



# Roglit 25

## Prihodnost shranjevanja podatkov S3.Procloud

[Jernej.romih@unistarpro.si](mailto:Jernej.romih@unistarpro.si)

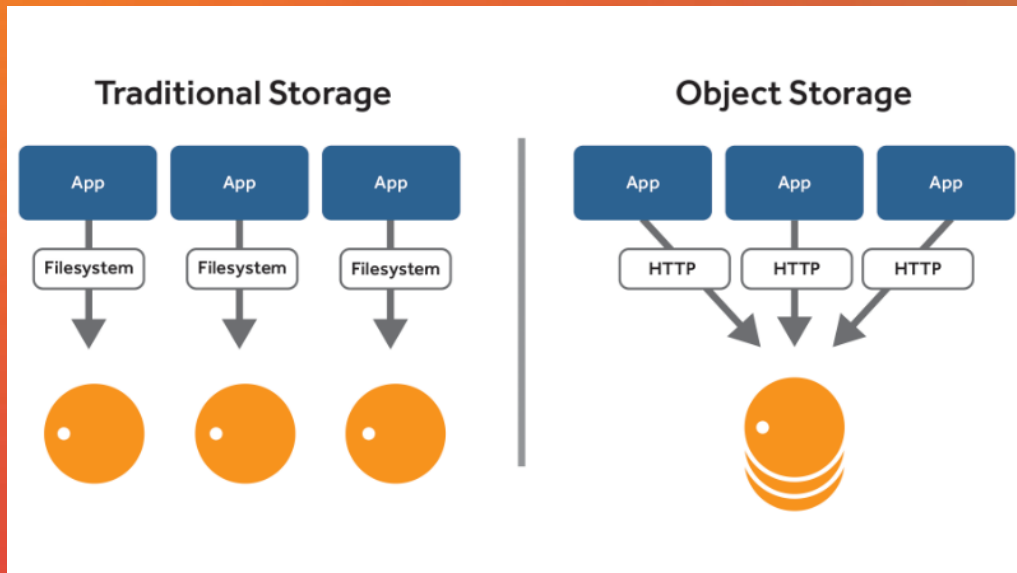
Zavezništvo za močnejši IT ekosistem – Building a Stronger IT Ecosystem



# S3

- Amazon S3 – Simple Storage Service
- Prvič predstavljen 2006 kot storitev AWS
- Storitev za shranjevanje objektov v oblaku
- Preprost vmesnik API
- Ključne lastnosti
  - Skalabilnost
  - Shranjevanje podatkov v obliki objektov (meta podatki)
  - Orzanizacija v t.i. kontejnerjih ali „bucketih“

