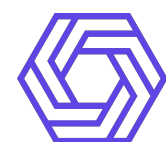


# Enhancing Ceph Security Encrypting OSDs With Hashicorp Vault Integration

**Naufal Gholib Shiddiq**  
*Cloud Engineer @Btech*



**EasyStack**  
open cloud computing



datacomm

flexi

WOWRACK



SIVALI  
CLOUD  
TECHNOLOGY

boer  
technology

NASHTAGROUP  
TECHNOLOGY AND SERVICES COMPANY

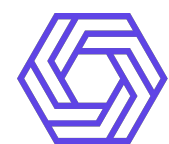
nevacloud

Yogyakarta, 19 July 2025

# Agenda

1. Pengenalan
2. Ceph Encryption
3. Integrasi Ceph dengan HashiCorp Vault
4. Tantangan dan Limitasi
5. Rekomendasi dan Best Practice

# Pengenalan



**EasyStack**  
open cloud computing



**datacomm**

flexi

WOWRACK

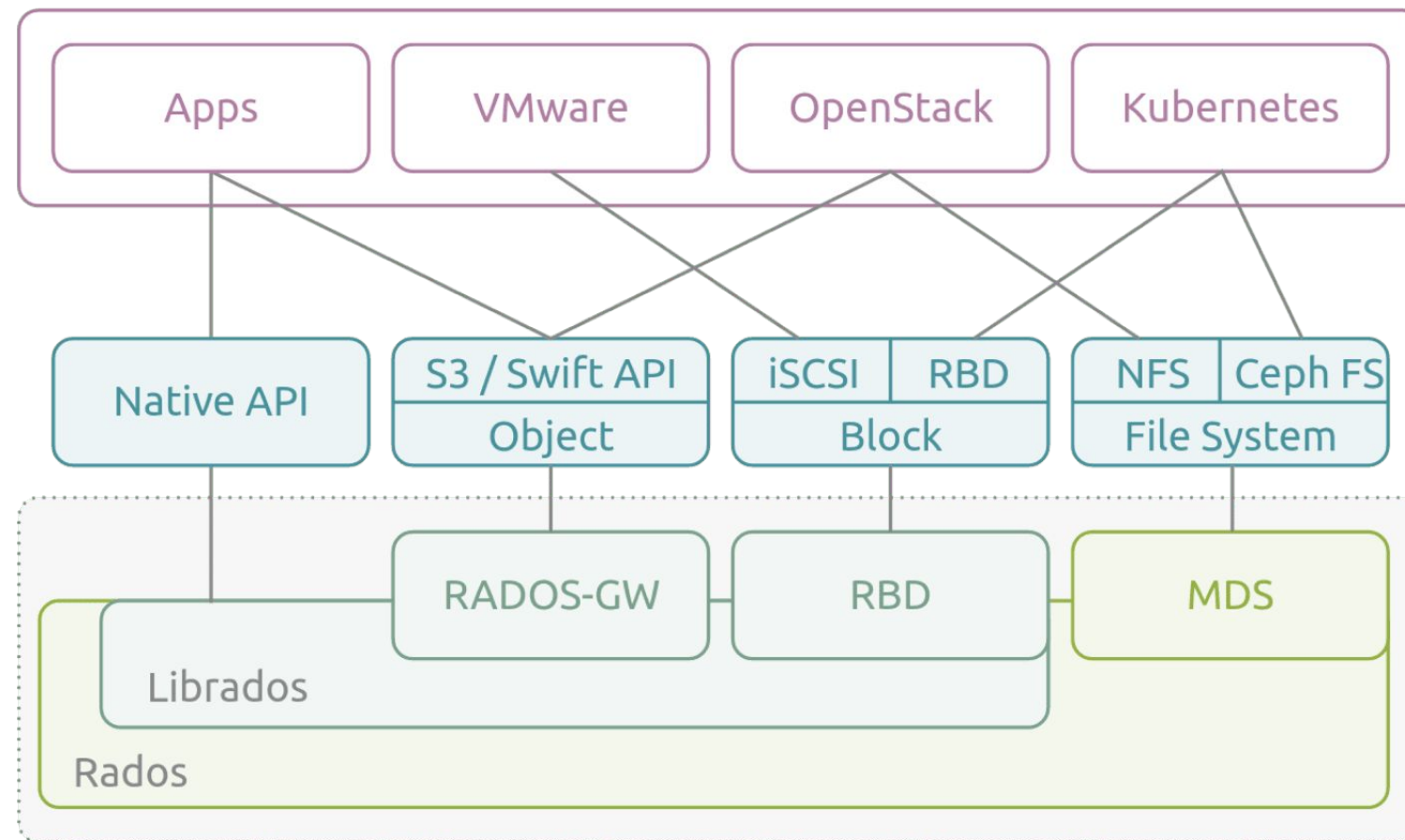


boer  
technology

NASHTAGROUP  
TECHNOLOGY AND SERVICES COMPANY

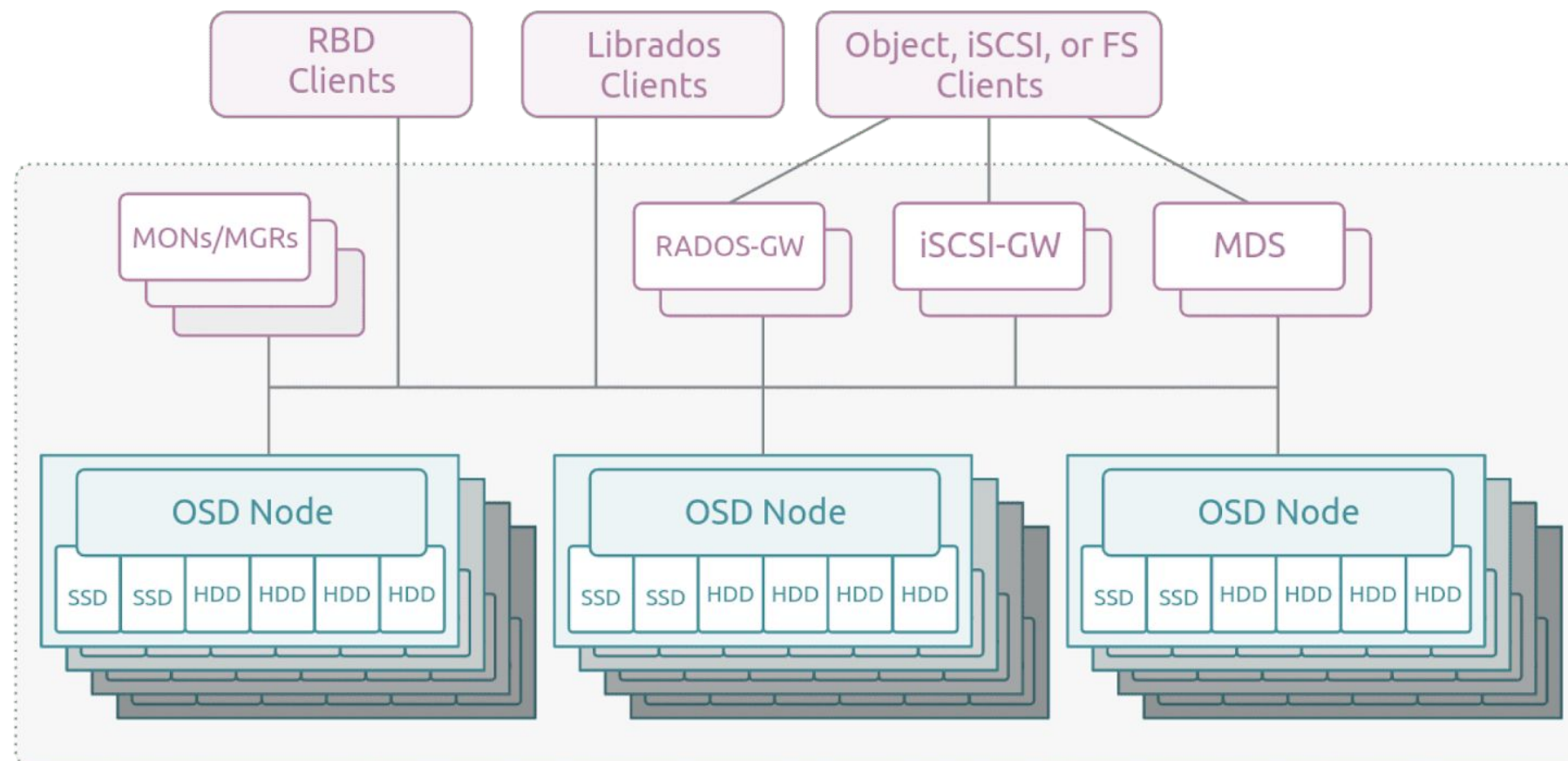
nevacloud

Yogyakarta, 19 July 2025



## Apa itu Ceph?

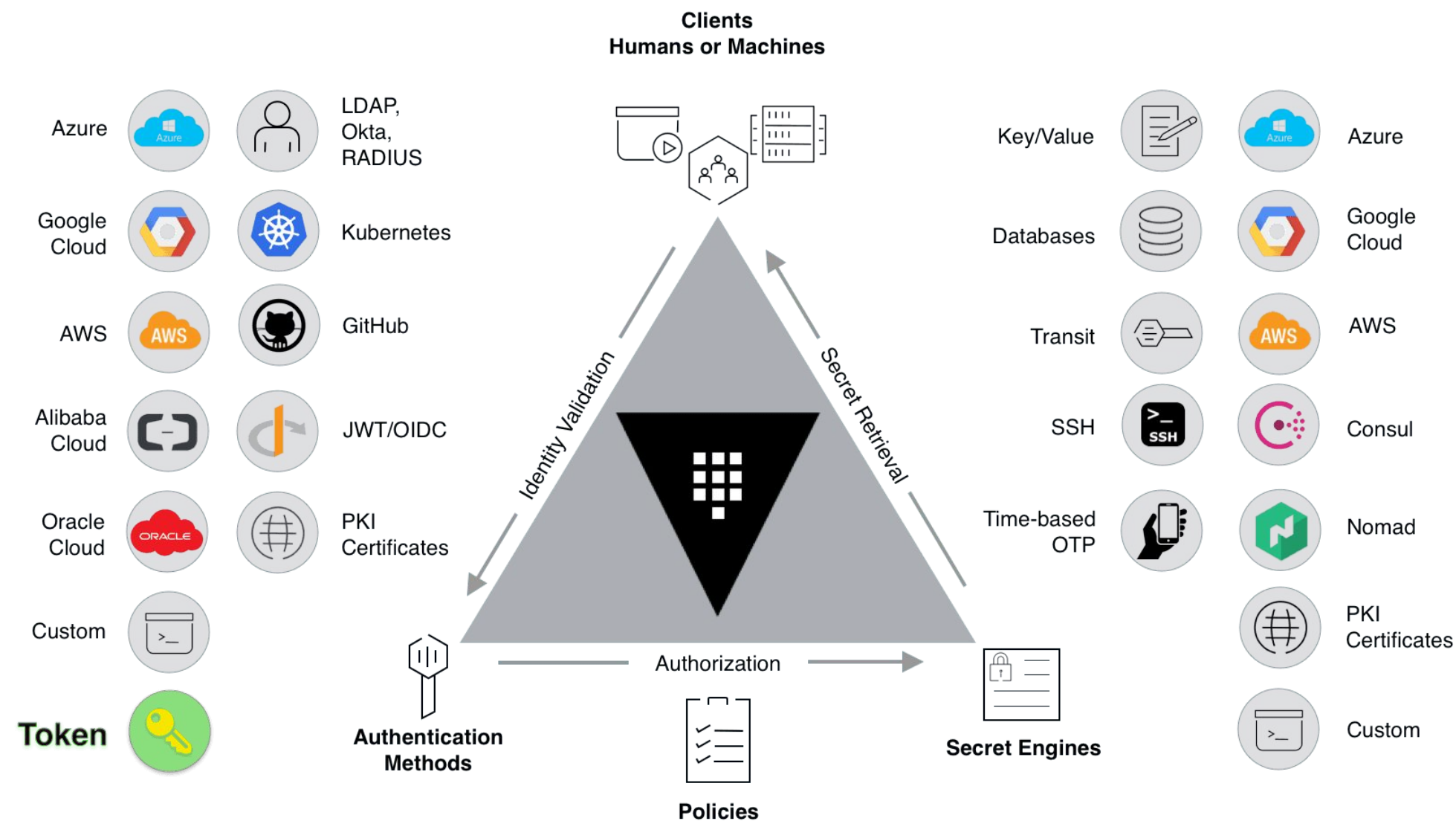
Ceph adalah open-source distributed storage platform yang di design untuk mengintegrasikan object, block, dan file storage ke dalam satu kesatuan sistem yang terpadu.





