

SKALABILNA WEB RJEŠENJA

**Regulatorna reforma u Vijetnamu
na eZ Publish CMS-u... i Linuxu**

Dinko Korunić (InfoMAR)

Još jedan CMS...

- sadržaj:
 - 75 GB statičkog sadržaja (dominantan!): dokumenti (dosjei) i višerazinski međuspremnici samog CMS-a,
 - 3 milijuna datoteka, 1 milijun direktorija
 - 300 tisuća objekata u samom CMS-u
- tipični zahtjevi:
 - visoka redundancija (hardverska i aplikativna)
 - centralizirani spremnik sadržaja
 - otpornost na DoS napade, ispade poslužitelja, itd.
 - nadogradnja/servisiranje poslužitelja bez utjecaja na ostatak sustava (frontend, backend, itd.)
 - konkurentna finalna cijena (hardver, postavljanje, održavanje, edukacija)
 - lako horizontalno skaliranje i proširenje kapaciteta

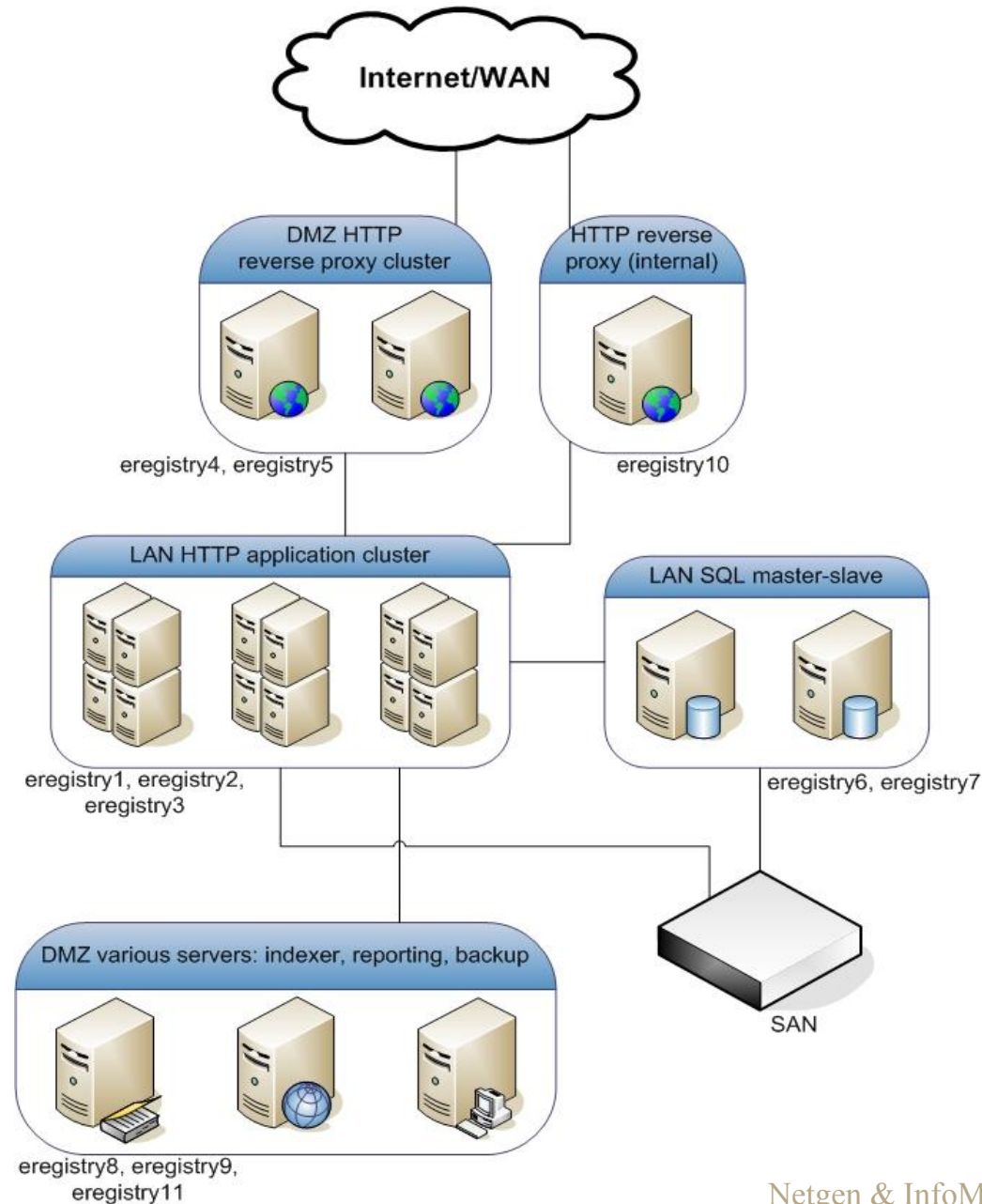
Sistemska implementacija

- Linux za "krojeno" rješenje
- HTTP reverse proxy-cachevi (Varnish):
 - uobičajeni DNS RR + HA IP klaster: automatska migracija IP adresa, međusobni nadzor, nadzor nadležnog usmjernika
 - load-balanceri: slučajna raspodjela prema backendovima + kontinuirana provjera stanja backend poslužitelja
 - integrirani lokalni međuspremnicima serviranog sadržaja
 - anti-DoS mogućnosti
- iSCSI (Open-iSCSI) prema centralnom SAN-u:
 - IBM DS3300 kao entry-level SAN iSCSI model
 - iSCSI + multipathing + OCFS2 (Web) / Ext3 (SQL)
 - očekivano 500-600 IOPS

Sistemska implementacija (2)

- Web aplikacijski poslužitelji:
 - cluster-aware datotečni sustav kroz postojeću infrastrukturu (iSCSI vs. FC)
 - OCFS2 za zajednički Web pool – samostalno rješenje bez dodatnih klaster-servisa