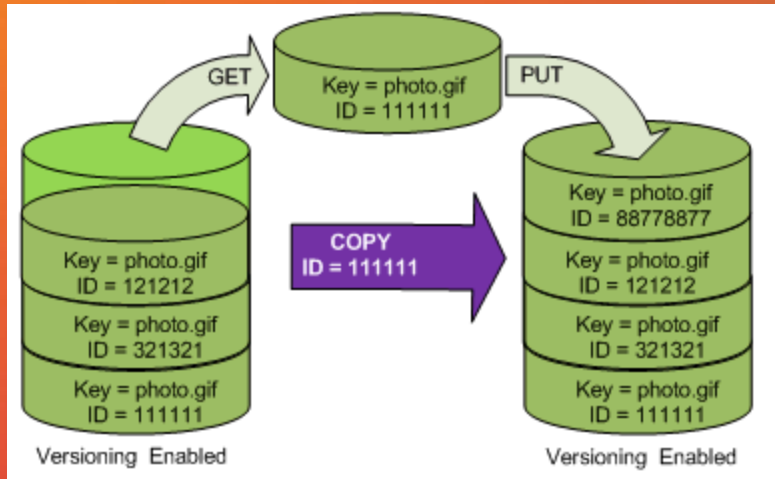
# Protokol S3



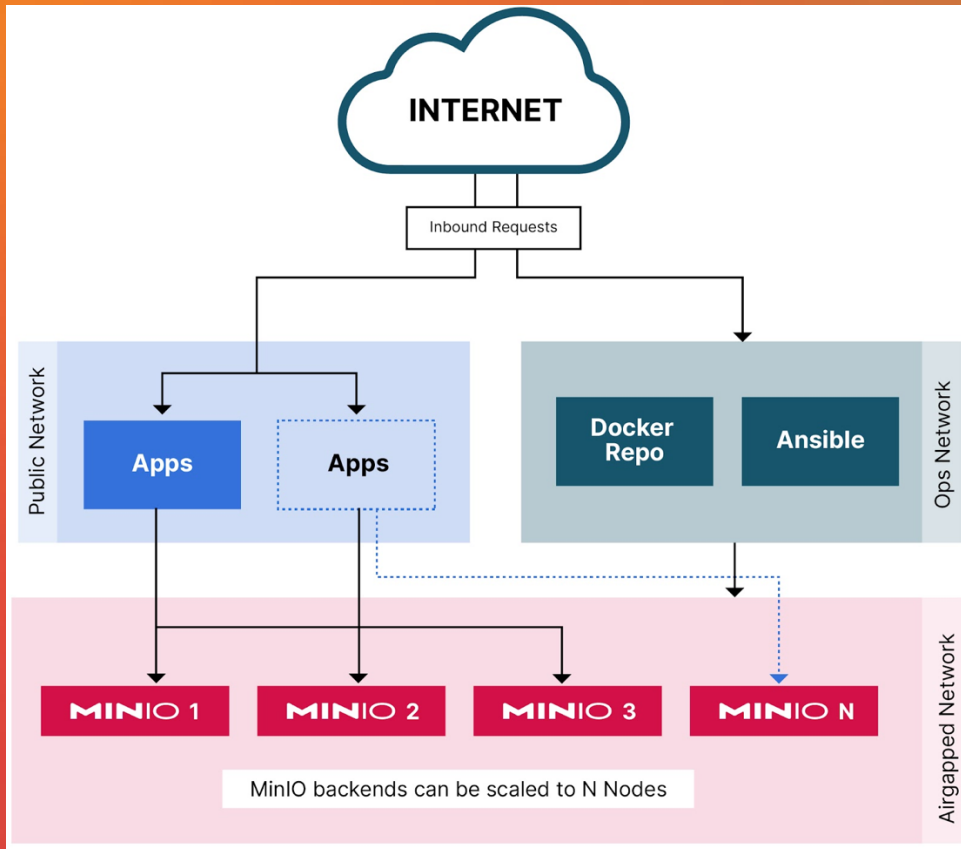
- Osnova je http/https
- Uporablja RESTful API za operacije:
  - PUT: naloži objekt
  - GET: preseni objekt
  - DELETE: briši objekt
  - HEAD: preveri metapodatke objekta
- Preverjanje identitete – AWS Signature (v1, v2, v3, v4)
- S3 protokol je postal standard za mnoge ponudnike shranjevanja podatkov v oblaku (Azure, IBM, Google, Wasabi...)

# Protokol S3

- Podpora verzij,
  - možnost obnove objekta iz starejših verzij v primeru nenamerne brisanja
  - Možnost obnove verzije objekta v primeru zlonamerne spremembe objekta
- Šifriranje
  - Podatki S3 so avtomatsko šifriran med transportom –TLS/SSL
  - Možnost server side enkripcije ali client key mgmt (SSE-S3, SSE-KMS,SSE-C)
- Nespremenljivost
  - Object Lock
  - Zagotavljanje skladnosti z regulativo

