RUSSIE CLOUD IAAS

Study of prerequisites

***Prerequisites and Ecosystems of Russia CLOUD***

RESG/GTS/IBF/APS

Version 0.9 of 15/11/2017

State: evaluation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| History of the versions | | | | | |
| **Version** | **Date** | **Author** | **Status** | **Validation** | **Number of page** |
| **0.1** | 09/10/2017 | Amine ELOUALID ELALAOUI | Creation FR Version |  |  |
| **0.9** | 15/11/2017 | Amine ELOUALID ELALAOUI | Creation of ENGLISH Version |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| History of updates | | | |
| **Version** | **Date** | **Type of the update** | **Number of page** |
| **0.1** | 09/10/2017 | Creation of document |  |
| **0.7** | 09/11/17 | Network urbanization plan of urbanization of the network,  VCenter of Management in Russia (phase project) | 10,11,17,18 |
| **0.9** | 15/11/17 | Translation of document in English |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

| **Department** | **Recipient(Addressee)** | **Function(Office)** |
| --- | --- | --- |
| RESG / GTS / IBF / APS |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Contents

[Objective: 4](#_Toc498703977)

[The existing infrastructure: 4](#_Toc498703978)

[Network 4](#_Toc498703979)

[Cloud 4](#_Toc498703980)

[Datacenter 4](#_Toc498703981)

[Ecosystem 4](#_Toc498703982)

[The target design 4](#_Toc498703983)

[Targets 5](#_Toc498703984)

[The catalog of service 6](#_Toc498703985)

[Prerequisites 10](#_Toc498703986)

[The Network prerequisites 10](#_Toc498703987)

[Network of the CLOUD 11](#_Toc498703988)

[Network urbanization 11](#_Toc498703989)

[The security prerequisites 12](#_Toc498703990)

[The Cloud prerequisites 12](#_Toc498703991)

[VRO 12](#_Toc498703992)

[VRA 13](#_Toc498703993)

[DNS 13](#_Toc498703994)

[Marley 14](#_Toc498703995)

[AD 14](#_Toc498703996)

[Netmap 15](#_Toc498703997)

[Template and Post Install cloud: 16](#_Toc498703998)

[Storage 17](#_Toc498703999)

[Trigrams: 20](#_Toc498704000)

[Taxation: 20](#_Toc498704001)

[Notification: 21](#_Toc498704002)

[Backup 21](#_Toc498704003)

[Licensing 21](#_Toc498704004)

[Conclusion 23](#_Toc498704005)

# Objective:

The objective of this document is to define the high-level architecture of the instance cloud IAAS in Russia, and to display the necessary prerequisites to set up it.

# The existing infrastructure:

## Network

On the sites of the Russia we have a network not SGNA.

## Cloud

An infrastructure VMware Vsphere dedicated for the traditional virtualization.

Not existing cloud.

## Datacenter

Two distant sites (20 KM between both DC)

## Ecosystem

The existing ecosystem will not be used in the cloud of Russia.

For the executive of the project of the cloud IAAS of Russia, the objective is to use the same standard ecosystem of the GTS Private cloud.

# The target design

The target for Cloud of Russia is to create a CLOUD IAAS on two Datacenters in Russia, to deploy VMs of test, development and the production.

The services proposed by the cloud of Russia will be the same that those proposed by the GTS CLOUD with a progressive delivery of the services (see chapter catalog of service for more information and to have an idea on the services of the first version and then the vision of the future solution.

The cloud IAAS in Russia is going to offer the possibility of creating VMs in the region of Russia with two availability zones, every AZ consists of a DC.

## Targets

Consist in:

* Central use of the VRA / VRO of GTS (Paris) private Cloud, to pilot the resources presented in Russia.
* Deployment of SGNA networks.
* Creation of a new access network in Russia sites (RIX-Russia)
* Extend the ecosystem used by the GTS (Paris) private cloud towards the infrastructures of Russia (DNSonDemand, Marley,…).
* Creation of the clusters of the resources of compute and storage on both Datacenters of Russia.
* Creation of a management cluster on both Datacenters of Russia.
* Creation of an extended network between both sites of Russia (DCs).
* Use of the network of the subsidiary of the ROSBANK for the management of the platform cloud of Russia.
* Creation of a CLOUD-IAAS to accommodate the platform of TEST, DEV, and ready to accommodate the platform of the production.
* The implementation of the necessary prerequisites for this design (see chapter prerequisite).

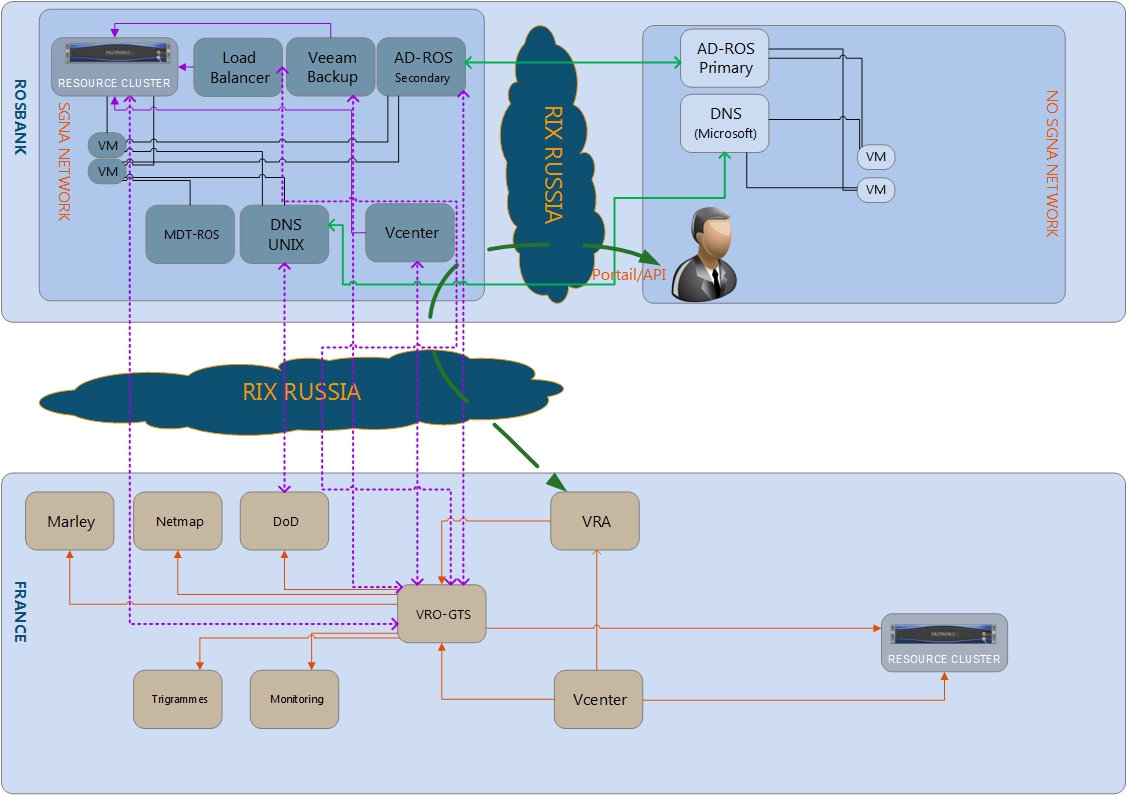
Advantages:

* Benefit from new services deployed in Paris.
* Perfect control of the service cloud deployed on the portal of the cloud of Russia.
* Use of the same ecosystem of the GTS (Paris) cloud; eventually the management of UPDATES and modifications in the APIs of the ecosystem is assured by the GTS (Paris) CLOUD team.
* Simplification of the operations and the support.
* VRA / VRO managed(run) by the team CLOUD of GTS.
* Deployment of an SGNA network.
* Follow-up of the standards of GTS.

Inconveniences:

* Creation of the accounts of service for the cloud (Paris) team for the piloting of the resources located to Moscow.
* Management of the openings of flows between Paris and Russia (PAX)
* Require integrating the ecosystem GTS (DoD, Marley, AD) with the infrastructures of Russia.

Below the diagram illustrates the target summarized:

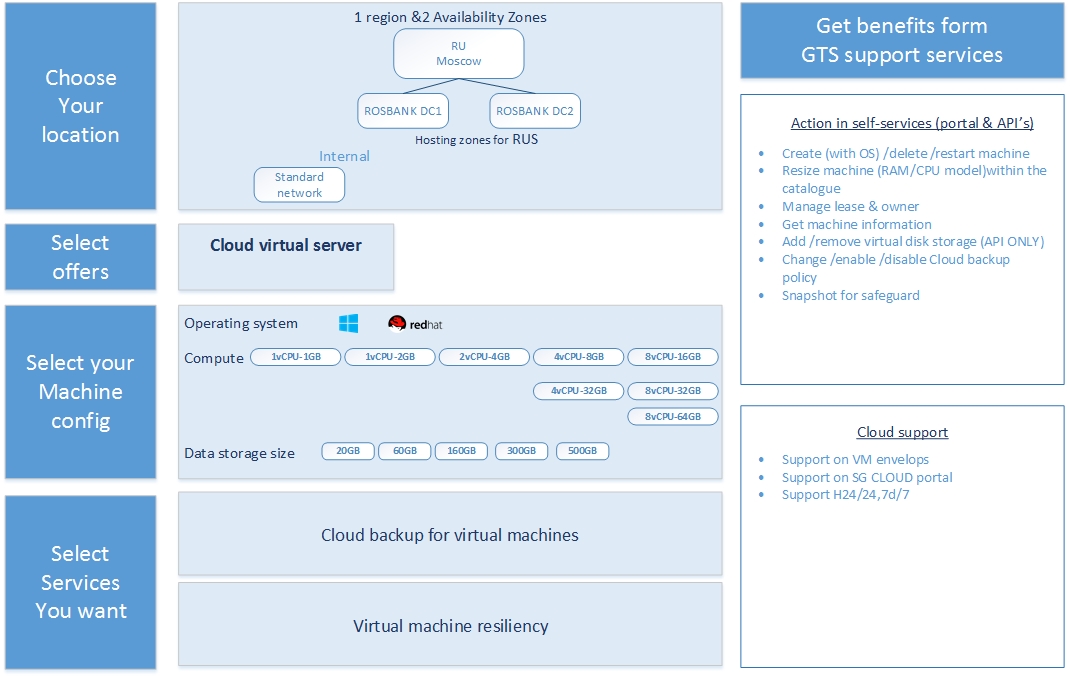


# The catalog of service

**First iteration:**

* Creation of the region of Russia with both zones of availability (zone DC1 and zones DC2)
* Creation of the Standard VMs COMPUTE and STORAGE.
* Creation of the VMS in the standard zones in the environments of TST, DEV, UAT, PRD
* Proposal of the standard Templates GTS Redhat 7.2, Windows 2012.
* Proposal of the service of the Backup of the VMs in the production environment.
* Proposal of the replication of the VMs of the production.

