



**Partner
Program**

Discover Security Solutions

Summary



01

Compliance

01 Global certifications

02 Regional certifications

02 Sectoral 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

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)

**GDPR**

Compliance with Regulation (EU) 2016/679, known as the General Data Protection Regulation (GDPR)

**SOC 1, 2, 3**

AICPA certification SSAE 16/ISAE 3402 Type 2 for control over financial reporting

**CSA STAR**

Cloud Security Alliance (CSA) Level 1: Best Practices Self Assessment

**G-Cloud UK**

G-Cloud Digital Marketplace for Public Sector Cloud Service Procurement in the UK

[Find out more →](#)

**SWIPO**

Signatory of the SWIPO IaaS Code of Conduct on cloud service portability

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



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

**HDS**

Certification by the French Digital Health Agency (ANS) for hosting healthcare data

**Healthcare data in Europe**

Compliance for hosting healthcare data from French, British, Italian, German and Polish citizens

**HIPAA & HITECH**

Compliance with the United States Health Insurance Portability and Accountability Act in our US datacentres.

**PCI DSS**

Certification to protect PCI DSS 3.2 PSP level 1 payment card information

**EBA**

Compliance with the European Banking Authority (EBA) Outsourcing Guidelines for Financial Service Operators in Europe

02

Information security

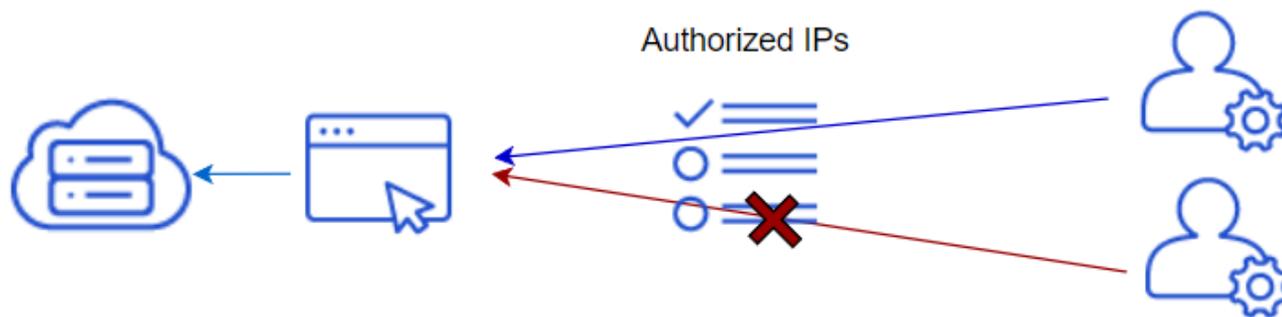
01 Securing accesses

02 Handling security flaws

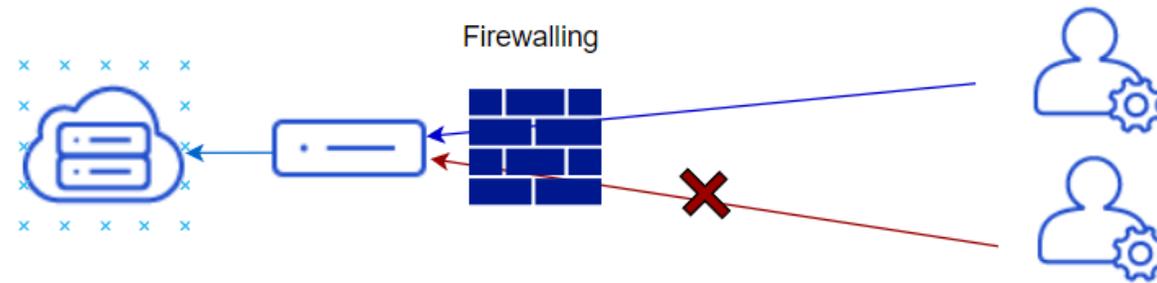
03 Patch management

04 Logs management

IP Whitelisting

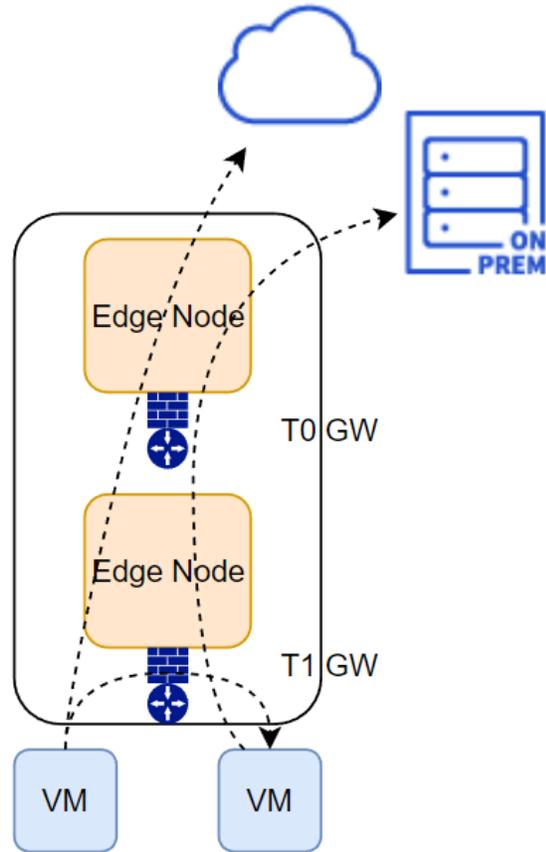


Firewalling

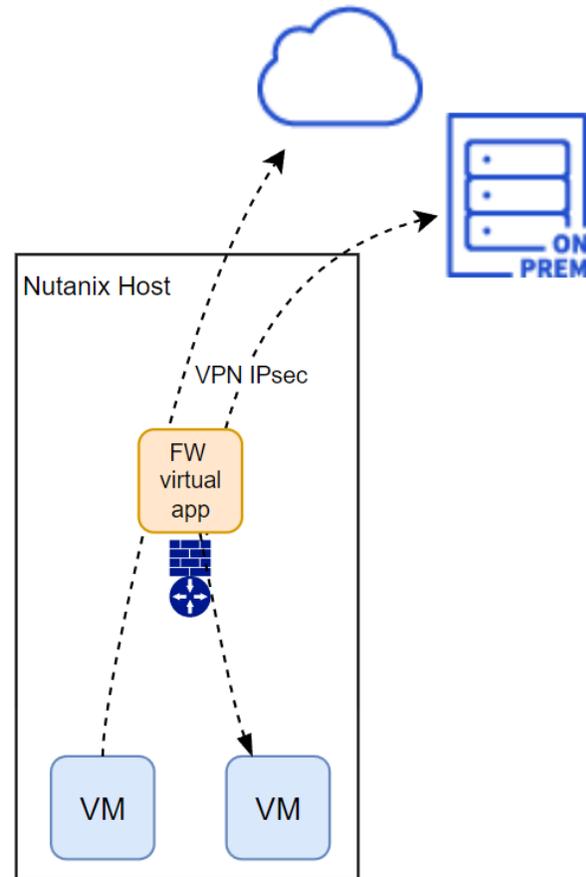
[+ Add a rule](#)Enabled 

Priority	Mode	Protocol	Source IP	Source port	Destination port	TCP status	Status
0	Authorise	ICMP	10.15.122.0/32				Active 
1	Authorise	TCP	10.15.122.0/32	389	389		Active 

Firewalling



Firewalling



OVHcloud Anti-DDoS protection



Dashboard Bare Metal Cloud Hosted Private Cloud Public Cloud Web Cloud Telecom Sunrise Marketplace Standard version English Dev & test Product.

Order

- Dedicated servers
- Virtual private servers
- Managed Bare Metal
- NAS and CDN
- Platforms and services
- Metrics Data Platform
- Logs Data Platform
- Network
 - IP
 - Network Security Dashboard **active**
 - Load Balancer
 - vRack private network
 - OVHcloud Connect
- Storage and backups
- Licenses

Network / Network Security Dashboard

Anti-DDoS dashboard

By constantly monitoring network traffic, we can observe a number of suspicious activities. To shield against these, we transparently redirect inbound network traffic to our cleaning centres for a more thorough analysis and potential attacker cleanup, ensuring a seamless, uninterrupted experience.

Please note that source IP addresses are not displayed as they cannot be trusted for most attacks (i.e., identity theft or reflection attacks).