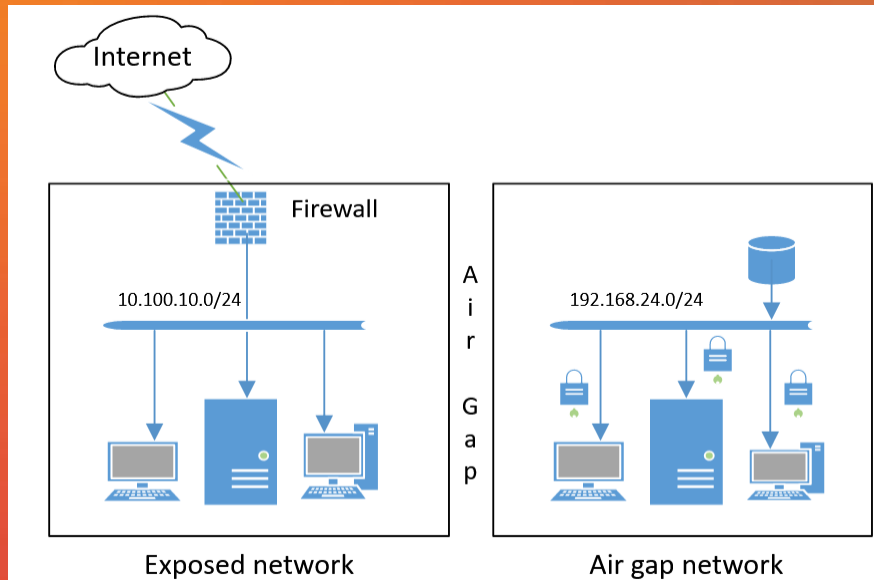


# Protokol S3



- Izolacija shrambe – Air-gapped
  - Sistem deluje v „air-gapped“ omrežju zaradi zaščite podatkov pred kibernetскими napadi
- S3 Air-gapped shramba
  - Npr. MINIO on-prem (air-gapped network)
  - Funkcije protokola S3 (verzije, nespremenljivost)
  - Strogo nadzorovan dostop do sistema (Ops Network)
- ILM – Life Cycle Management
  - Premik podatkov med „storage“ tiri
  - Samodejno brisanje zastarelih objektov
  - Enostavno upravljanje življenjske dobe podatkov glede na zahteve

# Primeri uporabe

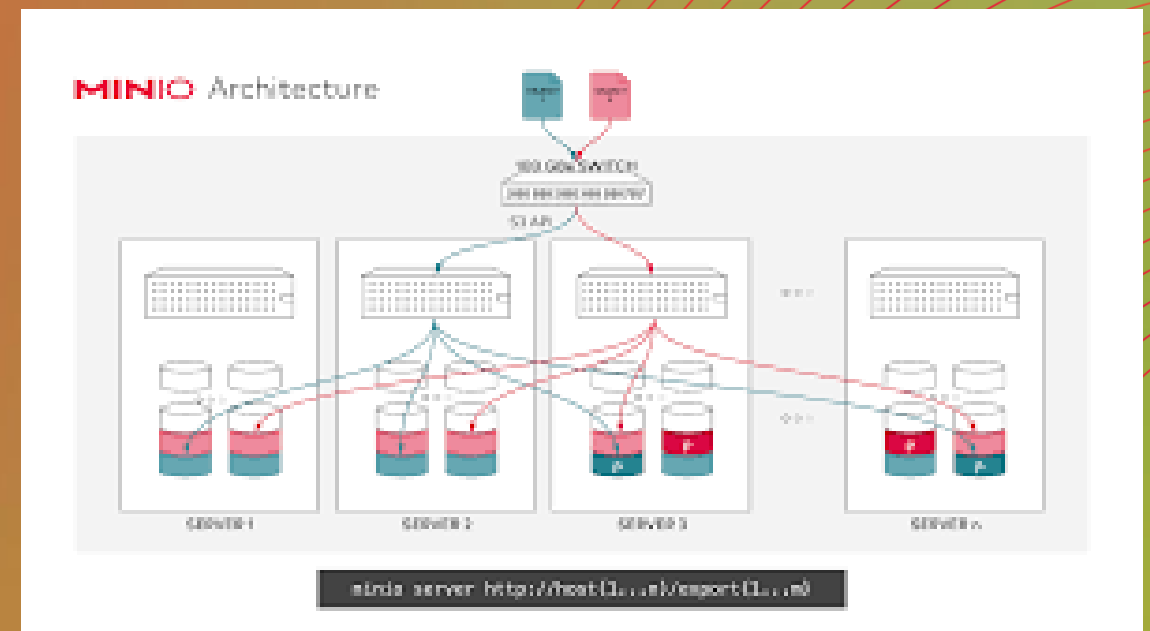


- Ponudniki storitev npr. **S3.PROCLOUD**
- Shranjevanje varnostnih kopij/Disaster Recovery
  - Primarna kopija
  - Druga oz. tretja kopija
  - Air-gapped kopija (lahko nadomesti tračno enoto)
- Centralizirano shranjevanje logov
- Shranjevanje podatkov za obdelavo z AI orodji
- Analitika – big data (spark, hadoop)
- S3 kot orodje za deljenje datotek med napravami/uporabniki (CDN)
- Distribucija vsebin: multimedija, programska oprema

