POWERING IT AHEAD

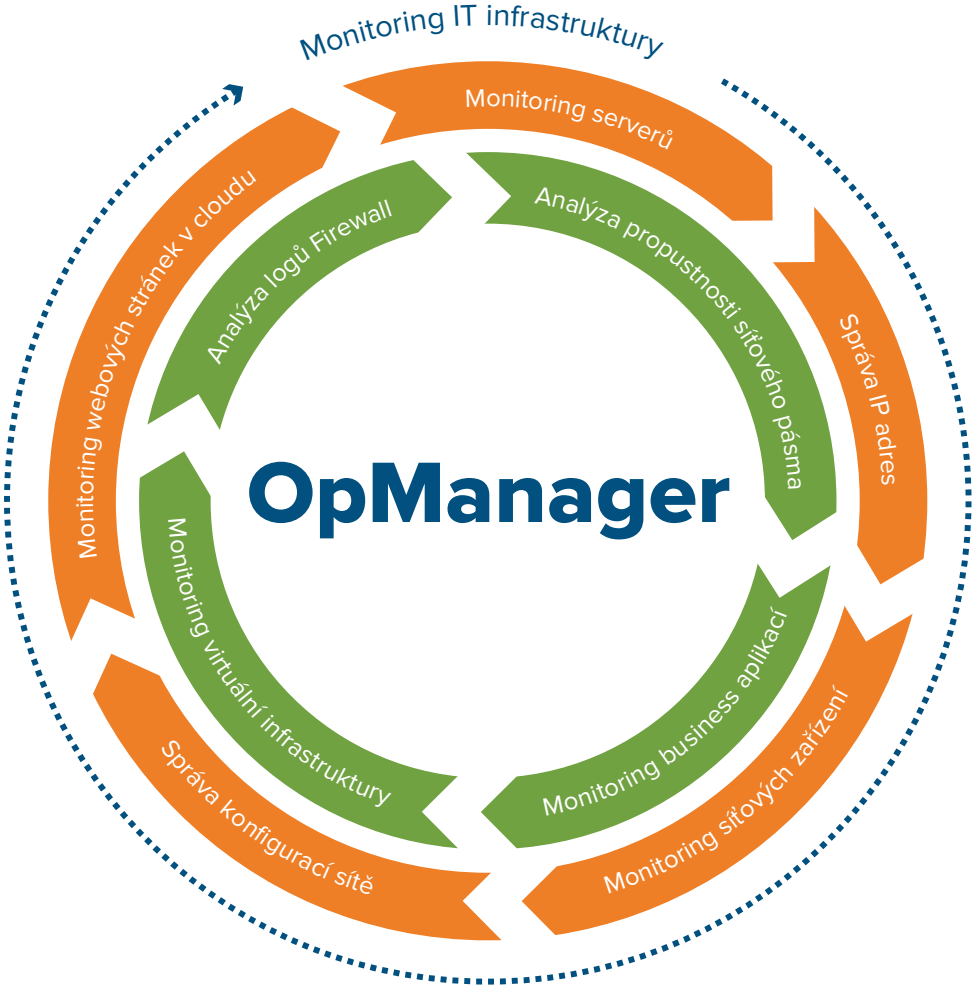
ManageEngine

+ Monitoring IT

Kdy jste naposledy zkontrolovali, zda má vaše auto skutečně tolik koní výkonu, kolik výrobci uvádějí v reklamách? Podívali jste se někdy pod kapotu a hrabali se v motoru? Jednoduše sešlápneme plyn a díváme se na budíky. Stejným způsobem většina organizací přistupuje k výkonu sítě - je OK, dokud funguje.

A co v případě závodních stájí? Žijí z testování a zvyšování výkonu motoru, je to tak? Měří každý takt motoru a věnují mnoho času a energie zvyšování otáček. Několik organizací, které znáte, má přesně stejný přístup ke své síťové infrastruktuře, protože je silně spojena s jejich hlavní podnikatelskou činností. Bez výkonné sítě nemohou obvykle provozovat svou činnost a málokdy je tato činnost spojena s IT.

Sekce ITOM této publikace je pro ty organizace, jež potřebují výkonnou a spolehlivou síťovou infrastrukturu, která je stále a účinně kontrolována.