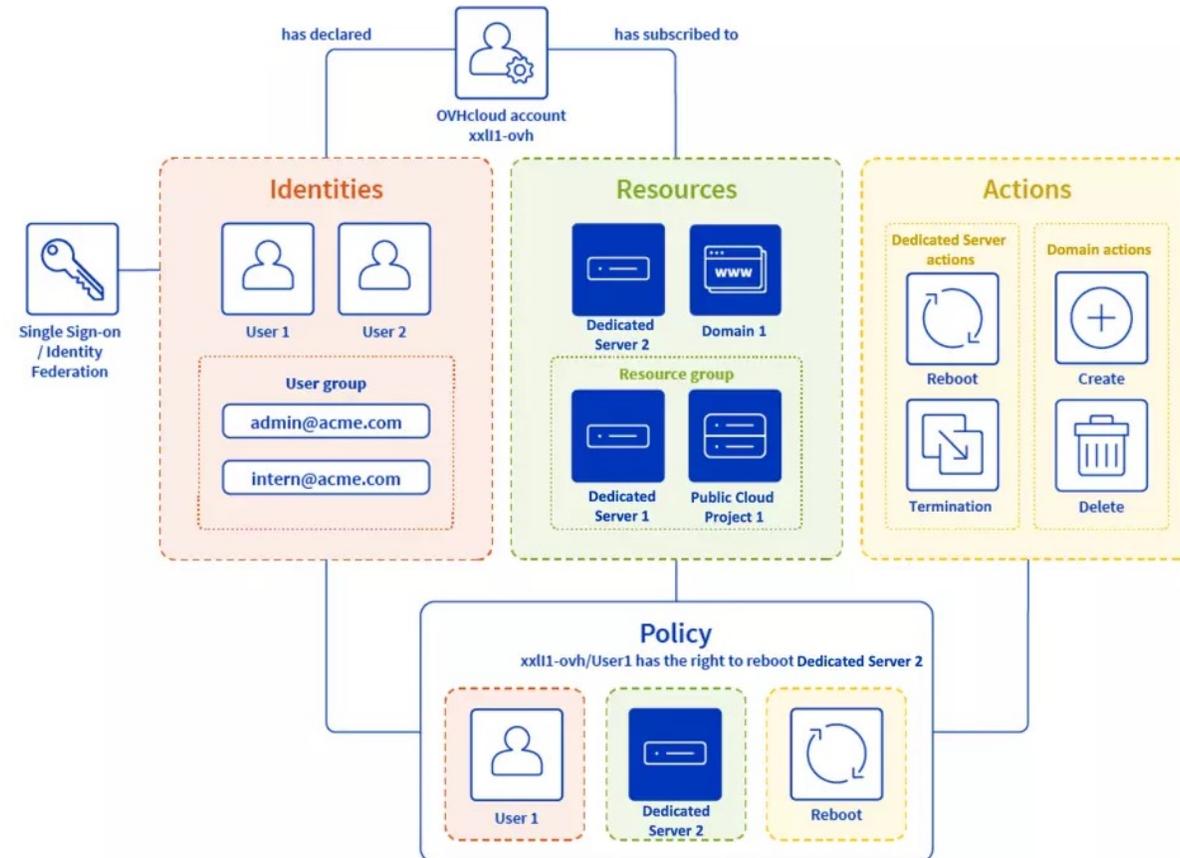
Guides Like it?

Cleaning centre activity log Traffic graphs

View infrastructure activity log for: All services Enter an IP address... Period: Last month Filter

Detection time	End time	Destination IP	Attack vectors	
2023-12-18 12:20:05		192.168.1.1	TCP_NULL	...
2023-12-14 14:13:30	2023-12-14 14:53:30	192.168.1.1	ICMP	...
2023-12-14 13:34:07	2023-12-14 14:04:56	192.168.1.1	UDP	Show traffic
2023-12-12 17:53:14	2023-12-12 18:04:56	192.168.1.1	TCP_PSH	...
2023-12-12 14:04:29	2023-12-12 14:16:56	192.168.1.1	TCP_PSH	...
2023-12-12 10:01:29	2023-12-12 10:13:56	192.168.1.1	TCP_PSH	...
2023-12-11 15:19:03	2023-12-11 15:54:28	192.168.1.1	UDP	...
2023-12-11 14:53:35	2023-12-11 15:04:56	192.168.1.1	TCP_SYN	...
2023-12-07 18:41:43	2023-12-07 18:56:11	192.168.1.1		...
2023-12-07 17:31:11	2023-12-07 18:06:56	192.168.1.1	UDP	...

IAM : Identity Access Management



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

Connect via SSO

To enable your users to use your own identity provider, we need their information in order to configure your account.

Please enter the SSO details

Keep active OVHcloud users

Group attribute name (groupAttributeName)

XML metadata

```
<EntityDescriptor ID="_34318115-898e-4227-a0b7-3e19b6225f47"
entityID="http://sso.<my-domain>.com/adfs/services/trust"
xmlns="urn:oasis:names:tc:SAML:2.0:metadata"><ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml
```

Enable two-factor authentication

Step 2 of 5

Select your method

SMS
 Authenticate using a security code received by SMS.

Mobile application
 Authenticate using a free mobile app (compatible with Android/iOS/Windows Phone).

Security key
 Authenticate using a U2F-compatible security key.

 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

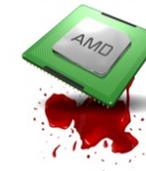
By Julien Levrard / 2023-07-27 / AMD, OVHcloud, Security

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.