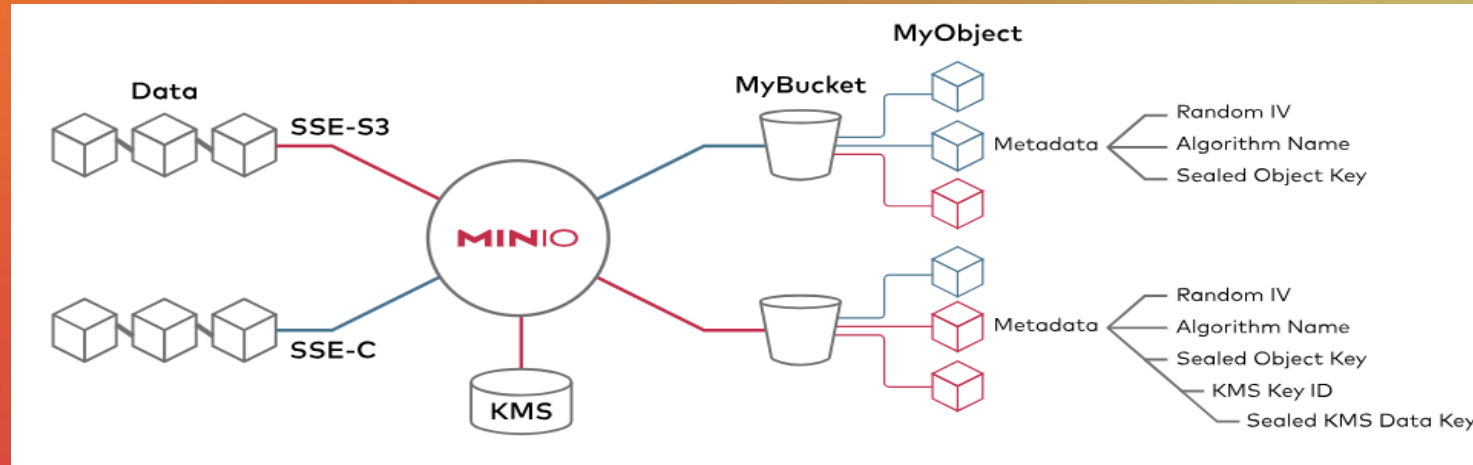
# Kaj je MinIO

- Zmogljiva odprtokodna rešitev za shranjevanje objektov
- Na voljo kot rešitev v oblaku, on-prem ali na robu (edge)
- Minimalistična zasnova – razvit v GO (Google)
  - Integrirana zaščita podatkov z algoritmom ErasureCoding z nastavljivo redundanco
- Popolna podpora S3 API, kar omogoča integracijo z S3 aplikacijami

- Optimiziran za delovanje s tehnologijami NVMe, SSD, SAS, 100GB omrežja – visoka zmogljivost
- Skalabilnost:
  - Horizontalno
  - Dodajanje strežnikov in diskov



