Disaster Recovery & HA

mgr inż. Jakub Woźniak

Zarządzanie Systemami Rozproszonymi
Instytut Informatyki
Politechnika Poznańska

Wprowadzenie

- Znaczenie bezpieczeństwa, wysokodostępności i Disaster Recovery
- Problemy: awarie, naruszenia bezpieczeństwa, utrata danych
- Powiązania: bezpieczeństwo wspiera HA, DR jako plan awaryjny

Bezpieczeństwo systemów rozproszonych

- Zabezpieczenie komunikacji: TLS/SSL, Mutual TLS (mTLS)
- Zarządzanie dostępem: OAuth2, OpenID Connect, RBAC
- Zarządzanie sekretami: HashiCorp Vault, Kubernetes Secrets
- Monitorowanie i reagowanie: Prometheus, Alert Manager

High Availability (HA)

- Minimalizacja przestojów, ciągłość działania aplikacji
- Load Balancing: HAProxy, NGINX, Traefik
- Failover: automatyczne przełączanie na zapasowe instancje
- Autoskalowanie: HPA, VPA w Kubernetes

Przykłady HA

- Replikacja danych: CockroachDB, Cassandra
- Architektura wieloklastrowa: dostępność w różnych regionach
- Wykorzystanie stref dostępności (AWS, GCP)

Disaster Recovery (DR)

- Minimalizacja strat danych i przestojów
- RTO (Recovery Time Objective) i RPO (Recovery Point Objective)
- Backup i archiwizacja: Velero, AWS Backup
- Replikacja geograficzna: Cloud Spanner, MongoDB Atlas

Testowanie Disaster Recovery

- Regularne testy odzyskiwania systemów
- Chaos Engineering: Chaos Monkey, LitmusChaos
- Przywracanie aplikacji Kubernetes za pomocą Velero

Przyszłość i najlepsze praktyki

- Wdrażanie AI do przewidywania awarii
- Wieloklastrowe i wielochmurowe rozwiązania HA
- Automatyzacja procesów DR i bezpieczeństwa
- Minimalizacja punktów awarii (SPOF)

Podsumowanie i dyskusja

- Kluczowe punkty: bezpieczeństwo, HA i DR
- Dyskusja: największe wyzwania w implementacji
- Znaczenie tych mechanizmów w środowiskach produkcyjnych