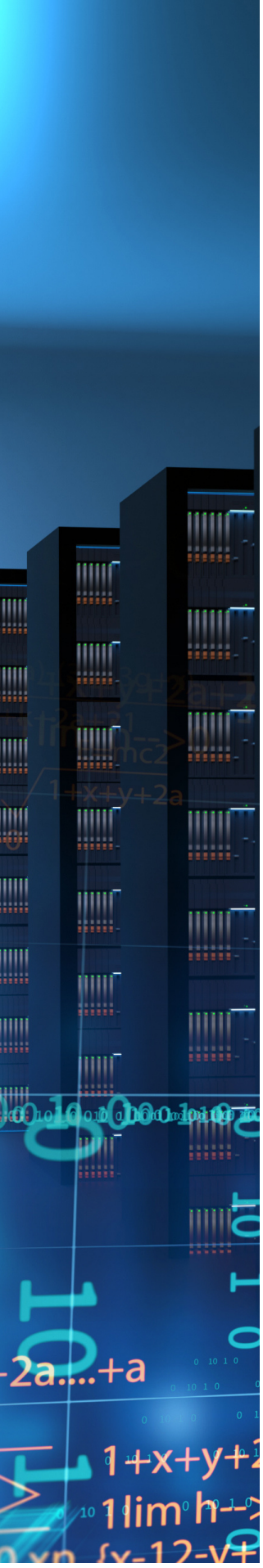
eTRUST

TECHNICKÉ ŘEŠENÍ

Zabezpečení aplikace pro komplexní správu majetku a svěřenských fondů

2021/1



OBECNĚ

- Aplikace eTrust běží na PHP 7.4,
- Je založena na framework Symfony 5, Doctrine 2 a databázi MySQL.
- Provozuje se v Docker containerech na Amazon ECS.

ZABEZPEČENÍ

- Do AWS účtu mají přístup pouze správci aplikace pomocí IAM uživatelů s dvoufázovým ověřením.
- Z vnějšku se do prostředí mohou dostat pouze správci přes AWS konzoli.
- Z veřejné IP adresy se lze dostat pouze na TCP porty 80 resp 443. Veškerý provoz je přesměrován na HTTPS protokol.

DOCKER

Všechny použité komponenty jsou pravidelně aktualizovány, testovány a poté probíhá deployment do produkčního prostředí.

- Alpine Linux image
- PHP-FPM engine
- NGINX webserver

AMAZON ELASTIC CONTAINER SERVICE (ECS)

Cluster tvořen virtuálními stroji ve více lokalitách. Jejich počet je automaticky navyšován v závislosti na požadavcích na výkon. Každá aplikace má vždy minimálně 2 spuštěné instance, na které je pomocí Elastic Load Balanceru (ELB) směřován provoz. Počet instancí je automaticky navyšován dle požadavků na výkon. Všechny stroje jsou ve Virtual Private Cloud (VPC) bez možnosti přístupu z venku. ELB používá AWS Certificate Manager pro přidělování SSL důvěryhodných cerifikátů

S3 STORAGE

Veškeré nahrávané dokumenty jsou ukládány do privátních bucketů v S3 storage. Každá aplikace má vlastního IAM uživatele pro přístup ke svým datům. Data jsou šifrována přímo v aplikaci 256bit šifrováním. Klíč je uložen v Key Management Service (KMS).

Data jsou tedy čitelná pouze IAM uživatelem konkrétní aplikace a pouze pomocí této konkrétní aplikace. Data jsou ukládána verzovaně a tím je zároveň zabezpečeno jejich zálohování.

RDS

Každá instance má přístup pouze do své databáze na Amazon Aurora MySQL RDS cluster. Databáze má repliku ve fyzicky jiné lokalitě. Záloha každý den s retencí 7 dní. Komunikace s databází probíhá šifrovaně pomocí SSL protokolu. K databázovému serveru se lze připojit pouze z VPC. Není tedy dostupný na veřejném IP adrese.

EXPORT DAT

Aplikace eTrust nabízí možnost exportů dat ze svých agend automaticky ve formátu Excel. V případě ukončení využívání aplikace eTrust je možnost exportu všech dokumentů do XML v ZIP archivu.