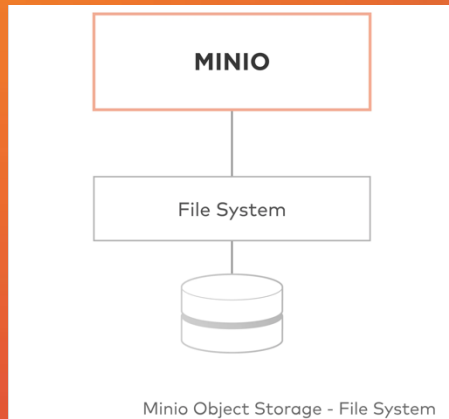
# Zasebnost podatkov



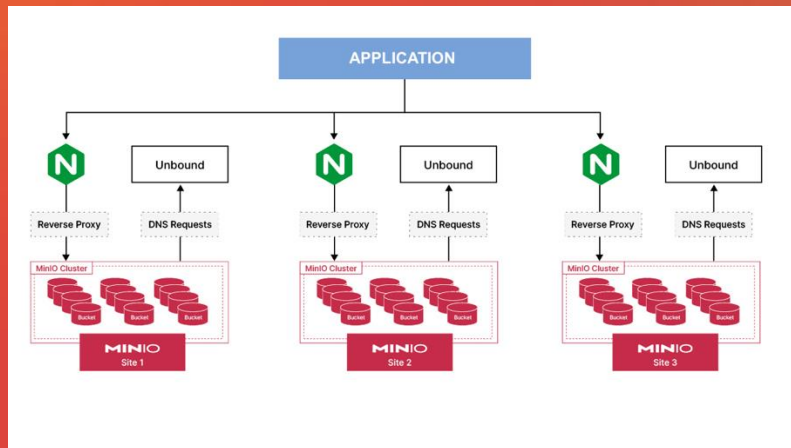
- Data-in-motion
- Data-at-rest
  - MinIO podpira SSE - enkripcijo podatkov v mirovanju (AES-256-CGM, ...)
  - Transparentna za uporabnike
  - KMS (HashiCorp Vault, Microsoft Azure Key Vault, AWS KMS...)
  - Dostop do ključa ima administrator S3 serverja oz. lastnik podatkov (SSE-C)
  - Šifriranje z uporabo TLS/SSL



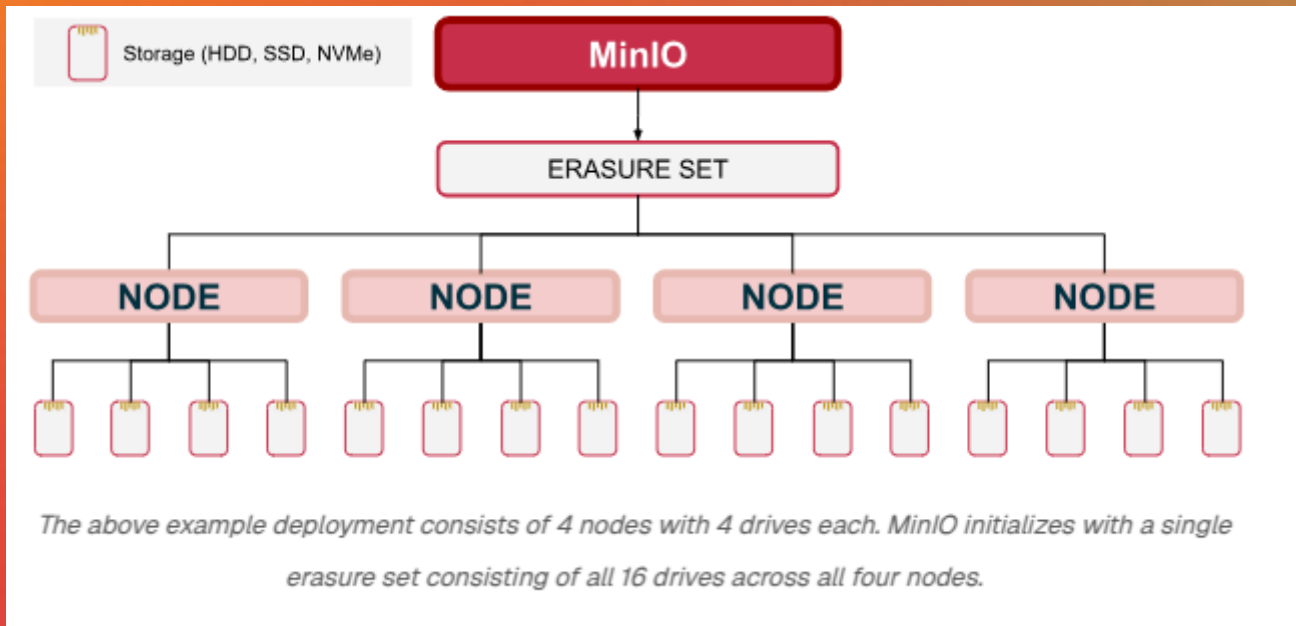
# Različne postavitve



- Samostojna postavitve
  - Manjše postavitve ali razvoj
  - Minimalne zahteve brez vgrajene redundance (procesor/ram, 1 disk)
- Porazdeljena postavitve (SINGLE SERVER MULTI DRIVE, MULTI SERVER MULTI DRIVE)
  - Podatki shranjeni na več strežnikih (3+) z vgrajenimi diski JBOD
  - Redundanco zagotavlja MINIO – porazdelitev med skupinami diskov in serverji –Erasure Coding algoritem, BitRot protection
  - linearna razširljivost z dodajanjem strežnikov in diskov JBOD
- Geo-zrcaljenje
  - Zrcaljenje (tudi dvosmerno) podatkov med več podatkovnimi centri
  - Na nivoju S3 instance ali na nivoju „bucketa“
- Kubernetes/Openshift/Docker integracija
  - MinIO Operator za provisioning
  - Privzeta shramba podatkov za varnostne kopije Kubernetes/openshift
  - Ponudniki storitev



