Testovací infrastruktura v CZ.NIC

pohledem admina

Jan Hroten • 12.10.2024

CZ.NIC | SPRÁVCE DOMÉNY CZ

Co cheme od Testovacího prostředí

- *Umožnit spouštět a vyvíjet testy (duh..)*
- *Bezpečnost*
- *Stabilita*
- *Výkon*
- *Spravovatelnost*
  - *Kolik času + energie stojí údržba a provoz prostředí*
  - *Nejen adminy, ale i SQA, vývojáře, ...*

Typy testů

- *„Vývojové testování“*
- *„Adminské testování“*
- *„Testování pro veřejnost“*

Typy testů

- *„Vývojové testování“*
  - *Data anonymizovaná, (ne)pravidelně přepisovaná*
- *„Adminské testování“*
  - *Data produkční*
- *„Testování pro veřejnost“*
  - *Data perszistentní, zálohovaná, specifické pro toto použití*

Typy testů

- *„Vývojové testování“*
  - *Data anonymizovaná, (ne)pravidelně přepisovaná*
  - *Verze bleeding edge, často několik updatů denně*
- *„Adminské testování“*
  - *Data produkční*
  - *Verze shodné s produckí, update jen předmět testování*
- *„Testování pro veřejnost“*
  - *Data perszistentní, zálohovaná, specifická pro toto použití*
  - *Verze shodné s produkcí, navíc případné preview*

Typy testů

- *„Vývojové testování“*
  - *Data anonymizovaná, (ne)pravidelně přepisovaná*
  - *Verze bleeding edge, často několik updatů denně*
  - *Plná izolace, co se stane v Testu, zůstane v Testu*
- *„Adminské testování“*
  - *Data produkční*
  - *Verze shodné s produckí, update jen předmět testování*
  - *Plná izolace, přístup jen admini*
- *„Testování pro veřejnost“*
  - *Data perszistentní, zálohovaná, specifická pro toto použití*
  - *Verze shodné s produkcí, navíc případné preview*
  - *Veřejně dostupné, izolace od zbytku infrastruktury*

Admintest™

- *2 prostředí, 1 hypervizor, funkční UCarp/Keepalived*
- *1:1 kopie produkce – secrety, konfigurace, data, verze*
- *Síťová izolace na úrovni firewallu (DNAT/SNAT), černá magie*
- *Velmi „drahé“ na údržbu – technický dluh a spousta drobných odlišností*
- *V průběhu tohoto roku finálně opuštěno a zrušeno*

Regtest™

- *1 prostředí, 1 hypervizor*
- *Výrazně odlišné – vlastní data, secrety, neobsahuje vše co produkce*
- *Síť na veřejných adresách, oddělená adresace + DNS*
- *Bohužel používáno i pro testování specifických scénářů ze strany SQA*
  - *Mobily, 2FA, aplikace s přístupem mimo naší síť*
  - *Cílem je toto postupně eliminovat a zachovat pouze veřejnou funkci*
- *Stát ve státě*

TestEnv™

- *3 nezávislá prostředí, X hypervizorů*
- *Extrémně vytížené, často víc relasů v jednom prostředí*
- *Releasy jsou naprostá anarchie. =)*
- *1:1 kopie produkce, mimo secretů – alespoň v ideálním světě*
- *Dlouhodobě „drahé“ – komplexnost prostředí a časté releasy*
- *Ještě se k němu dostaneme*

Nástroje

- *Monitoring sdílený se zbytkem infrastruktury*
- *Vlastní NMS, mailserver, Sentry, Jenkins*
- *DBA, MojeWC, Moo-farma, Datel*
- *Desktop*
  - *X2GO + ssh*
  - *Spouštění testů a zároveň vývojové prostředí*
  - *Nevyhovující – zdroje, malá izolace uživatelů*
- *VirtualBox image + VPN*
  - *Postupná adopce, odchytávání much*
  - *Zatím (snad) pozitivně přijato*

(Nejen) technický dluh

- *Všechny prostředí navrhli a implementovali lidi chytřejší než já*
- *Až na výjimky bohužel už v CZ.NIC nepracují*
  - *Ztráta know-how*
- *HW vždy vyřazený z produkce*
  - *nejen slabý, ale i nekonzistentní*
- *V poslendí době ale do testovacích prostředí investujeme*
- *GO TestEnvů, nový HW, reinstalace*
- *...a velké plány =)*

