OVHcloud Partner Program

Discover Security Solutions

Summary

01
Compliance
02
Information security
03
Data protection
Data resilience
04

01 Compliance

01 Global certifications

02 Regional certifications

02 Sectoral certifications

01 Global certifications

OVHcloud has global ISO certifications : 27001, 27017, 27018 and protection of personal data ISO 27701

ISO 27001 / 27017 / 27018

ISO/IEC 27001:2013 Certification and ISMS relating to information security management systems for cloud services

ISO 27701

ISO/IEC 27701:2019 Certification and PIMS relating to personal data processing security management

01 Regional certifications

OVHcloud is also compliant (among others certifications) with :

- GPDR for EU (General Data Protection Regulation)
- SOC1,2,3 (control over financial reporting)
- CSA STAR (Cloud Security Alliance)
- G-Cloud UK for Public Sector Cloud Service Procurement in the UK
- SWIPO (related to cloud service portability)

OVHcloud is also one of the few companies that has a SecNumCloud qualification solution (ANSSI French highest ranked security cloud qualification)

02 Sectoral certifications

OVHcloud is also compliant with sectoral certifications such as :

- HDS (Health Data Services) on Hosted Private Cloud, Baremetal servers Adv,n Scale and HGR, Public Cloud, NAS-HA and EFS
- Healthcare data in Europe
- HIPAA & HITECH in the US
- PCI DSS for card payments on Hosted Private Cloud Vmware Premier
- EBA for European Banking services

02 Information security

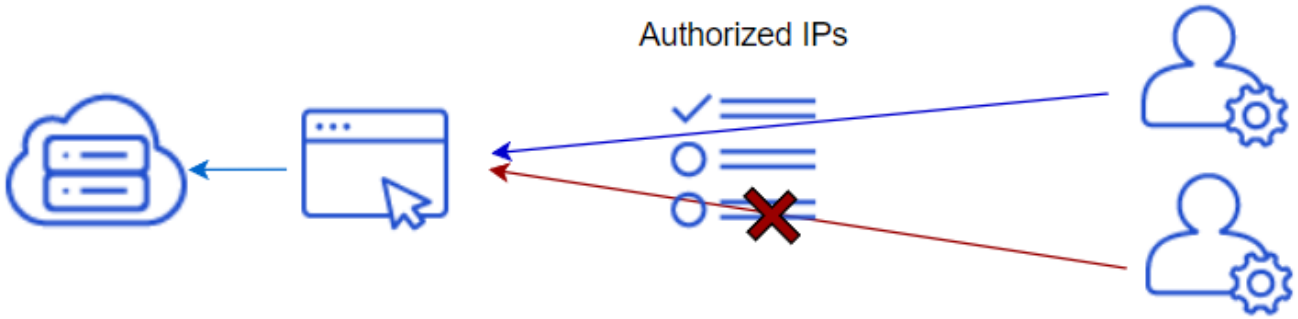
01 Securing accesses

02 Handling security flaws

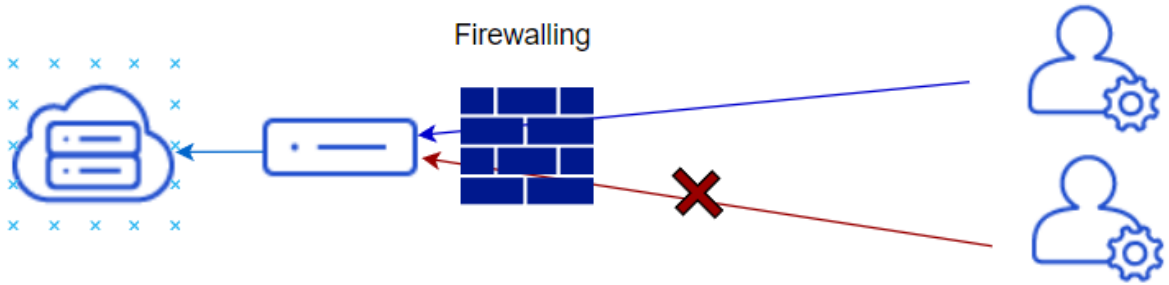
03 Patch management

04 Logs management

IP Whitelisting



Firewalling

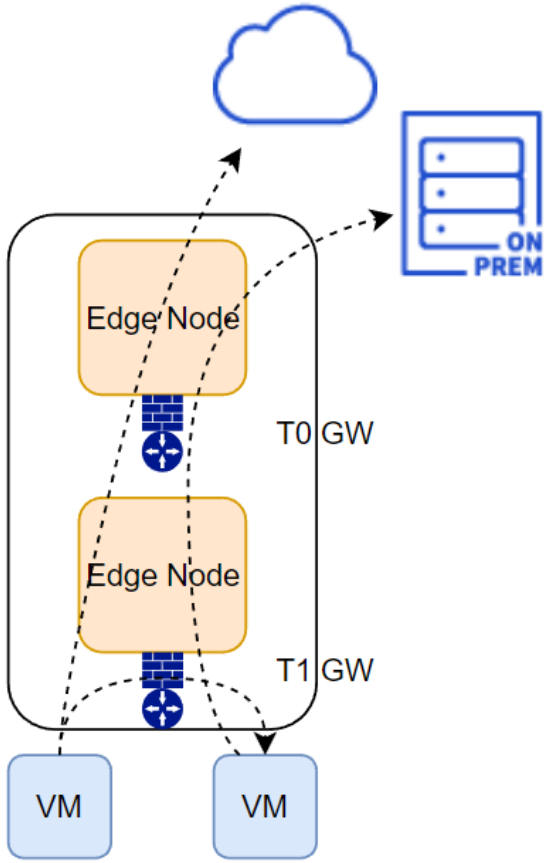


+ Add a rule

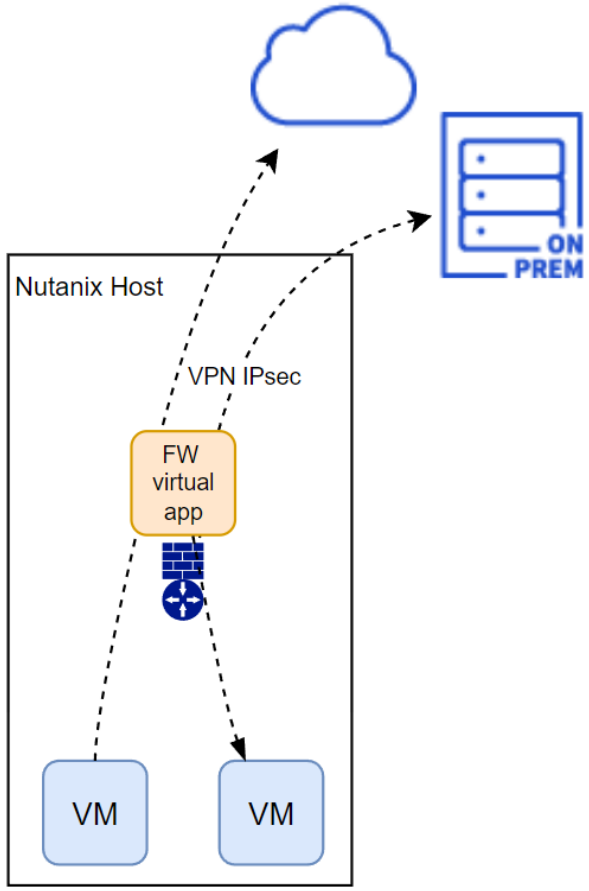
Enabled

Priority	Mode	Protocol	Source IP	Source port	Destination port	TCP status	Status
0	Authorise	ICMP	10.15.122. /32				Active
1	Authorise	TCP	10.15.122. /32	389	389		Active

