

DATASHEET

V moderní síťové architektuře jsou IP sítě a síťové aplikace stále více závislé na klíčových síťových službách (Core Network Services) jako DHCP, DNS, IP management a jejich vzájemné výměně informací. Právě vzájemná provázanost a komplikovanost těchto síťových prvků jako jsou NTP, ftp a tftp servery nebo např. VoIP zařízení způsobují, že stávající řídicí prostředky ActiveDirectory si s jejich komplexní správou nedokáží poradit a vystavují tak často společnost napospas nemalým finančním a časovým výdajům, nemluvě o ztrátě přehledu o dění uvnitř její životně důležité buňky.

Společnost Infoblox přichází z řešením, které jde v oblasti kontroly a automatizace síťových služeb hned dva kroky napřed. Nejen, že umožňuje oba tyto zásadní funkční procesy zpracovávat v rámci jediné konzoly, ale zároveň své služby poskytuje s garancí maximálního zabezpečení a minimální náchylnosti k chybám, a to díky provozu na výkonných appliancesch a použitému zabezpečenému operačnímu systému NIOS™, který se pomalu ale jistě stává novým standardem pro bezpečný provoz klíčových síťových služeb. Díky svým širokým možnostem nasazení, nabízené úrovni ochrany a značné flexibilitě si řešení Infoblox získává stabilní podporu širokého spektra zákazníků i odborných kapacit na soudobou síťovou problematiku.

Klíčové charakteristiky:

- ⇒ Komplexní řešení pro high-availability a central-management: poskytuje kritické síťové služby: **DNS/DNSSEC, DHCP, IPAM, NTP** aj.
- ⇒ Vestavěná podpora souvisejících protokolů **HTTP, FTP, TFTP, NTP VoIP**.
- ⇒ Disaster recovery: Zastupitelnost včetně centralního management serveru a databází v HA provozu při **nasazení Grid modu**.
- ⇒ **Vzájemná provázanost** DHCP a DNS s nadstavbovým centralizovaným IP managementem
- ⇒ **Role Based administrativní systém**
- ⇒ **DNS Firewall** – volitelný modul, který nabízí ochranu před DNS-based malwarem
- ⇒ **DNS Traffic control a loadbalancing**
- ⇒ **DHCP Fingerprinting** – poskytuje přehled všech zařízení připojených do podnikové sítě.
- ⇒ **Podpora virtualizace** řešení identifikuje i virtuální infrastrukturu a následně poskytuje jednotný pohled na fyzickou a virtuální infrastrukturu
- ⇒ **Podpora protokolu IPv6** – řešení dovoluje díky systému dual stack pracovat současně s IPv6 a IPv4

Přínosy:

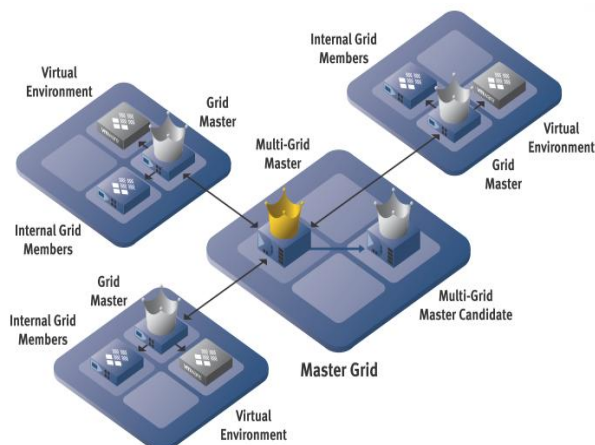
- ⇒ **Zřetelná úspora investic do vyhrazeného personálu:** minimalizuje personální náklady spojené s provozem kritických síťových služeb
- ⇒ **Maximální využití stávajících investic** díky integraci se službami Microsoft DNS a DHCP
- ⇒ **Vyloučení nebezpečí ztráty důležitých firemních informací:** díky vyspělým automatizačním procesům a konsolidaci služeb nedochází ke ztrátám informací, ke kterým tak často dochází kvůli decentralizovanému zálohování dat, servisním síťovým výpadkům či havarijním recovery procesům.
- ⇒ **Celkové zjednodušení síťové infrastruktury:** heslo „V jednoduchosti je síla“ platí v každém odvětví a v otázce síťových služeb dvojnásob. Nechte se překvapit. Vaši zaměstnanci vám poděkují!