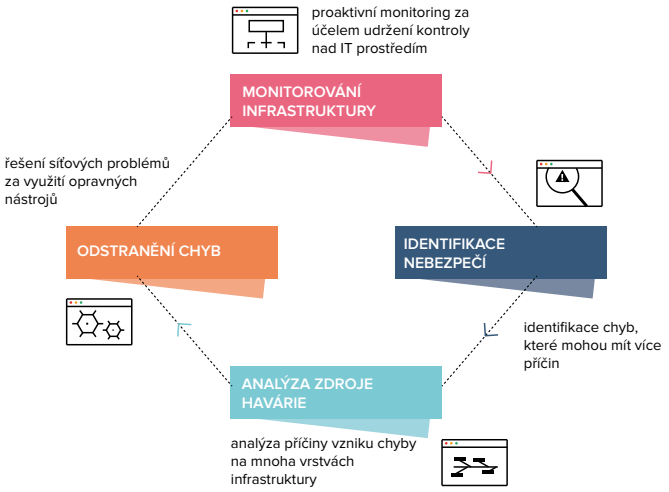
Komplexní správa a monitoring IT infrastruktury

OpManager

„Chtěli jsme řešení, které bude obsahovat všechny klíčové systémy obsluhy sítě a současně bude uživatelsky přívětivé."

Jarosław Leśniak
Oddělení správy sítě
Centrum informačních služeb ve Vratislavi

OpManager je kompletní systém pro správu síťové infrastruktury v organizaci.



Spojuje v sobě možnost monitorování síťových zařízení, serverů, aplikací, analýzy vytížení pásma a správu konfigurace sítě, IP adres a protokolu událostí. Vyspělý nástroj umožňuje správu celé sítě prostřednictvím jedné konzole. Díky monitorování celé IT oblasti v reálném čase je možné rychle reagovat na veškeré prostoje nebo chyby vyplývající z různých oblastí IT. Systém poskytuje vyspělé nástroje pro analýzu dat a tvorbu výkazů, díky kterým se mohou pracovníci IT racionálně a rychle rozhodovat v oblasti infrastruktury, za kterou jsou zodpovědní.

MONITORING DOSTUPNOSTI A VÝKONU
- Monitoring atributů síťových zařízení na základě SNMP, WMI, CLI
- Podpora pro Cisco IPSLA (monitoring VoIP a WAN RTT)

VYSPĚLÉ SYSTÉMY PRO GENEROVÁNÍ ALARMŮ A OZNÁMENÍ
- Oznámení emailem a SMS na základě překročení mezních hodnot
- Provádění automatických akcí v reakci na události

MONITORING VIRTUÁLNÍCH STROJŮ, KONTROLÉRŮ DOMÉNY, DATABÁZOVÝCH SYSTÉMŮ, ATD.
- Vyspělá, nastavitelná sada atributů monitoringu s možností úpravy mezních hodnot
- Jasný přehled hromadných náhledů a grafických prezentací

SPRÁVA KONFIGURACE SÍŤOVÝCH ZAŘÍZENÍ
- Roll-out konfigurace na vybraná zařízení
- Správa verzí, workflow (model potvrzování změn)

ANALÝZA VYTÍŽENÍ PÁSMA
- Náhled nejpopulárnějších aplikací v síti na základě technologie netflow
- Ověření politik QoS díky průzkumu markerů DSCP

SPRÁVA IP ADRES A MAPOVÁNÍ PORTŮ PŘEPÍNAČŮ
- Analýza vytížení rozsahu IP adres v segmentech sítě
- Ověření portů síťových přepínačů z hlediska připojených zařízení

MONITORING VÝKONU APLIKACE
- Monitoring aplikačních, databázových a webových serverů
- Tvorba skupin komponentů mapujících strukturu IT služeb

Monitoring a analýza IT komponentů v heterogenním prostředí

NEJDŮLEŽITĚJŠÍ VLASTNOSTI:
- Funkce RunBook Automation – automatizace procesů workflow
- Správa konfigurace síťových zařízení
- Analýza vytížení pásma
- Správa IP adres
- Automatická, pravidelná detekce sítě
- Automatická tvorba mapy sítě

