* Connecter l’infrastructure réseau du cloud de la Russie à ce réseau d’accès.

L’objectif de ce réseau d’accès est de permettre aux différentes filiales d'utiliser le cloud de la Russie en sécurité.

Le schéma ci-dessous représente la vue globale de la vision d'urbanisation du réseau du cloud de la Russie :



Plages @ IP SGNA

Classe SGNA

Fournir les @ IP a la ROSBANK , faire les annonces de route

Routage de VLAN l’écosystème de paris vers RIX RUSSIE

Réseau CLOUD Schéma et le matériel

Comment on développe le truc, comment en consommation.

HCS

## 

## Les prérequis Sécurité

#### Cible

Pour ouvrir les flux entre le réseau SGNA de l’instance cloud de la Russie et l’écosystème de cloud de GTS.

* Faut fournir un document de sécurité (DS)
* Faut valider ce document par le métier.

## Les prérequis Cloud

### VRO

**Cible**

Ce scénario consiste à :

* L’utilisation du VRO déployé en France
* L’utilisation des workflows existants avec ajout du contexte Russe.
* Le paramétrage du VRO France pour qu’il utilise les infrastructures (AD/DNS/NTP/Master Servers) de la ROSBANK sur le réseau SGNA.
* L’ouverture des flux d’administration entre le VRO et l’infrastructure de la ROSBANK.

### VRA

**Cible**

Pour ce scénario on a besoin de :

* Une modification dans le VRA de cloud de GTS afin qu’il prendre en charge l’ajout d’une nouvelle infrastructure de la ROSBANK.
* Pilotage de VCenter ROSBANK à partir du VRA de GTS par des end point.
* Ouvrir des flux d’administration entre le VRA et l’infrastructure de la ROSBANK.
* Ouvrir accès à vRA depuis la Russie (au travers du PAX)
* Création de comptes dans l’AD MSD EUR pour toute personne souhaitant pouvoir provisionner dans le cloud

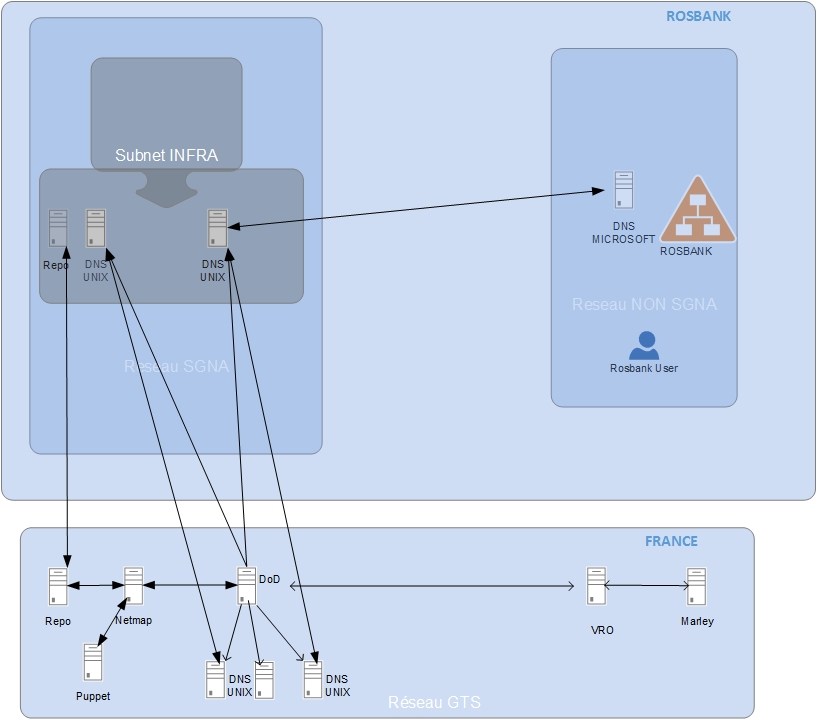
### DNS

**Cible**

Ce scénario consiste à :

* La configuration de DoD pour gérer les DNS de la ROSBANK.
* Ouverture des flux nécessaires entre le DoD et les serveurs DNS de la ROSBANK.
* Le VRO utilise l’API de DoD pour gérer les noms DNS des VMs de l’instance cloud de la ROSBANK.
* Déclaration des zones DNS de la ROSBANK dans le DoD.
* Vérification que les VLANs ROSBANK peuvent résoudre le nom DNS fr.world.socgen.
* Création des serveurs DNS UNIX dans la zone SGNA.
* Federer ces serveurs DNS a DoD de la France pour les gérés. (Une fois fédérer le DoD est le seul qui peut modifier et écrire dans ces serveurs DNS).
* Configuration de ces serveurs DNS UNIX avec les serveurs DNS (MICROSOFT) existants pour assurer la résolution entre les deux zones (existante et la nouvelle zone Cloud(rosbank.ru.roof.socgen))
* Création d’une nouvelle zone rosbank.ru. roof.socgen
* Synchronisation de la zone rosbank.ru. roof.socgen
* Nécessité des ouvertures des flux.