# Apa itu HashiCorp Vault?

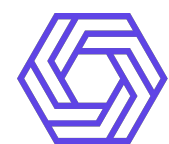
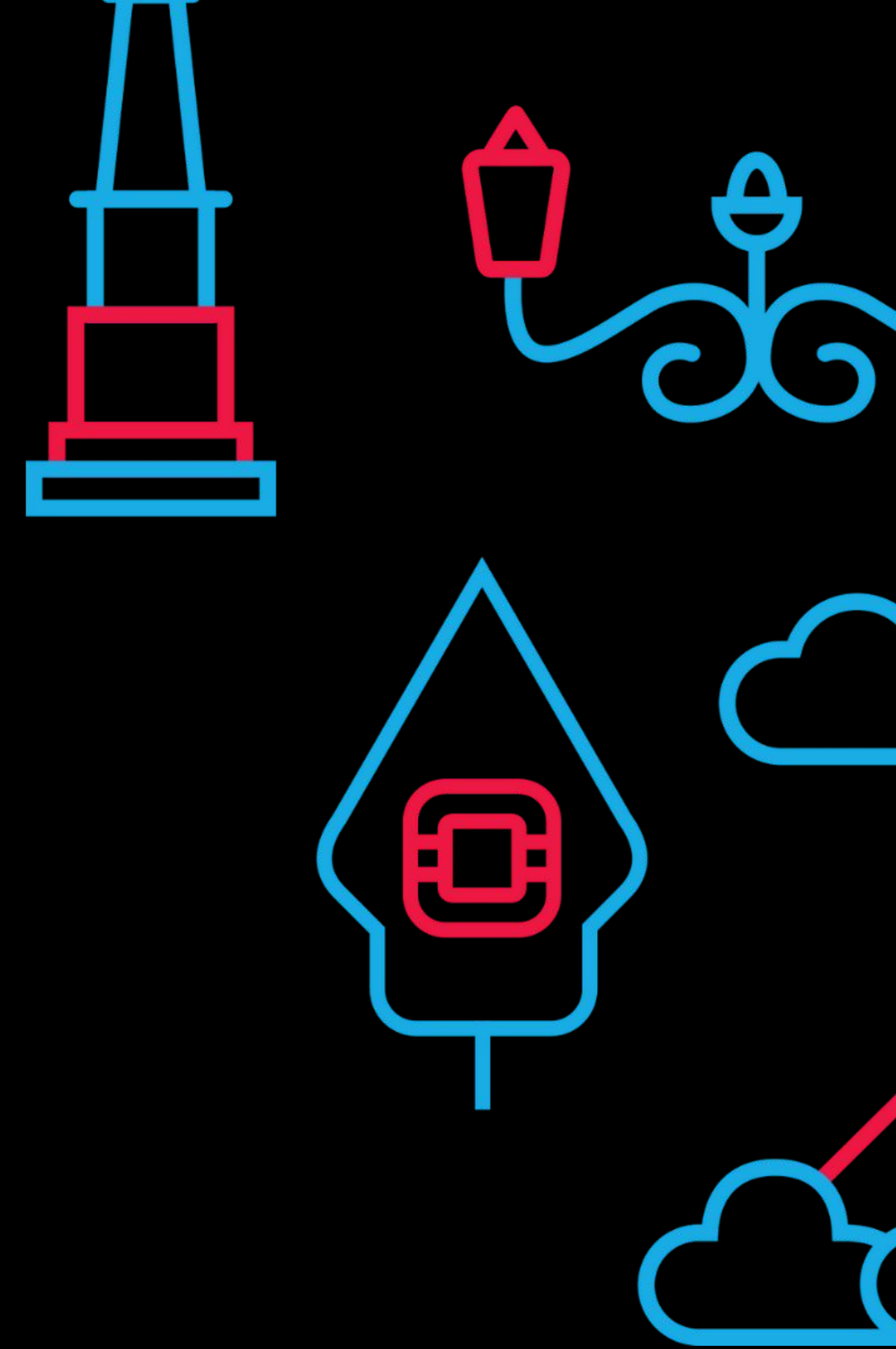
HashiCorp Vault adalah alat open-source untuk secrets management, seperti kata sandi, API Key, Certificate, dan data sensitif lainnya, secara aman dalam infrastruktur IT.



# Kenapa Perlu Encryption?

1. Untuk organisasi yang menyimpan sensitive data
2. Compliance-driven industries (healthcare, finance, government)
3. Multi-tenant environments dengan shared infrastructure
4. Cloud deployments dengan third-party management
5. International organizations dengan cross-border data flows

# Ceph Encryption



**EasyStack**  
open cloud computing



**datacomm**

flexi

WOWRACK



**ZConverter Cloud**



SIVALI  
CLOUD  
TECHNOLOGY

boer  
technology

**NASHTAGROUP**  
TECHNOLOGY AND SERVICES COMPANY

nevacloud

Yogyakarta, 19 July 2025

# Ceph Encryption

1. Native Ceph Way
2. Charmhub Ceph
3. Manual Ceph & Vault Integration



# Native Ceph Way

1. Ceph menyediakan enkripsi native untuk OSD menggunakan LUKS
2. Menggunakan *ceph-volume xxx --dmccrypt* untuk membuat encrypted OSD
3. Encryption key disimpan di Ceph Monitor dalam bentuk lockbox keyring
4. Encryption key di lockbox hanya dapat diakses oleh OSD dengan ID dan UUID yang sesuai
5. OSD untuk mengambil kunci secara aman saat boot untuk decrypt

# Charmhub Ceph

Kita bisa dengan mudah mengaktifkan ceph osd encryption dengan native ceph encryption ataupun vault backend pada charmhub dengan konfigurasi berikut



```
ceph-osd:  
  osd-encrypt: True  
  osd-encrypt-keymanager: vault # use this to integrate with vault
```