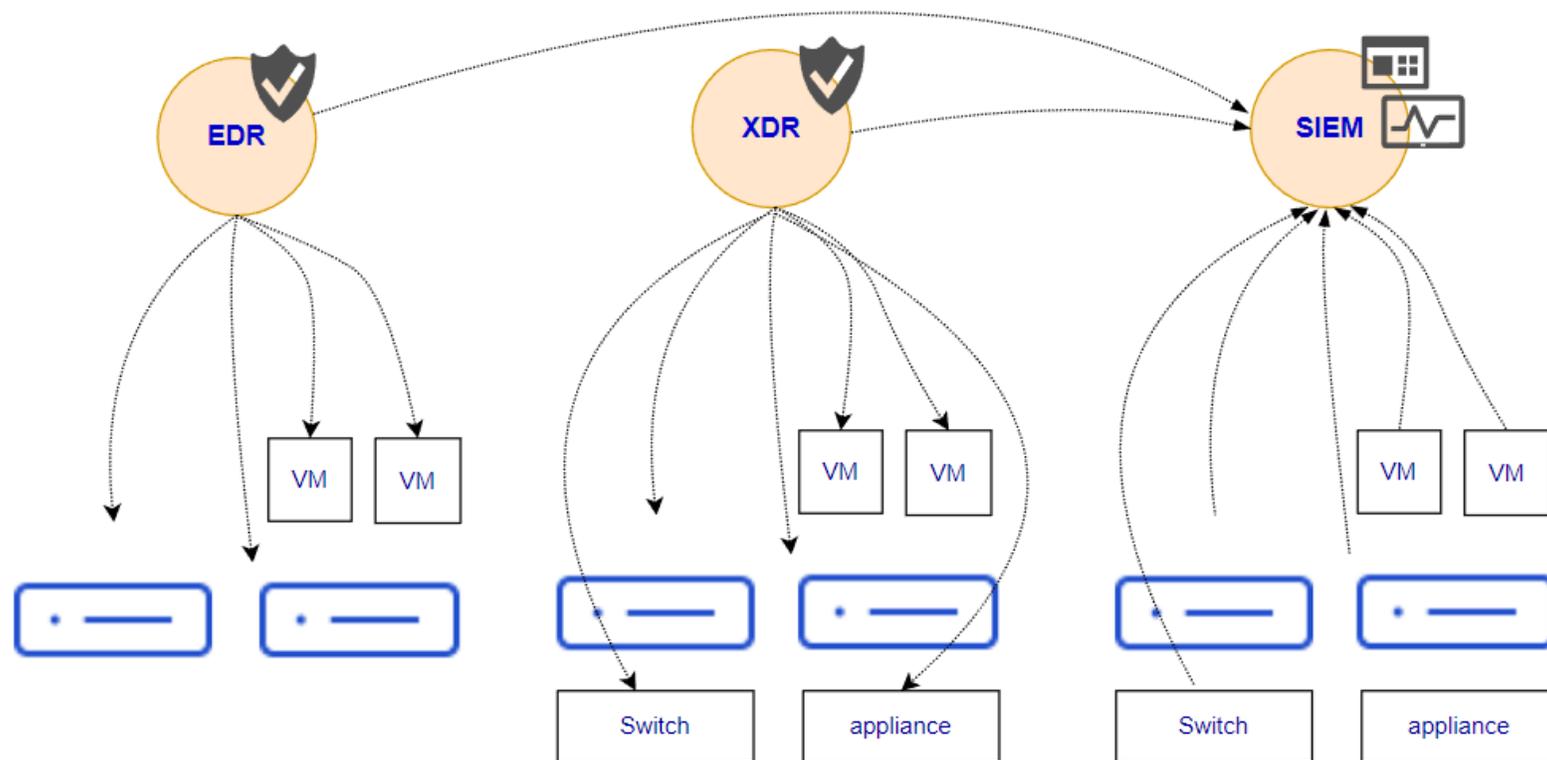


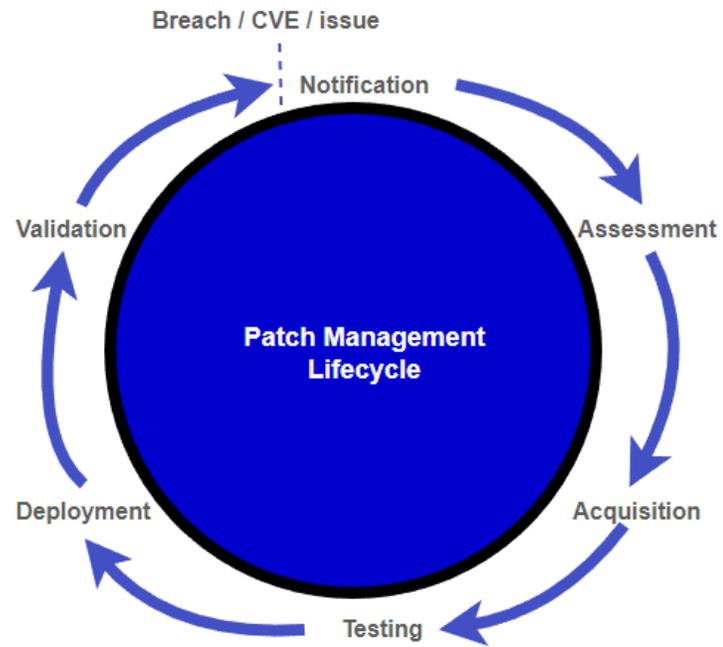
Zenbleed CVE-2023-20593

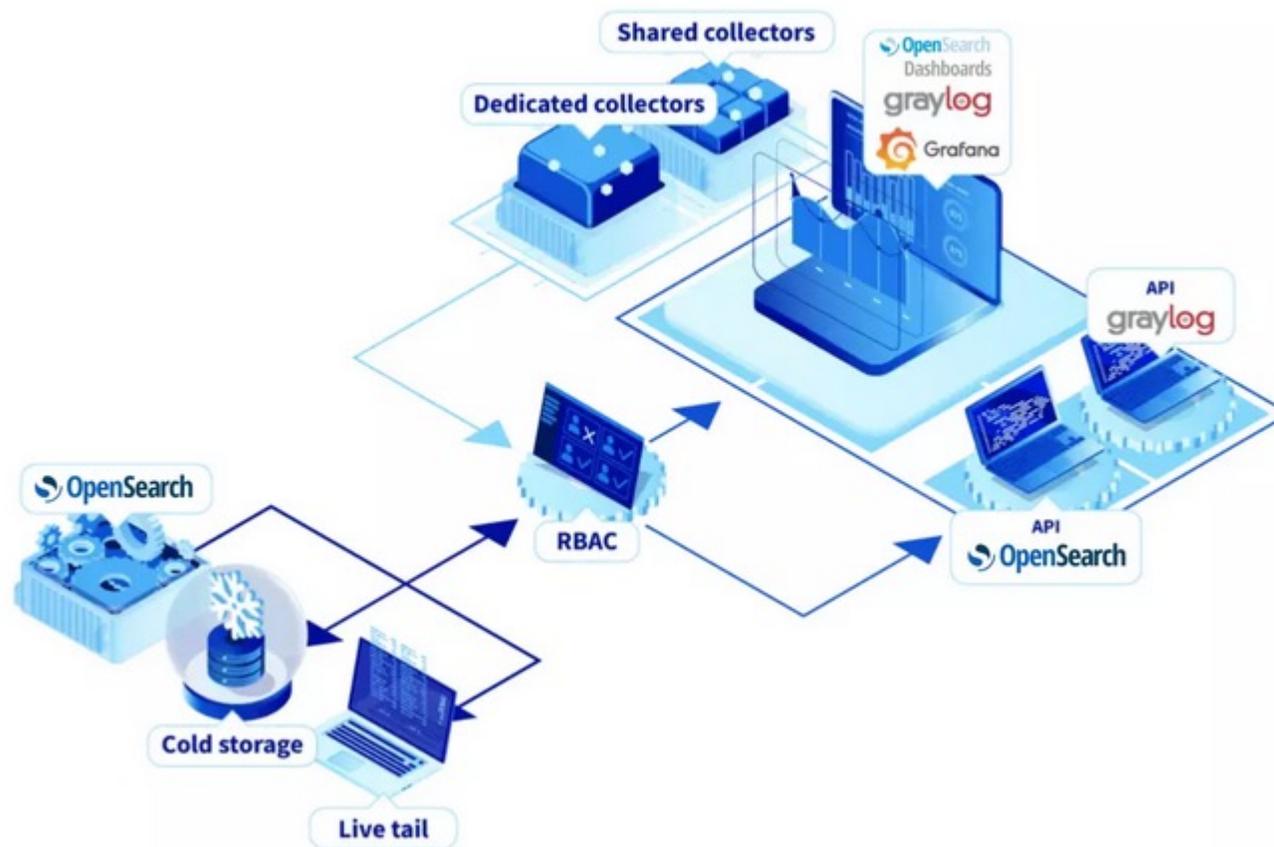
the AMD Zen 2 vulnerability