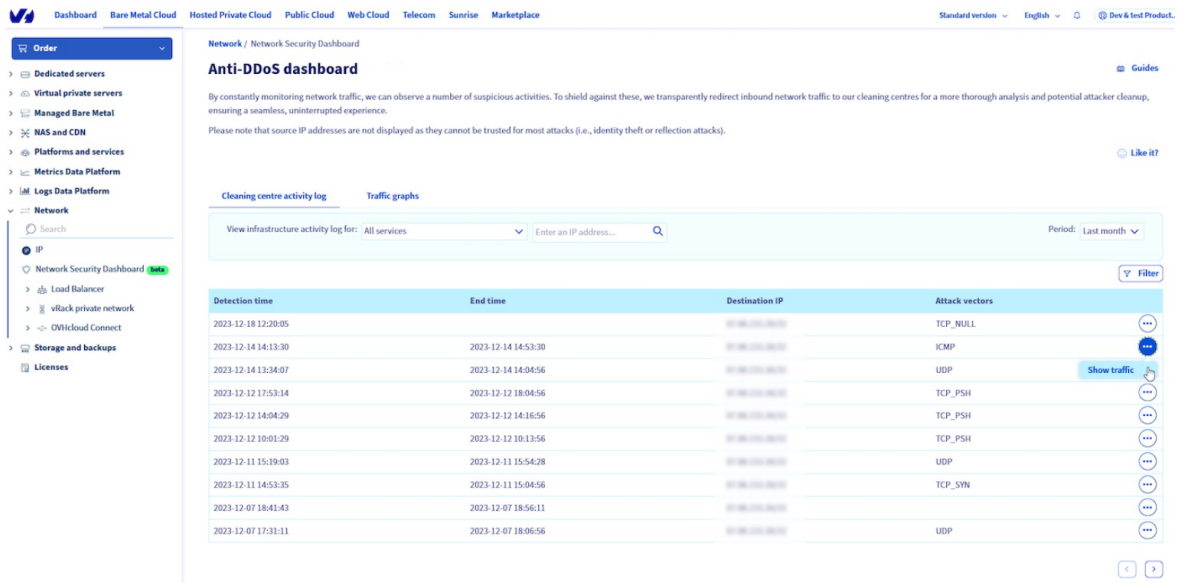
Firewalling



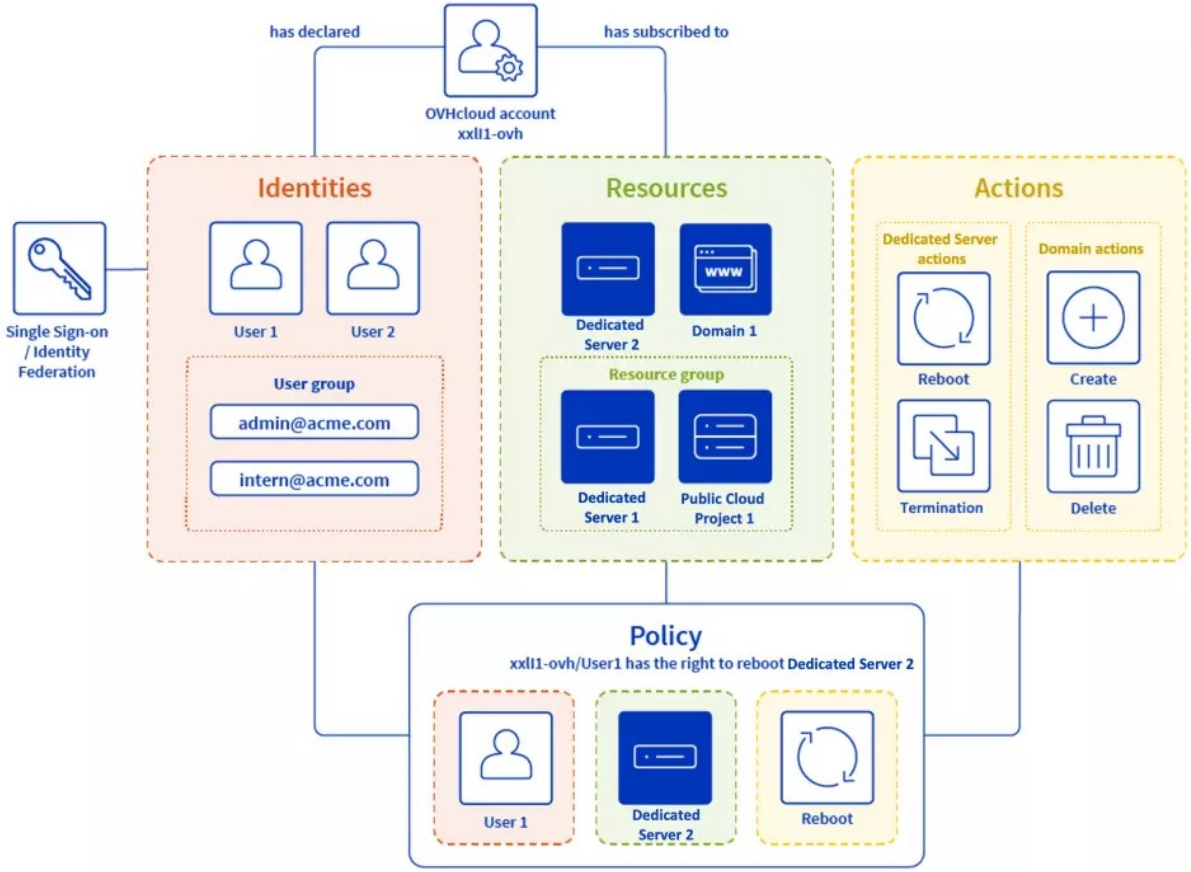
Firewalling



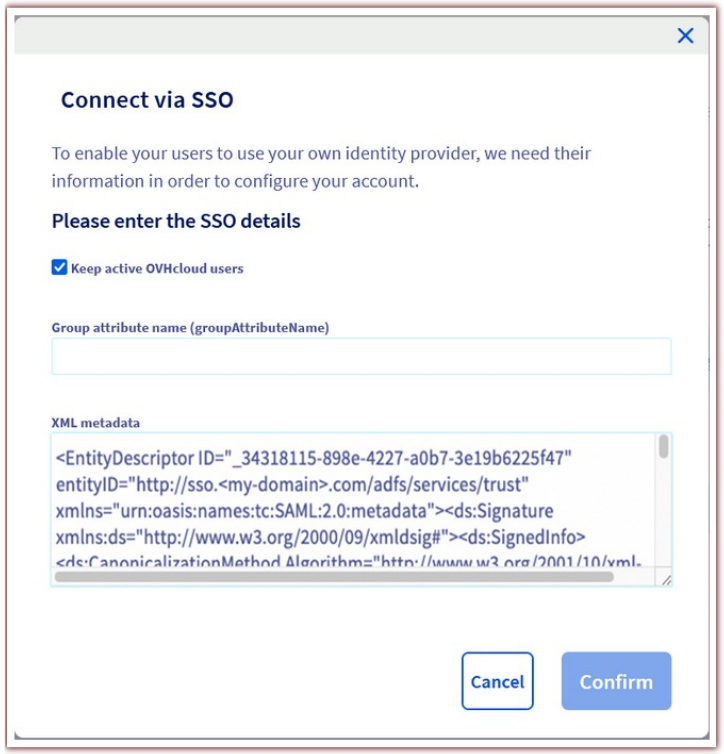
OVHcloud Anti-DDOS protection

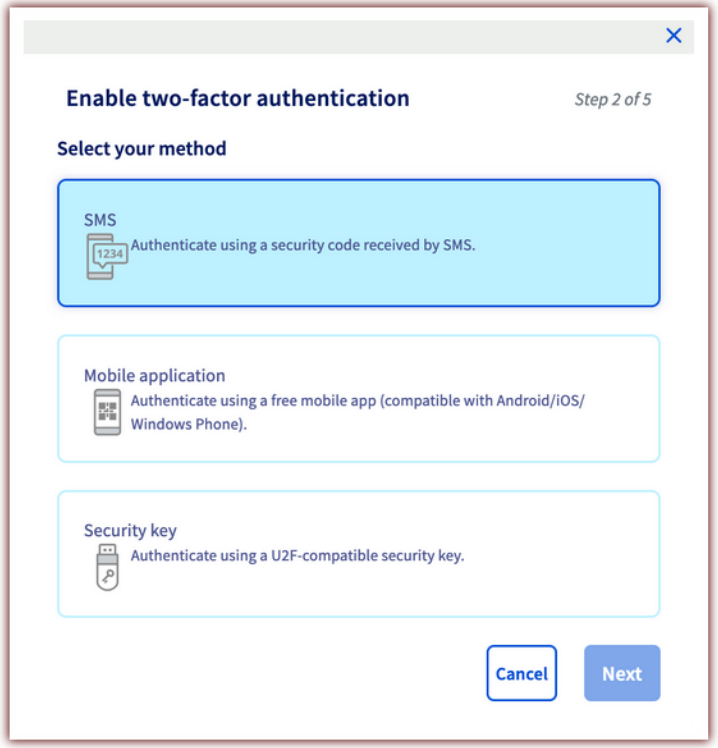


IAM : Identity Access Management



SSO (Single Sign On) and MFA (Multi Factor Authentication)





02 Handling security flaws

OVHcloud

Chère cliente, cher client,
Dans le cadre de notre processus de Gestion de la Sécurité, les équipes Hosted Private Cloud d'OVHcloud ont analysé la vulnérabilité Veeam publiée le 7 mars 2023. Cette faille concerne Veeam.Backup.Service.exe accessible sur le port 9401/TCP
Cette vulnérabilité concerne toutes les versions de Veeam Backup & Replication.
Voici le détail concernant cette vulnérabilité et les plans d'action associés :
CVE-2023-27532

1. **Lien** : https://www.veeam.com/kb4424
2. **Périmètre** : Offres Veeam Enterprise et Veeam Managed d'OVHcloud
3. **Score** : 7.5
4. **Impact** :
    1. Notre offre Veeam Managed n'est pas impactée. Notre configuration comporte une sécurité spécifique qui empêche l'exploitation de la faille. Toutefois, une maintenance de type « Emergency » a été planifiée dans les heures à venir pour bloquer le port 9401/TCP. Cette maintenance peut causer une indisponibilité de 5 minutes sur votre service Veeam Managed.
    2. Concernant notre offre Veeam Enterprise, vous pouvez être impacté en fonction de votre configuration. Nous vous conseillons d'appliquer les correctifs suggérés par Veeam dans la KB suivante : https://www.veeam.com/kb4424.

