



OnCloud Infrastructure

IdSurvey Cloud

We've been hosting customers' data with a special focus on its protection for more than 15 years. To guarantee the highest security we use efficient devices and we adopt a set of best practices to all levels of our organization and infrastructure.

Security systems:

- Only credited employees can physically access the servers.
- Access to the datacenter with badge only.
- Video and human surveillance 24/7.
- Rooms with fire detection systems.
- Tech staff available 24/7.
- Electrical generators with 48 hours autonomy.



Cloud Infrastructure

Our Cloud is based on VMware Enterprise PLUS and it's located in the European Union. By demand, we can also activate the service in countries outside the EU.

Characteristics of every physical server

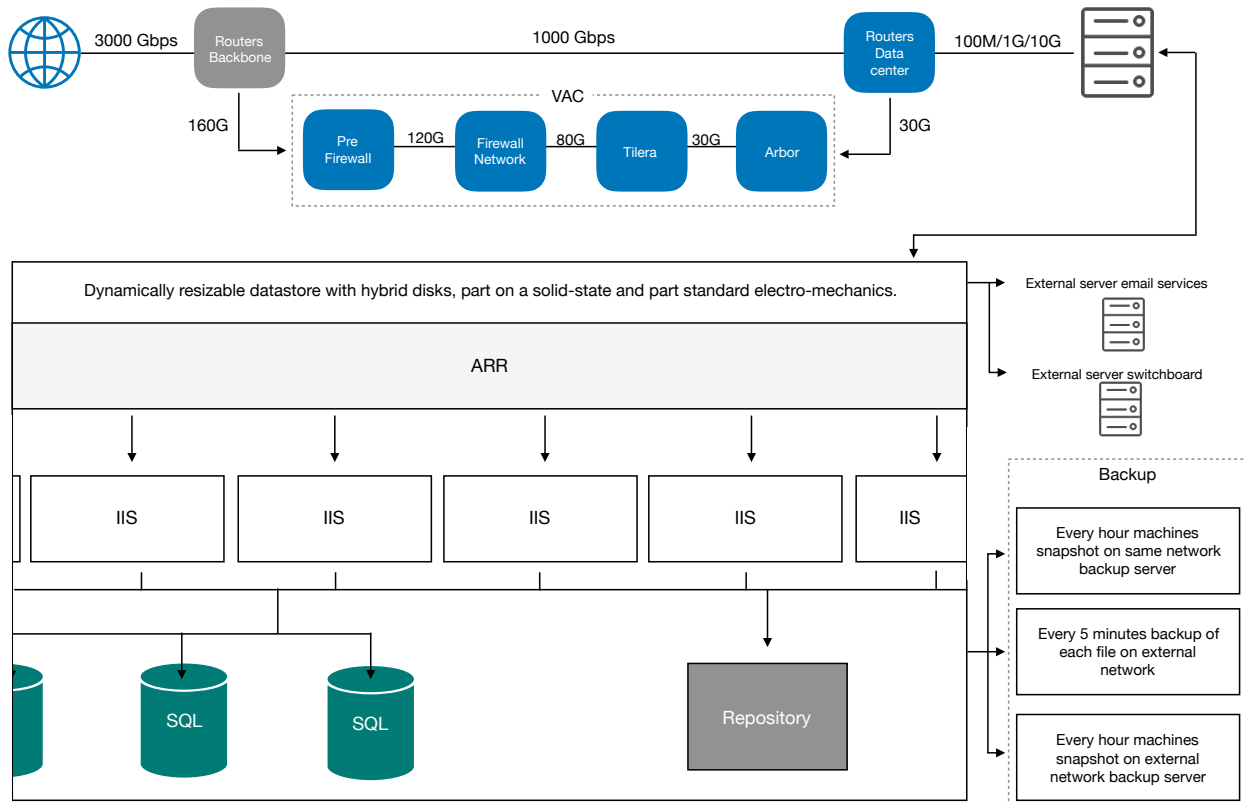
| | |
|---------------------|---------------------------------------------------|
| RAM | 128 GB ECC |
| Processor | Intel Xeon E5-2690v2 |
| Core/Thread | 10/20 |
| FrequenCY | 3 GHz |
| DISK | SSD - Intel DC S3500+ "Read Intensive" 4x 10 Gbps |
| Connectivity | 4x 10 Gbps |
| Uptime | 99.99% |
| Connection | 4x 10 Gbps |
| VMDq | 64 per porta |
| SR-IOV / VF | 64 per porta |
| Chipset | Intel X540 |

Virtual servers managing the platform with Application Request Routing (ARR). All virtual machines have the windows server datacenter operative system.