TestEnv™

Základní myšlenka: izolovaná veřejná adresace serverů

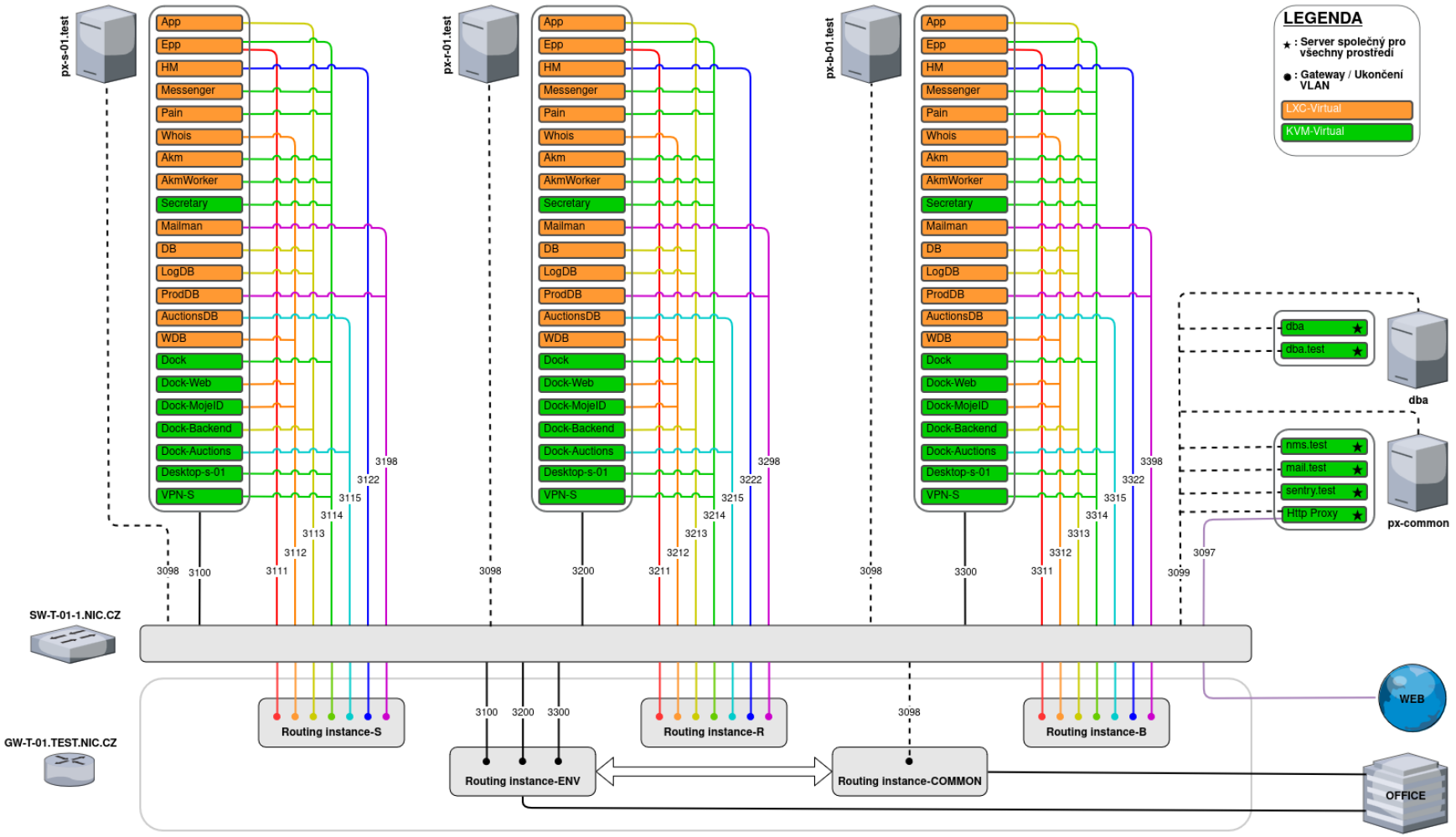
- *Kařdý server má totožnou síťovou konfiguraci jako v produkci*
- *+ 1 interface na soukromé adrese pro správu a přístup z interních sítí*
- *Všechna aplikační komunikace po veřejných adresách – jako v produkci*
- *..ale vše se drží uvnitř prostředí*
- *Produkční DNS (!)*
- *Všechna magie je na routeru na hranici prostředí*
  - *servery jsou „oklamány“*
- *Hlavní výhoda – konfigurace a deployment shodný s produkcí*