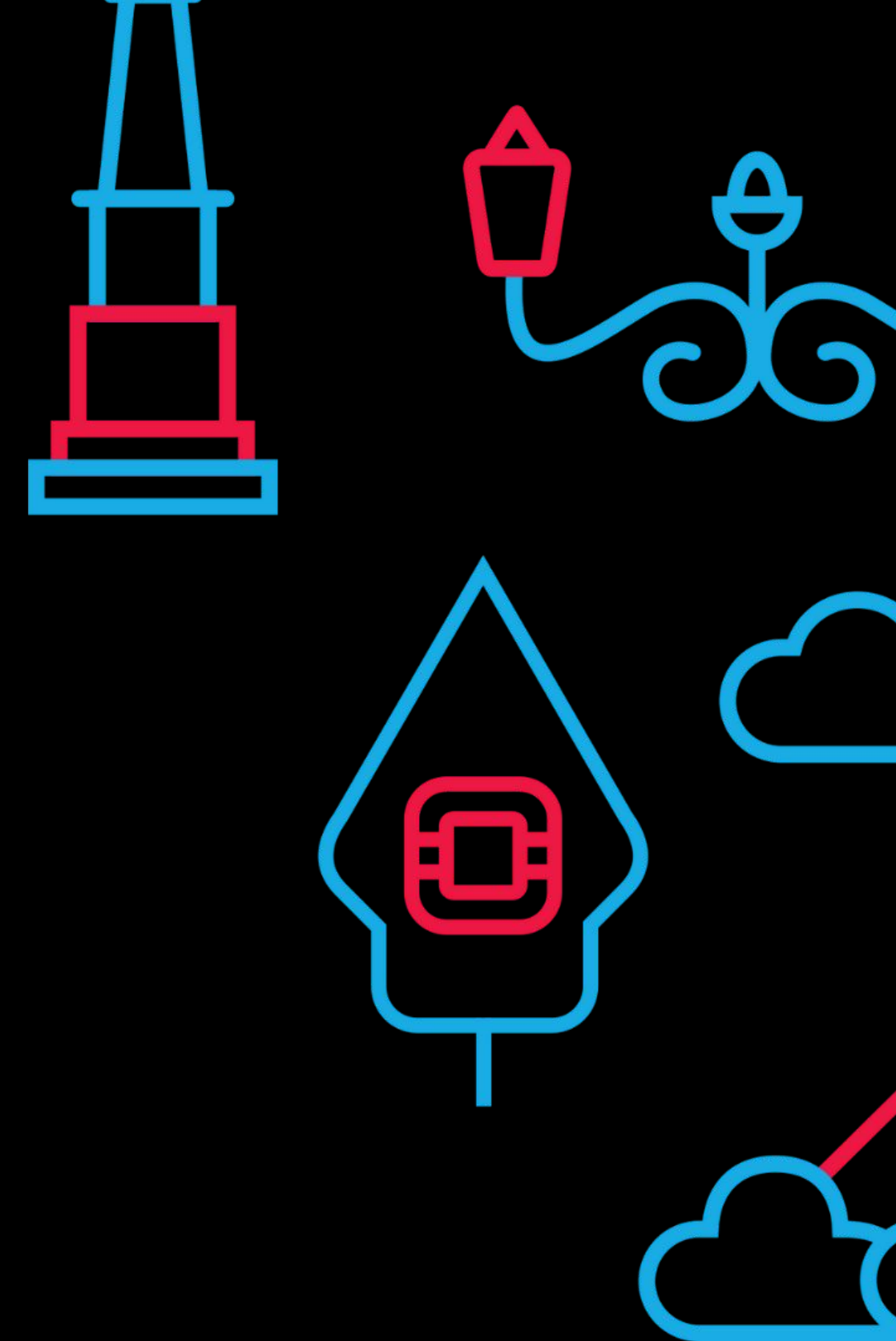
# Manual Ceph & Vault Integration

1. Fokus bahasan materi kali ini
2. Terinspirasi dari Ceph Charmhub
3. Mencoba mengimitasi apa yang dilakukan Ceph Charmhub
4. Fokus utama **untuk pembelajaran**
5. Pada akhirnya bisa diterapkan secara lebih luas dan works juga di luar Ceph Environment

# Kenapa pakai vault?

1. Centralize system untuk semua encryption keys dan multi platform
2. Keys terpisah dari storage infrastructure
3. Possible untuk automated secret lifecycle management
4. Comprehensive logging dan monitoring capabilities
5. Designed untuk enterprise scale
6. Compliance requirements