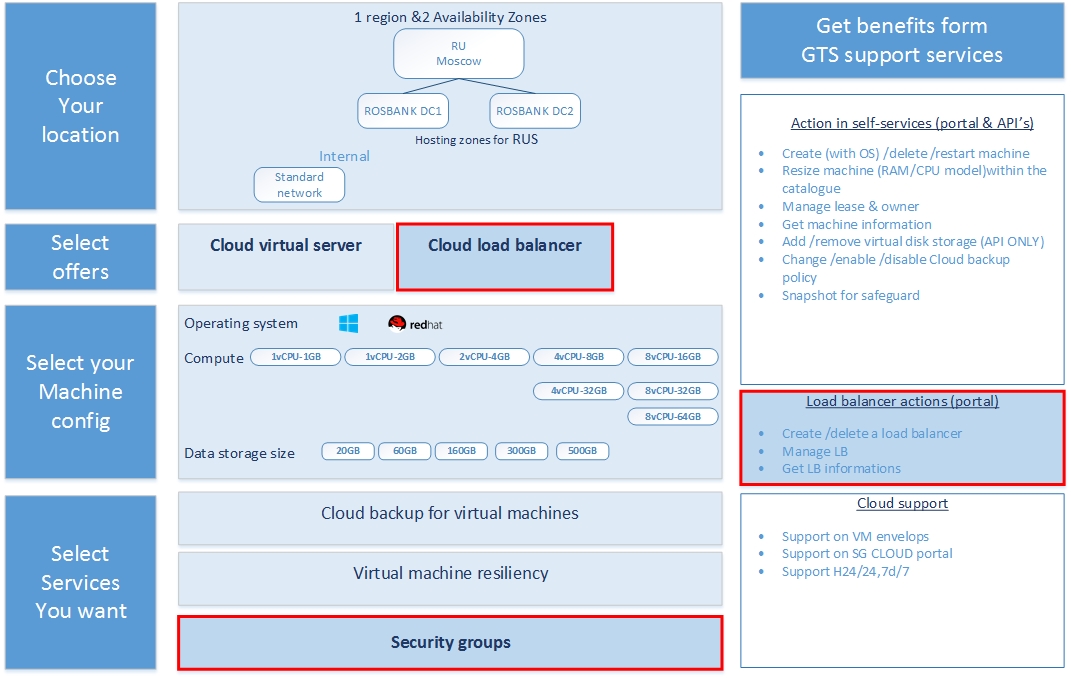
Below the catalog of service V0 wished in a first iteration:



**Second iteration:**

* Addition of the feature of load balancer, consumed by the portal cloud.
* Addition of the service of Security groups.

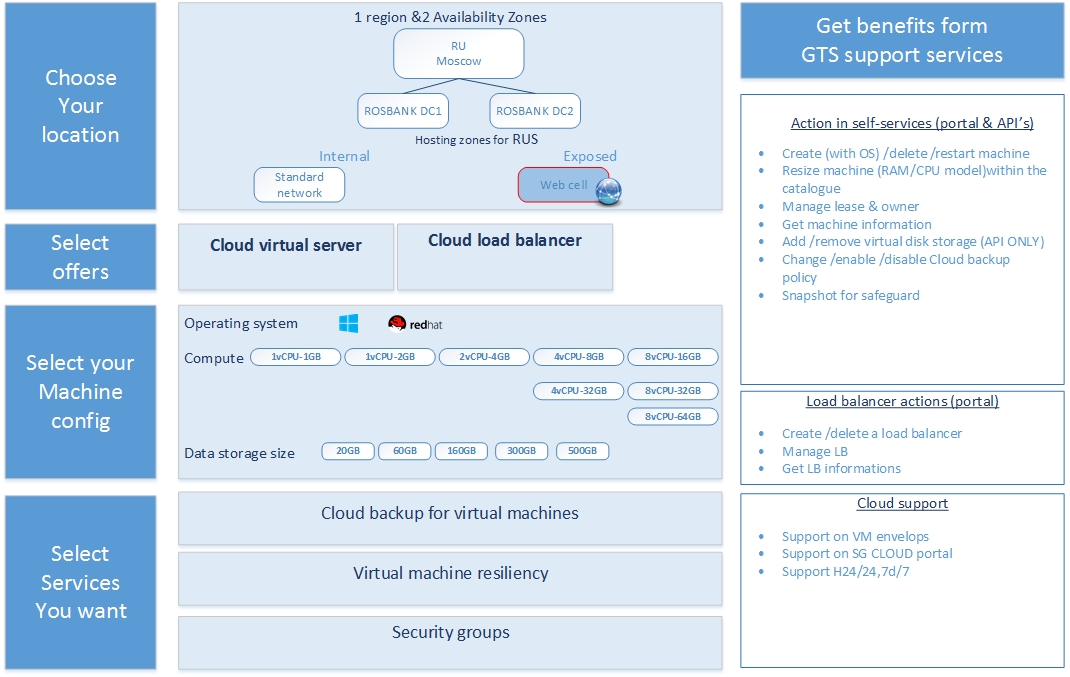
Below the catalog of service V1 wished in the second iteration:



**Third iteration:**

Below the catalog of service V2 wished in the third iteration:

* Addition of the Webcell zone.



The technical workshops can be set up on the specific points which could appear during the phase of project.

The perspective of the catalog of service V3 is to add the DMZ zone.

# Prerequisites

The following chapter is going to present us the components which constitute the necessary prerequisites to elaborate the cloud IAAS of Russia and they are going to help us for the setup of a right actions plan.