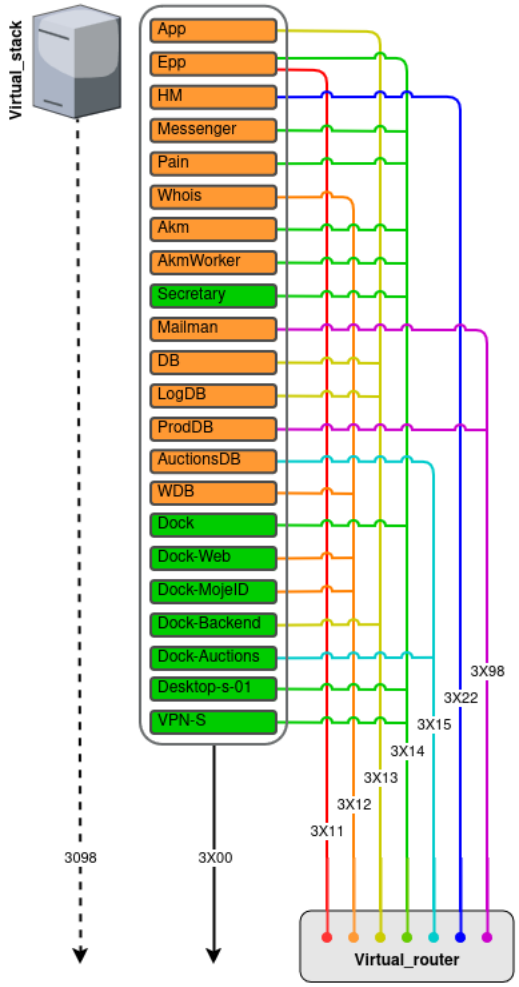
TestEnv™

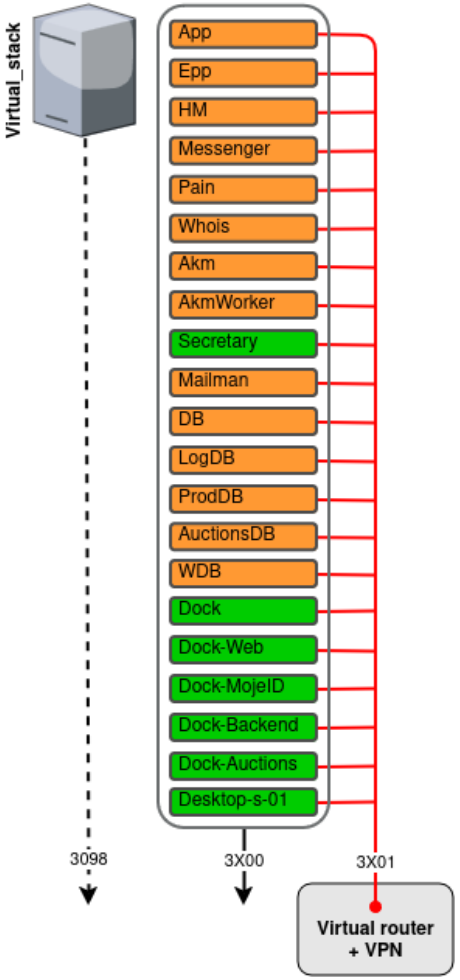
- *Problémy:*
  - *Izolace a nutnost jí porušit (platební brány, embedding...)*
  - *Zdroje uvnitř i vně testu ve stejném subnetu*
  - *Přístup do testu po soukromé adrese a komunikace dovnitř testu po „veřejné“*
  - *Sdílené zdroje mezi testy*
  - *Nutnost asistence s releasy - docker, samoobslužný deployment*
- *Hotfixovaná síť (pinger), VirtualBox*
  - *Ladíme dětské nemoci*