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







03

Data protection

01 Data encryption at rest

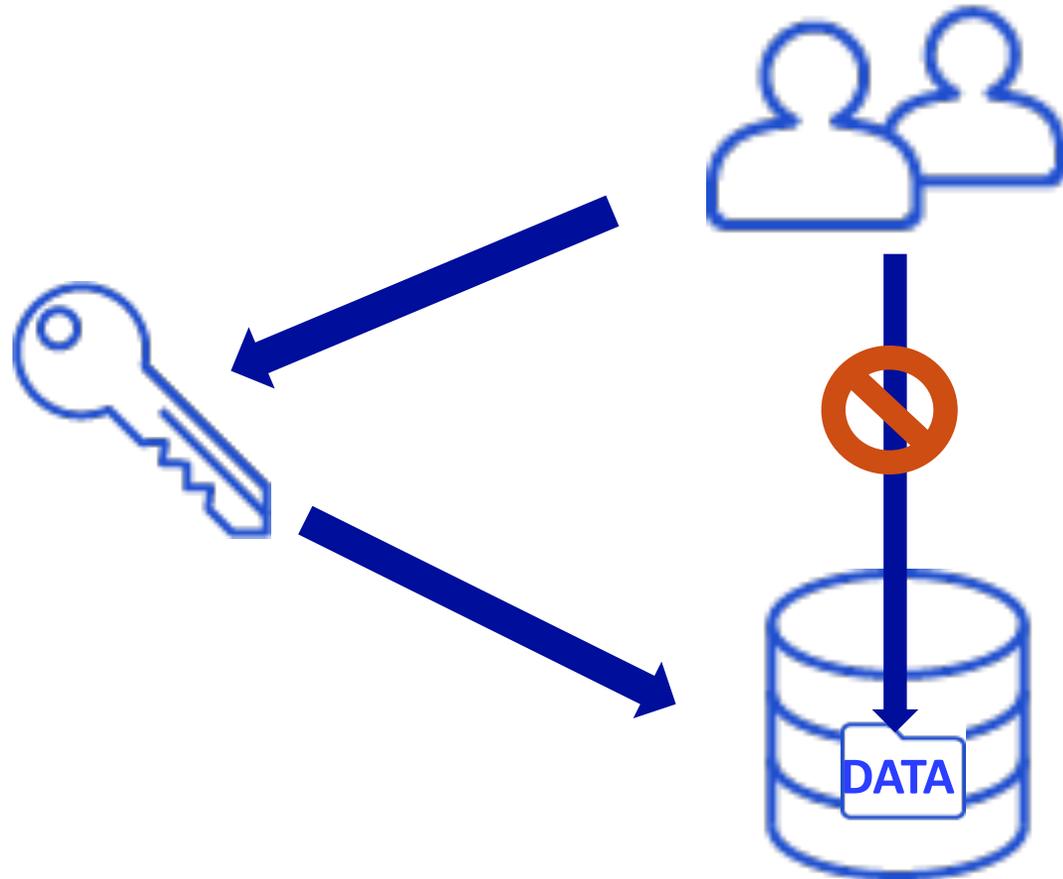
02 Data encryption in transit

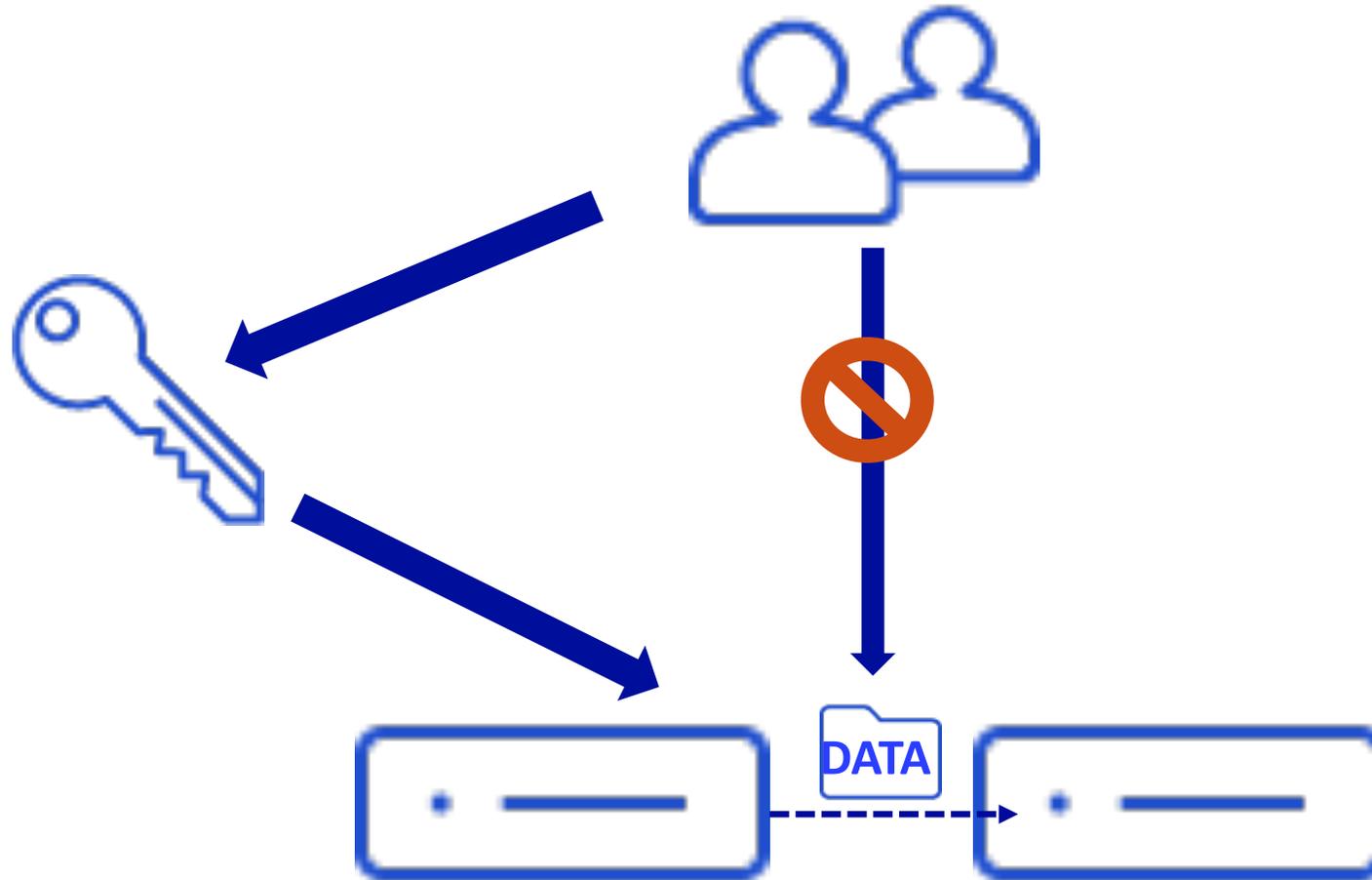
03 Segmentation