 - rezultat – međusobno nezavisni! (servisiranje, nadogradnje)
 - lako proširenje s novim poslužiteljima (online)
- SQL poslužitelji:
 - lako mijenjanje uloga
 - Ext3 zadovoljava performanse
 - ne pretjerano jednostavno proširenje, ali nije usko grlo
 - budućnost: multimaster, SQL proxy, IPVS, itd.

Sistemska implementacija (3)



Sigurnost, nadzor, redundancija

- nadzor i alerting:
 - sigurnosni pregled (zaštitne sume, logovi): OSSEC HIDS
 - kontinuitet rada servisa: Monit
 - centralni nadzor: ZenOSS (SNMP, sistemsko i aplikativno nadziranje, reporting, praćenje performansi, ...)
 - praćenje autentikacije: Fail2Ban
- redundancija:
 - 2x iSCSI portovi na poslužiteljima (multipath)
 - 2x LAN portovi na poslužiteljima (bonding)
 - 2x mrežni preklopnici u klaster načinu
 - 4x iSCSI portovi na SAN (multipath, 2x kontroler)
 - 2x mgmt portovi na SAN
 - te uobičajeno (2x PSU, LightPath dijagnostika, itd...)

Iskustva

- loša iskustva:
 - lokalni IT i njihovo "znanje" + vremenska razlika
 - sve je potrebno raditi udaljeno (šahovska igra...)
 - obavezno imati punu "remote konzolu" (DRAC/iLO/RSA/..., IP KVM)
 - proprietary QLA HBA driveri i non-RHEL kerneli
 - nestabilni "enterprise" datotečni sustavi GFS, GFS2
 - nestabilni RHCS u Debian Lennyju
- dobra iskustva:
 - nadzor: Monit, ZenOSS!
 - spremišta: OCFS2, Open-iSCSI
 - akceleracija: Varnish, APC
 - sigurnost: Suhosin, OSSEC HIDS

Kraj!

- pitanja, komentari, sugestije, diskusija?
- kontakt:
 - Vjeran Vlahović <vjeran@netgen.hr>
 - Dinko Korunić <dinko.korunic@infomar.hr>