# S3.PROCLOUD - platforma

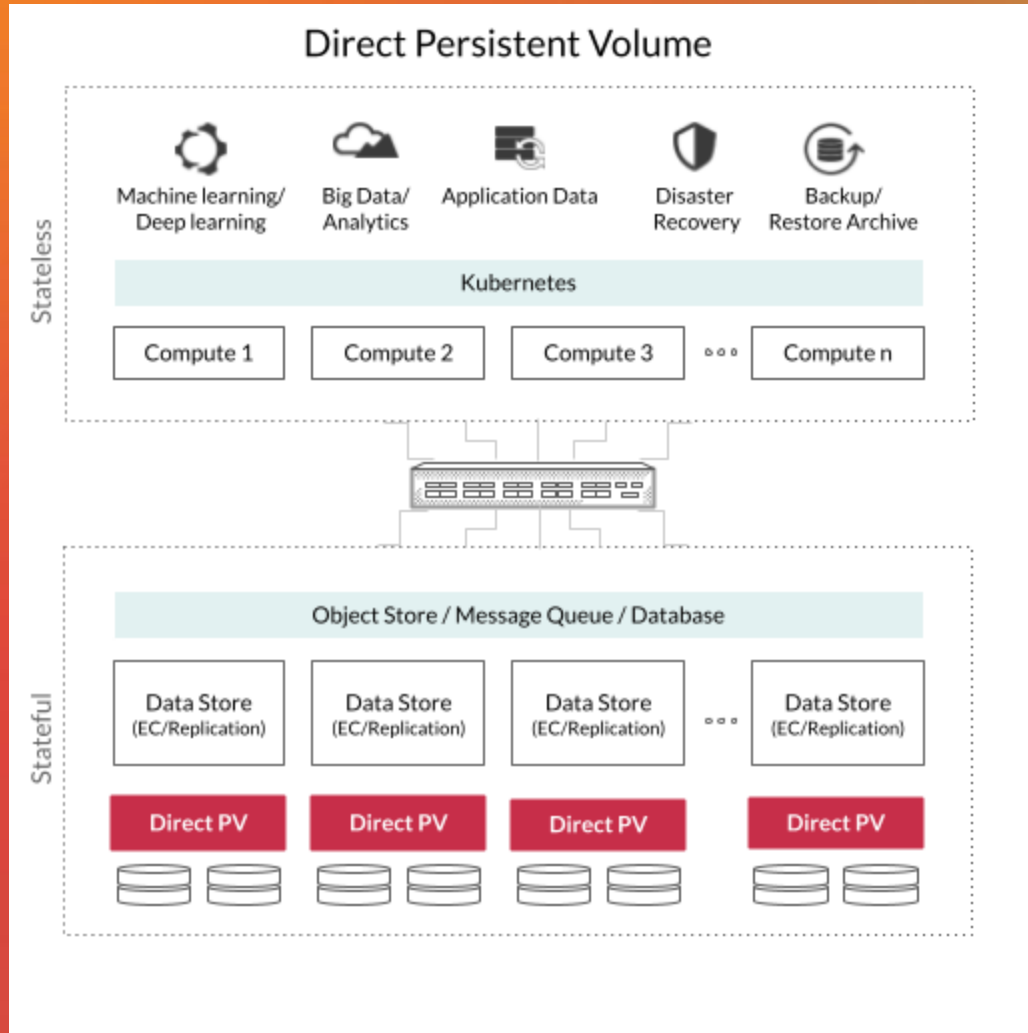


- Strojna oprema

- Lenovo SR650
- Vgrajeni diski kapacitete 20TB – JBOD
- LAN povezava – 25Gbps, možnost 100GBPS
- 4 strežniki na lokacijo
- MinIO Multi Node Multi Drive
- Capacity tier (SAS)

