

Klíčové služby DNS, DHCP, IPAM na rozcestí

Dnes 0:00

V dnešní době je každá firma závislá na správné funkci „core“ síťových služeb jako například DNS, DHCP, TFTP, NTP. Bez jejich správné funkce aplikace nefungují, nefunguje ani autentizace pomocí Kerberos protokolu, a faktický dopad na infrastrukturu je téměř totožný s fyzickým výpadkem sítě.

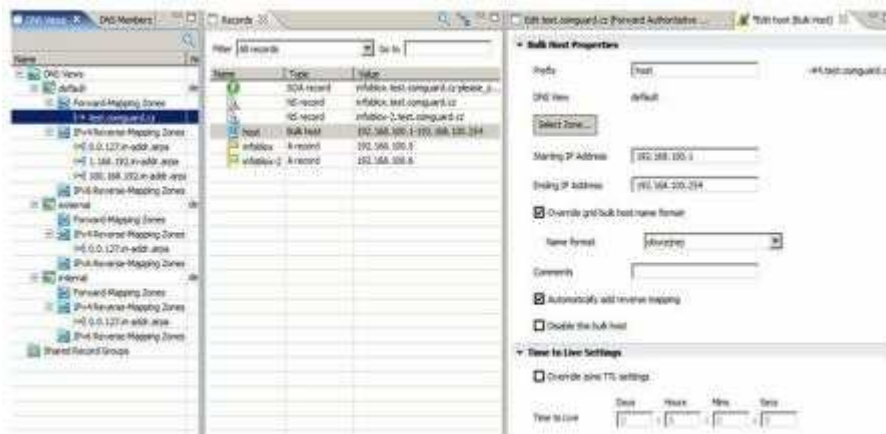
Toto je komerční sdělení. Server Lupa.cz není jeho autorem a neodpovídá za jeho obsah.

Obvykle jsou dnes uvnitř firem pro DNS a NTP používány MS AD servery, ale i ony jsou při startu závislé na fungujícím DNS. Navíc je celkem typický problém v nevyřešené vazbě mezi síťovými službami DHCP a DNS, a další obvyklý problém je vlastní management IP rozsahu a management jeho přidělování.

Typicky pak existuje několik navzájem nepropojených a nespolupracujících zdrojů. IP plány většinou ve formě tabulek v rukou managementu sítě, DHCP servery s obtížně dohledatelnými logy o přidělování IP adres jednotlivým počítačům, a MS Active Directory v rukou Microsoft administrátorů. K tomu chaosu ještě přispívají často povolené registrace do windows DNS záznamů koncovými stanicemi, což může vést ke snadnému zneužití v případě útoků, kdy by si například pracovní stanice zaregistrovaly názvy používané síťovými servery.

Rovněž v běžném MS prostředí není příliš vyřešen přístup k administraci DNS záznamů z pohledu omezení oprávnění na principu rolí, aby například správce pošty směl pouze manipulovat s A recordy pro poštovní servery a příslušnými MX záznamy bez možnosti poškodit ostatní záznamy ve stejné zóně, atp.

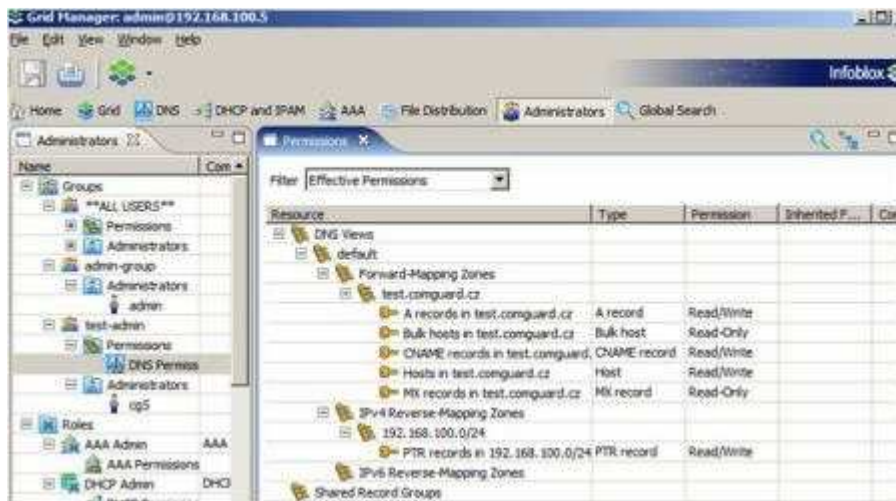
Obvykle se pak řeší přidělení nového síťového rozsahu pro novou pobočku mezi 3 až čtyřmi skupinami lidí, IP adresace a DHCP většinou lokálně na zařízeních na pobočce, DNS naopak centrálně se správci MS AD, a ostatní správci služeb (web, pošta atp) většinou posílají požadavky na rezervace IP adres, na přidělení DNS záznamů, a to vše se odehrává bez centrální dokumentace a mezi různými skupinami lidí.