- Přes 700 šablon zařízení
- Podpora 64bitových systémů
- Monitoring AD, MSSQL, MS Exchange
- Monitoring virtuálního prostředí (VMware, HyperV, Citrix)
- Vestavěné adresáře MIB pro nejpopulárnější zařízení SNMP
- Monitorování deníku systémových událostí
- Monitoring pomocí skriptů
- Monitorování procesů, disků, procesorů, pamětí
- Přes 100 přednastavených výkazů s možností nastavení harmonogramu a editace
- Monitorování služeb Windows
- Prohlížeč adresářů MIB
- Vyspělé systémy notifikace a automatizace operací
- Monitorování dostupnosti
- Monitoring URL
- Rozvinuté systémy obsluhy událostí s možností eskalace
- Nasazený REST API
- Monitoring VoIP a WAN s využitím Cisco IPSLA

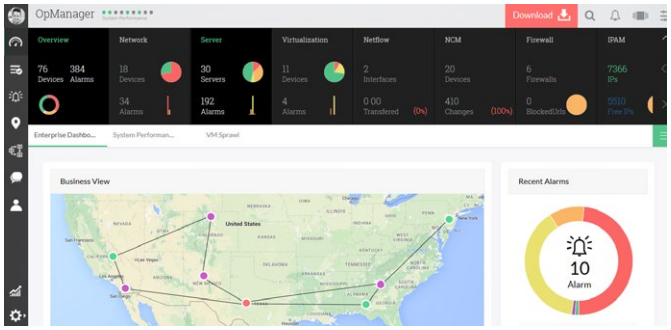
ESSENTIAL EDITION

- Obsluha až 1000 zařízení
- Monitoring síťových zařízení a serverů
- Upravitelné hromadné náhledy a CCTV
- Obsluha eventlog, syslog a protokolů SNMP
- Diagramy provozu v reálném čase
- Funkce automatizace workflow
- Obsluha IPSLA

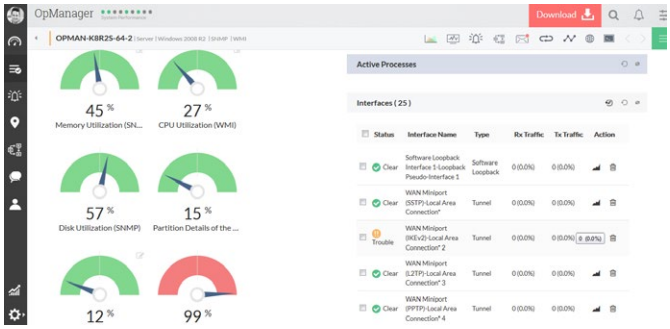
- Hromadný náhled pro SLA
- Monitoring virtuálního prostředí
- Analýza provozu v síti

ENTERPRISE EDITION

- Obsluha až 50.000 zařízení
- Pro organizace, které mají rozsáhlé prostředí a rozptýlenou strukturu
- Obsahuje všechny funkce verze Essential
- Rozšiřitelný: podpora pro monitoring až 5000 zařízení
- Architektura založená na proxy serverech
- Centrální konzole agregující údaje ze všech proxy serverů
- Podpora pro geograficky rozptýlené a rozsáhlé sítě
- Funkce Fail-Over (vysoká dostupnost) pro architekturu založenou na MSSQL



Základní náhled monitorovaného zařízení obsahuje několik prvků: výrobní štítek, na kterém se nacházejí informace o kategorii, výrobci, IP adrese, závislostech, přehled grafů, seznam monitorů, profilů oznámení a alarmů. Na této úrovni lze také provádět správu.

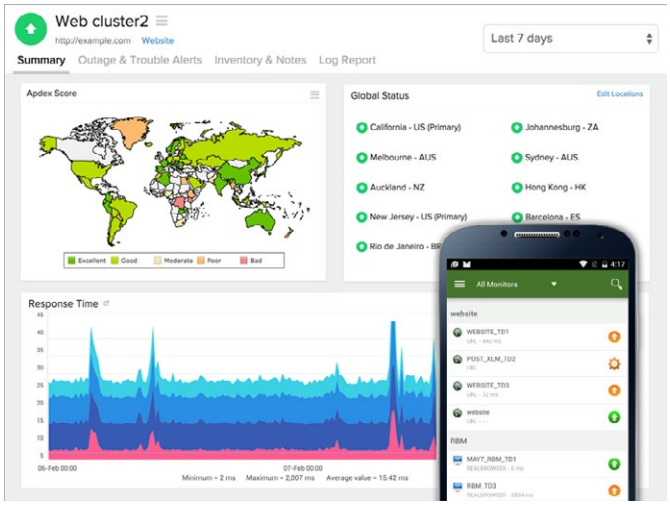


Ucelený náhled v systému OpManager umožňuje rychlé hodnocení stavu monitorované IT infrastruktury. Prezentované statistiky se týkají výkonu, dostupnosti zařízení a vygenerovaných výstrah podle kategorie. Přehled grafických prezentací znázorňuje využití zásob a jejich rozmístění v podniku.