Le résumé est dans le schéma ci-dessous :



### Marley

**Cible**

Pour ce scénario :

* Le VRO utilise l’API de Marley pour gérer l’inventaire des VMs du cloud IAAS de la Russie.
* Une configuration sur Marley pour gérer les inventaires de la ROSBANK est nécessaire.
* Ouvertures des flux entre Marley et les sites de la ROSBANK.

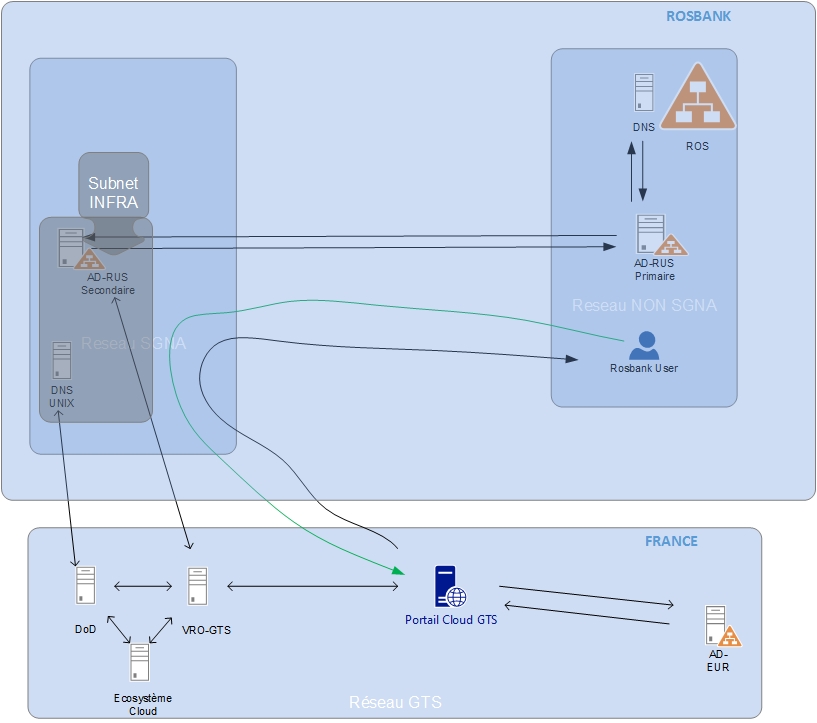
### AD

**Cible :**

On a besoin de :

* Utilisation de l’AD EUR pour l’authentification dans le portail du cloud.
* Modification dans l’AD-RUS pour automatiser la déclaration des VMs créés à partir de portail cloud dans le domaine de la ROSBANK.(pour ajouter un computer account dans l’AD-RUS)
* La création d’un DC-RUS secondaire sur le réseau SGNA.
* Synchronisation de DC-RUS secondaire sur le réseau SGNA avec l’AD-RUS primaire sur le réseau NON SGNA.
* Modification dans VRA/VRO pour communiquer avec l’AD-RUS via le réseau SGNA.
* Ouverture de flux afin d’autoriser l’accès à Groupmembership à la Rosbank.

Le résumé est dans le schéma ci-dessous :



-Pour les autres filiales :

### Netmap

**Cible :**

Pour ce scénario on a besoin de :

* Déclaration des Vlans et la configuration de réseau SGNA de la Russie dans Netmap par les équipes de TFO de GTS.
* Pas de déploiement de l’instance Netmap dans le site de la Russie.
* Création des comptes de consultation sur l’application Netmap pour l’équipe IT de la Russie.
* Ouverture de flux vers l’application web Netmap.

### Template et Post Install cloud :

**Cible :**

Pour Windows

Pour ce scénario on utilise :

* Le master standard de la SG (GWIM)
* Le même Template unique de GWIM,
* La post-install dédiée à la ROSBANK.