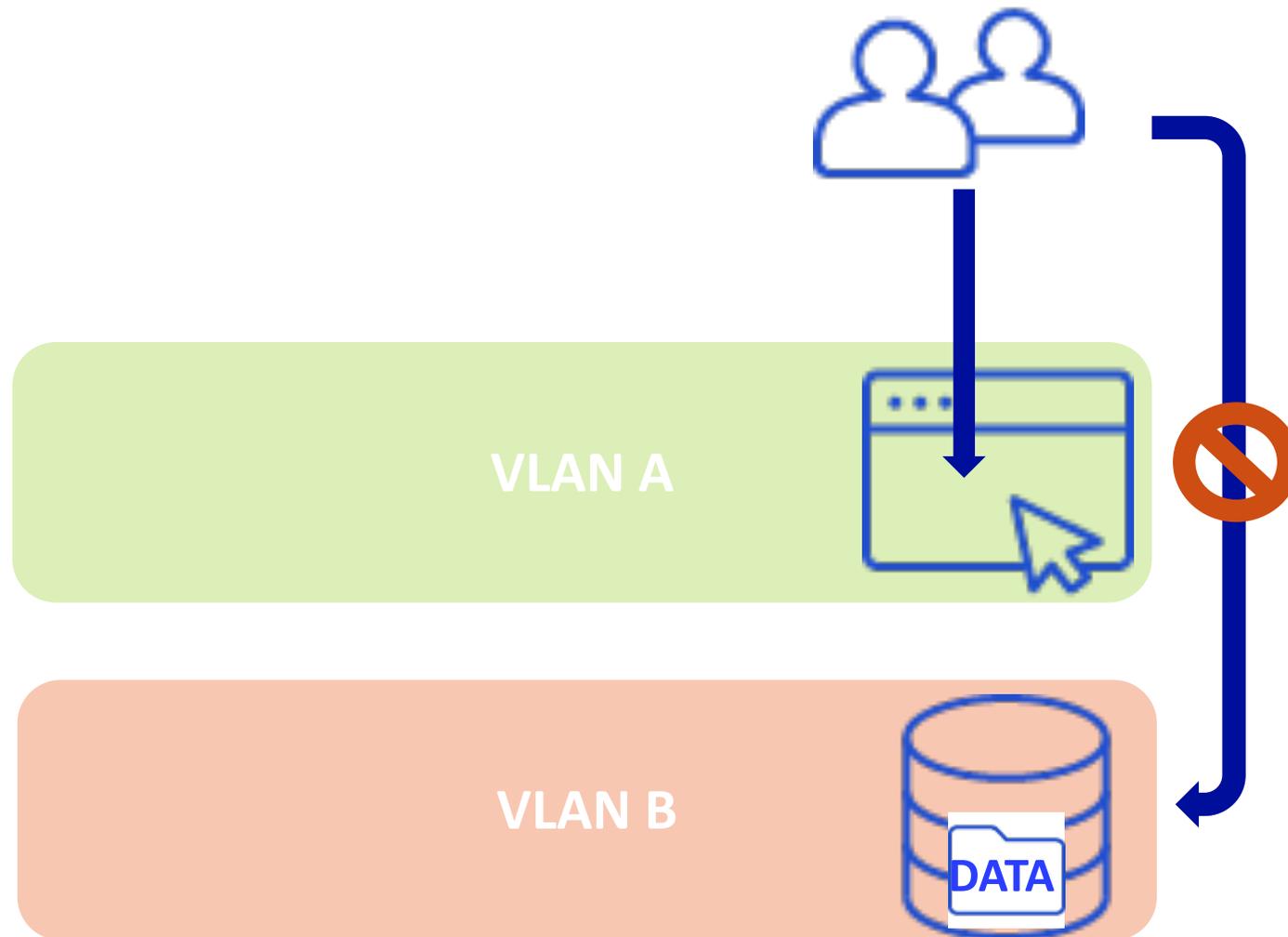
04 Backup and Immutability

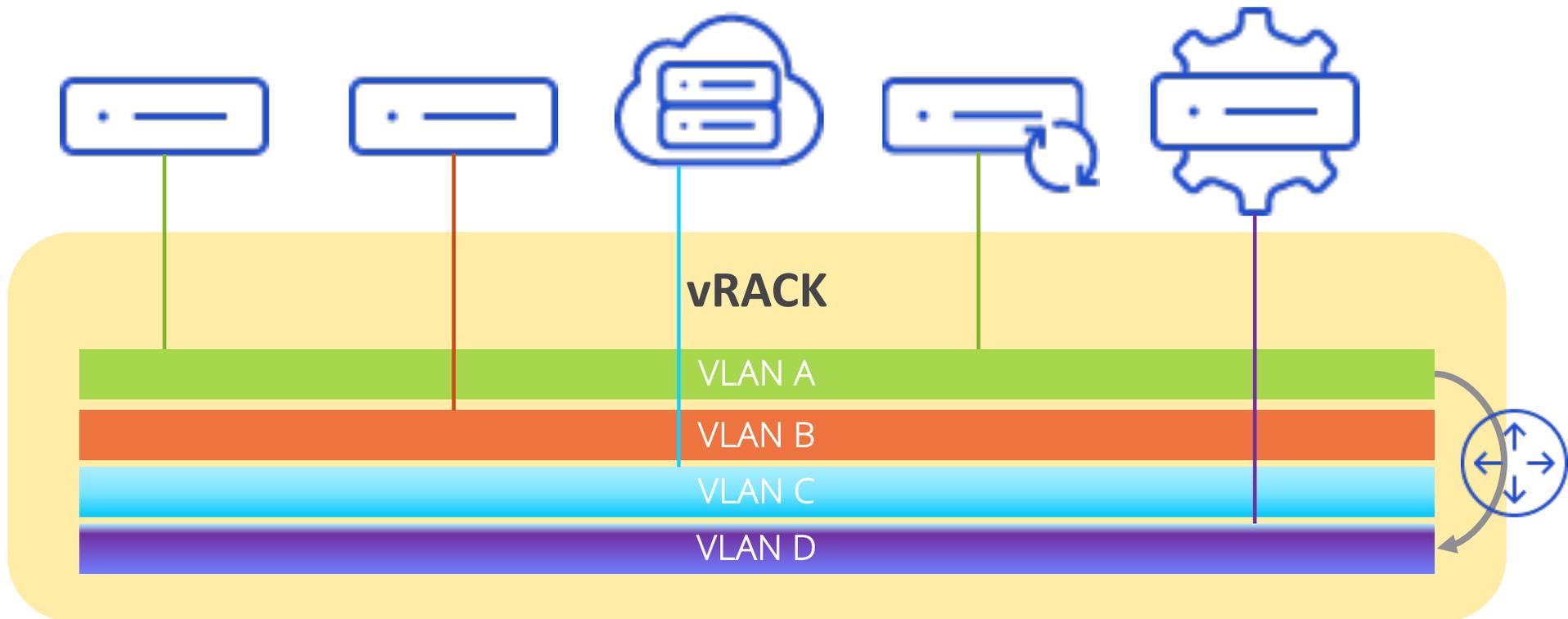
01

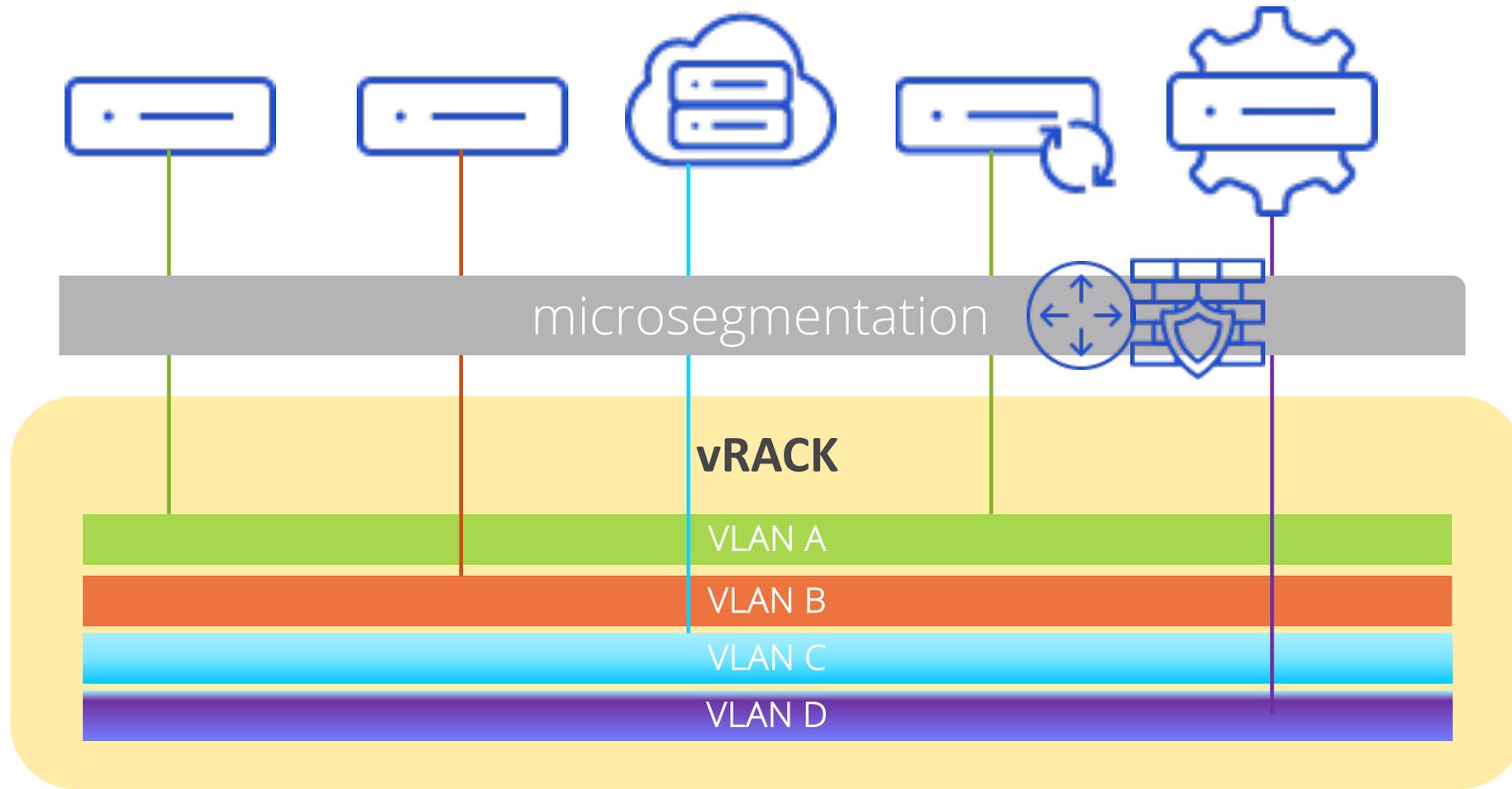
Data encryption at rest



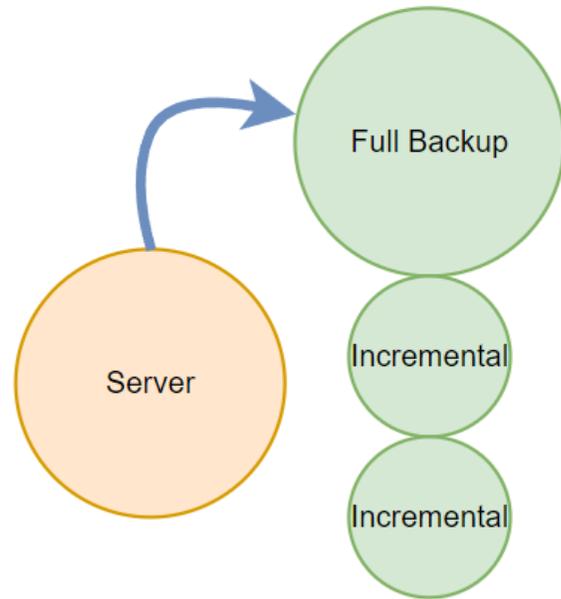