[viz:

http://i.iinfo.cz/urs/Comg_obr_1-124695464549001.jpg]

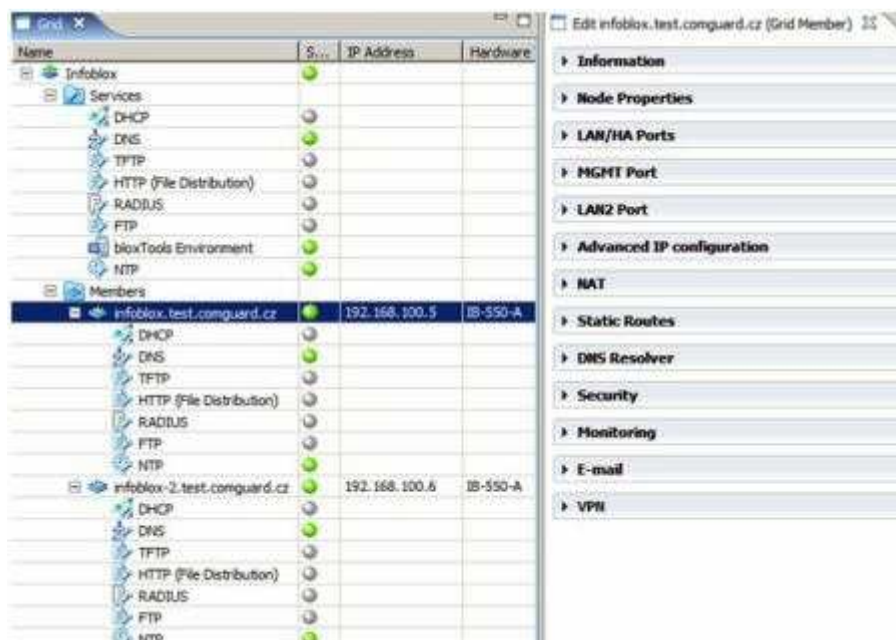
Poměrně unikátní řešení, které jsem měl příležitost testovat, nabízí společnost Infoblox. Jejich appliance představují ucelené centralizované řízení s možností velmi jemné definice práv a rolí administrátorů, kde v jedné centrální databázi jsou přehledně a provázaně uložena všechna data týkající se IP managementu, konfigurace DHCP, DNS, NTP, TFTP (pro bootování diskless zařízení například VOIP telefonů), HTTP (například pro uložení proxy autoconfiguration souborů). Pro ověřování administrátorů a uživatelů na INFOBLOX lze samozřejmě využít stávajících účtů v MS AD.



[viz:

http://i.iinfo.cz/urs/Comg_obr._2-124695472538535.jpg]

INFOBLOX následně umožňuje pomocí tzv. grid technologie zapojit jednotlivé výkonné boxy do grid sítě a na centrálním management serveru se již pouze nakonfiguruje, který z nodů má obsluhovat kterou část sítě, a jakou část informací mají mít klienti k dispozici (které domény, IP rozsahy via DNS, DNS view atp bude výkonný box propagovat pomocí služeb DNS, DHCP, TFTP, HTTP, RADIUS). Jako přídatek je podporováno NAC s využitím **802.1X** protokolu a RADIUS protokolu.