On a besoin aussi de :

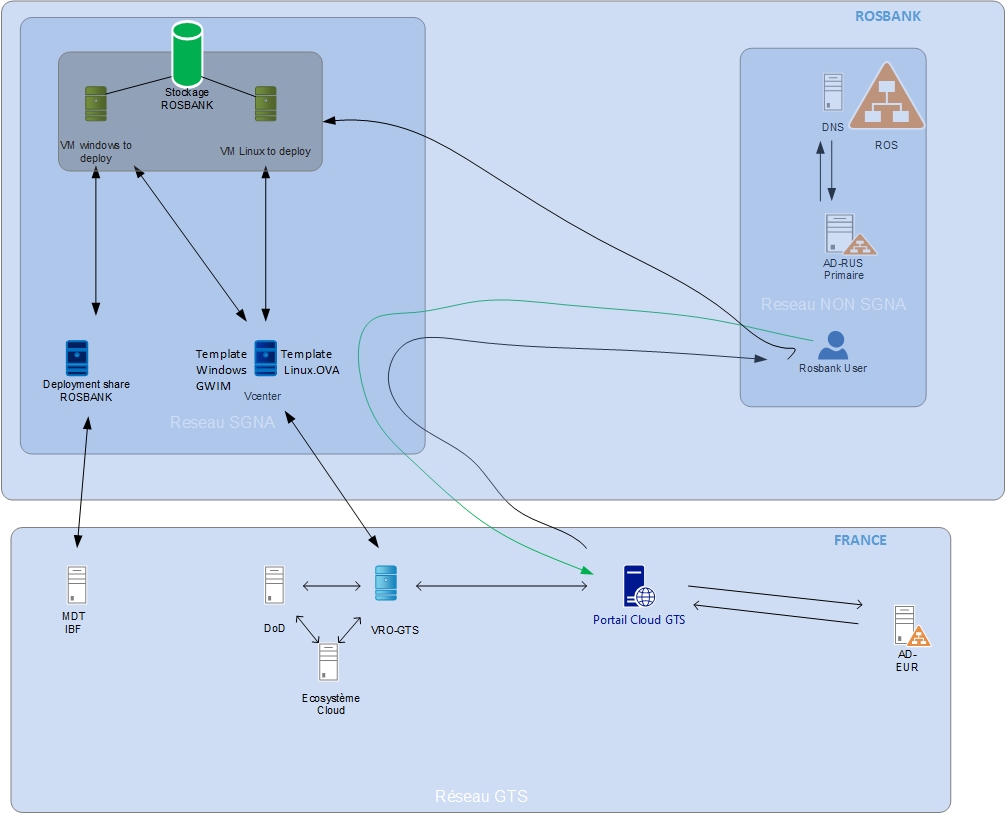
* Création d’un DS dans le cloud de la ROSBANK.
* Ouverture des flux entre le DS de la ROSBANK et le MDT d’IBF
* Changement dans le MDT d’IBF pour ajouter le nouveau DS de la ROSBANK.

La gestion de la post-install est assurée par l’équipe IT de la ROSBANK.

Pour Linux :

On utilise le Template IBF en l’exportant sur le format OVA, ensuite en l’important sur l’infra de la ROSBANK.

Le résumé est dans le schéma ci-dessous :



### Stockage

**Cible :**

Pour ce scénario on a besoin de :

* Utilisation des nœuds NUTANIX sur les deux Datacenter de la ROSBANK.
* Le déploiement de la même version de NUTANIX OS (GTS) sur les nœuds de la ROSBANK.
* Utilisation du machinisme de la réplication native de NUTANIX (Asynchronous Replication service) pour assurer la réplication asynchrone entre les deux Datacenter de la ROSBANK.
* Sur chaque data center de la Russie on va déployer un POD de la production avec un cluster des ressources constitué de :

* 3 nœuds pour le cluster de ressource du POD de la production.
* La configuration des nœuds est la suivante :
* 1x DELL XC630-10
* 1x Intel Xeon E5-2690v4 (2,6GHz, 14C, Cache 35Mo, 9,6GT/s QPI, 135W )
* 1x Intel Xeon E5-2690v4 (2,6GHz, 14C, Cache 35Mo, 9,6GT/s QPI, 135W )
* 16x 32Go RDIMM, 2133MT/s, Dual Rank, x4
* 1x 16Go, Carte SD pour IDSDM
* 1x Disque 64Go SSDR SATA-DOM
* 2x Disques Hot Plug 800GB Solid State Drive SATA Mid Endurance 2.5in Hot-plug Drive
* 8x Disques dur Hot Plug 2To NL-SAS 12Gbit/s 512e 7200tr/min 2,5 pouces, 13G
* 1x PERC H730 RAID contrôleur, 1Go NV Cache
* 1x Carte fille réseau Intel X520, Double port, 10Gb, 1GbE, DA/SFP+, I350 DP
* 1x iDRAC8 Enterprise

Schéma à faire :

Infrastructure de calcul :

**Cible :**

Pour ce scénario on a besoin de :

Sur chaque Datacenter de la Russie on va déployer un POD de production pour le cluster de ressource constitue de :

* 3 nœuds de calcul NUTANIX.