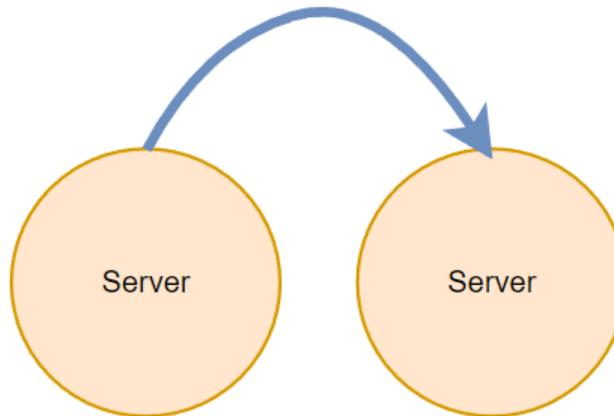




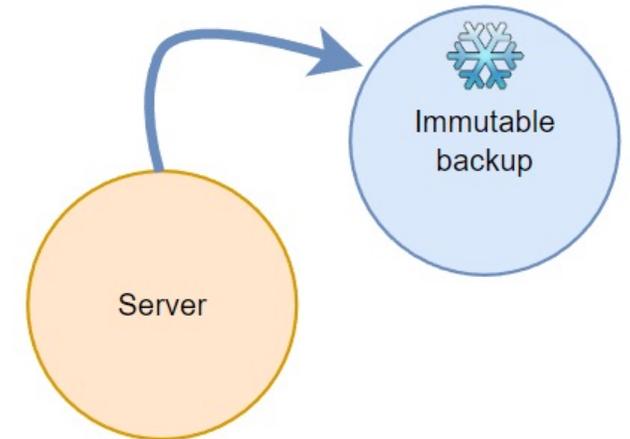
Backup

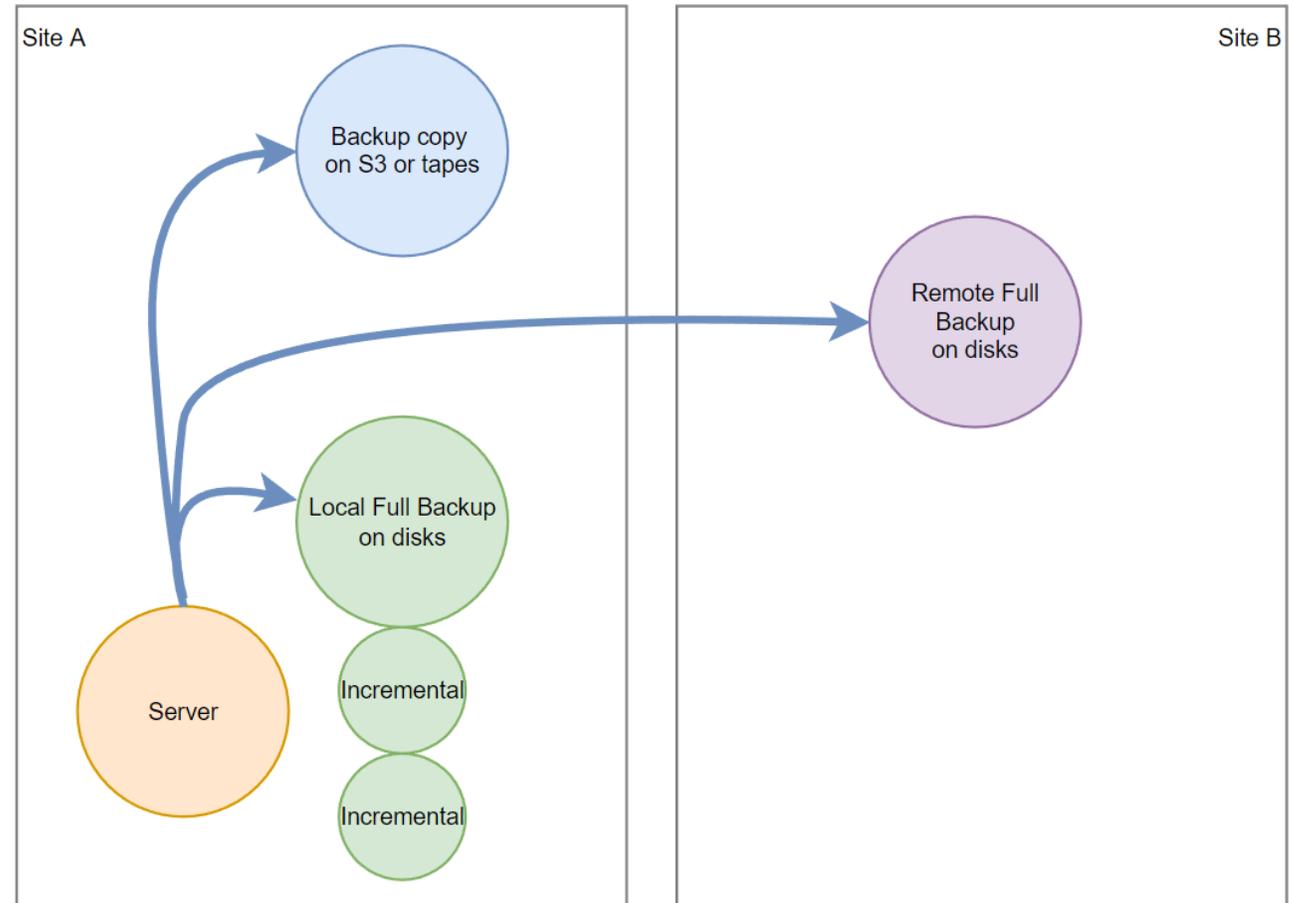


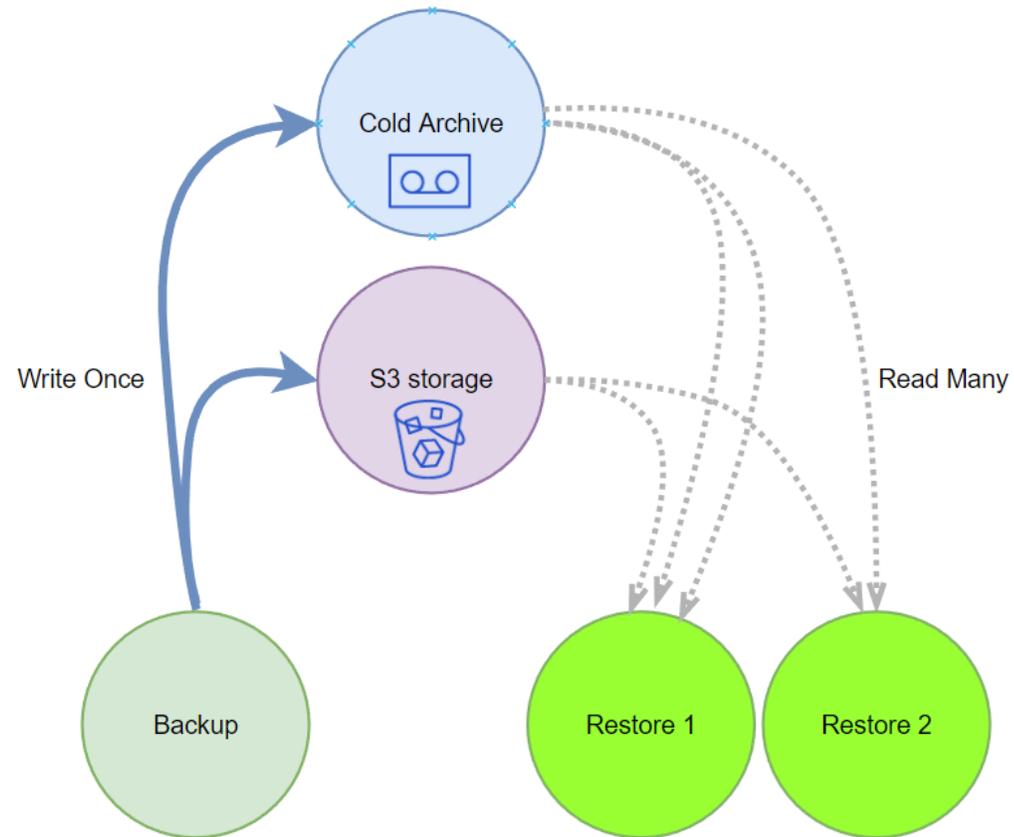
High Availability