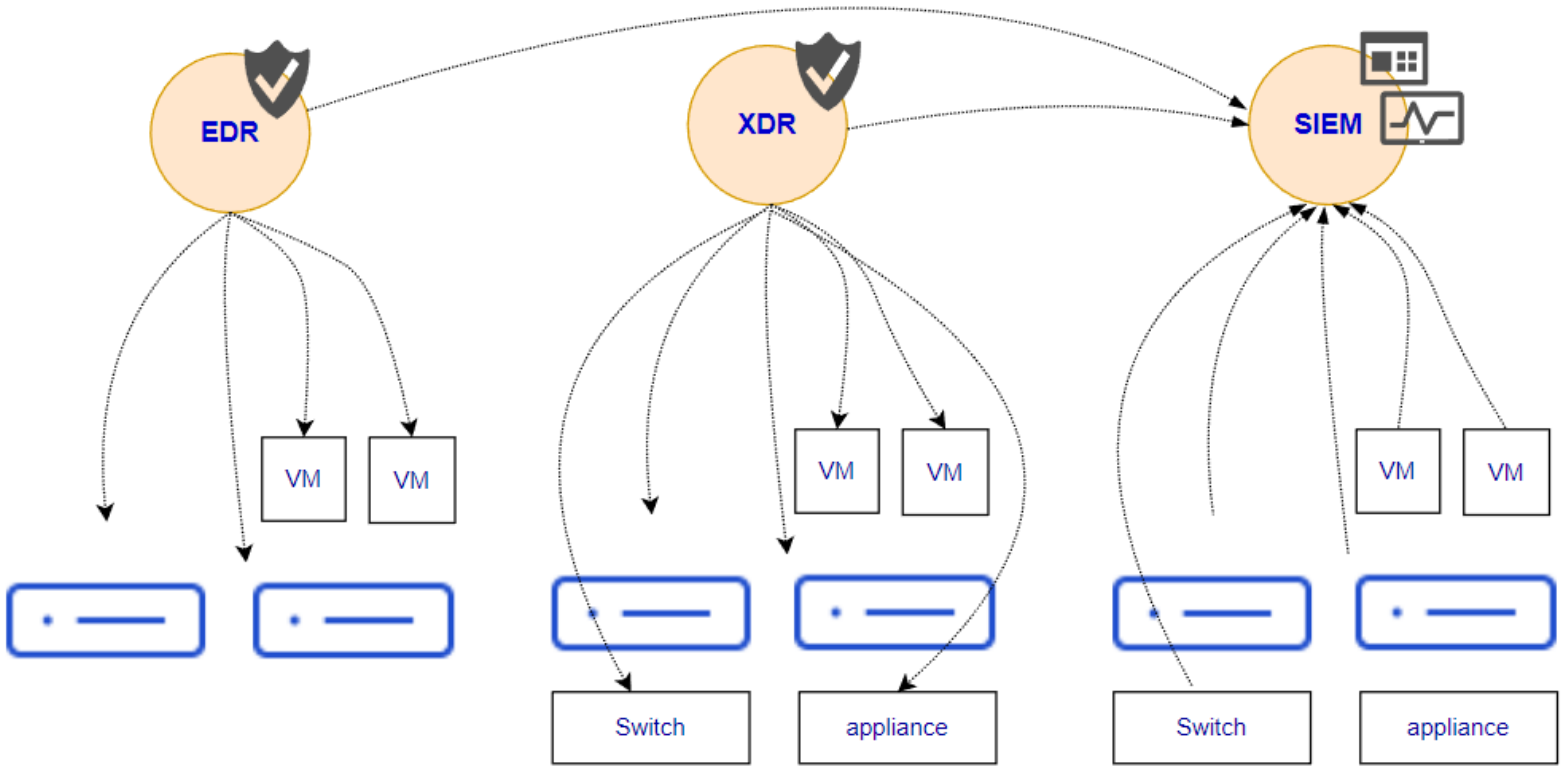
Notre équipe Support reste à votre disposition si vous avez des questions supplémentaires.
Nous vous remercions pour la confiance que vous nous accordez.
L'équipe OVHcloud