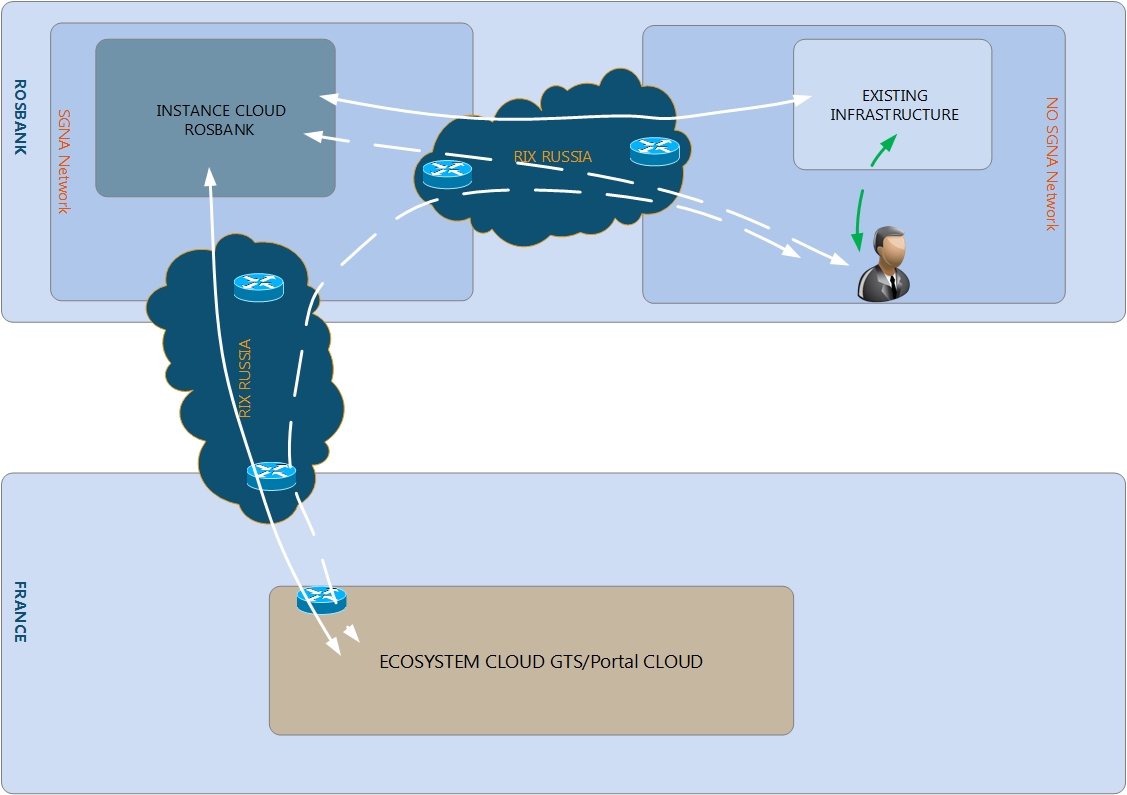
## The Network prerequisites

**Target**

The implementation of the cloud IAAS of Russia will require:

* The creation of the SGNA network for Cloud on Russia sites.
* The opening of flows between the SGNA network of the Russia sites and the ECOSYSTEM of the GTS (Paris) CLOUD.
* The existing of flows between the SGNA network and the not SGNA network of subsidiary in Russia.

The summary is in the diagram below: (we take an example of ROSBANK subsidiary)



### Network of the CLOUD

For this point of prerequisite, we need to:

* Create a redundant network infrastructure dedicated for the multi-tenant cloud of Russia on both DCs with a SGNA addressing.
* Assure that the network Subnet for the Security Zone is stretched between the different datacenters.
* Use even equipment’s type as Paris, for the choice of network equipment we need to plan a workshop (generally the Cisco N2K, N5K, N7K, N9K)

The diagram below presents the objective of this network.

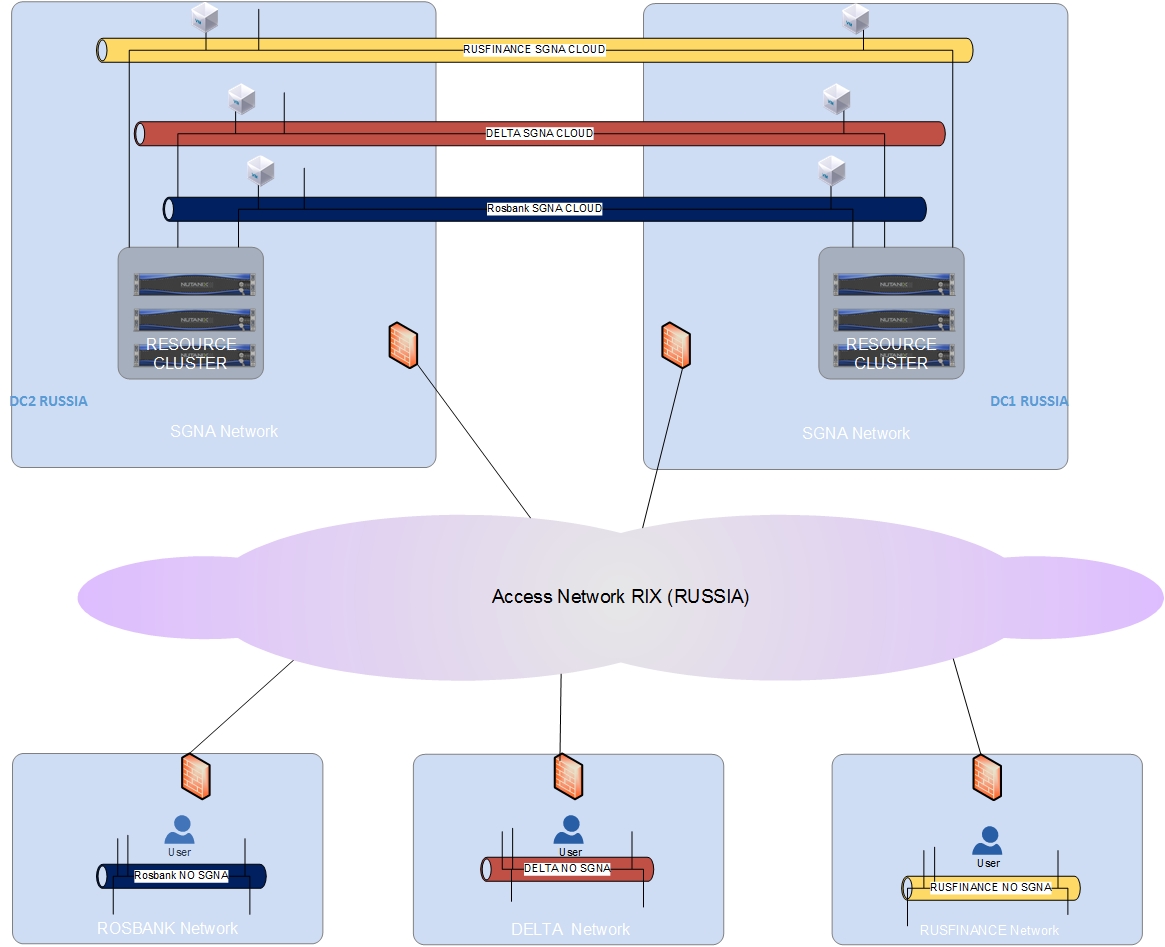
### Network urbanization

To respect the urbanization of the network we need:

* Create an access network in Russia. (RIX Russia)
* Connect subsidiaries to this access network.
* Connect the infrastructure network of the cloud of Russia to this access network.

The objective of this access network is to allow the various subsidiaries to use the cloud of Russia in safety.

The diagram below represents the global view of the vision of urbanization of the network of the cloud of Russia:



## The security prerequisites

**Target**

To open flows enter the SGNA network of the instance cloud of Russia and the ecosystem of GTS (Paris) cloud.