Unlimited resources

When you define your Cloud settings, you don't have to worry about your company growing requirements or about your projects ambition. You set the limit! You can increase your resources by request in a couple of hours - even for limited period of time. Dynamically resizable datastore with hybrid disks.

Infrastructure scheme



Security and characteristics

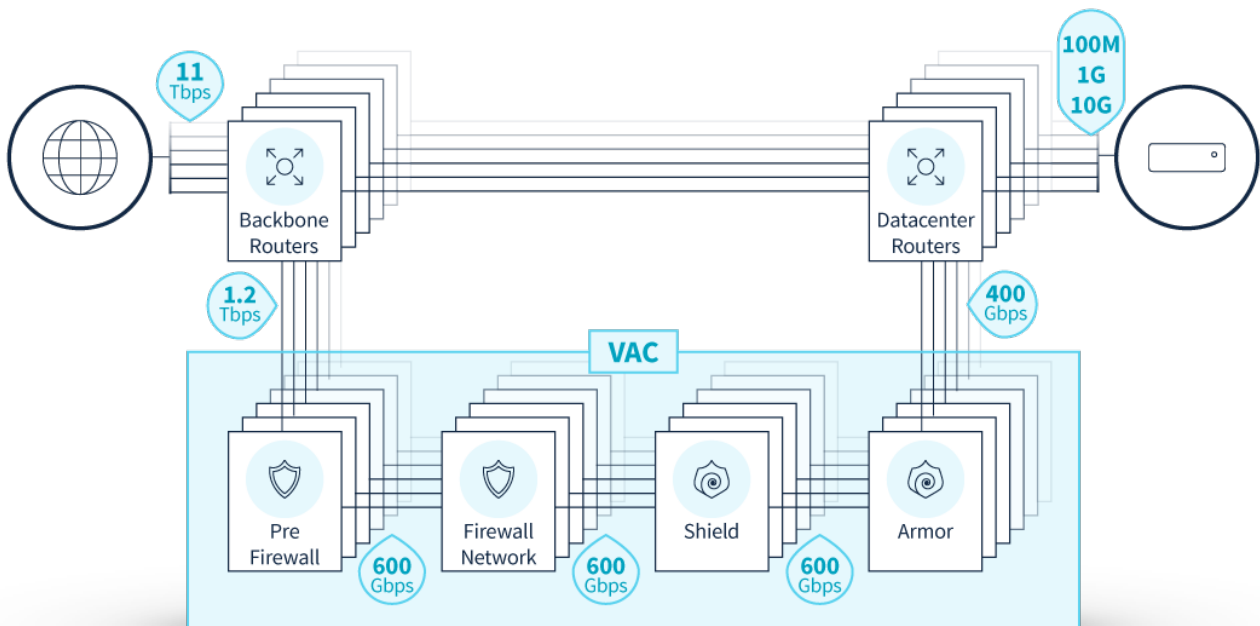
- VMware with automatic Deploy updates included
- Guaranteed bandwidth: 1,5 Gbps
- Up to 4000 preconfigured vLAN
- Support 24/7/365
- Customized vSphere Client
- Resilience test
- Monitoring vScope
- Automatic Host management
- Dedicated extra resources in just 20 minutes
- Automatic deploy
- Multi Datacenter
- 100% VMware standard
- SSL
- Backup

Anti-DDoS PRO protection

Mitigation is a term we use to describe means and measures that reduce the negative effects of a DDoS attack. Mitigation consists of filtering illegitimate traffic and hoovering it up with the VAC, while letting legitimate packets pass.

The VAC consists of multiple devices, each one with a specific function to block one or more types of attack (DDoS, Flood, etc.). Depending on the attack, one or more defensive strategies may be put in place on each VAC device.