# Integrasi Ceph dengan Vault



**EasyStack**  
open cloud computing



SIVALI  
CLOUD  
TECHNOLOGY



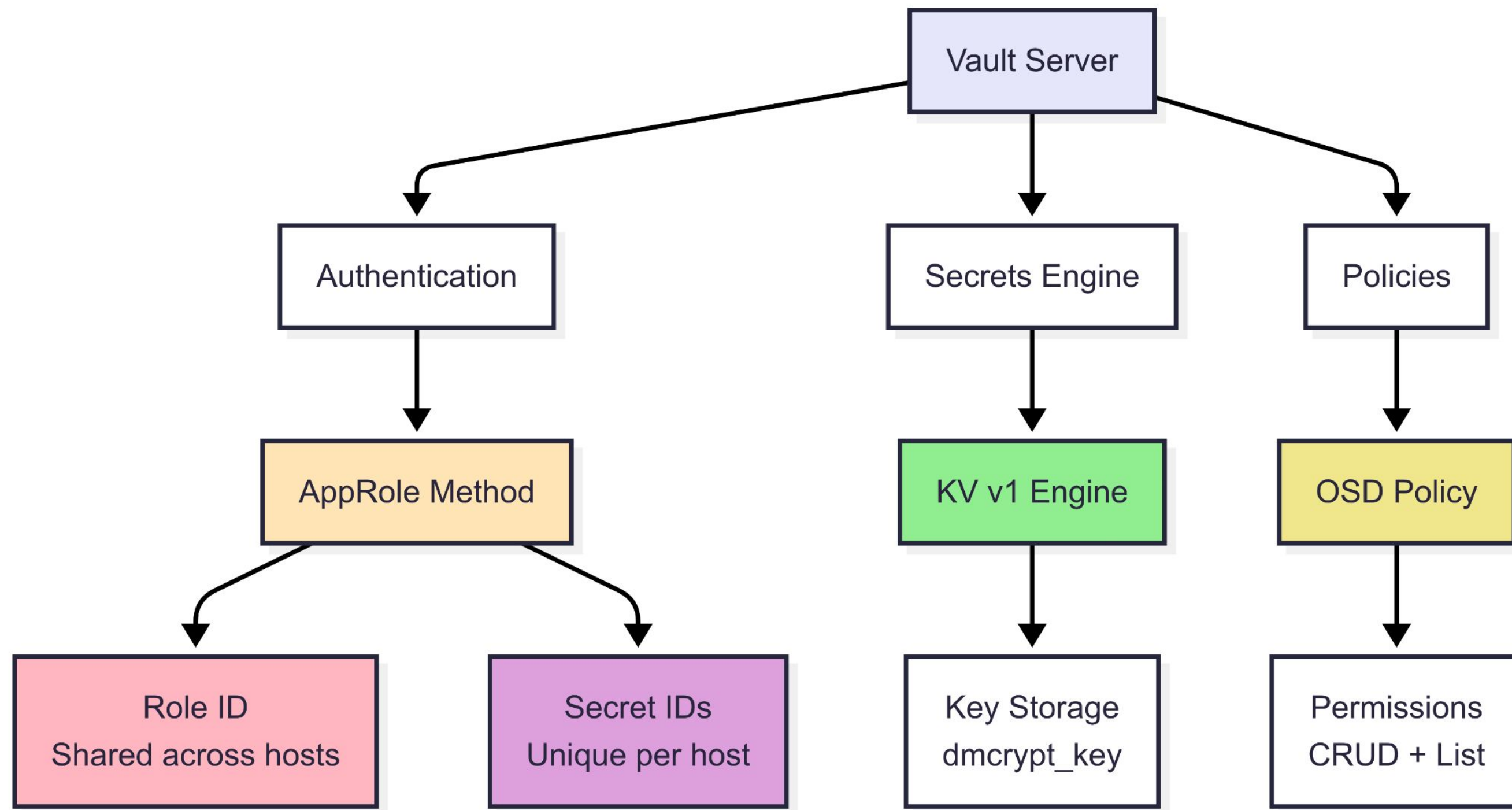
Yogyakarta, 19 July 2025



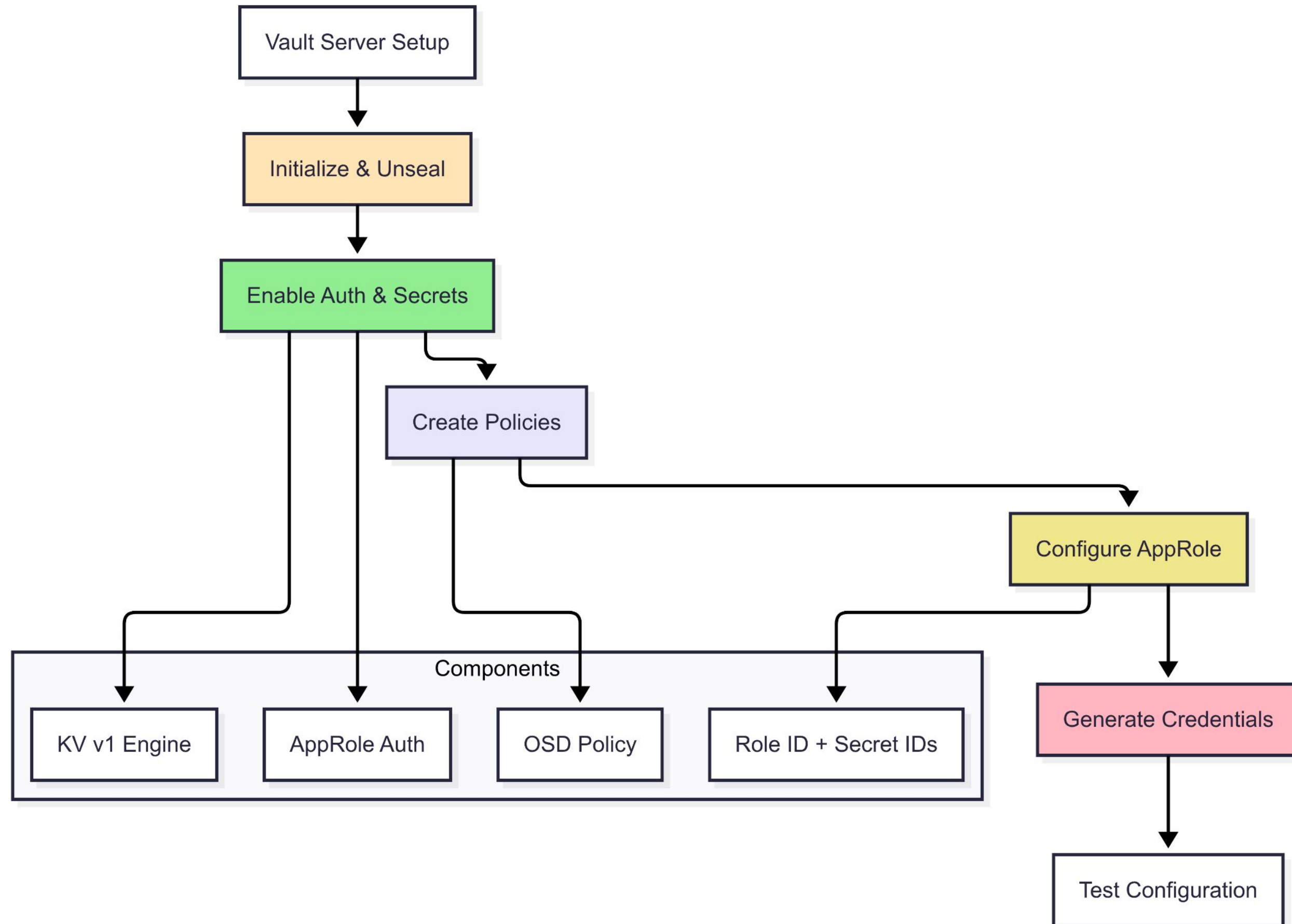
# Integrate Ceph with Vault

1. Install dan Setting Vault
2. Install dan Setting Vaultlocker
3. Membuat Encrypted Ceph OSD

# 1. Install dan Setting Vault



# 1. Install dan Setting Vault



## 2. Install dan Setting Vaultlocker



*# you can install directly via apt*

```
sudo apt install vaultlocker
```

*# edit according to your env*

```
cat /etc/vaultlocker/vaultlocker.conf
```

```
[vault]
```

```
url = http://192.168.10.14:8200
```

```
approle = 8529a1f8-28b2-f1d5-f93a-48ea66985ff1
```

```
secret_id = f62033b7-997d-630b-ab6b-2987aaf4c8a3
```

```
backend = vaultlocker
```

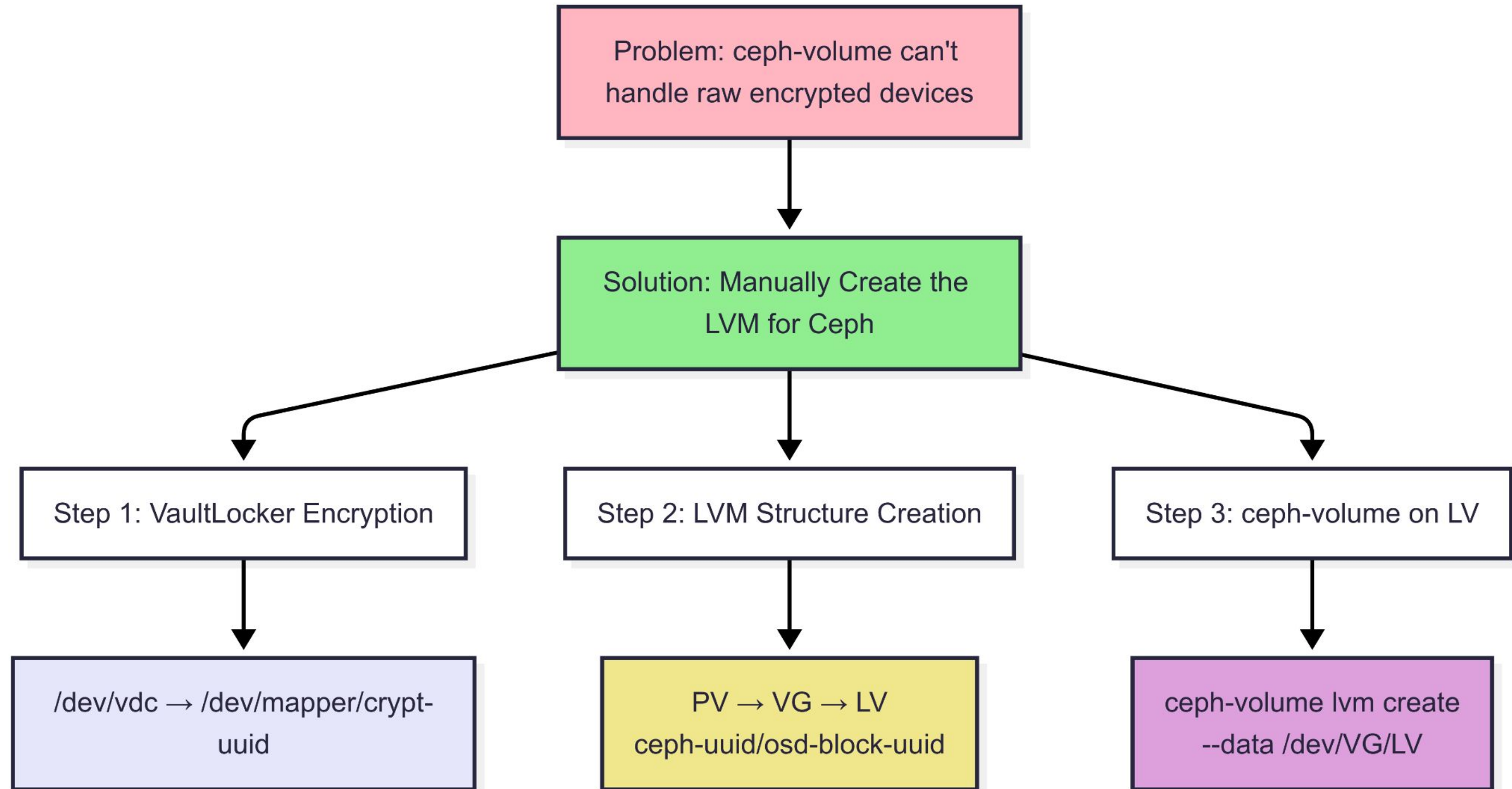
Kita bisa install langsung Vaultlocker melalui APT dan tinggal sesuaikan file config nya