* Needs to supply a security folder (DS).
* Needs to validate this DS by the business line.

## The Cloud prerequisites

### VRO

**Target**

This design consists in:

* The use of the central VRO deployed in France.
* The use of the existing workflows with addition of the Russian context.
* The setting of VRO France that it is using the various subsidiaries infrastructures (AD / DNS / NTP / MASTER'S DEGREE SERVERS) on the SGNA network.
* The opening of the flows of administration between the VRO and the infrastructure of the various subsidiaries in Russia (ROSBANK,…).

### VRA

**Target**

For this design, we need of:

* A modification in the VRA of GTS (Paris) cloud so that it to supports the addition of a new infrastructure of the instance cloud of Russia.
* Piloting of Vcenter of the Instance Cloud of Russia from the VRA of GTS (Paris).
* Open flows of administration between the VRA of GTS (Paris) and the infrastructure of the Instance cloud of Russia.
* Open access in vRA (Portal Cloud GTS Paris) since Russia (through the PAX)
* Creation of accounts in the AD MSD EUR for every person (in Russia) wishing to be able to provision in the cloud.

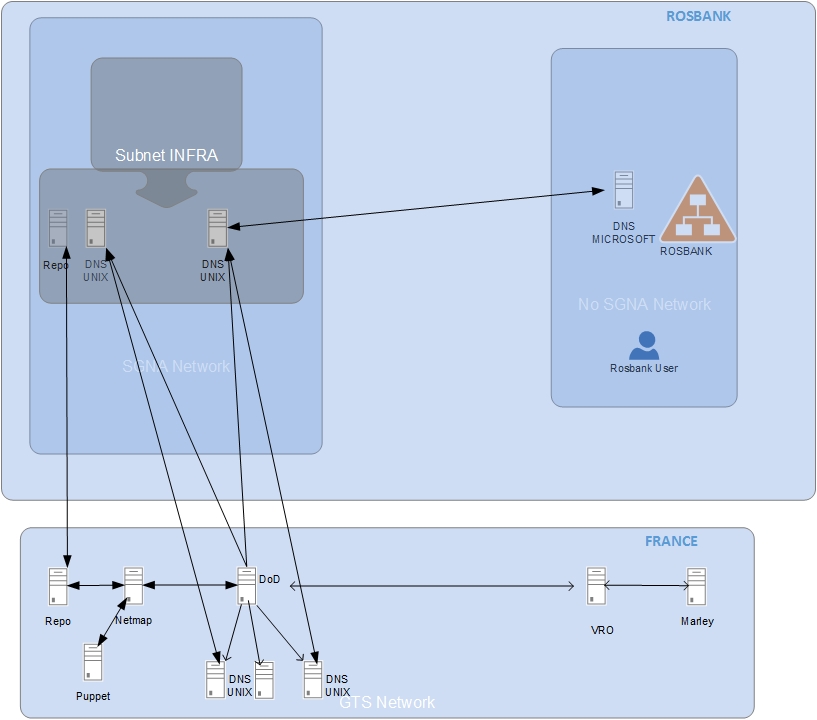
### DNS

**Target**

This design consists in:

* The configuration of DoD to manage the DNS of each subsidiary in Russia.
* Opening of the necessary flows between the DoD and the DNS servers of the subsidiaries in Russia.
* The VRO (GTS Paris) uses DOD'S API to manage the DNS names of the VMs of the instance cloud of Russia (precisely names of subsidiaries VMs in the cloud).
* Declaration of the DNS zones of the subsidiaries in the DoD.
* Check that the VLANs of the subsidiaries can solve the DNS name fr.world.socgen.
* Creation of DNS servers UNIX in the zone SGNA for all subsidiaries in Russia.
* Federate these DNS servers to DoD for the managed. (Once federated to DoD, it is the only one who can modify and write in these DNS servers).
* Configuration of these DNS UNIX servers with DNS servers (MICROSOFT) existing to assure the resolution between both zones (existing and the new zone of Cloud (*subsidiary.ru.roof.socgen*))
* Creation of a new zone of each subsidiary (example: rosbank.ru. roof.socgen )
* Synchronization of the new zones.
* Necessity of the openings of flows.

The summary is in the diagram below: (we take an example of ROSBANK subsidiary)



### Marley

**Target**

This design consists in:

* The VRO uses the API of Marley to manage the inventory of the VMs of the cloud IAAS of Russia.
* A configuration on Marley to manage the inventories of the subsidiaries is necessary.
* Openings of flows between Marley and the sites of the Cloud in Russia.

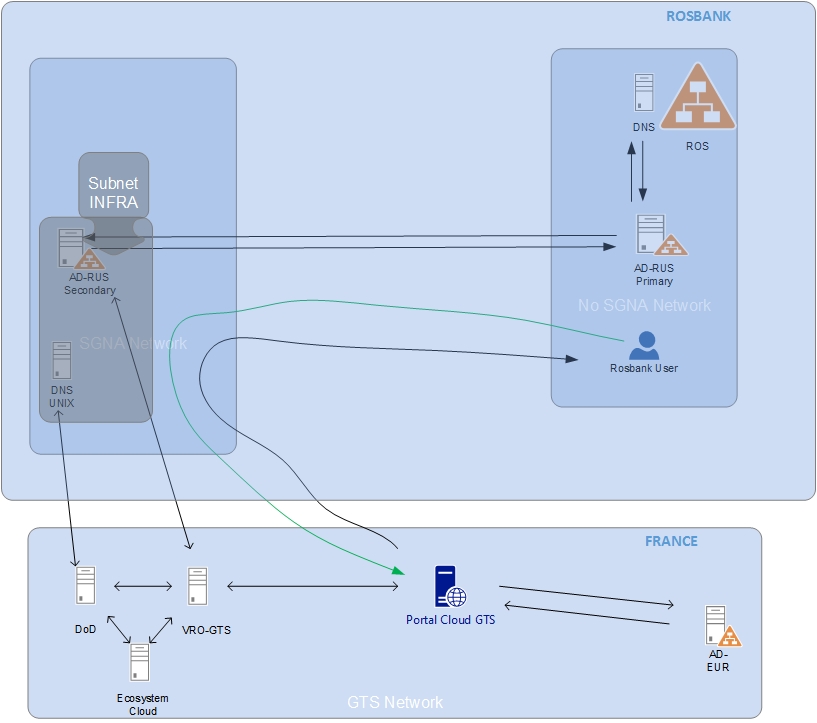
### AD

**Target:**

For this design, we need of:

* Use of the AD EUR for the authentication in the portal of the cloud.
* Modification in the AD of each subsidiary to automate the declaration of the VMs created from cloud portal in the domain of the subsidiary. (To add an account computer in the AD)
* The creation of a secondary DC-RUS on the SGNA network of each subsidiary.
* Synchronization of secondary DC-RUS on the SGNA network with the primary AD-RUS on the network NOT SGNA for each subsidiary.
* Modification in VRA / VRO to communicate with the AD-RUS through the SGNA network.
* Opening flows to authorize the access to Groupmembership in each subsidiary.

The summary is in the diagram below: (we take an example of ROSBANK subsidiary)



### Netmap

**Target:**

For this design, we need of:

* Declaration of Vlans and the configuration of SGNA network of each subsidiary in Netmap by the TFO teams of GTS (Paris).
* No deployment of the Netmap instance in the site of Russia is needed.
* Creation of the accounts with consultation privilege on the Netmap application for the IT team of Russia.
* Opening of flows towards the Web application of Netmap.

### Template and Post Install cloud:

**Target:**

For Windows

For this design, we use:

* The standard Master of the SG (GWIM)
* The same unique Template of GWIM,
* The post--install dedicated to each subsidiary.

We also need of:

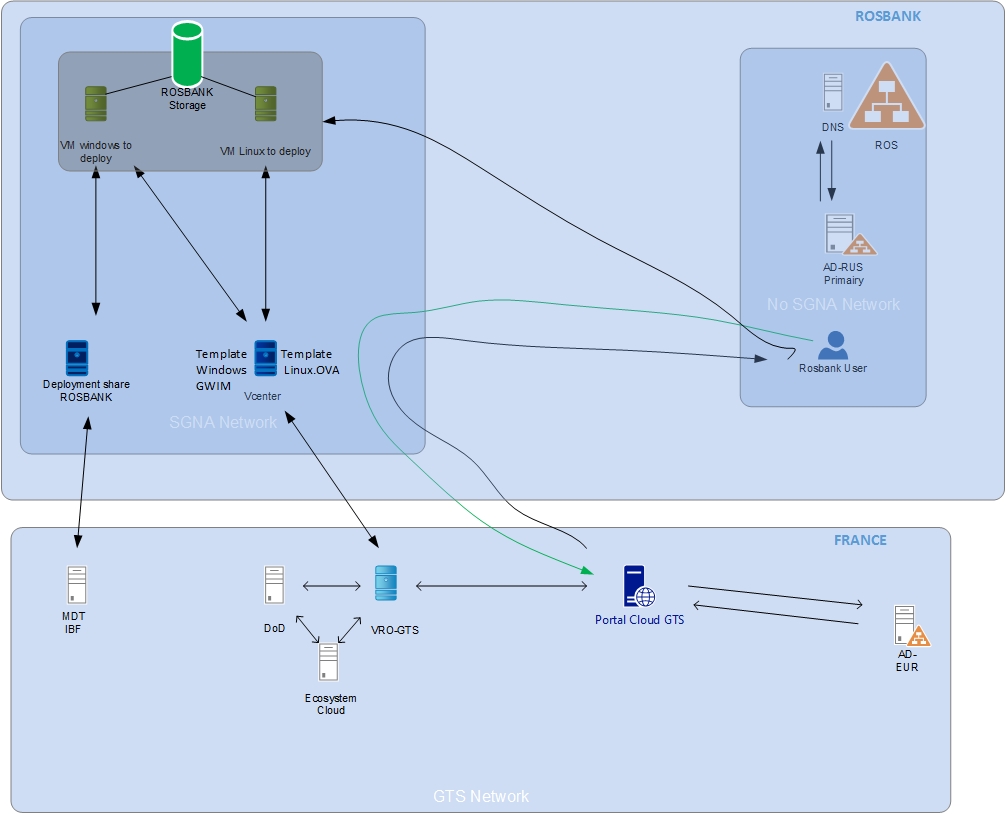
* Creation of a Deployment share (DS) in the instance cloud in Russia for each subsidiary.
* Opening of flows between the DS of the subsidiaries and the MDT of IBF
* Change in the MDT of IBF to add the new DS of the subsidiaries.

The management of the post-install is assured by the IT team of Russia.

For Linux:

We use the IBF Template by exporting it on the OVA format, then in the importing on the infrastructure of the instance cloud in Russia.

The summary is in the diagram below: (we take an example of ROSBANK subsidiary)