s garancí maximálního zabezpečení a minimální náchylnosti k chybám, a to díky provozu na výkonných appliancesch a použitému zabezpečenému operačnímu systému NIOS™, který se pomalu ale jistě stává novým standardem pro bezpečný provoz klíčových síťových služeb. Díky svým širokým možnostem nasazení, nabízené úrovni ochrany a značné flexibilitě si řešení Infoblox získává stabilní podporu širokého spektra zákazníků i odborných kapacit na soudobou síťovou problematiku.

První DNS Firewall & centralizovaný IP management na jedné konzole!!



Infoblox Grid technologie: unikátní patentovaná technologie společnosti Infoblox propojuje jednotlivé prvky do jednotného centrálně řízeného celku. Distribuce dat následně probíhá v reálném čase do všech připojených appliances. Tato struktura zajišťuje do budoucna jednoduchý růst sítě.



DATASHEET

Přehled funkcí

DNS/DHCP služby – možnosti dnes již klasických DNS a DHCP služeb rozšiřuje Infoblox o nadstandardní jednoducho správu IP prostoru organizace, podporu vytvoření template pro Help Desk oddělení, auditní a reportovací nástroje. Nezávislé testy dokazují vyšší funkčnost a menší poruchovost služeb počínaje Active Directory, přes web aplikace, ERP až po IP telefonii.

DNS module – vytváří vrstvu dynamických ochran v závislosti na výsledcích analýz zranitelnosti konkrétní sítě a chrání před útoky na DNS servery. Navíc plně podporuje DNSSEC pro zajištění maximální úrovně bezpečnosti.

DNS Firewall – rozšiřující modul, který chrání proti tzv. DNS-based malwaru. Zamezuje klientům v přístupu k infikovaným stránkám, využívá komplexní a přesná data o malwaru k jeho detekci, eliminaci a blokování a umožňuje přesměrování NXDOMAIN.

DNS Traffic control a loadbalancing – integrovaná GSLB funkcionalita a autoritativní DNS server s vícero distribučními algoritmy

IP Address Management (IPAM) – vestavěný modul Infoblox IPAM poskytuje komplexní přehled o používaných IP adresách a plnohodnotné informace o jejich přidělování, čímž zajišťuje shodu s korporátními standardy, real-time controlling a celkovou transparentnost sítě. Navíc plně podporuje **propojení s technologiemi Microsoft DNS a DHCP**, čímž výrazně urychluje a usnadňuje práci administrátorů.

Havarijní recovery procesy bezpečně! – Recovery procesy jsou nákladné, ale nezbytné procedury údržby síťových služeb, které zároveň představují vysoké riziko ztráty důležitých informačních aktiv. Integrací řešení Infoblox v tzv. „Gridu“ lze minimalizovat nebezpečí i servisní výdaje stisknutím jediného tlačítka a zajistit tak kontinuitu kritických síťových služeb.

DHCP module – je úzce propojen s databází bloxSDB, která poskytuje DHCP služby s maximálním výkonem při dodržení standardů ISC DHCP. Navíc Infoblox implementuje DHCP failover, který zajistí nepřetržitý chod služby. Nedílnou součástí systému je **kontrola přístupu k síti** a zajišťuje tak účinné propojení centralizovaného access managementu se stávajícími metodami autentizace, síťovými a klientskými bezpečnostními zařízeními. Je nutno zmínit, že do modulu je plně integrována podpora DHCP pro IPv6.

