

Význam monitoringu sítí

Ze zkušeností zákazníků víme, že mnozí z nich podceňují význam monitoringu. Tento fakt je to pochopitelný, protože to není ta nejdůležitější součást IT procesů. Jde spíše o doplněk, který je při současné optimalizaci stavu lidí něčím navíc.

Základem monitoringu je použití aktivních prvků s agentem, který monitorovacímu nástroji poskytuje informace. Pro získávání základní informace „žije/nežije“ stačí i ten nejjednodušší webagent. Odpovídá na ping (icmp echo). Pokud chceme automatizovaně získávat víc informací, takový prvek nám stačit nebude a potřebujeme agenta chytrějšího – podporujícího protokol SNMP.

Máme-li vhodné prvky, je dalším krokem zmapování topologie. Buď se přidružujeme dokumenta-

ce, které věříme, nebo objedeme areál a provedeme revizi. Další možností je použití vhodného softwarového nástroje.

Jakmile jsme si zmapovali topologii, zaneseme ji do monitorovacího nástroje a pustíme monitoring dostupnosti jednotlivých komponent. Samozřejmě lze použít i jednoduchý nástroj bez grafického podkladu – např. s tabulkovým výstupem. Pak nám ale chybí informace o vztazích mezi uzly, což komplikuje řešení problémů.

Inventarizace

Doplňkovými informacemi, které pomáhají při plánování rozvoje, jsou:

- jednorázové nebo průběžné monitorování prostředků sítě, jejich typů, sériových čísel,
- sledování a reportování stavu portů přepínačů ve vztahu k jejich použitelnosti (používaný, volný, zakázaný),
- sledování a reportování portů – co je na nich připojeno (jedno zařízení, více zařízení),
- sledování použitých IP adres v síti – máme přehled, které IP adresy jsou využívány (jde o problém vyskytující se v některých sítích, které přerůstají svůj původní návrh).

Pasivní bezpečnost

Informace čtené ze sítě mohou sloužit i jako doplněk informací souvisejících s bezpečností. V některých sítích se používají striktní pravidla pro připojení do sítě (např. ověřováním pomocí 802.1x, případně některým rozšířeným způsobem typu Cisco NAC, Microsoft NAP,...). Většina sítí je bez jakékoliv ochrany. Je užitečné minimálně sledovat výskyt MAC adres v síti. Lze tím získat minimálně tyto informace:

Přidaná hodnota

Přidanou hodnotou monitoringu je zejména:

- sledování chybovosti na portech,
- sledování zátěže na vybraných portech (zejména WAN, ale i LAN),
- sledování změn topologie,
- sledování vytížení CPU aktivních prvků.

Monitoring nás upozorní na potenciální problémy ještě dříve, než si uživatelé začnou stěžovat, nebo nám usnadní identifikaci problému.

- sledování množství MAC adres na portech je jedna z cest jak objevit access pointy načerno nainstalované zaměstnanci,
- sledováním seznamu MAC adres v síti a porovnáváním se seznamem autorizovaných MAC adres lze získat informaci o připojování nových zařízení do sítě.

Průběžná analýza datového provozu

V případě, že dochází k přetěžování linek (týká se to především WAN linek), je dobré vědět, jaký provoz přes ně prochází a kdo je největším konzumentem pásma.

Monitoring a správa aktivních prvků jsou příkladem služeb, které lze dát mimo firmu. V případě služeb Dohledového centra společnosti Infinity jde o službu poskytovanou s nepřetržitým monitorováním (7 x 24 x 365). Infinity používá software vlastního vývoje, což umožňuje pružně reagovat na nové požadavky zákazníků, resp. rychlé zavádění monitorovacích technik pro další produkty. Je tedy schopna reagovat na události kdykoliv a pomoci eliminovat problémy co nejrychleji. Na monitoring lze navázat i servis. ■

IP of switch	Port	Port description	Operational	Admin name	VLAN	Down reason	Type of Connected device	Last time of last change of	Known name of last change	Status of Connected device	Known name of last change	Port (only)
192.168.1.101	24	FastEthernet24/24	Up	192.168.1.101	10		192.168.1.101	2023-10-27 10:00:00	192.168.1.101	Up	192.168.1.101	24
192.168.1.102	24	FastEthernet24/24	Up	192.168.1.102	10		192.168.1.102	2023-10-27 10:00:00	192.168.1.102	Up	192.168.1.102	24

Data jednoho switchu

Prvek	Typ	IP	Operativní	Administrativní	Operativní	Administrativní	Operativní	Administrativní	Operativní	Administrativní	Operativní	Administrativní
192.168.1.101	Switch	192.168.1.101	Up	192.168.1.101	Up	192.168.1.101	Up	192.168.1.101	Up	192.168.1.101	Up	192.168.1.101
192.168.1.102	Switch	192.168.1.102	Up	192.168.1.102	Up	192.168.1.102	Up	192.168.1.102	Up	192.168.1.102	Up	192.168.1.102

Přehled prvků