VOTING-Services

Data Protection (en)

Author	Abraxas Informatik AG
Classification	public
Version	0.91
Date	21. Aug 2022

For digital Switzerland. For Sure.

abraxas

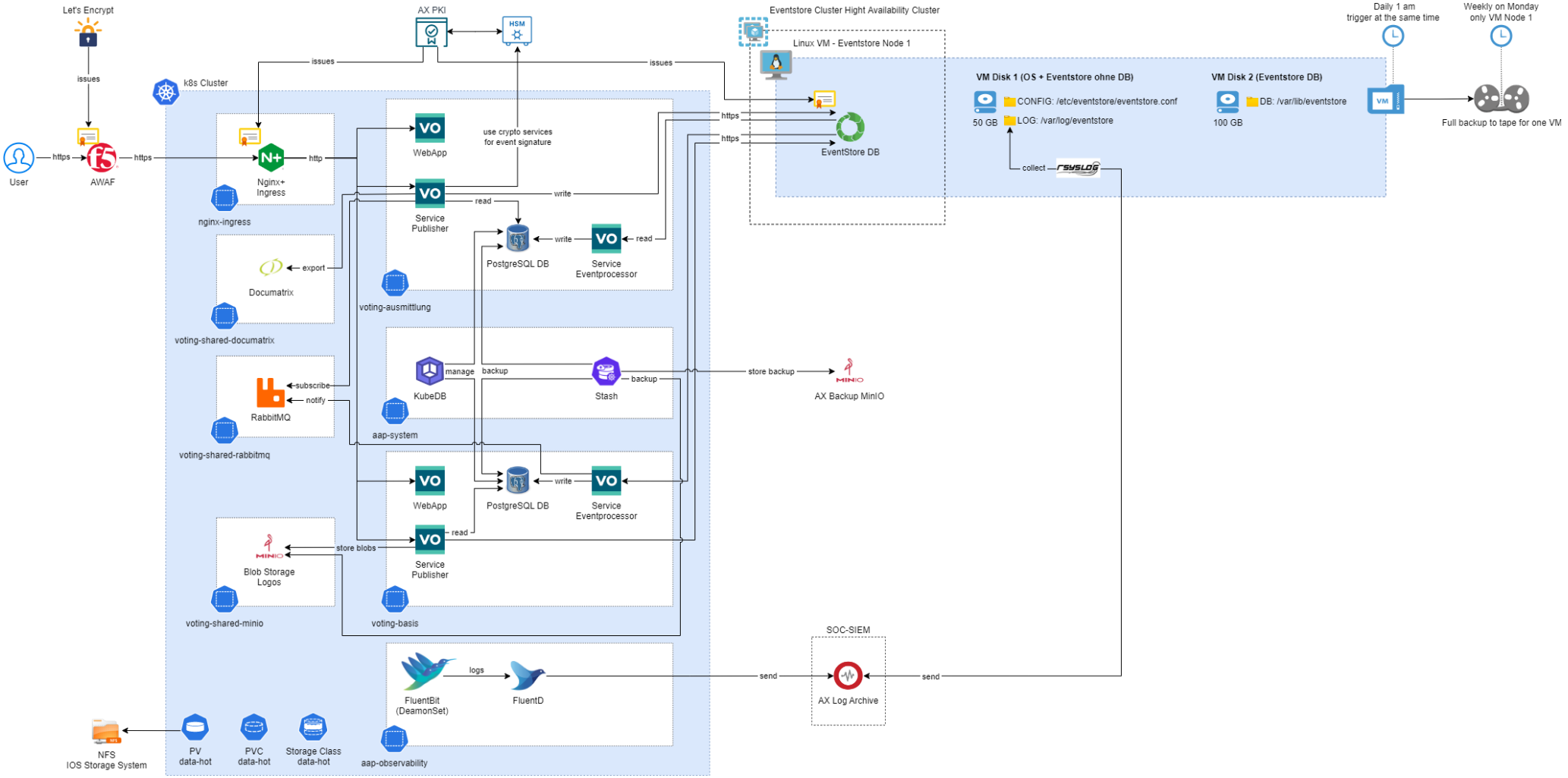
Table of contents

1. Overview

This chapter covers how data protection is covered across our VOTING services:

- VOTING Basis
- VOTING Ausmittlung

The following diagram illustrates communication ways and where data is stored and backed up:


Let's Encrypt
issues
AX PKI
HSM
issues
issues
Eventstore Cluster Hight Availability Cluster
Linux VM - Eventstore Node 1
Daily 1 am
trigger at the same time
Weekly on Monday
only VM Node 1
k8s Cluster
VM Disk 1 (OS + Eventstore ohne DB)
VM Disk 2 (Eventstore DB)
CONFIG: /etc/eventstore/eventstore.conf
LOG: /var/log/eventstore
DB: /var/lib/eventstore
50 GB
100 GB
Full backup to tape for one VM
User
https
AWAF
https
Nginx+
Ingress
http
WebApp
use crypto services
for event signature
https
https
EventStore DB
nginx-ingress
Service
Publisher
read
write
collect
rsyslog
write
read
PostgreSQL DB
Service
Eventprocessor
export
Documatrix
voting-ausmittlung
voting-shared-documatrix
manage
backup
backup
store backup
KubeDB
Stash
AX Backup MinIO
subscribe
notify
RabbitMQ
aap-system
voting-shared-rabbitmq
WebApp
write
PostgreSQL DB
Service
Eventprocessor
read
store blobs
Service
Publisher
Blob Storage
Logos
voting-shared-minio
voting-basis
SOC-SIEM
logs
send
send
FluentBit
(DeamonSet)
FluentD
AX Log Archive
NFS
IOS Storage System
PV
data-hot
PVC
data-hot
Storage Class
data-hot
aap-observability