DHCP Fingerprinting – jedná se o neinvazivní funkcionalitu, která zajišťuje přehled a kontrolu nad všemi zařízeními připojenými do sítě včetně BYOD. Rozpoznání typu zařízení je založeno na DHCP procesu, kdy nově připojené zařízení zašle požadavek na DHCP server o přidělení IP adresy. Tyto požadavky jsou zpracovány také DHCP Fingerprintingem, který tak pasivně získá informace o nově připojených zařízeních. Získané informace lze pak využít pro aplikaci korporátních politik na veškeré typy zařízení v síti pomocí automatických procesů.

Podpora pro VoIP služby – na speciálně vyvinuté platformě nedochází k tzv. „otevírání portů“ a je výrazně omezena HW napadnutelnost vznikající při provozování těchto služeb na univerzálních serverech. Příznačná je taktéž kvalita přenosu, kterou dokazují certifikace a doporučení předních světových výrobců VoIP stanic Cisco, Avaya, Siemens...aj.

Infoblox Network Insight appliance – integruje data z jednotlivých zařízení infrastruktury s managementem IP adres. Sběr a korelace těchto dat poskytuje administrátorům komplexní přehled o zařízeních v síti. Umožňuje tak snadno shromáždit potřebné informace, analyzovat je a přijmout vhodná opatření. Infoblox Network Insight pomáhá ke snížení bezpečnostních a servisních rizik výpadků, odhalení podvodných zařízení, identifikaci chyb, detekci nespravovaných zařízení a sítí a obnovení jejich správy. Je plně integrován do technologie Infoblox Grid Member. Infoblox nabízí Network Insight jako fyzickou nebo virtuální appliance.



Technologie Infoblox

Infoblox NIOS™ OS – je zabezpečený real-time operační systém s integrovanou databází a nativní podporou High Availability pro transparentní management kritických síťových služeb DNS, DHCP, IPAM, ... s podporou protokolů HTTP, FTP, TFTP, NTP a centralizovaného logování přes Syslog. Komunikační rozhraní BloxTools™ je založeno na technologiích Web 2.0 a šifrované komunikaci SSL a zajišťuje ochranu před zkompromitováním informací a integraci se všemi rozšířenými typy enterprise aplikací jako CRM, ERP a umožňuje naprogramování vlastních rozhraní přes toolkit SNAPins. Infoblox řešení jsou navíc schopna **importovat data** ze stávajících MS i Unix based řešení, a komunikovat s vašimi aplikacemi přes vlastní API.

Infoblox Grid Mode, disaster recovery – Slouží k propojení několika Infoblox serverů do unifikované a centrálně spravované platformy. Jeho základnu tvoří jednotná **databáze bloxSDB™ se schopností vlastní on-line reprodukce na všechny appliance** InfoBlox pro zajištění celistvosti a kontinuity datového oběhu. Grid Modul představuje revoluci v podobě real-time servisních datových updateů, možnosti automatické opětovné synchronizace síťových složek po rekonstrukcích LAN a WAN a ochraně informačních aktiv po dobu neplánovaných síťových výpadků. S pomocí Infoblox Grid manager lze ovládat NIOS software z libovolného PC s OS Windows nebo Linux.

| Model | Trinzic 815 (250-A) | Trinzic 825 (550-A) | Trinzic 1415 (1050-A) | Trinzic 1425 (1550-A) | Trinzic 2215 (1552-A) | Trinzic 2225 (1852-A) | Trinzic 4010 (2000-A) |
|-----------------------|---------------------|---------------------|---|---|---|---|---|
| Počet objektů | 33k | 110k | 440k | 880k | 1.2M | 3M | 10M |
| DNS dotazy/1 sek. | 6.000 | 22.500 | 45.000 | 75.000 | 90.000 | 200.000 | 200.000 |
| DHCP přiřazení/1 sek. | 90 | 150 | 300 | 450 | 550 | 900 | 1020 |
| HW redundance | ne | ne | Volitelně Redundant power supply (hot swap) | Volitelně Redundant power supply (hot swap) | Redundant power supply, fans, RAID10 (hot swap) | Redundant power supply, fans, RAID10 (hot swap) | Redundant power supply, fans, RAID10 (hot swap) |