Monitoring webových stránek a aplikací z globální perspektivy (Cloud)

Site24x7

Site24x7 je služba v cloudu (SaaS), která nabízí monitoring kritických webových aplikací, viditelných mimo organizaci, a vnitřních IT aktiv, jako servery nebo síťová zařízení (s využitím kolektoru v síti LAN). Umožňuje tvorbu analýz dostupnosti a výkonu kritických prvků webových aplikací z mnoha míst na světě, bez nutnosti otevírání portů, instalace agentů nebo rekonfigurace sítě.

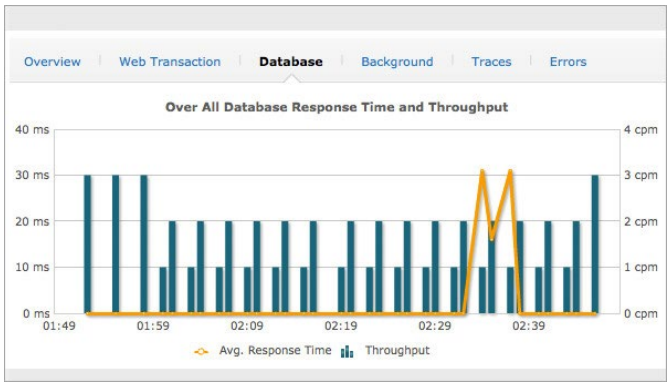


Pokud má být stránka viditelná mimo organizaci, pak ji nelze monitorovat standardním monitorovacím systémem, který funguje zevnitř sítě.

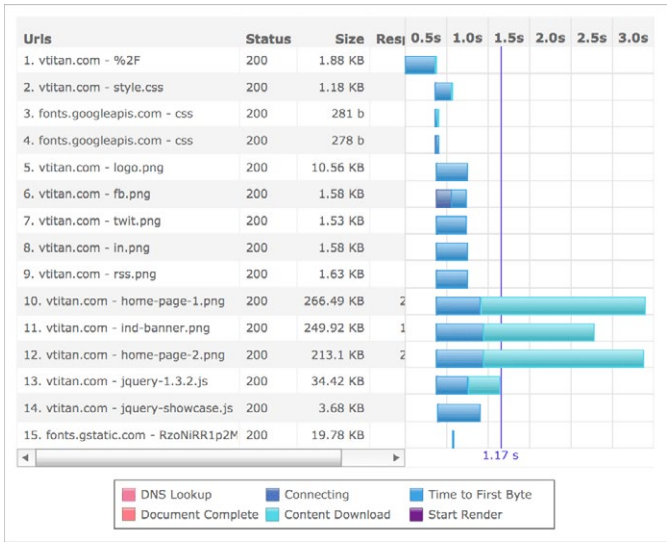
Site24x7 je ideální řešení pro monitorování dostupnosti a výkonu kritických podnikových aplikací, se zohledněním víceúrovňových webových transakcí. V případě vzniku problémů jsou odeslána automatická oznámení osobám, které jsou odpovědné za obsluhu aplikací. Díky tomu mohou tyto osoby velmi rychle reagovat. Monitoring webových aplikací poskytuje informace o jejich dostupnosti a výkonu.

NEJDŮLEŽITĚJŠÍ VLASTNOSTI:

- Monitoring dostupnosti a výkonu stránek
- Monitoring serverů a síťových zařízení
- Monitoring webových transakcí
- Monitoring webových aplikací
- Okamžité oznámení
- Monitoring serverů DNS
- Monitoring poštovních serverů
- Správa SLA
- Globální síť monitorovacích agentů



V případě vzniku problémů s webovými aplikacemi jsou odeslána automatická oznámení osobám, které jsou odpovědné za obsluhu aplikací. Díky tomu mohou tyto osoby velmi rychle reagovat. Monitoring webových aplikací poskytuje informace o jejich dostupnosti a výkonu.



