RAMP interactive

# GET IN THE GAME!

## Security and Privacy

## Technical Environment

RAMP’s service provider is OVH.ca with their datacentre located in Beauharnois, Quebec. The backbone consists of a 20Tbps fiber-optic network. The network is guaranteed connectivity at 99.95% with exceptions of scheduled downtime. RAMP’s products run on private dedicated hardware with virtualization, our hardware is not a shared resource. Our bandwidth is dedicated and burstable to 10Gbps per machine. We can increase compute capacity and scale on demand.

## Network Architecture / Infrastructure

**OVH Weathermap (Beauharnois, QC)**

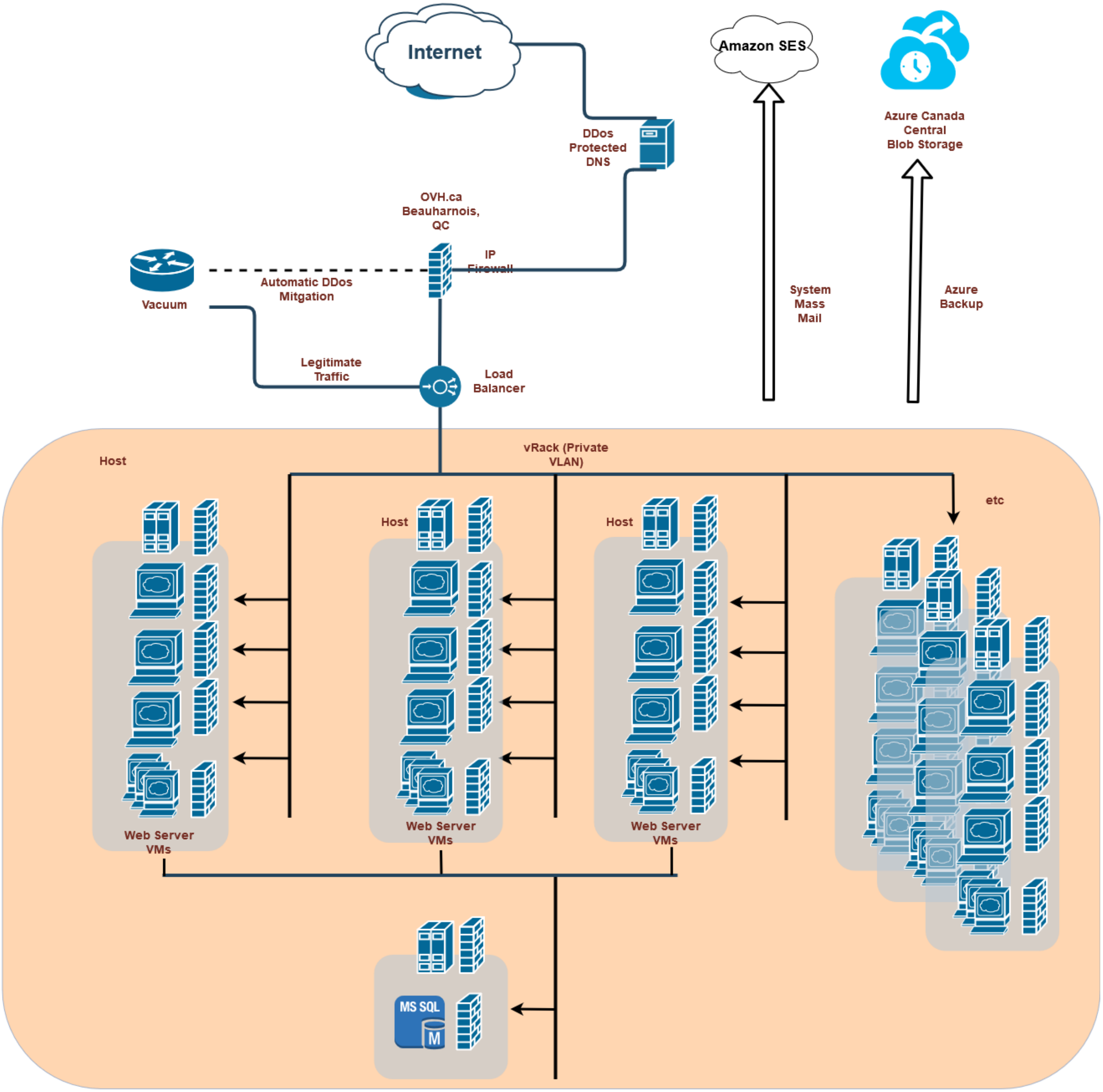
- http://weathermap.ovh.net/#beauharnois_core
- http://weathermap.ovh.net/#beauharnois1
- http://weathermap.ovh.net/#beauharnois2
- http://weathermap.ovh.net/#beauharnois4
- http://weathermap.ovh.net/#beauharnois5
- http://weathermap.ovh.net/#beauharnois6
- http://weathermap.ovh.net/#beauharnois7