2. Reliability

To ensure data reliability the following measures are taken.

2.1 Event Signature

Within the event sourcing architecture there is an additional security layer implemented which signs all events with cryptographic methods to ensure data integrity. For more information see "VOTING-Ausmittlung_Event-Signature.pdf"

2.2 Data Encryption

The services use industry-accepted encryption products to protect data and communications during transmission between a client's network and the services, i.e. HSTS-Enforcement, Certificate-Pinning etc.

2.2.1 Data at rest

2.2.1.1 AAP - Kubernetes Cluster

Services that store data and run within the k8s cluster (i.e. PostgreSQL DB) are able to use one of the following storage classes to provision their persistent volume claim:

- data-hot
- logs

These classes are bound to a NFS provisioner which stores data on the Network File Share provided by the IOS Storage System. At the moment there is no encryption in place for data at rest on the NFS Share, but it is on the roadmap.

2.2.1.2 VMs - EventStore

Currently, there is no data at rest encryption for VMs/disks in use, but it is on the roadmap. VMware offers support for data at rest encryption, but therefore a key management server is required, which is not in place for the VOTING VMware infrastructure right now.

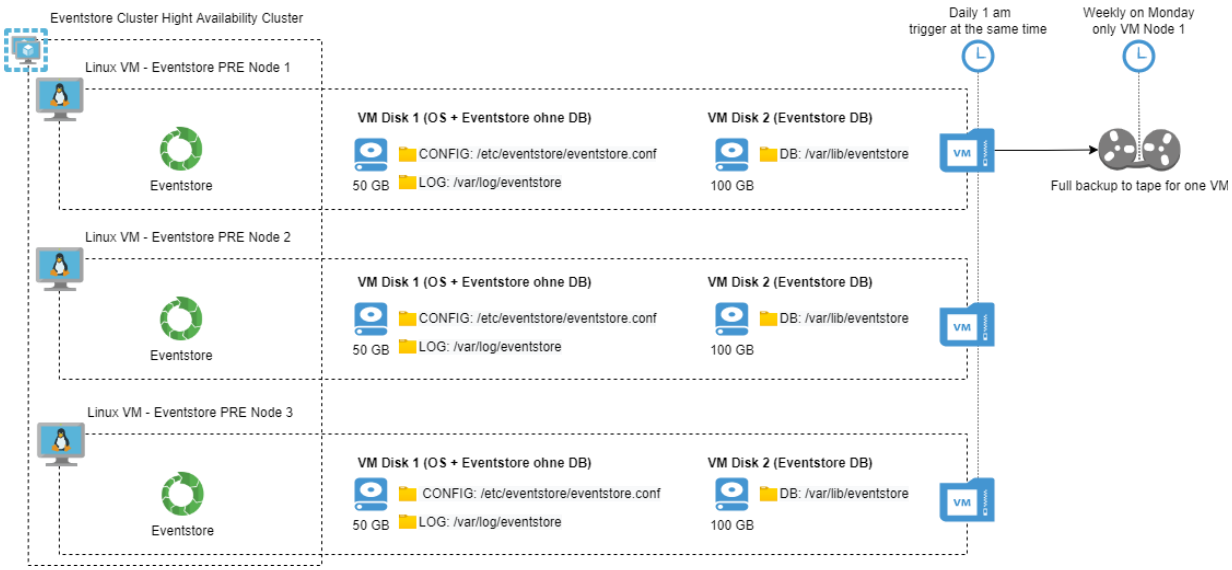
3. Backup

3.1 EventStore DB Backup

Since the VOTING EventStore DB infrastructure is virtualized on Linux rhel 8 VM's, the database is backed up with disk snapshots as recommended by EventStore backup and restore procedures.

The chosen backup service is "Premium - mirrored", which means it is geo-replicated in two Abraxas data centers.
Additionally every week one backup is getting outsourced to the Abraxas Tape Storage.

Eventstore Cluster Backup



3.1.1 Backup Scheduling and Retention

Since every appended event is persisted in EventStore DB every historical state can be replayed. Therefore the main purpose of the EventStore DB backup is for disaster recovery if the DB gets corrupted for some reason. That's why retention policies are set short as follows:

- Daily Backup at 1 am per VM including all disks, max age: 30 days
- Weekly tape backup on Monday

4. Logs

All applications log information to their respective system log facility or a centralised Log Archive server in order to enable security reviews and analysis.