Immutability







04

Data resilience

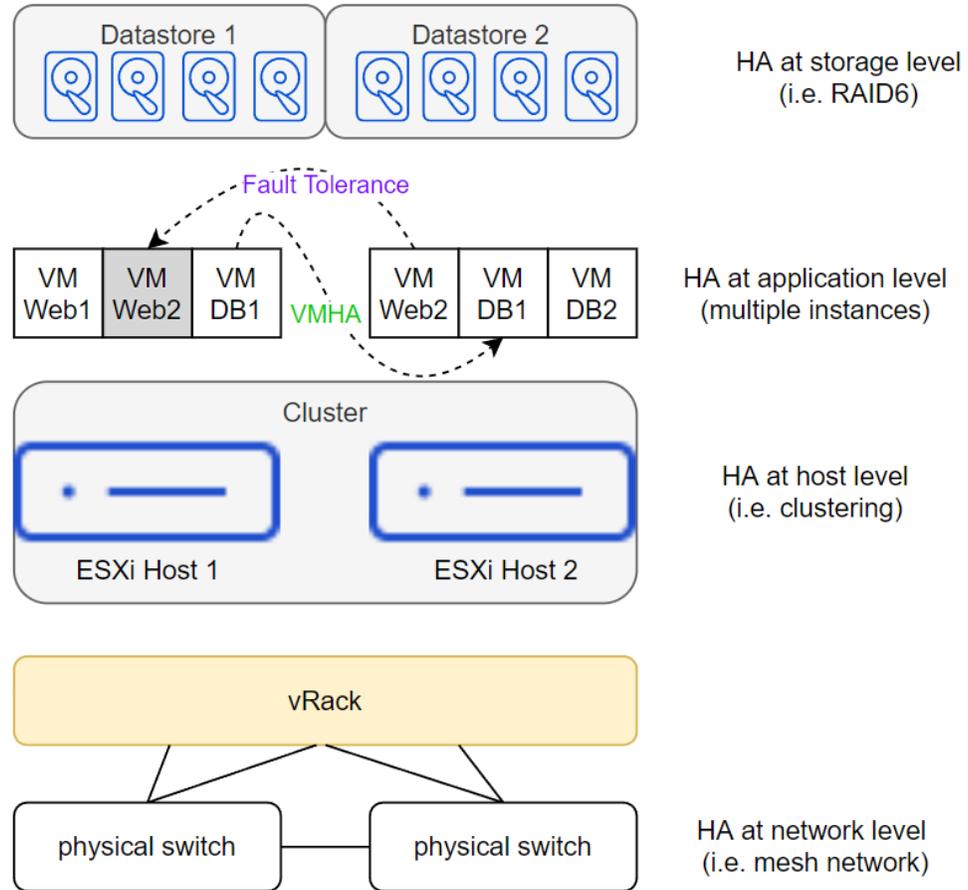
01

High Availability

02

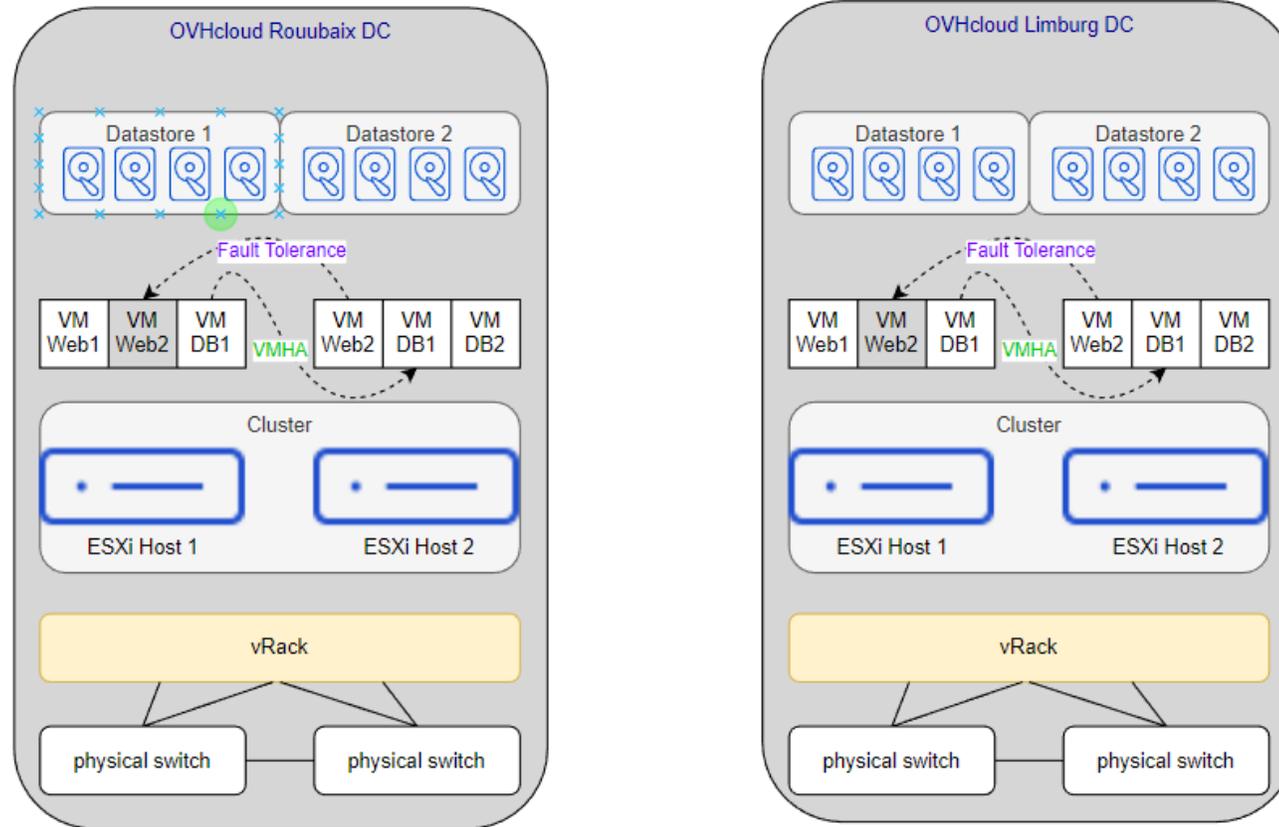
Disaster Recovery and Business Continuity Plans