V souladu se zprávou Gartnerů – přes 50 % návštěvníků WWW stránek rezignuje a odejde, pokud musí čekat na otevření stránky déle než 15 sekund. Díky Site24x7 získáte okamžitou informaci o sníženém výkonu stránky a můžete rychle zabránit ztrátě potencionálních zákazníků.

Integrovaný monitoring IT infrastruktury z pohledu poskytovaných služeb.
Analýza IT komponent orientovaná na poskytované služby.

Applications Manager

„Realizace idejí proaktivního přístupu ke správě informační infrastruktury má, v případě systému Applications Manager, relevantní výsledky v podobě eliminace značného množství hlášení uživatelů ohledně námi poskytovaných služeb IT."

Dominik Adamik
Obchodní ředitel
Avatia Sp. z o.o.

IT infrastruktura podniků se rozvíjí společně s rozvojem obchodu.

Proto je zajištění vysoké dostupnosti a výkonnosti kritických podnikových aplikací stále obtížnějším úkolem. Záležitosti výkonu aplikací již navíc nejsou spojeny pouze s technologií. Mají reálný vliv na obchod. Applications Manager pomáhá při monitorování výkonu a dostupnosti webových aplikací, serverů aplikací, databází, dedikovaných aplikací, systémů a služeb v komplexním podnikovém prostředí. Systém uceleně prezentuje IT infrastrukturu, umožňuje detekci problémů předtím, než ovlivní práci uživatelů, identifikuje zdroje událostí a umožňuje analýzu trendů vytížení infrastruktury pomocí hromadných výkazů.

ORIENTACE NA SERVISNÍ PŘÍSTUP K IT INFRASTRUKTUŘE
- Možnost třídění IT komponentů do skupin prezentujících služby
- Automatická tvorba relací mezi komponenty, odpovídajících stavům služeb

ŘEŠENÍ PROBLÉMŮ SOUVISEJÍCÍCH S PRACÍ PODNIKOVÝCH APLIKACÍ
- Analytické nástroje RootCause
- Systém generování alarmů, který podporuje proaktivní monitoring

GENEROVÁNÍ HROMADNÝCH VÝKAZŮ
- Výkazy pro personal management
- Přehledy z hlediska dostupnosti a výkonu jednotlivých služeb

SPRÁVA SLA
- Podpora pro základní ukazatele SLA
- Monitoring služeb z hlediska plnění podmínek SLA

SPRÁVA SLA
- Analýza funkce IT komponent na základě historických údajů
- Vyspělé metody porovnávání stavů

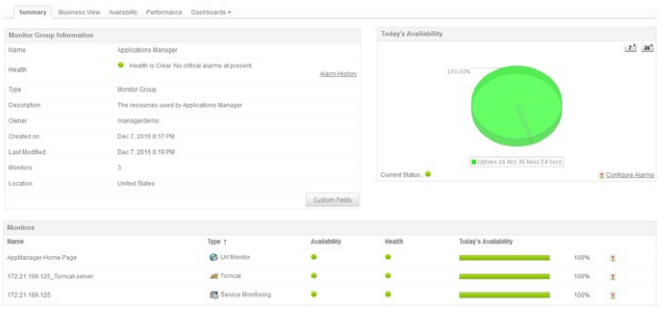
NEJDŮLEŽITĚJŠÍ VLASTNOSTI:
- Monitoring virtuálního prostředí
- Monitoring operačních systémů
- Monitoring služeb a procesů
- Monitoring serverů aplikací
- Monitoring portálů Middleware
- Testování zkušeností koncových uživatelů
- Rozšířený systém generování výkazů
- Monitoring systémů ERP
- Monitoring transakcí J2EE, .NET, Ruby-on-Rails
- Vyspělý systém alarmů a reakcí na události
- Monitoring databází
- Monitoring poštovních systémů
- Podpora proaktivního monitoringu
- Monitoring serverů a webových služeb
- Monitoring dedikovaných aplikací
- Správa SLA
- Monitoring webových aplikací
- Možnost definování vlastních, atypických monitorů
- Zjišťování anomálií
- Modul automatické detekce aplikací a závislostí (ADDM)