### 3. Membuat Encrypted Ceph OSD

```
root@na-host3:~# lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0                              7:0      0   50.9M  1 loop /snap/snapd/24718
loop1                              7:1      0   73.9M  1 loop /snap/core22/2010
loop2                              7:2      0  204.7M  1 loop /snap/vault/2399
loop3                              7:3      0   100M   0 loop
└─crypt-9f8c3e19-2dde-46e3-9633-92f21b33a89b 252:1    0    84M   0 crypt
loop4                              7:4      0   49.3M  1 loop /snap/snapd/24792
loop5                              7:5      0   73.9M  1 loop /snap/core22/2045
sr0                                11:0     1    366K   0 rom
vda                                253:0    0    50G   0 disk
├─vda1                             253:1    0    49G   0 part /
├─vda14                            253:14   0     4M   0 part
├─vda15                            253:15   0   106M   0 part /boot/efi
└─vda16                            259:0    0   913M   0 part /boot
vdb                                253:16   0    50G   0 disk
└─ceph--a48e1f82--83c5--4b17--80c6--799a4f91f4ed-osd--block--ca4b4916--9bef--4025--9c7b--bcf953568131 252:0    0    50G   0 lvm
vdc                                253:32   0    50G   0 disk
vdd                                253:48   0    50G   0 disk
root@na-host3:~# ceph-volume lvm create --data /dev/mapper/crypt-9f8c3e19-2dde-46e3-9633-92f21b33a89b
Running command: /usr/bin/ceph-authtool --gen-print-key
Running command: /usr/bin/ceph-authtool --gen-print-key
Running command: /usr/bin/ceph --cluster ceph --name client.bootstrap-osd --keyring /var/lib/ceph/bootstrap-osd/ceph.keyring -i - osd new ec06d352-465c-473c-9109-61c59fc8295f
→ Was unable to complete a new OSD, will rollback changes
Running command: /usr/bin/ceph --cluster ceph --name client.bootstrap-osd --keyring /var/lib/ceph/bootstrap-osd/ceph.keyring osd purge-new osd.5 --yes-i-really-mean-it
stderr: purged osd.5
→ RuntimeError: Unable to find any LV for zapping OSD: 5
root@na-host3:~# |
```



### 3. Membuat Encrypted Ceph OSD



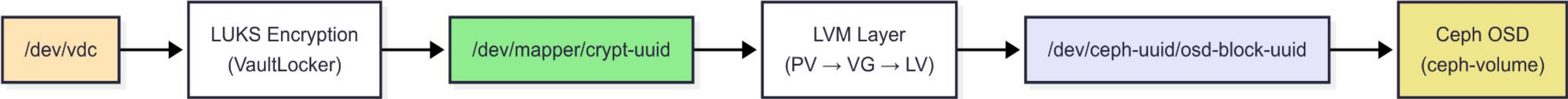
### 3. Membuat Encrypted Ceph OSD

```
root@na-host1:~# lsblk | head -15
NAME                                MAJ:MIN RM  SIZE RO TYPE
loop0                               7:0      0   49.3M 1 loop
loop1                               7:1      0   73.9M 1 loop
loop2                               7:2      0  204.7M 1 loop
sr0                                 11:0      1    366K 0 rom
vda                                 253:0      0    50G  0 disk
├─vda1                             253:1      0    49G  0 part
├─vda14                             253:14     0     4M  0 part
├─vda15                             253:15     0   106M  0 part
└─vda16                             259:0      0   913M  0 part
vdb                                 253:16     0    50G  0 disk
└─ceph--a7fbf7d0--87a1--4e93--a311--a0ea7b54f53c-osd--block--7351cbf5--d967--44d3--b6bd--def4b7bf1f7b 252:0      0    50G  0 lvm
vdc                                 253:32     0    50G  0 disk
└─crypt-d034f130-e34e-40a0-b69d-a404c9ad079a 252:1      0    50G  0 crypt
   └─ceph--d034f130--e34e--40a0--b69d--a404c9ad079a-osd--block--d034f130--e34e--40a0--b69d--a404c9ad079a 252:2      0    50G  0 lvm

root@na-host1:~# pvs
PV                                VG                                Fmt  Attr  PSize  PFree
/dev/mapper/crypt-d034f130-e34e-40a0-b69d-a404c9ad079a ceph-d034f130-e34e-40a0-b69d-a404c9ad079a lvm2  a--   49.98g    0
/dev/vdb                                ceph-a7fbf7d0-87a1-4e93-a311-a0ea7b54f53c lvm2  a--   <50.00g    0
/dev/vdd                                ceph-e45f0e46-df01-4c65-8ef4-e62e30a93d58 lvm2  a--   <50.00g    0

root@na-host1:~# lvs
LV                                VG                                Attr      LSize  Pool Origin Data% Me
osd-block-7351cbf5-d967-44d3-b6bd-def4b7bf1f7b ceph-a7fbf7d0-87a1-4e93-a311-a0ea7b54f53c -wi-ao-   <50.00g
osd-block-d034f130-e34e-40a0-b69d-a404c9ad079a ceph-d034f130-e34e-40a0-b69d-a404c9ad079a -wi-ao-   49.98g
osd-block-acbcd6ec-df75-4e06-8c4a-925b613941ea ceph-e45f0e46-df01-4c65-8ef4-e62e30a93d58 -wi-ao-   <50.00g

root@na-host1:~#
```



### 3. Membuat Encrypted Ceph OSD

Vault

Vault

Dashboard

Secrets Engines

Access >

Policies >

Tools >

Monitoring

Client Count >

Seal Vault

Secrets / vaultlocker

vaultlocker

version 1

Secrets

Configuration

Filter secrets

Create secret +

na-host1/

...

na-host2/

...

na-host3/

...