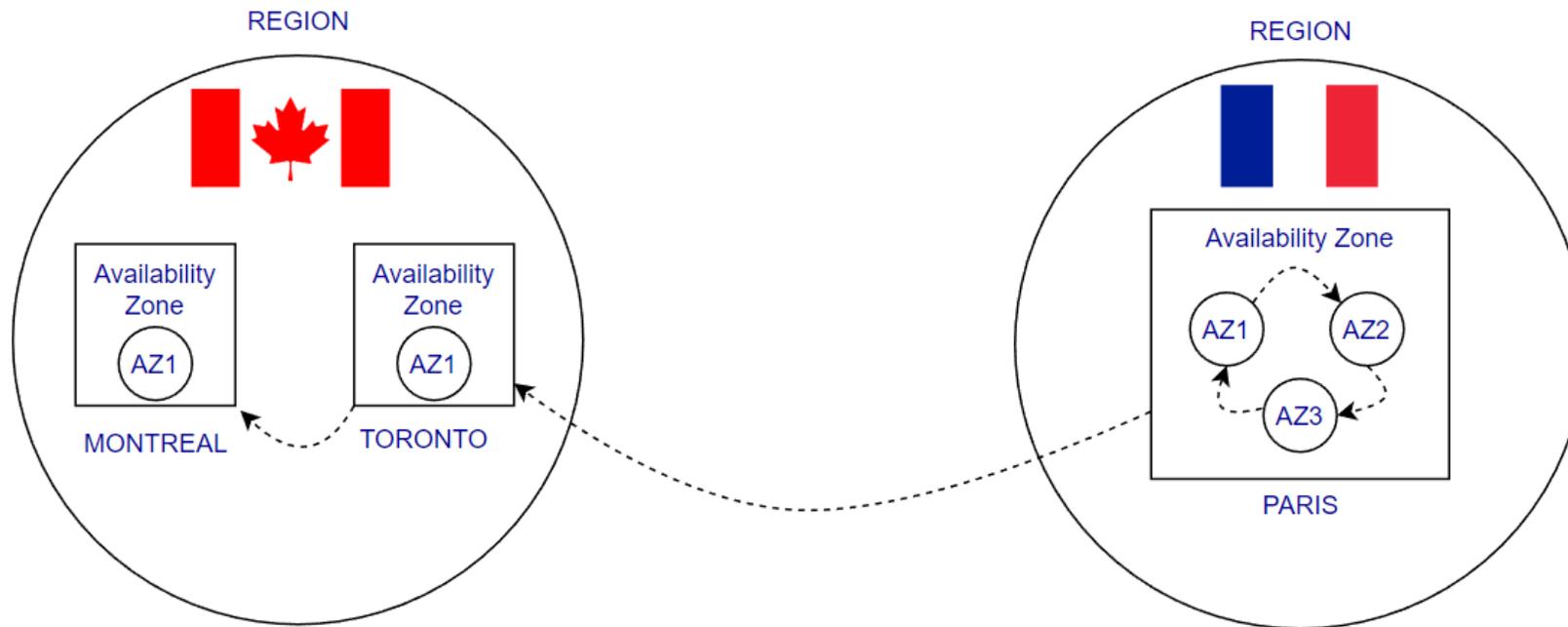
01 High Availability



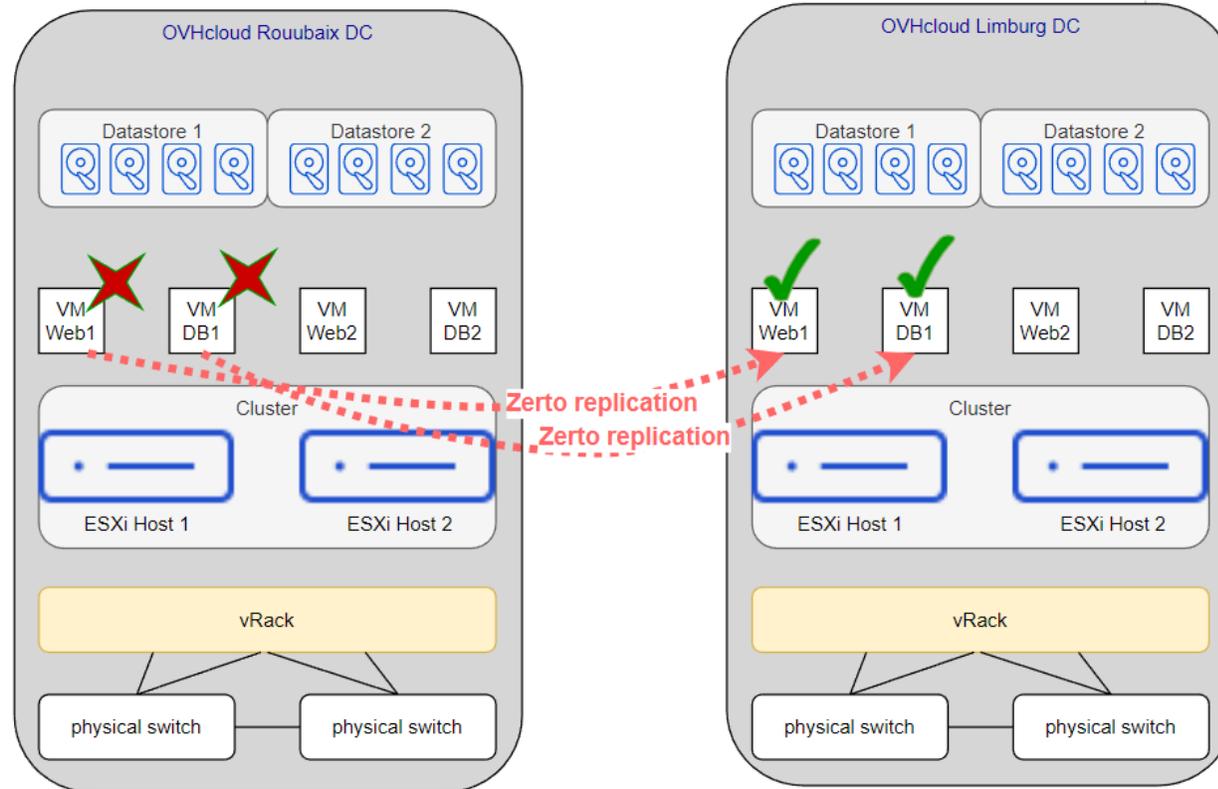
01

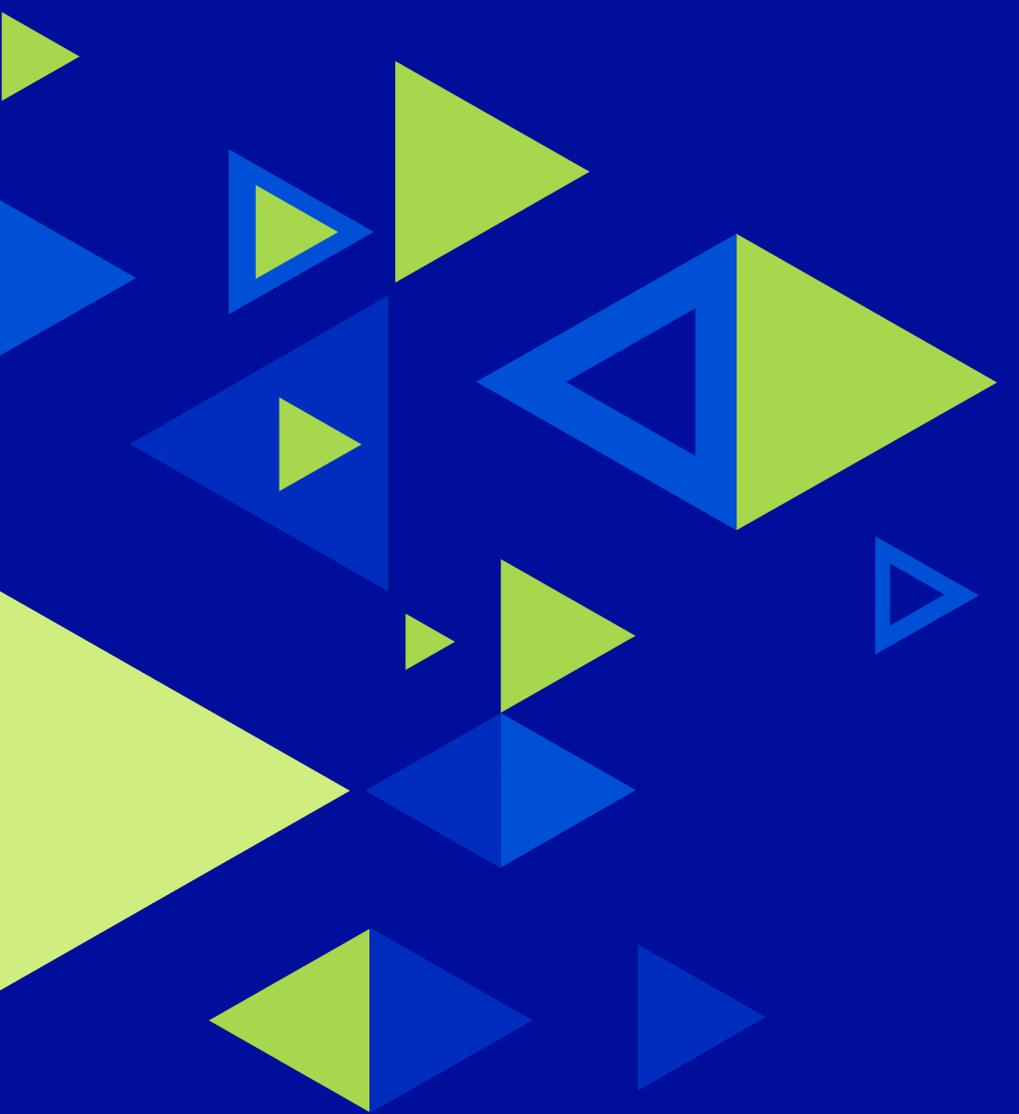
High Availability





01 Disaster Recovery and Business Continuity Plans





Thank you !