PROFESSIONAL EDITION

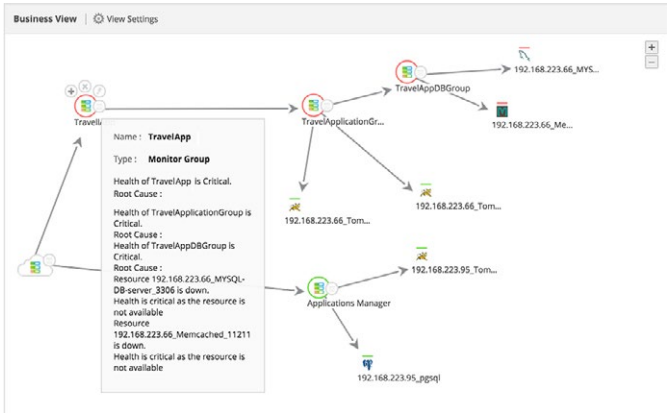
- Vhodná pro infrastrukturu do 250 monitorů
- Monitorování databází
- Monitorování serverů aplikací
- Správa smluv SLA
- Správa uživatelů (diferenciace oprávnění a rozsahu)
- Harmonogram výkazů

ENTERPRISE EDITION

- Bez omezení množství monitorů
- Obsahuje všechny funkce verze Professional
- Monitoring WAN
- Podpora klastrové architektury (Fail-over)
- Velká rozšiřitelnost (architektura Admin Server - Managed Server)
- Vysoká úroveň bezpečnosti (komunikace HTTPS)
- Konsolidované údaje z mnoha sítí s omezeným přístupem



Ucelený náhled v Applications Manageru zobrazuje celkové informace o stavu celé monitorované IT infrastruktury. Prezentované statistiky se týkají alarmů, stavu jednotlivých kategorií monitorů, dostupnosti a využití atributů.

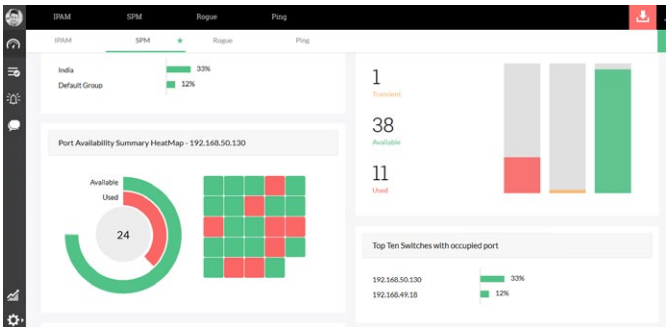


Podnikový náhled skupiny monitorů, která reprezentuje IT službu poskytovanou pobočkou, prezentuje relace mezi jednotlivými zúčastněnými komponenty, jež mají vliv na činnosti IT. Díky grafickému označení a použití barev lze stav služby zhodnotit jedním pohledem.

Správa IP adres a nástroj na mapování portů v přepínači v jednotném pohledu

OpUtils

OpUtils je nástroj pro správu IP adres v korporátní síti.



Systém ukazuje využití IP adres v jednotlivých subsítích a segmentech infrastruktury, informuje správce sítě o dostupnosti adresy, její obsazenosti, dočasnosti, atd. Skládá se z více než 30 nástrojů, jako: diagnostika sítě, monitoring adres, monitoring sítě, funkce SNMP. Umožňuje také tvorbu vlastních funkcí SNMP pro monitorování zařízení na základě knihovny MIB. Systém umožňuje řešení problémů spojených se správou portů přepínačů a adresováním v sítích. Díky výkazům inventarizace, zařízení SNMP, zloděj-ských systémů, dostupných IP adres, adres MAC systém poskytuje správcům sítě aktuální obraz sítě bez nutnosti neustálé a manuální aktualizace statických informací.

NEJDŮLEŽITĚJŠÍ VLASTNOSTI:

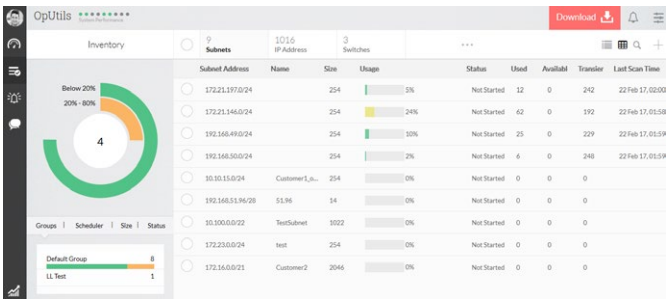
- Správa IP adres a nasycení adres v síťových segmentech
- Správa portů síťových přepínačů
- Detekce podezřelých událostí
- Zálohování konfiguračních souborů zařízení Cisco
- Monitorování propustnosti pásma
- Sada síťových správcovských nástrojů