1-3 of 3

< 1 >

Vault 1.20.0

[Upgrade to Vault Enterprise](#)

[Documentation](#)


[Support](#)

[Terms](#)

[Privacy](#)

[Security](#)

[Accessibility](#)

 © 2025 HashiCorp

### 3. Membuat Encrypted Ceph OSD

Vault

Vault

Dashboard

Secrets Engines

Access

Policies

Tools

Monitoring

Client Count

Seal Vault

Secrets / vaultlocker

vaultlocker

version 1

Secrets Configuration

na-host1/

Create secret +

0ce6c937-0fcb-4c08-9467-6c867eb14123

821f47dd-4e1d-4567-8a8a-b944c66cb452

d034f130-e34e-40a0-b69d-a404c9ad079a

1-3 of 3

< 1 >

Vault 1.20.0

Upgrade to Vault Enterprise

Documentation

Support

Terms

Privacy

Security

Accessibility

© 2025 HashiCorp



### 3. Membuat Encrypted Ceph OSD

Vault

Vault

Dashboard

Secrets Engines

Access

Policies

Tools

Monitoring

Client Count

Seal Vault

vaultlocker / na-host1 / 0ce6c937-0fcb-4c08-9467-6c867eb14123

na-host1/0ce6c937-0fcb-4c08-9467-6c867eb14123

Secret

JSON

Delete

Copy

Edit secret

Key	Value
dmgcrypt_key	<div><div></div><div></div><div>dNICfJUIC9Wk/ wFbsweiEWWz+yvrJtaQ4+CiTMf1Lko5qQKNhBsJd2d8hCzig1LJTcpQWk+LrA04US3Z6F5yhOVf1cL/ re4hqhzcYMo0m3cVwcVXEKFHIRmzcu663xRv911KJ2Erg0r78v03tAkzuZ2fz5bHm92x+m+68u9oEmCu98fqzmvn0tor8YLGjaqih7MYe7fwa60D1S7yGVFfz5Lcxjv96bPRLPAype125LxcUsJC5s udNpEuuBZmHLcAz3aJ4dWU7fK02cuzHpM7KU715PWY4awkAeVAtqs0klQ3g+MQ6N+iUshfEi6tXIXdGYBwgoDxuwB1CK5BSI6v11rP9q+DthbmFCXwP241NydPchqYNzpm1KrGoA5wg0bXb8iKxF/ Mb0CoL+HJVDyA2t7CccXX/i699g3d/ ESKb+RyEqU7UM+anbnpyRxDLUTs9mTh2faGhaaZIb0hLpyuDU+synqAFP0LGhvd/ k5p1553RR77E85FWRU9sdGuZ0mdjerrPK7DzgJ7VLPjxEu3I3T1UQANDUFqtS78r1yIIoZfPCrp4CV0NKJ+OAxAJMsmC4HepV1Sg7hLzWiyN13cIz3Xf9nYV/k+Sn50kKE9+it8gw3sGUjhrDk4/ tP170rfsx9cMI04yHd/0DABkgFCIJLCs79QQDZjg4kh1CJmhM=</div></div>