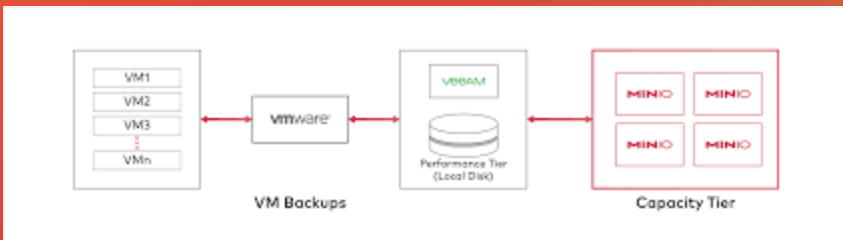
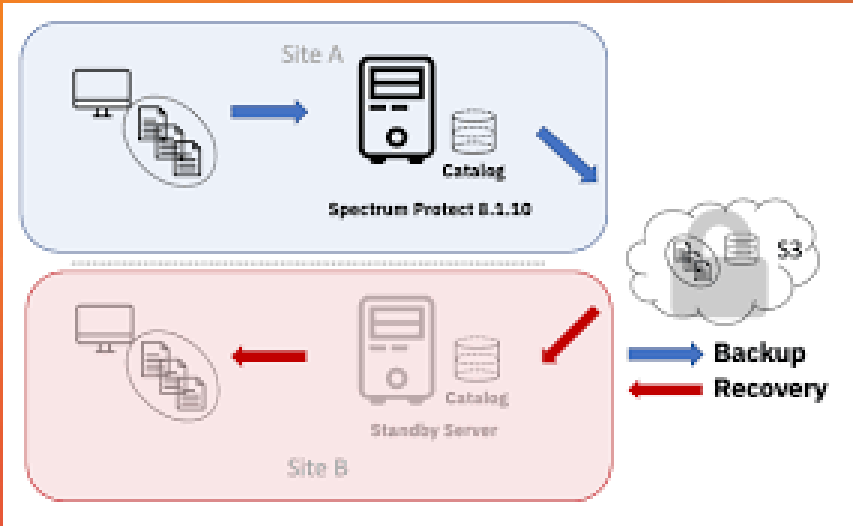


# S3.PROCLOUD - platforma



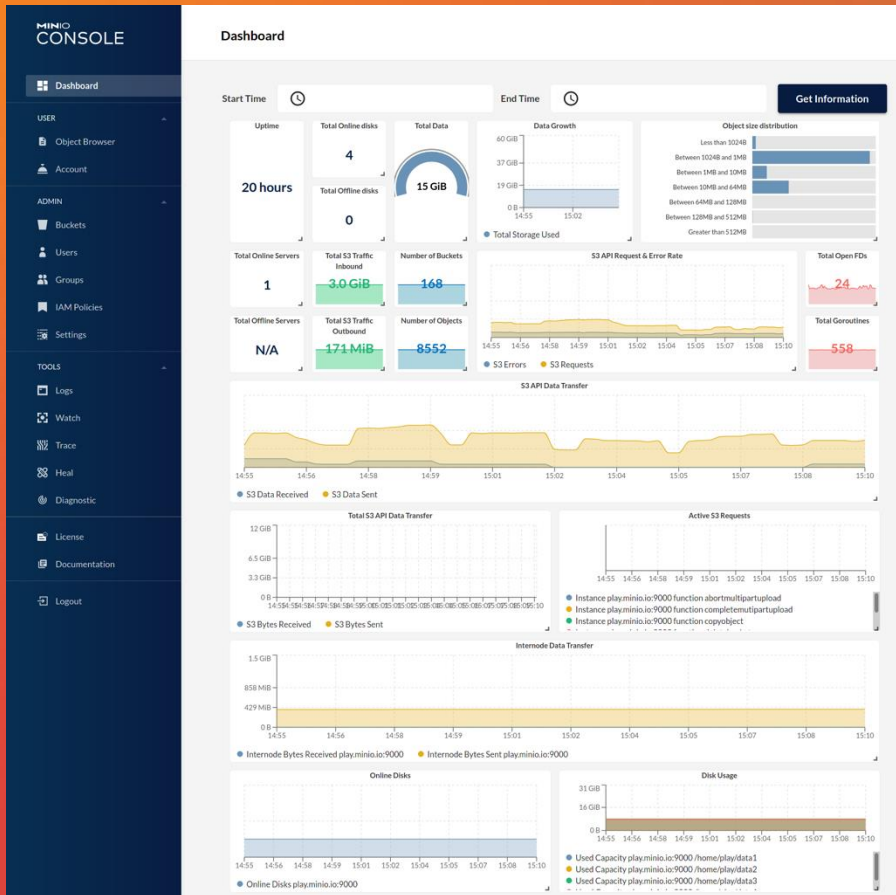
- Kubernetes/Openshift
  - MINIO Operator
  - DirectPV
  - Minio Console
- Erasure Coding – single site, 1 server loss/20 drives