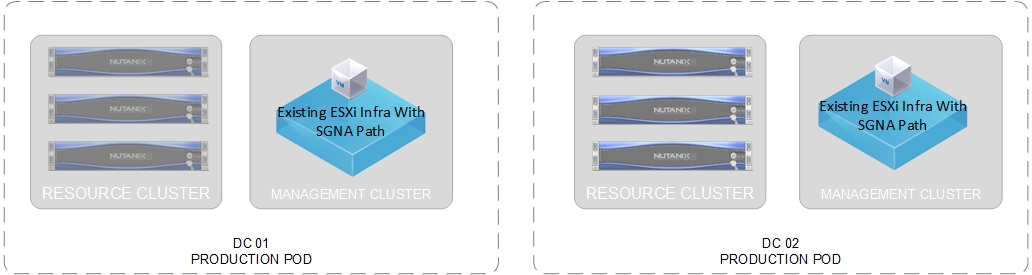
Sur chaque nœud de calcul on installe VMware ESXI 6.5.

Un VCenter sera déployé sur chaque Datacenter pour gérer les ressources locales du cluster. (Soit dans le cluster de management dédié, ou bien dans l’infrastructure de la virtualisation existante avec un path SGNA).

Un compte administrateur sera créé pour l’équipe cloud de GTS sur le VCenter de la ROSBANK, pour des raisons de support.

Un compte de service sera créé pour le Proxy Agent de la suite VRA afin de pouvoir piloter le vCenter.

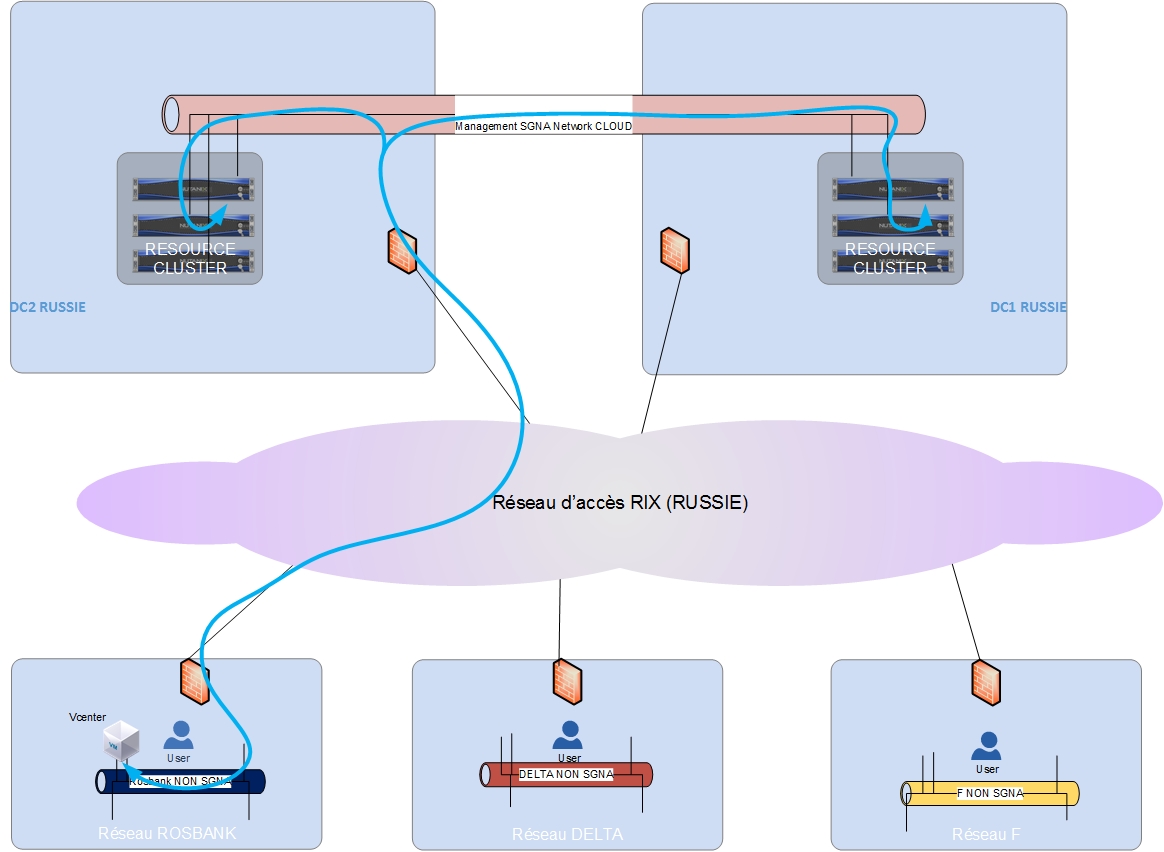
Le résumé est dans le schéma ci-dessous :