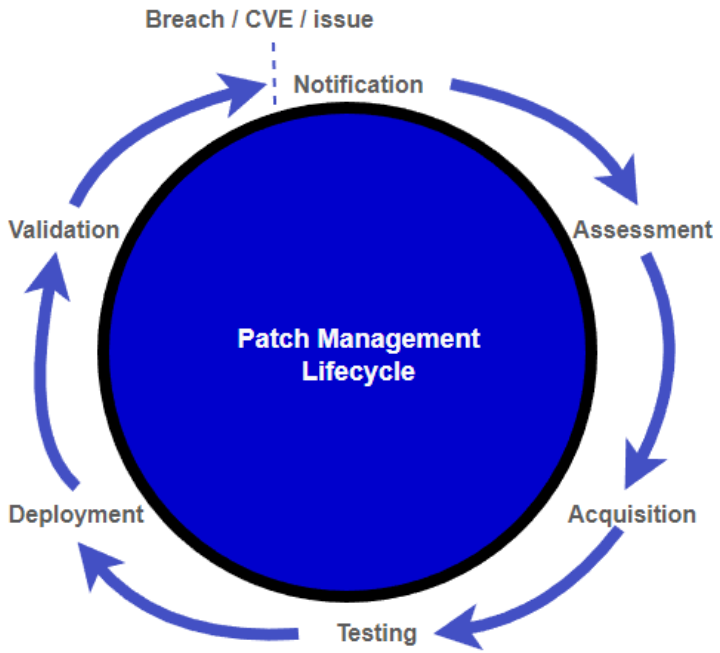
CVE-2023-20593/Zenbleed

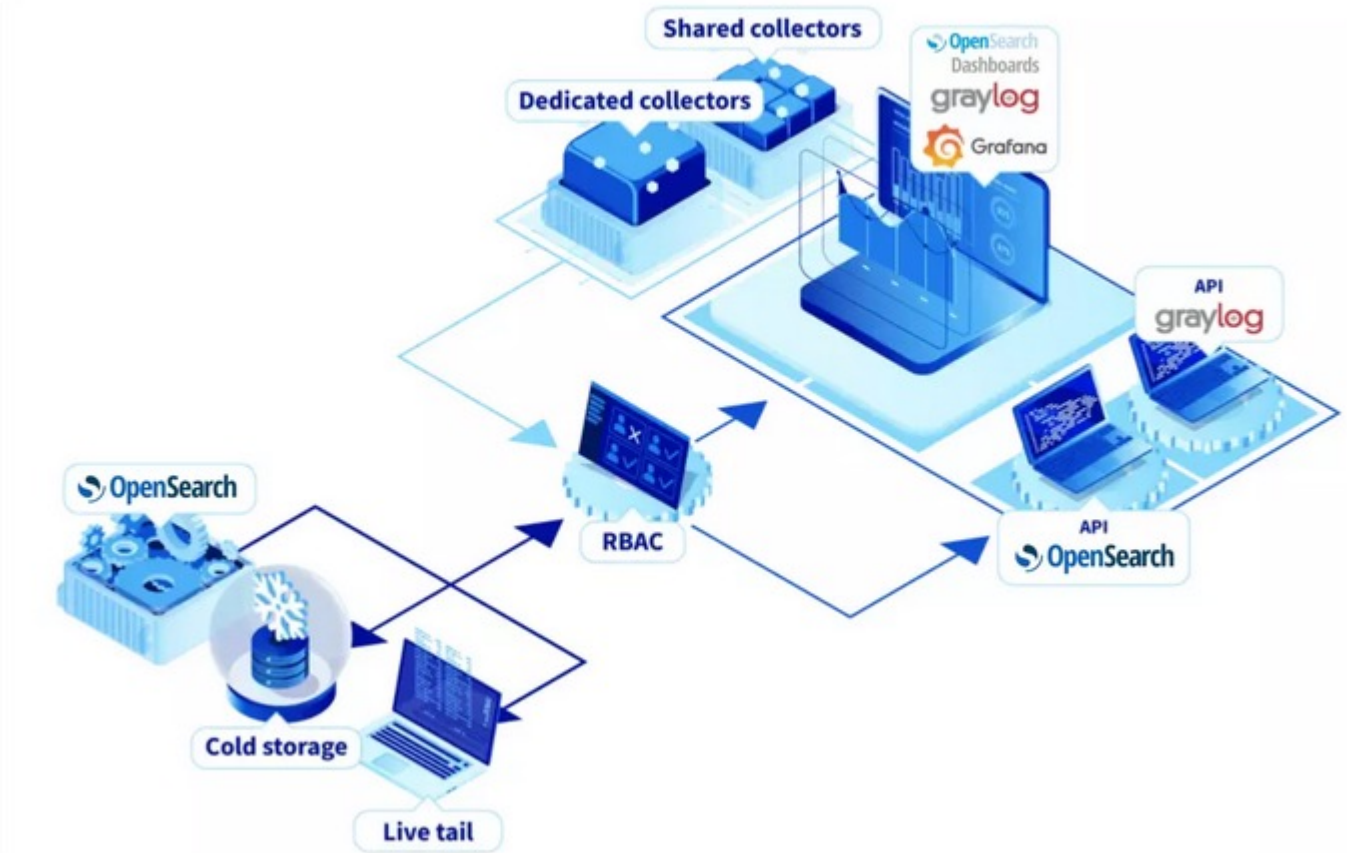
By Julien Levrard / 2023-07-27 / AMD, OVHcloud, Security

On July 24th 2023, AMD has issued a security bulletin disclosing a vulnerability in its Zen2 computer processor microarchitecture. Named "Cross-Process Information Leak" by AMD, the vulnerability is also known as "Zenbleed". Labelled CVE-2023-20593 and rated by AMD as Medium, the issue allows an attacker to potentially access sensitive information processed by the CPU in specific circumstances. The issue affects all software running on the AMD Zen2 based processors, including virtual machines, sandboxes, containers, and processes. Exploitation software is likely available, and we expect that attacks based on this vulnerability will occur soon.

All AMD Zen2 CPUs, including EPYC Rome processors, are vulnerable:


EDR
XDR
SIEM
VM
VM
VM
VM
VM
VM
Switch
appliance
Switch
appliance


Breach / CVE / issue
Notification
Assessment
Acquisition
Testing
Deployment
Validation
Patch Management
Lifecycle


Shared collectors
Dedicated collectors
OpenSearch Dashboards
graylog
Grafana
API
graylog
RBAC
OpenSearch
API
OpenSearch
Cold storage
Live tail