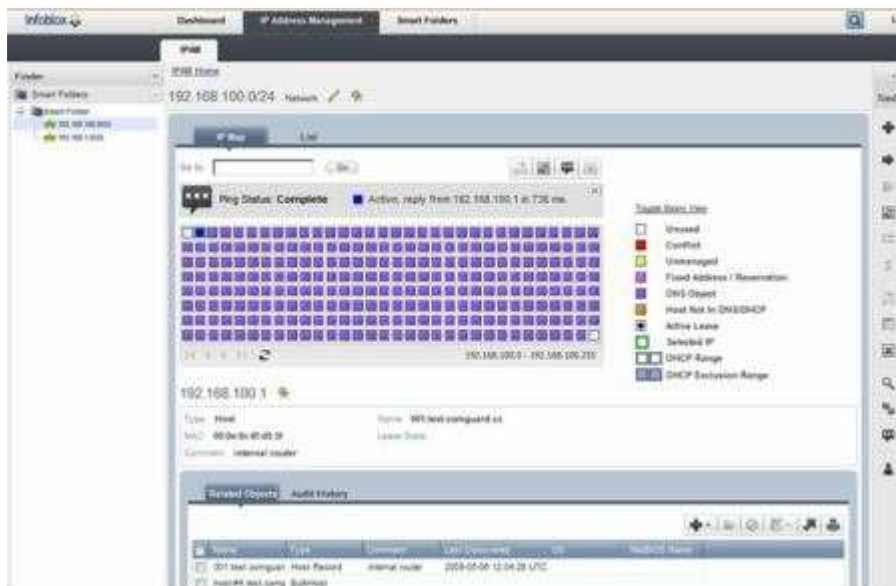


[viz:

http://i.iinfo.cz/urs/Comg_obr._3-124695486292326.jpg]

Samotná grid technologie je zajímavá tím, že se jednotlivé boxy v grid topologii jsou schopny při výpadku vzájemně zastoupit. Výpadek jednoho tedy nutně nezpůsobí nedostupnost služby v lokalitě. Pokud chcete nespolehat jen na dostupnost jiného nodu grid topologie INFOBLOXu, a chcete mít jistou funkci i v případě izolace kvůli selhání linkové nebo síťové vrstvy, lze konfigurovat i klasické high-availabilityy zapojení dvou boxů jako jednoho nodu gridu (VRRP).

Z pohledu funkce jednotlivých serverových služeb INFOBLOX samozřejmě žádným způsobem nezobrazuje a nepropaguje Vaše doprovodné údaje z centrální management databáze sloužící k účelům IPAM (IP address management), a naopak je schopný generovat přehledné reporty a dokumenty sloužící místo klasických, mnohde ručně vedených IP adresních plánů.



[viz:

http://i.iinfo.cz/urs/Comg_obr._4-124695497347769.jpg]

Z pohledu bezpečnosti je INFOBLOX vždy o krok napřed, můžete očekávat okamžitou podporu nových zabezpečení standardních síťových služeb (např. DNSSec), automatický bez-výpadkový patch management atp. Jeden z viceprezidentů společnosti INFOBLOX, Cricket Liu, je ostatně uznávanou autoritou v oblasti DNS a spoluautorem O'Reilly "DNS and Bind", "DNS on Windows NT", "DNS on Windows 2000", "DNS on Windows Server 2003" a "DNS&BIND Cookbook" a autorem "Managing Internet Information Services".



[viz:

http://i.iinfo.cz/urs/Comg_obr._5-124695508969646.jpg]

Samotný OS na kterém běží, samozřejmě dosahuje vysoké míry ochrany, a INFOBLOX jako takový se dodává buď jako ucelená řada appliance modelů (vlastní OS NIOS), nebo jako moduly buď do WAN akceleratorů Riverbed Steelhead, či dokonce jako Cisco moduly (ISR s AXP).

Z pohledu integrace do stávající infrastruktury je zajímavou možností využití IPAM web rozhraní aplikace, díky kterému lze pro helpdesk či administrátory serverů zveřejnit webové rozhraní, kde zadávají požadavky na přidělení IP, rezervace v DHCP, A či PTR DNS záznamů pro spravovanou část sítě. Tyto požadavky se pak řadí do fronty ke schválení příslušným administrátorům Infoblox zodpovědným za management příslušné části sítě, a ti je pak pouze schvalují, což jednak zabraňuje různým překlepům a omylům vzniklým během předávání informací a také značně zrychlí a zpřehlední IP management uvnitř organizace.

Zdeněk Havelka, Senior Consultant, COMGUARD a.s.