Dans une première phase du projet et pour des raisons de budgétaire, faut créer un nouveau VCenter dans l'infrastructure existante de la ROSBANK avec un path réseau SGNA du cloud et avec une ouverture de flux en large entre ce Vcenter et le réseau de management du cloud.

Faut faire la même chose dans les deux DCs de la ROSBANK, avec le HA des deux Vcenter pour assurer la continuité de service.

Le schéma ci-dessous illustre ce point :



### Trigrammes :

**Cible :**

Pour ce scénario on a besoin de :

Utilisation de l’application Iappli de GTS pour gérer les trigrammes.

* Nécessite de créer un compte dans iappli pour le gestionnaire des trigrammes côté de la Russie.
* Nécessite d’avoir un compte SESAME pour utiliser iaapli.

### Taxation :

**Cible 1 :**

Taxation par rapport aux trigrammes à partir de Iappli.

### Notification :

**Cible :**

Pour ce cible on a besoin de :

* Utilisation de l’option de transfert des emails entre la boîte SOCGEN du compte eur et la boîte email de l’utilisateur de la ROSBANK
* Vérification de la possibilité de l’utilisation de la messagerie interne de la ROSBANK.

### Sauvegarde :

**Cible :**

On a besoin de :

* Utilisation de la solution Veeam Backup avec la même configuration de GTS.
* Ouverture des flux entre le VRO et les serveurs Veeam dans le réseau SGNA de la ROSBANK.
* Utilisation de la même politique de sauvegarde proposée par le cloud de GTS.
* Sauvegarde uniquement des VMs de la production.

Les politiques de sauvegarde pour la plate-forme de la production qui seront implémentées sont les suivantes :

* Daily backup with 31 days retention launched at 2 AM.
* Daily backup with 31 days retention launched at 4 AM.

### Scénario création d’une VM cloud Russie.

**CIBLE :**

1. Création d’un compte AD eur pour l’utilisateur ROSBANK.
2. Création d’un trigramme du projet sur l’application Iappli de GTS.
3. Vérification de l’existant de ce trigramme dans Marley. (La synchronisation est automatique entre Iappli et Marley
4. Création d’un BG dans le cloud portal pour gérer les trigrammes et les utilisateurs qui vont utiliser le trigramme.
5. Ajout les utilisateurs de la ROSBANK qui vont utiliser l’instance de ce BG sur l’application groupmembership
6. Ajout des Templates windows nécessaires sur les nœuds des ressources de la ROSBANK.
7. Ajout des Templates linux sur les nœuds des ressources de la ROSBANK.
8. Ajout de Vlan ROSBANK dans le référentiel Netmap de GTS.
9. Vérification que le Vlan ROSBANK est visible depuis l’infra cloud GTS (vRA/vRO)
10. Vérifier que l’AD\_RUS Secondaire est visible par VRO.
11. Vérifier que VRO peut accéder à l’AD-RUS via un compte de service pour créer le compte de serveur.
12. Vérifier que Le VLAN ROSBANK existe dans le DNonDemand. Il sera utilisé par VRO pour réserver une @ip et un nom dans le DNS,
13. Vérifier que le Vlan ROSBANK existe dans netmap de GTS. Il sera utilisé par VRO pour récupérer (getway ,netmask,dns server)
14. Vérifier le DNS forwarder ; le réseau SGNA de la ROSBANK doit résoudre le nom fr.world.socgen.
15. Accès depuis le réseau SGNA du cloud ROSBANK vers l’infrastructure AD/DNS/Master/NTP du ROSBANK, pour assurer la post Install.

# Conclusion