03 Data protection

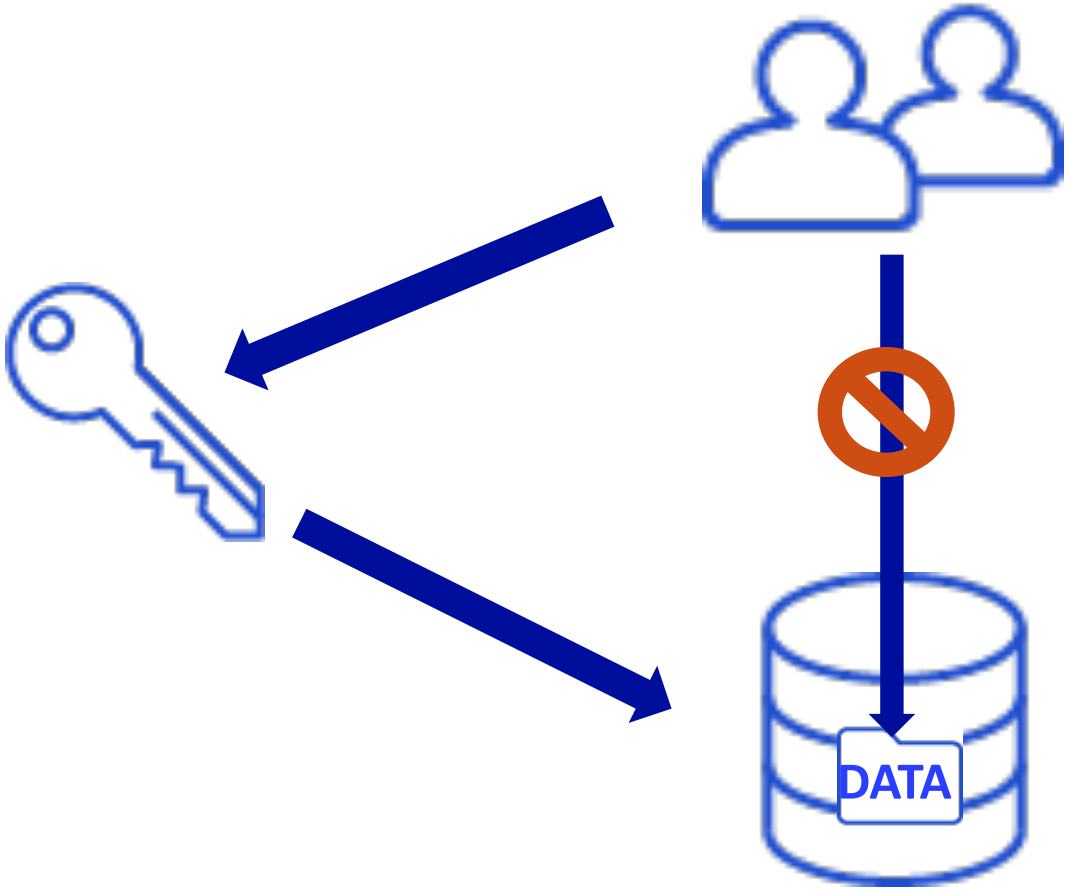
01 Data encryption at rest

02 Data encryption in transit

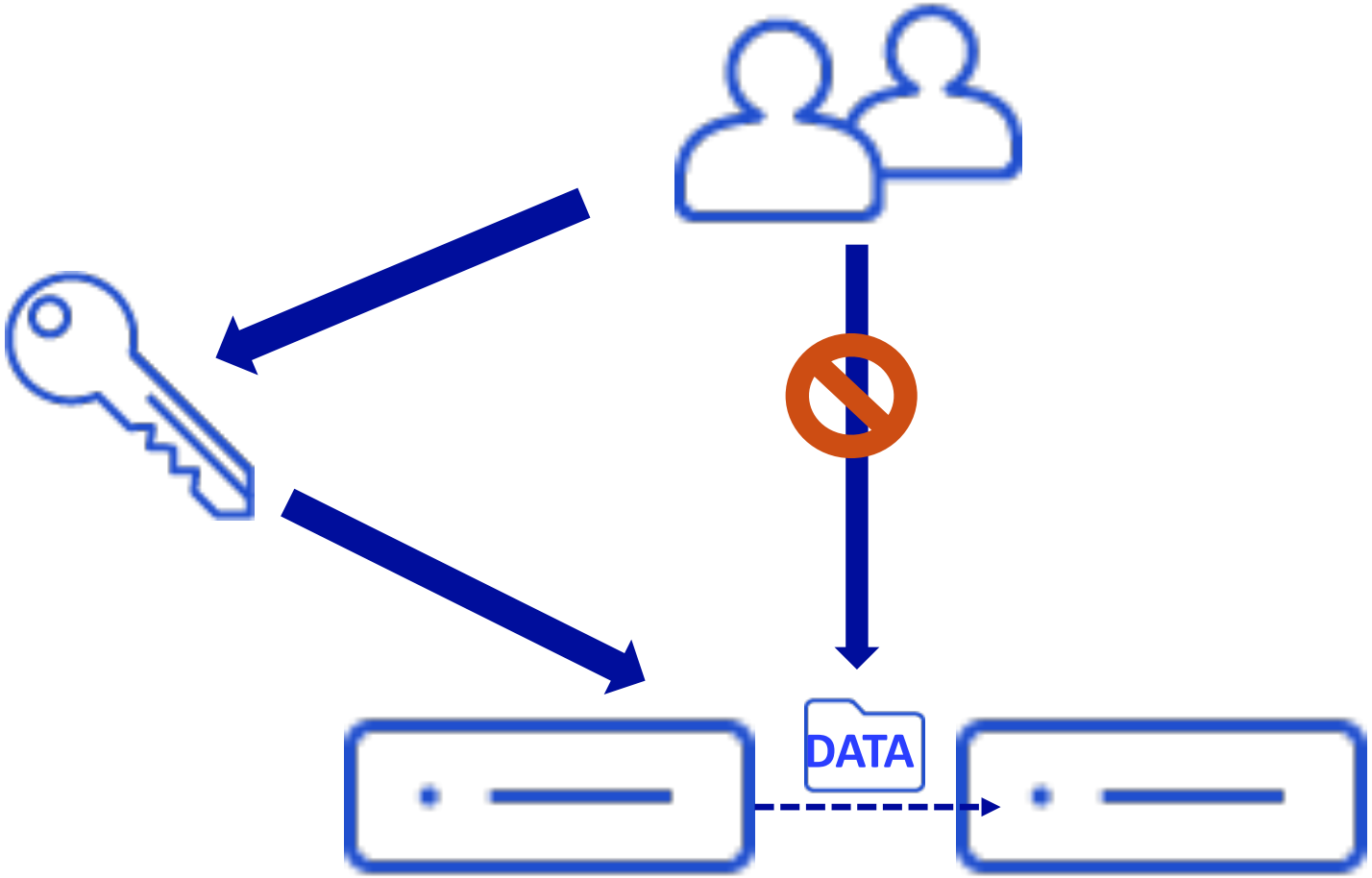
03 Segmentation

04 Backup and Immutability

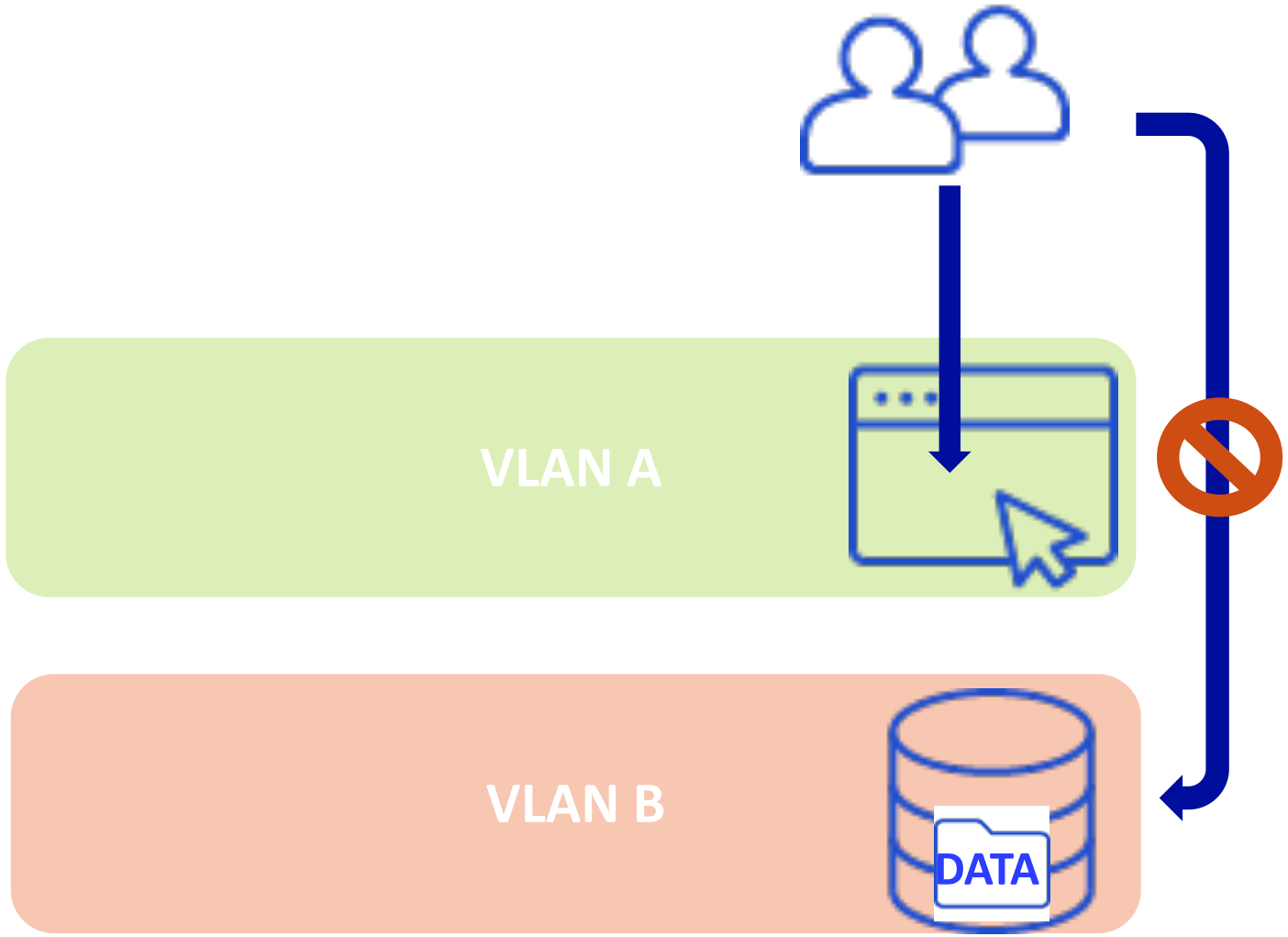
01 Data encryption at rest



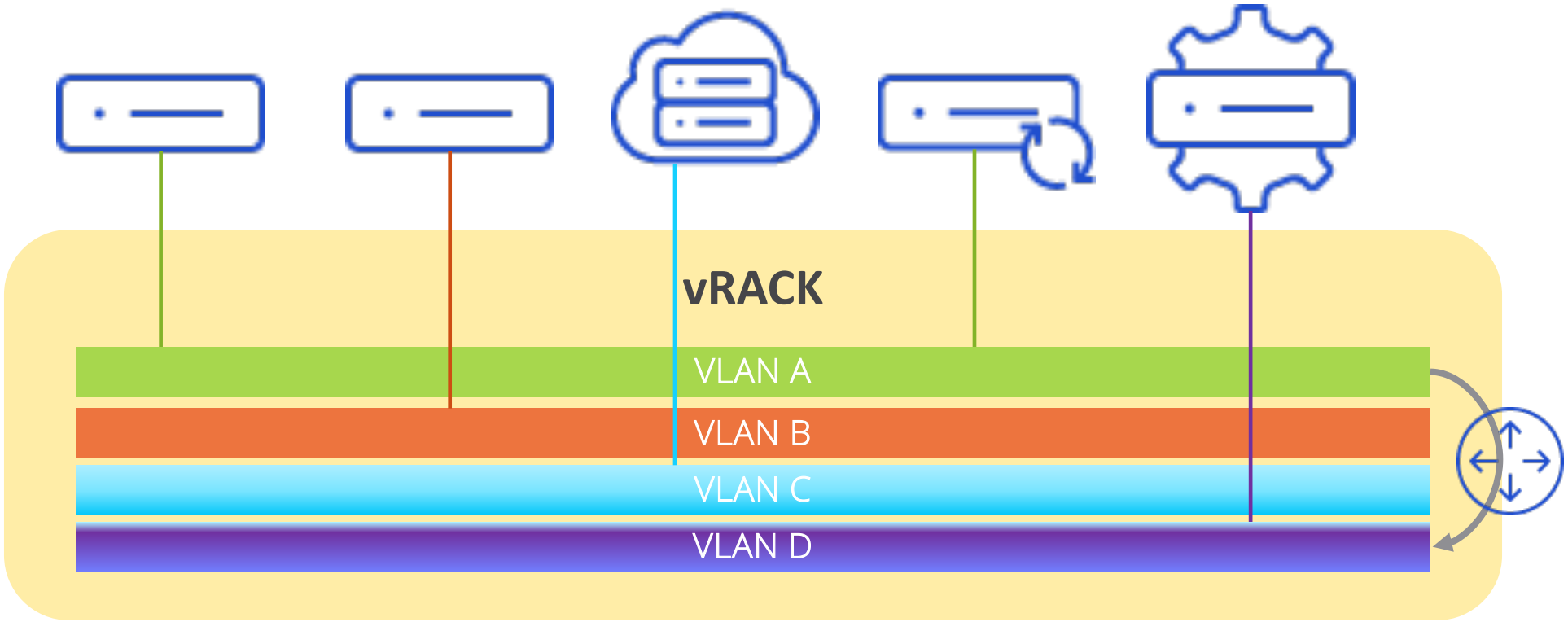
02 Data encryption in transit