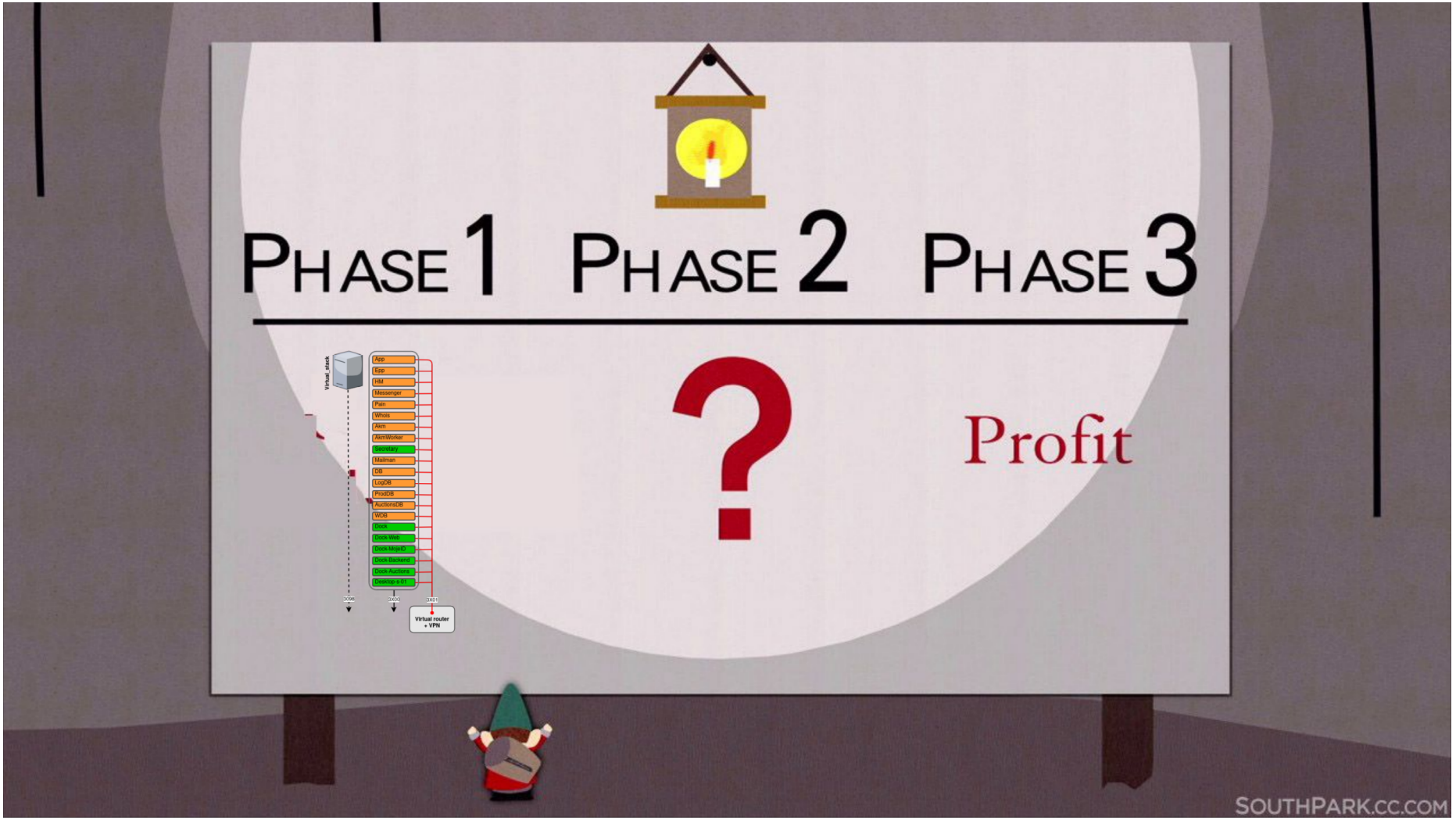
Shrnutí

- ***Relativně** robustní a zavedená infrastruktura*
- *Hodně místa ke zlepšní, málo času =)*
- *Všechna prostředí jsou virtualizovaná a sjednocená na Proxmoxu…*
- *...ale persistentní – s časem se zvyšuje „cena“ správy*
- *Proč to nezkusit jinak – TestEnv™ 2.0 NG Turbo!*
  - *V rámce reinstalace na nový HW*
  - *Výměna HW routeru za virtualizovaný linuxový box*
  - *Ve spolupráci s net-admins jsme zcela zrevidovali síť VLANy, adresace, FW…*
  - *???*
  - *PROFIT!*








PHASE 1
PHASE 2
PHASE 3
?
Profit
Virtual_stack
App
Epp
HM
Messenger
Pain
Whois
Akm
AkmWorker
Mailman
Dig
LogDB
ProdDB
AuctionsDB
WDB
Dock
Dock-Web
Dock-MojeID
Dock-Backend
Dock-Auctions
Desktop s-01
3006
3000
3001
Virtual router
+ VPN
SOUTHPARK.CC.COM

Děkuji vám za pozornost!

Jan Hroten

CZ.NIC | SPRÁVCE DOMÉNY CZ