## RAMP employs various infrastructure level security features such as:

- Server IP restrictions
- IP Firewalls
- Software Firewalls
- Private Networks
- Server Isolation
- Failover IPs
- HTTPS (TLS), HSTS, Modern Ciphers
- FTP over TLS (restricted IP)
- Restricted VPN
- DDoS Protection

## RAMP Platform Features include:

- Encrypted Sessions and Session Timeouts
- IP restricted API access
- Available Multi-Factor Authentication
- Restricted Access (Role Based Authentication)
- Password Rules, Expiry, & Forced Resets
- Encrypted data
- Multi-Level data failsafe implementation to ensure encapsulation and isolation of data


Internet
Amazon SES
Azure Canada
Central
Blob Storage
DDos
Protected
DNS
OVH.ca
Beauharnois,
QC
IP
Firewall
Vacuum
Automatic DDos
Mitgation
System
Mass
Mail
Azure
Backup
Legitimate
Traffic
Load
Balancer
Host
vRack (Private
VLAN)
Host
Host
etc
Web Server
VMs
Web Server
VMs
Web Server
VMs
MS SQL
M

## Additional Network Features:

### DDos Protected DNS

Our Managed DNS Service provider has 27 Anycast Data Centers on 6 continents and provides DDoS Protected DNS hosting with a 1,000% uptime SLA.

### Network DDoS Mitigation

As the volume of data that exists on the internet grows exponentially, distributed denial-of-service (DDoS) attacks are becoming increasingly common.

A DDoS attack aims to make a server, service or infrastructure unavailable. An attack can take on different forms. It may saturate the server's bandwidth to make it unreachable, or it may overwhelm the machine's system resources, stopping it from responding to legitimate traffic.

Our Anti-DDoS solution precisely fights against these distributed denial-of-service attacks. With all of our services, we include a migration solution based on a unique technology, which combines three technologies to:

- analyze data packets quickly in real-time
- divert your server's incoming traffic
- separate non-legitimate requests from others and let legitimate traffic pass through

### IP Load Balancer

Our Load Balancer distributes the workload among your various services across the data centre. It ensures the scaling of infrastructure in the event of heavy traffic, with optimized fault tolerance and response time. All this with a service level aiming for Zero Downtime.

### Backups

RAMP utilizes local datacentre and Microsoft Azure Blob Storage for data backups. Backups are done daily and incrementally every 15 minutes. Backups are located in Central Canada.

## Protection of Confidentiality and Privacy. Process of collecting Data to Ensure Isolation, Privacy and Integrity

RAMP's platform is a multi-tenant application. In terms of *tenants*, each Governing Body is a tenant, and every organization within Governing Body are tenants. The database strategy is a shared database used by all tenants – (e.g. Governing Body and its' member Regions, Leagues and Clubs). Isolating tenant specific data is done by using a discriminator column to every table which is tenant specific, and to make sure that all queries and commands will filter the data based on it.

With this strategy dealing with tenant shared data is simple, we don't just filter it. Isolating data is what we do. For this we make sure that ALL the queries and the commands that deal with tenant specific data get filtered by the discriminator. Having well encapsulated data access through which all the queries and commands go can play a key role in assuring this isolation. The data access layer is where we intercept each query and command and determine if it deals with tenant specific data.

## Canadian Privacy Laws and Anti-Spam Legislation

RAMP follows all Canadian Privacy Laws and Anti-Spam Legislation standards including specific guidelines on how we collect, use and disclose personal data. This includes, but is not limited to following these basics:

(i) You need consent to collect, use or disclose personal information.

(ii) When using information, you must only do so for the purpose to which the individual has consented.

(iii) Regardless of consent, you have to limit the collection, use and disclosure of information to what "a reasonable person would consider appropriate in the circumstances."

(iv) Individuals must have the ability to access the information they have provided and make changes or correct mistakes.

RAMP utilizes Privacy Impact Assessment tools and principles to develop a standardized commitment for its Customers and its Membership in the form of a document that covers the Ten Principles of Privacy Protection.