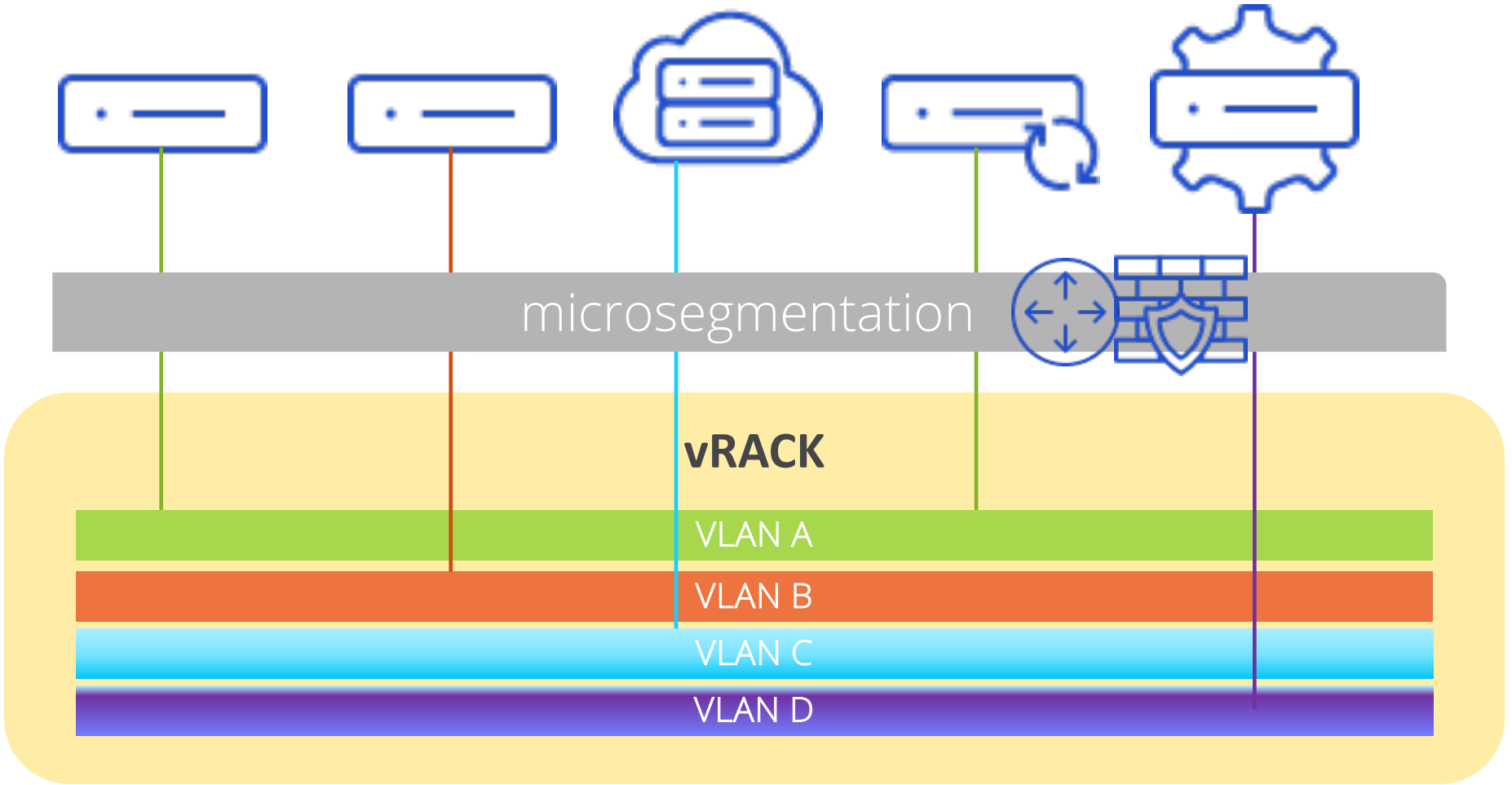
03 Segmentation



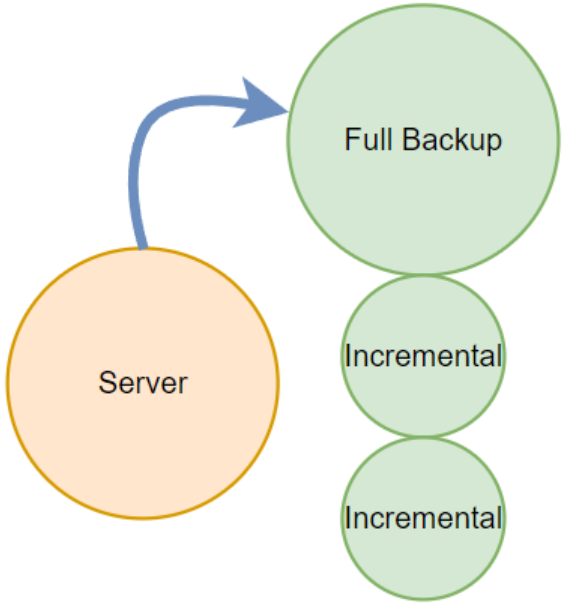
03 Segmentation



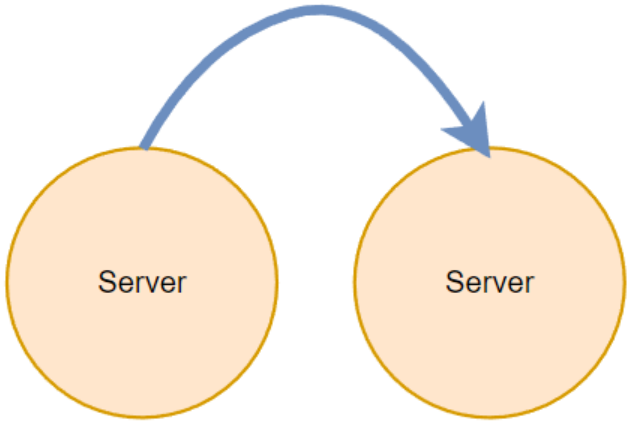
03 Segmentation



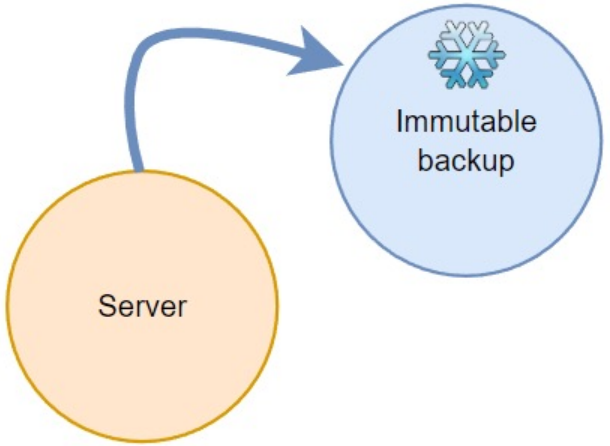
Backup



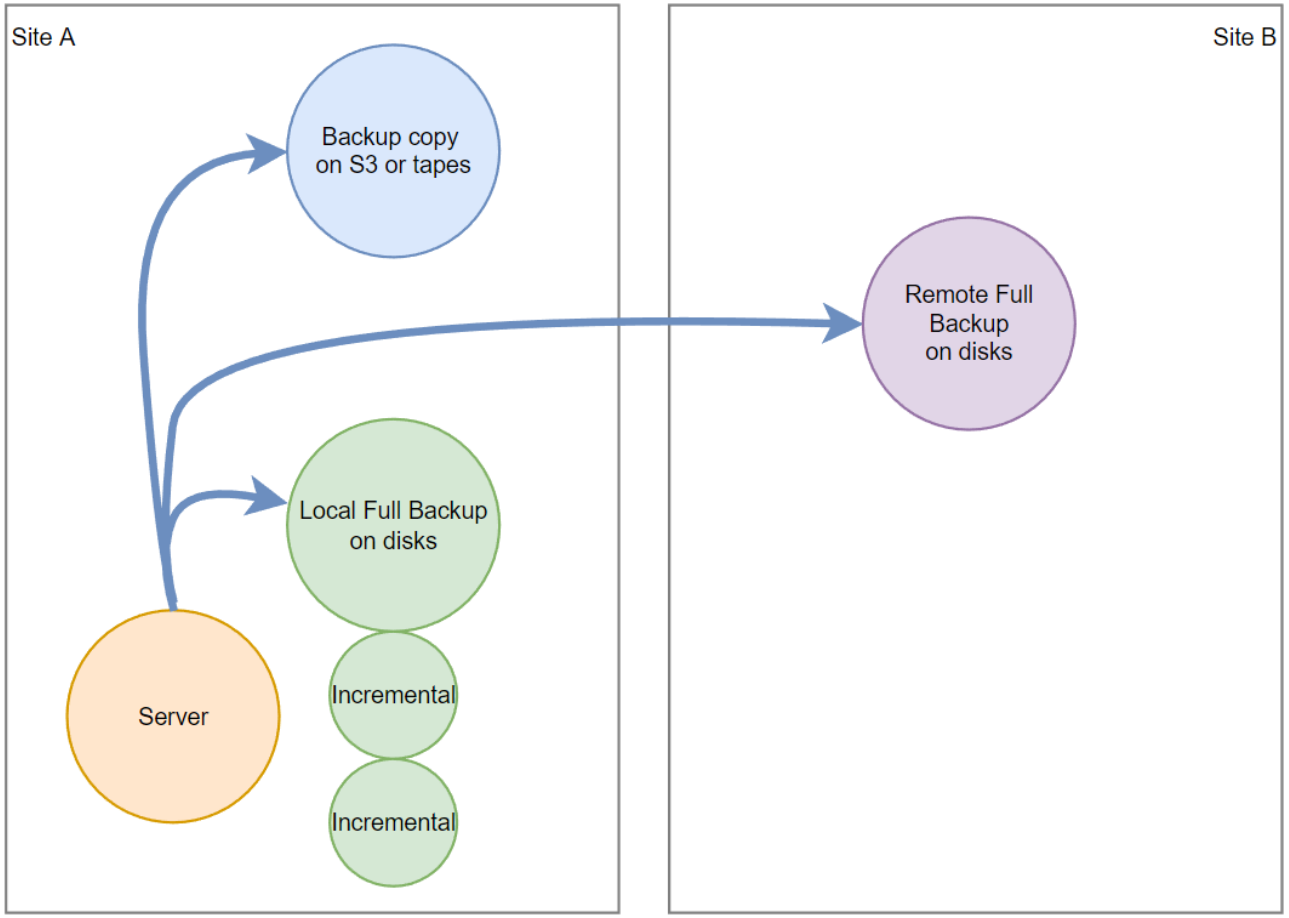
High Availability



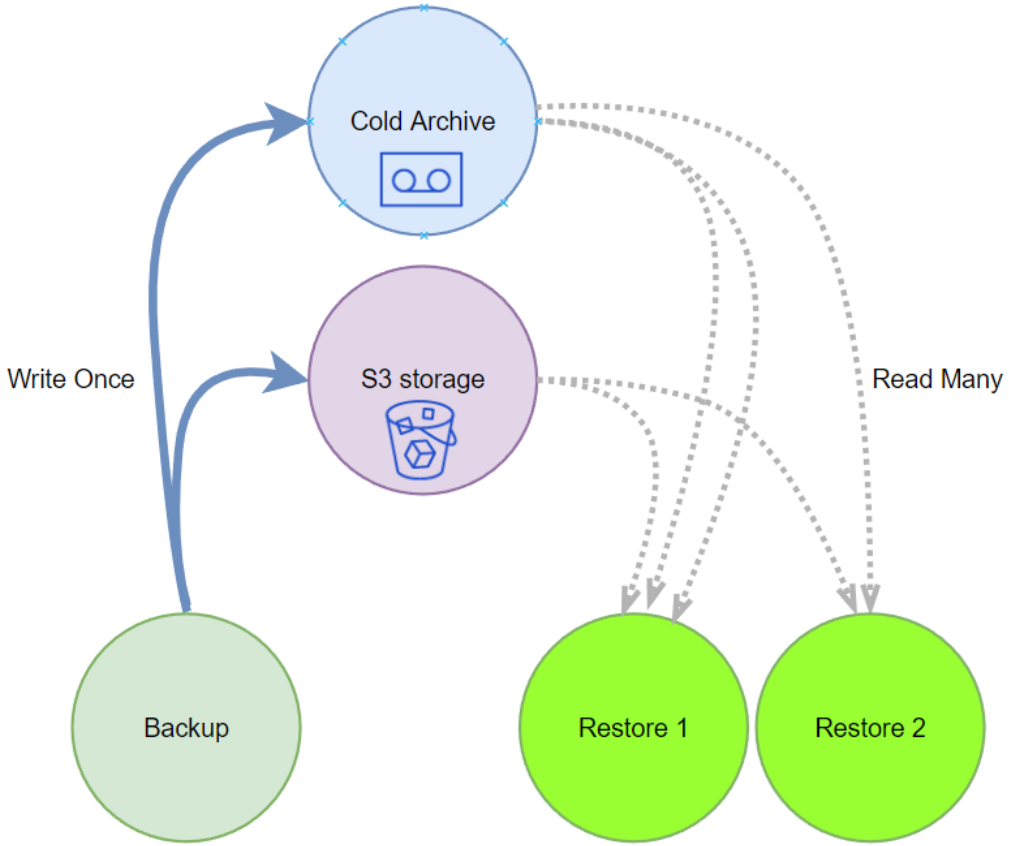
Immutability



04 Backup