### Storage

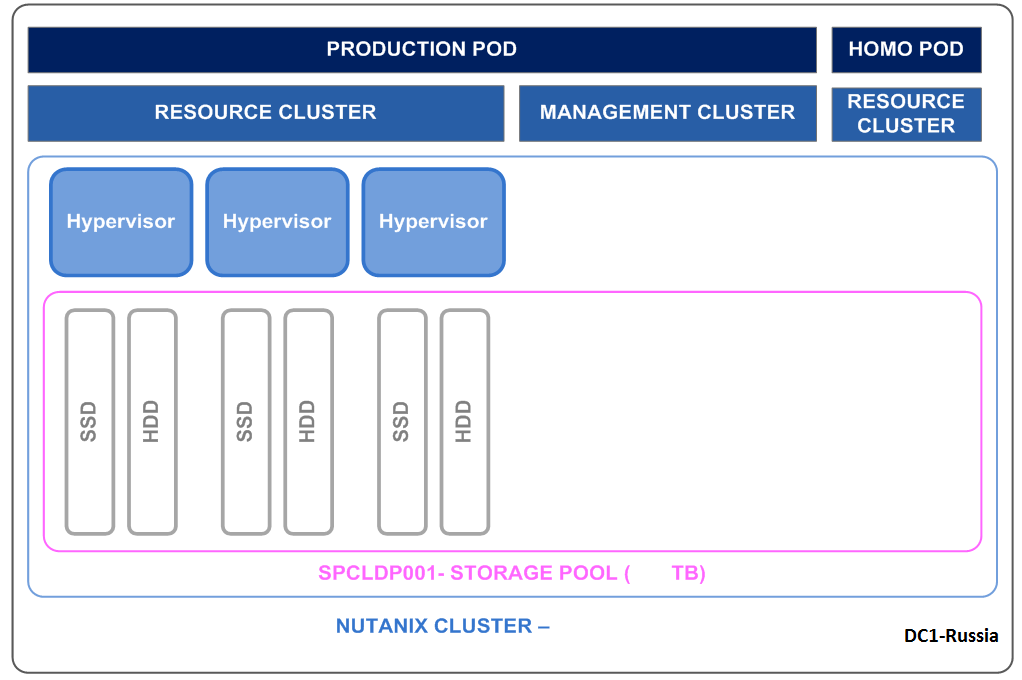
**Target:**

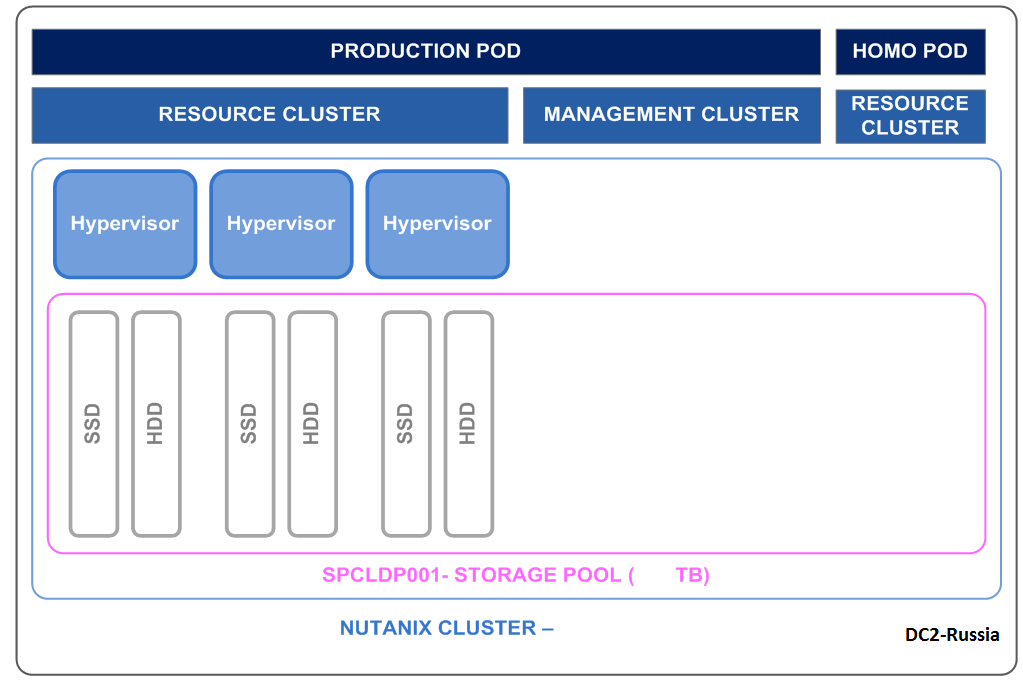
For this design, we need of:

* Use of the NUTANIX nodes on both Datacenter of Russia.
* The deployment of the same version of NUTANIX OS (GTS Paris) on each node of the Cloud infrastructure in Russia.
* Use native DR and replication capabilities of Nutanix to provide an Asynchronous Replication service between both Datacenters in Russia for production environment.
* On every Datacenter of Russia, we are going to deploy a POD of the production with a cluster of the resources constituted of:

* 3 nodes for the resource cluster of the production POD.
* The configuration of nodes is the following one:
* 1x DELL XC630-10
* 1x Intel Xeon E5-2690v4 (2,6GHz, 14C, Hide 35Mo, 9,6GT / QPI, 135W)
* 1x Intel Xeon E5-2690v4 (2,6GHz, 14C, Hide 35Mo, 9,6GT / QPI, 135W)
* 16x 32Go RDIMM, 2133MT/, Dual Rank, x4
* 1x 16Go, Card(Map) SD for IDSDM
* 1x Record(Disk) 64Go SSDR SATA-DOM
* 2x Records(Disks) Hot Plug 800GB Solid State Drive SATA Mid Endurance 2.5in Hot-plug Drive
* 8x Discs hard Hot Plug 2To NL-SAS 12Gbit / 512th 7200tr / min 2,5 thumbs(inches), 13G
* 1x PERC H730 raid(trek) controller, 1Go NV Hides
* 1x Card(Map) network girl Intel X520, Doubles port(bearing), 10Gb, 1GbE, DA / SFP +, I350 DP
* 1x iDRAC8 Enterprise

The summary is in the diagrams below





Infrastructure of compute:

**Target:**

For this design, we need of:

On every Datacenter of Russia, we are going to deployed a production POD for the resource cluster constitute of:

* 3 compute nodes of NUTANIX.

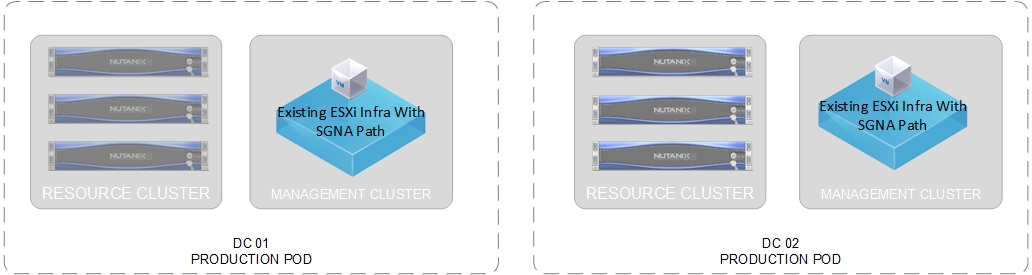
On every compute node, we install VMware ESXI 6.5.