Vault 1.20.0

Upgrade to Vault Enterprise

Documentation


Support

Terms

Privacy

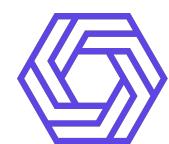
Security

Accessibility

 © 2025 HashiCorp



# Tantangan dan Limitasi



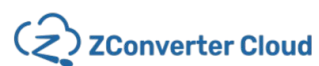
**EasyStack**  
open cloud computing



**datacomm**

flexi

WOWRACK



boer  
technology

NASHTAGROUP  
TECHNOLOGY AND SERVICES COMPANY

nevacloud

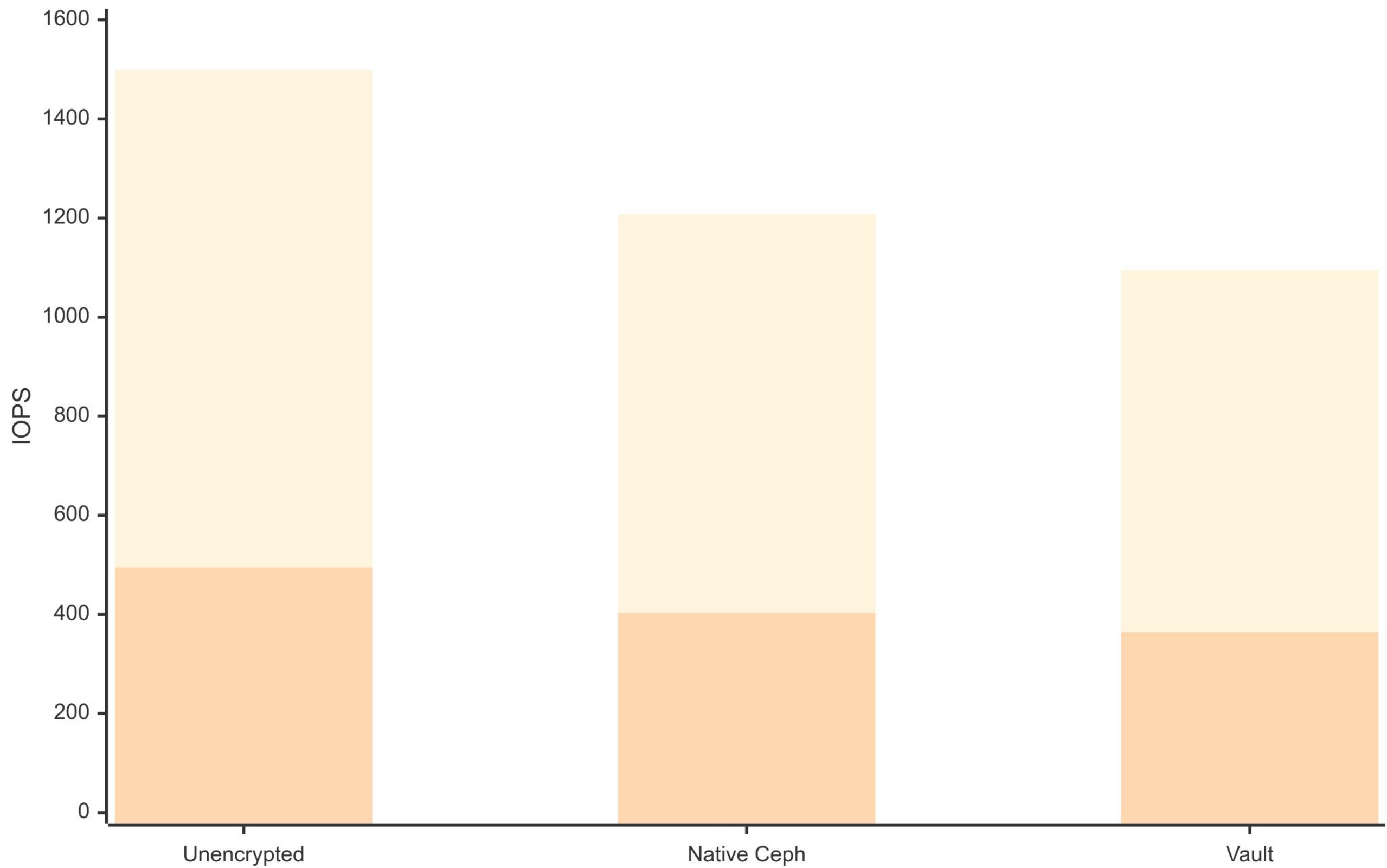
Yogyakarta, 19 July 2025

# Tantangan dan Limitasi

1. IOPS menurun secara signifikan
2. Integrasi manual butuh banyak effort

# Tantangan dan Limitasi

Read vs Write IOPS Performance



## Key Findings

- 1. **Native Ceph Encryption Impact:**
  - ~19-20% performance reduction compared to unencrypted
- 2. **Vault Encryption Impact:**
  - ~27% performance reduction compared to unencrypted
  - ~9% additional reduction compared to Native Ceph

# Rekomendasi & Best Practice



**EasyStack**  
open cloud computing



**datacomm**

flexi

WOWRACK



**ZConverter Cloud**



**SIVALI  
CLOUD  
TECHNOLOGY**

**boer  
technology**

**NASHTAGROUP**  
IT SOLUTION AND SERVICES COMPANY

**nevacloud**

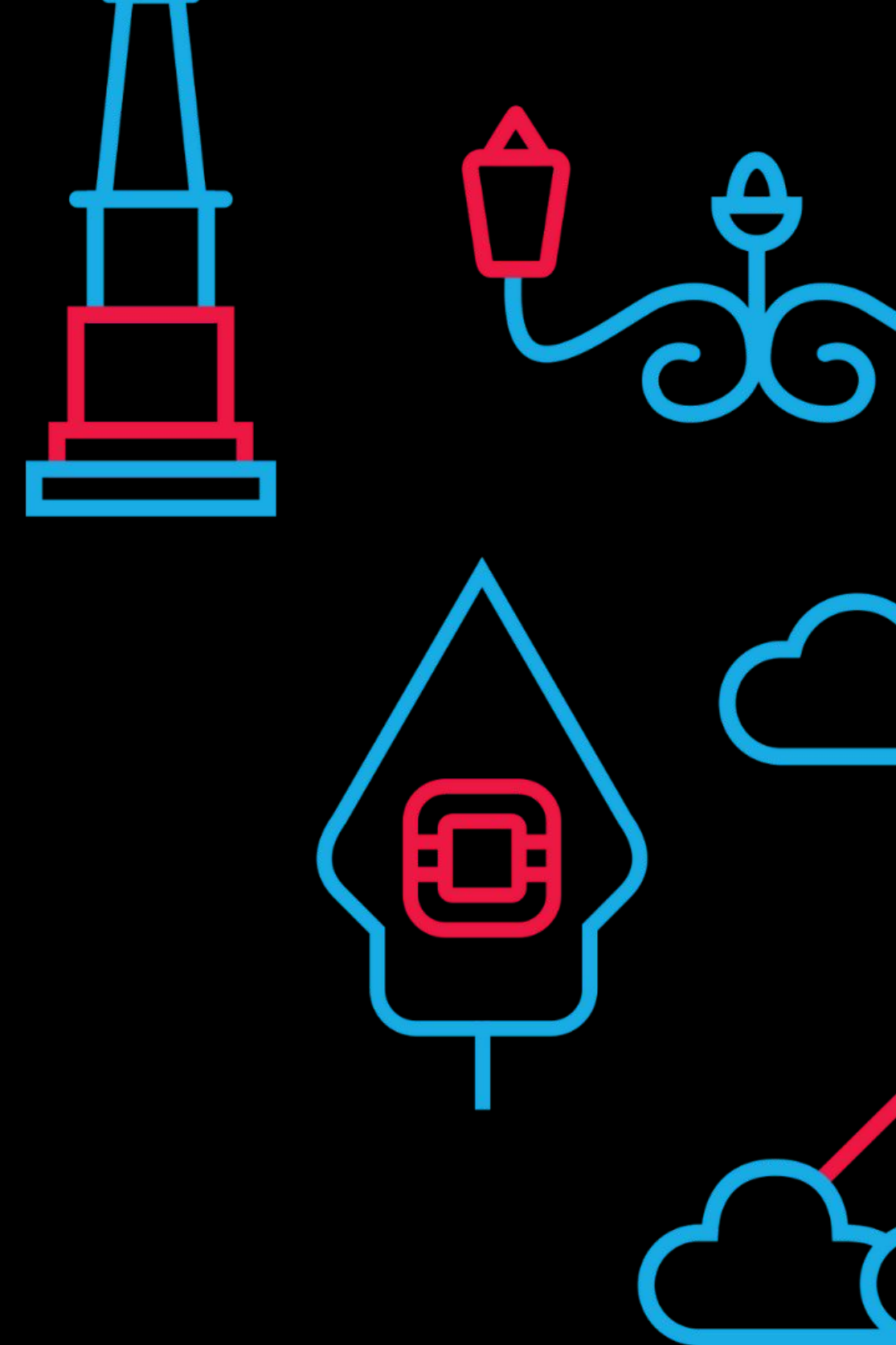
Yogyakarta, 19 July 2025

# Rekomendasi & Best Practice

1. Deploy HashiCorp Vault secara highly available (HA)
2. Aktifkan file audit logging
3. Buat Vault Policy dan Approle yang berbeda untuk setiap host
4. Buat config Approle lebih strict
5. Setup Secret ID rotation



# THANK YOU



**EasyStack**  
open cloud computing



**datacomm**

flexi

WOWRACK



boer  
technology

**NASHTAGROUP**  
TECHNOLOGY AND SERVICES COMPANY

nevacloud

Yogyakarta, 19 July 2025