# S3.PROCLOUD



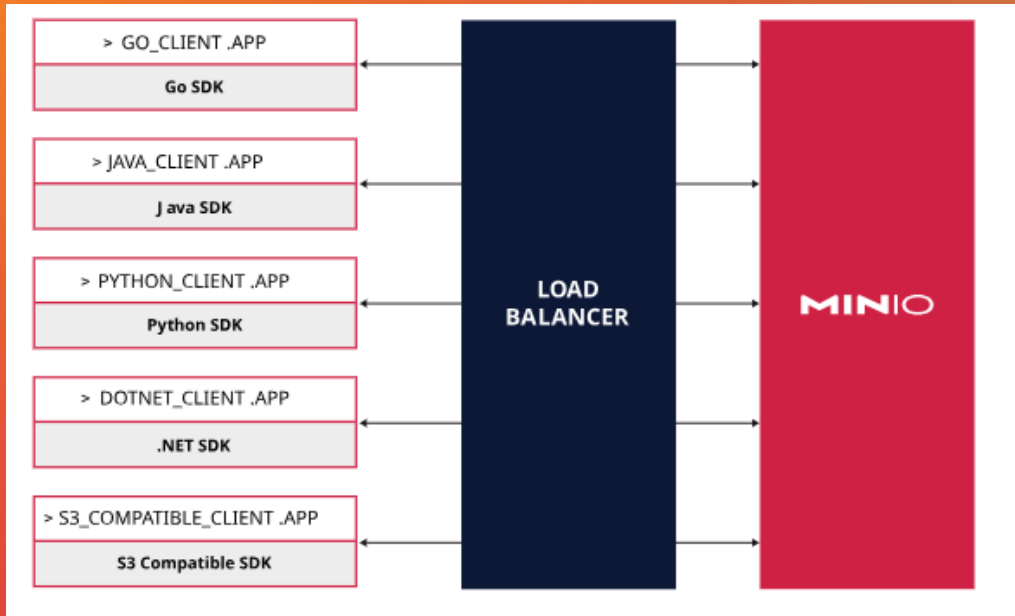
- Storitve v oblaku PROCLOUD
  - 2x DC – Ljubljana, Koper
  - MinIO porazdeljena postavitve, vsak DC svoj sistem
- Visoka razpoložljivost in odpornost na napake
  - ErasureCoding – porazdeljena postavitve
  - Zrcaljenje sistemov oz. bucketov med datacentroma
  - Primerna rešitev za uporabnike, ki zahtevajo geo zaščito pred izgubo podatkov
- Združljivost s programsko opremo
  - Veeam
  - Storage Protect
  - CommVault
  - NetBackup

# S3.PROCLOUD



- Možnost enkripcije podatkov (at-rest)
- Capacity tier
  - Primeren za dolgoročno hranjenje podatkov
  - Immutable repository za varnostne kopije (2. ali 3. kopija)
- Velike kapacitete – PB+
- Za poslovne uporabnike
  - Dodeljen S3 strežnik – instanca, fiksna kapaciteta
  - Upravljanje sistema (ILM, kapacitete, bucket)
  - Immutable
  - ILM, zrcaljenje
  - Dostop preko interneta ali VPN

# S3.PROCLOUD



- SOHO
  - Dodeljen bucket
  - Self service (faza 2)
  - Quota
  - Dostop preko interneta
- StartUP – kubernetes, openshift
- EDGE – on-prem uporabnik
  - Možnost postavitve pri uporabniku (Lenovo server, disk, mreža, VPN)
  - S3.PROCLOUD – target za zrcaljenje (DR), tiering

S3 „for dummies“  
S3.Procdoud  
S3 on-prem (edge)

# Q/A

Roglit is more than just another conference.



# Hvala!

Roglit is more than just another conference.