Site A
Site B
Backup copy
on S3 or tapes
Remote Full
Backup
on disks
Local Full Backup
on disks
Server
Incremental
Incremental

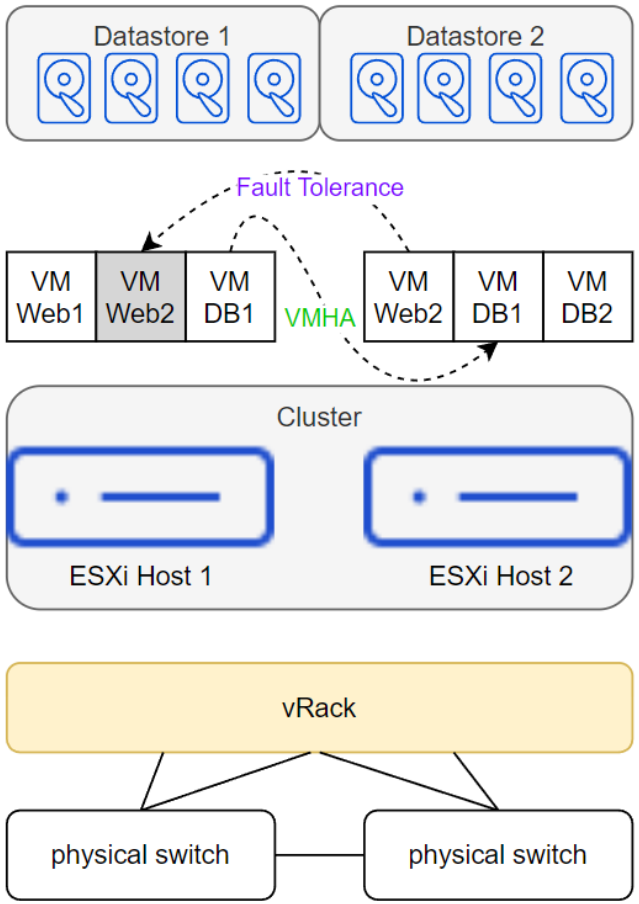
04 Immutability



04 Data resilience

01 High Availability

02 Disaster Recovery and Business Continuity Plans



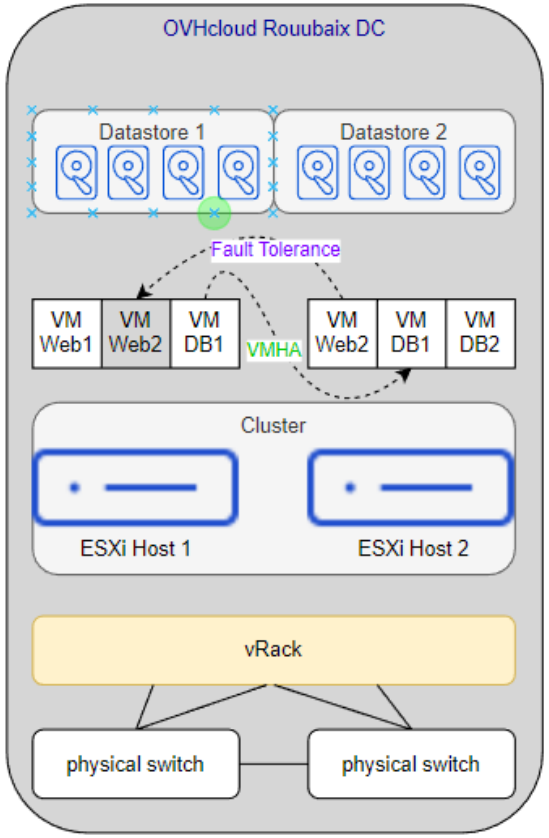
HA at storage level
(i.e. RAID6)