A VCenter will be deployed on every Datacenter to manage the local resources of the cluster. (That is in the dedicated management cluster, either in the existing virtualization infrastructure with a SGNA path).

An administrator account will be created for the cloud team of GTS (Paris) on the VCenter of the Cloud of Russia, for the support reason.

An account of service will be created for the Proxy Agent of the VRA suite to be able to pilot the vCenter.

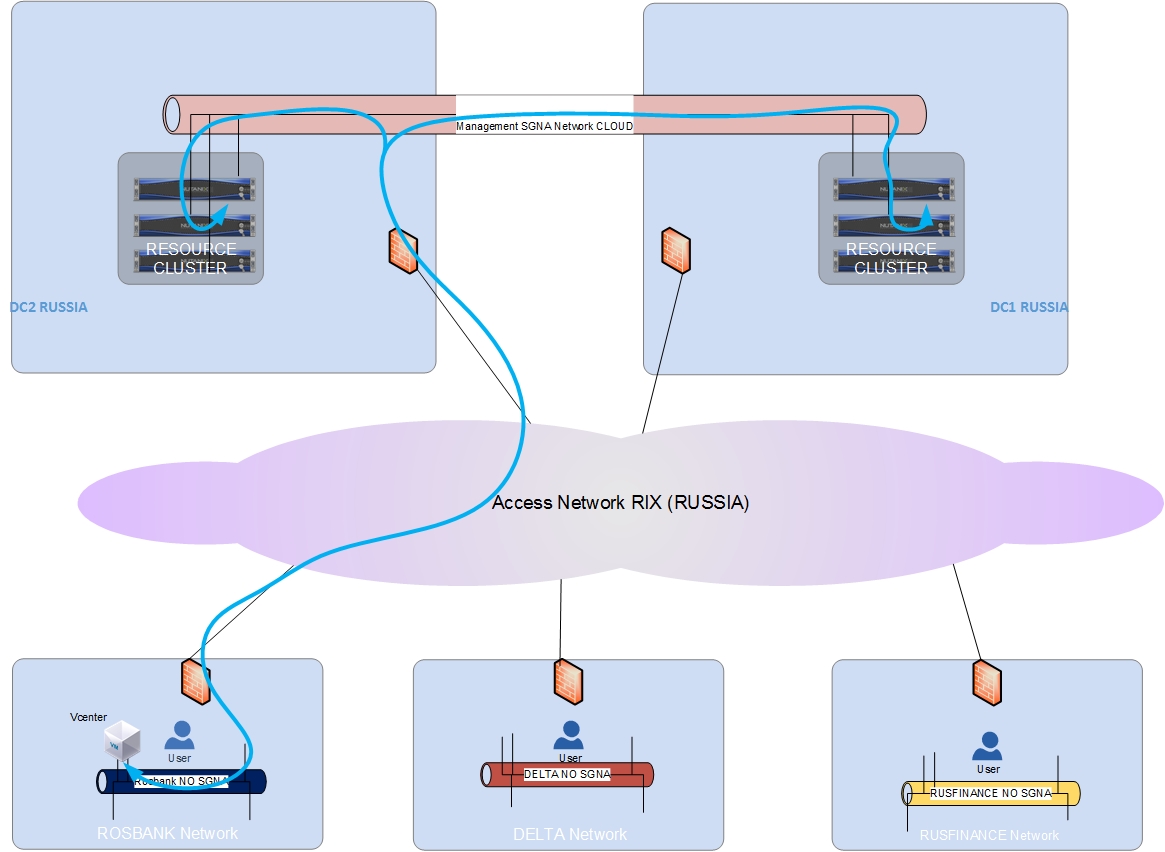
The summary is in the diagram below:



In a first phase of the project and for budgetary reason, we need to create a new VCenter in the existing infrastructure of the ROSBANK with a SGNA network path of the cloud and with an opening of flows in wide between this Vcenter and the network of management of the cloud.

We need to make the same thing in both DCs of the ROSBANK, with the HA for both Vcenter to assure the continuity of service.

The diagram below illustrious this point:



### Trigrams:

**Target:**

For this design, we need of:

Use of the application Iappli of GTS to manage subsidiary trigrams.

* Require creating an account in iappli for the manager of the subsidiary trigrams in Russia.
* Require having a SESAME account to use iaapli.
* Require Opening of flows to iappli .

### Taxation:

**Target 1:**

For this design, we need of:

* Using taxation from Iappli.

### Notification:

**Target:**

For this design, we need of:

* Use of the transfer option of emails between the SOCGEN box of the EUR account and the box email of the subsidiary user in Russia.
* Check of the possibility of the use of the interns messaging system of the Russia site.

### Backup

**Target:**

For this design, we need of:

* Use of the Veeam Backup solution with the same configuration of GTS.
* Opening of flows between the VRO (GTS Paris) and the Veeam servers in the SGNA network of the Russia site.
* Use of the same policy of Backup proposed by the cloud of GTS in Paris.
* Backup only VMs of the production environment.

The policies of backup for the platform of the production which will be implemented are the following ones:

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

### Licensing

To implement this solution and in term of licensing we need some licenses as mentioned below (list not exhaustive):

* NUTTANIX license
* Backup license
* VMware License Vcenter
* Microsoft license for (AD,MDT,…)
* Monitoring license
* Citrix Netscaler license

Charge estimation:

|  |  |  |  |
| --- | --- | --- | --- |
| Prerequisites | Actions | Who | Charge |
| Network |  |  |  |
| Security |  |  |  |
| Cloud (workflows,VRO,VRA) |  |  |  |
| DNS |  |  |  |
| Marley |  |  |  |
| AD |  |  |  |
| Netmap |  |  |  |
| Storage : |  |  |  |
| Trigrams: |  |  |  |
| Taxation: |  |  |  |
| Notification: |  |  |  |
| Backup: |  |  |  |
| Template and Post Install |  |  |  |
| Routes Opening |  |  |  |
| Design |  |  |  |
|  |  |  |  |

# Conclusion