STANDARD EDITION

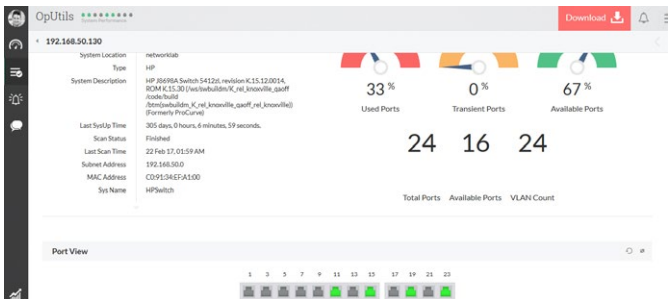
- Správa adres MAC
- SNMP Ping
- Skenování sítě
- Správa DNS
- Monitor pásma
- Monitor sítě
- Wake-On-Lan

PROFESSIONAL EDITION

- Všechny funkce Standard Edition
- Správa IP adres (IPAM)
- Mapování portů přepínačů (SPM)
- Správa konfiguračních souborů



Rozšířený náhled portů přepínače, prezentující informace o obsazenosti portu, IP adrese, připojených adresách MAC, názvu VLAN. Z této úrovně lze definovat také lokalizace zařízení a odečítat rychlost portu.

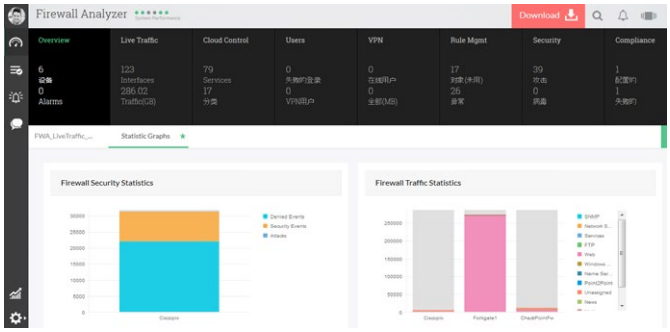


Náhled segmentu sítě s určitým balíčkem IP adres na zadané síťové masce. Obšírné informace o stavu DNS, řešení IP adres nebo doménových názvů, typu zařízení, s pohodlným přechodem do režimu dalších speciálních síťových nástrojů.

Správa konfigurace FW & Správa logů

Firewall Analyzer

Samotná instalace firewall síť neochrání. Nutné je neustálé monitorování a analyzování údajů z deníku FW. Tyto soubory obsahují mnoho důležitých informací. Na základě záznamů v denících lze detekovat ohrožení bezpečnosti, jako průnik do sítě, virové útoky, útoky typu „odmítnutí služby“ (DoS), abnormální chování, chování uživatelů v Internetu, provádět analýzu internetového provozu, atd.



Firewall Analyzer je software pro analýzu logů bez agentů a správu konfigurace, určený pro bezpečnostní zařízení. Program je určen k monitorování a analýze zabezpečení, správě změn, monitorování aktivit zaměstnanců v Internetu, monitorování propustnosti, plánování výkonu, vymáhání dodržování pravidel a tvorbě výkazů z inspekcí bezpečnosti a shody - činností prováděných v koncovém bodě. Firewall Analyzer není závislý na dodavateli a obsluhuje téměř všechny typy firewall open source i komerční (Check Point, Cisco, Juniper, Fortinet, Snort, Squid Project, SonicWALL, Palo Alto itd.), IDS/IPS, sítě VPN, proxy servery a podobná bezpečnostní zařízení. Určen je pro správce ochrany sítě a dodavatele spravovaných služeb ochrany (MSSP), kteří potřebují centralizované shromažďování, archivování a analyzování deníků ochranných zařízení a generování výkazů.