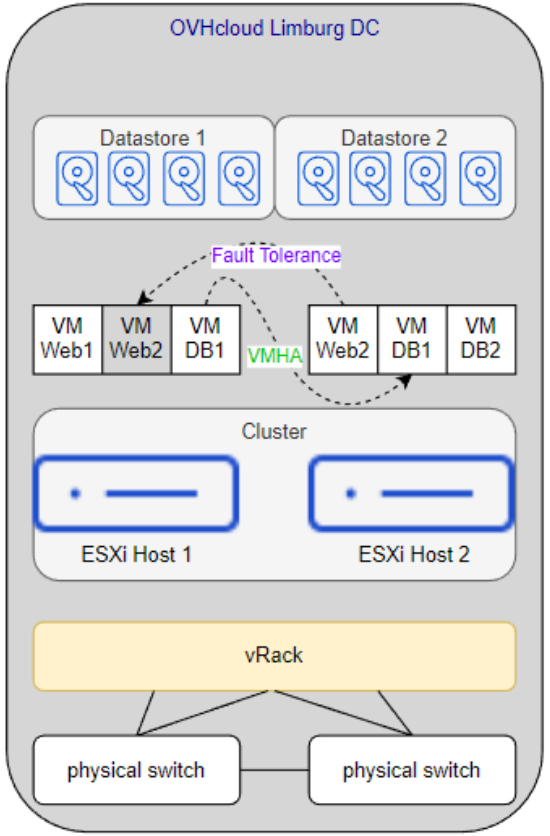
HA at application level
(multiple instances)

HA at host level
(i.e. clustering)

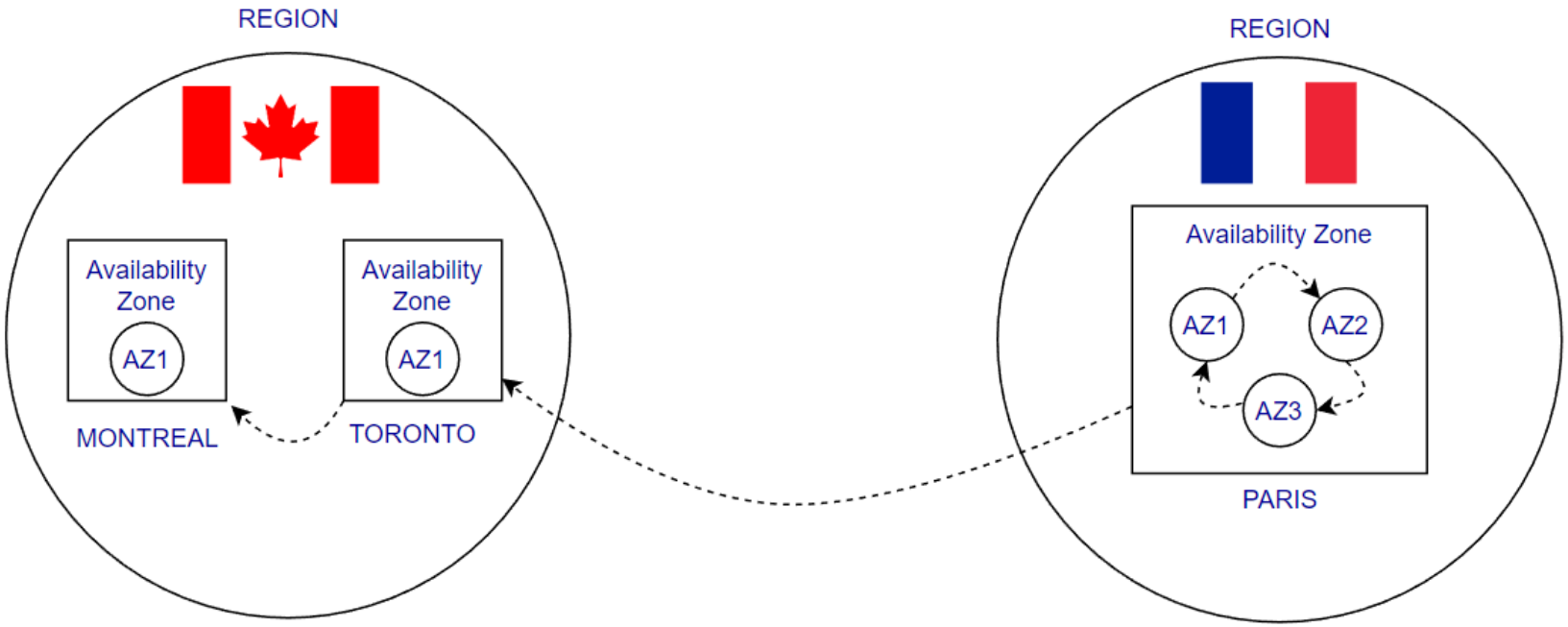
HA at network level
(i.e. mesh network)

01 High Availability

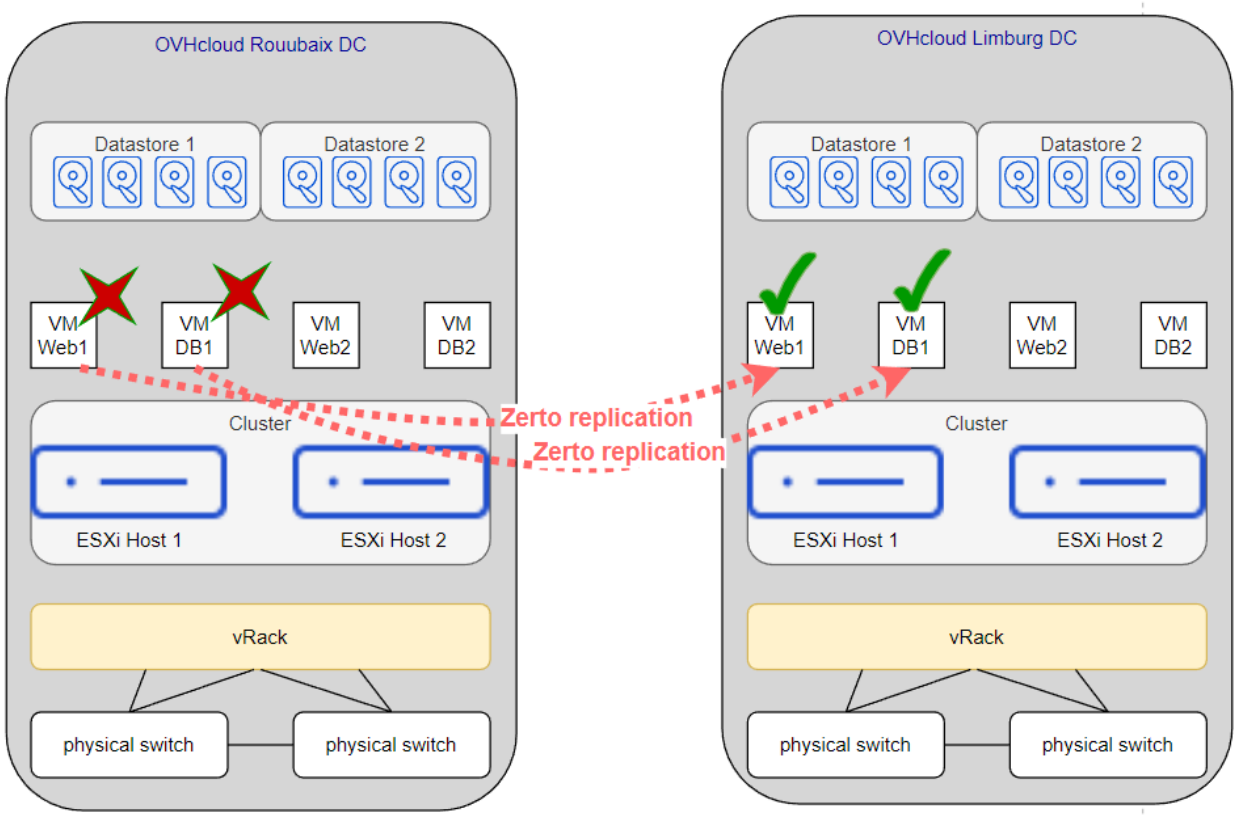




01 High Availability



01 Disaster Recovery and Business Continuity Plans



OVHcloud Partner Program

Thank you !