VAC



Actions carried out on the Pre-Firewall

Fragment UDP
Size of packets
Authorisation of TCP, UDP, ICMP, GRE protocols
Blocking all other protocols

Actions carried out on the Firewall Network

Authorize/block an IP or a sub-network of IPs
Authorize/block a protocol: IP (all protocols), TCP, UDP, ICMP, GRE
Authorize/block a port or TCP/UDP port interval
Authorise/block SYN/TCPs
Authorize/block all packets except SYN/TCPs

Actions carried out on the Armor

Malformed IP header
Incomplete fragment
Incorrect IP checksum
Duplicated fragment
Fragment too long
IP/TCP/UDP/ICMP packet too long
Incorrect TCP/UDP checksum
Invalid TCP flags
Invalid sequence number
Zombie detection
TCP SYN authentication
DNS authentication
Badly formed DNS request
DNS limitation

Actions carried out on the Shield

Malformed IP header
Incorrect IP checksum
Incorrect UDP checksum
ICMP limitation
Incorrectly fragmented UDP datagram
DNS amp

Backup

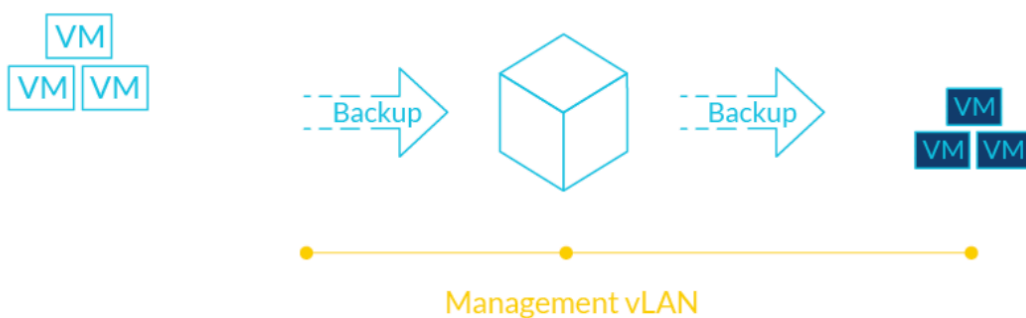
Snapshot every six hours on backup servers in the same net. Snapshot every six hours on backup servers in external net. Backup every hour of every single file in external net.

Backups are stored for 6 months. The backup is completely automatized. Backups are done on selected VM thanks to Veeam Server. The managing vLAN of your infrastructure allows data traffic to the Repository built in RAID.

The external and internal backup system allows data recovery even in case of serious crash in the principal servers headquarters.

If the external storage server is not available because of a serious crash, the system will immediately notify the tech staff of the malfunction and they will shortly restore the backup functioning on external net.

We want to stress out that the tested IdSurvey server infrastructure is completely redundant and we never needed a backup restoration up to now.



Server farm OnCloud Certifications

The Cloud generally complies with ISO / IEC 2700 1:2013 certification, SOC 1 Type II (SSAE 18 and ISAE 3401) and SOC 2 Type II international certifications, and PCI DSS Level 1 certification.



ISO 27001

ISO 27001 is a globally recognized standard for the establishment and certification of an information security management system (ISMS).

SOC 1 e SOC 2

SOC 1 type II certifies that the server farm defined and installed control systems for customers' data protection, while SOC 2 type II evaluates the controls for the international legislation established by AICPA (American Institute of Certified Public Accountants) on its « Trust Services Principles ».

CSA STAR Self-Assessment

Our system is included in the STAR registry of the Cloud Security Alliance for the Dedicated Cloud offer. This initiative informs customers on conformity to CSA procedures of Cloud Computing services and on measures to guarantee information system security.

Certificazione OpenStack Powered

Infrastructure Donor of the OpenStack in 2015, OVH got the OpenStack Powered certification in October 2016. The company works with other provers of the Community to standardize OpenStack to guarantee to the users compatibility with different services.



Viale Romagna 69
Città di Castello, 06012
Perugia, Italy - Time Zone GMT +1

Phone:
+39 075 851 14 73

Fax
+39 075 851 28 89

Web
www.idsurvey.com