PREMIUM EDITION

- Obsluha až 60 zařízení
- Podpora pro mnoho výrobců
- Monitoring virtuálních FW, proxy a VPN
- Výkazy bezpečnosti
- Výkaz internetové aktivity pracovníků
- Výkaz využití webových aplikací
- Audit bezpečnosti firewall
- Správa změn konfigurace
- Správa pravidel FW
- Diagnostika spojení
- Ověřování AD a RADIUS

DISTRIBUTED EDITION

- Obsluha až 1200 zařízení
- Všechny funkce Premium Edition
- Rozšiřitelná architektura
- Obsluha mnoha lokalizací
- Architektura server - kolektor

Monitoring propustnosti sítě & Analýza síťového provozu

NetFlow Analyzer

„Aplikace NetFlow Analyzer umožnila průběžné monitorování provozu v síti, sledování anomálií a detekování atypických balíčků. Přehledně prezentuje údaje a statistiky využití spojení. Program je velmi praktický a pomáhá při správě sítě.“

Grzegorz Staśkiewicz
Ředitel technické sekce IT
Ceramika Paradyż Sp. z o.o.

NetFlow Analyzer je nástroj pro analýzu provozu v síti bez agentů, využívající celou řadu technologií, které jsou součástí routerů, přepínačů, bariér a akcelerátorů WAN. Software podporuje Cisco netflow, Cisco NBAR, IPSLA a CBQoS. NetFlow Analyzer obsahuje velké množství funkcí, které umožňují hloubkový náhled do provozu sítě a hodnocení jeho vlivu na podnikovou činnost.

NetFlow Analyzer navíc podporuje sFlow®, cflowd®, jFlow®, IPFIX®, NetStream®, AppFlow®

RYCHLEJŠÍ ODSTRANĚNÍ INCIDENTŮ V SÍTI
- Náhled do nejpoužívanějších aplikací v síti
- Vzorce provozu pro rozhraní a oddělení

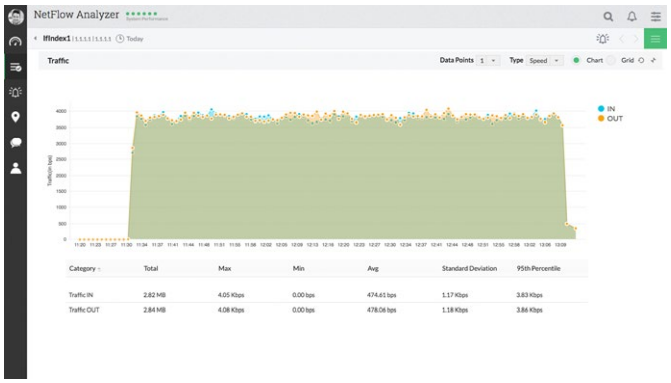
ZAJIŠTĚNÍ VÝKONU APLIKACÍ
- Zajištění optimální propustnosti pro kritické podnikové aplikace
- Ujištění, že aplikace pracují se správnou prioritou

MONITOROVÁNÍ VÝKONU VOIP
- Monitorování klíčových ukazatelů výkonu spojení VoIP
- Vykazování parametrů zpoždění, Jitter, MOS

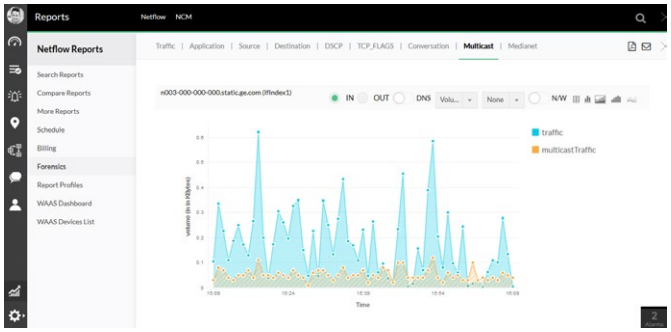
OCHRANA SÍTĚ PROTI HROZBÁM
- Pomoc při detekci červů a virů s detailní informací o počítačích a portech
- Vyspělý modul analýzy hrozeb

OVĚŘENÍ NASTAVENÍ QOS
- Tvorba výkazů na základě tříd
- Ověření toku dat v rámci markerů DSCP

NEJDŮLEŽITĚJŠÍ VLASTNOSTI:
- Tvorba skupin a oddělení na základě IP
- Možnost definování aplikací na základě portu a IP adresy
- Obsluha autonomních systémů (AS)
- Analýza provozu pro Medianet/Mediatrace
- Automatické upozornění po překročení mezních hodnot
- Harmonogramy pravidelných výkazů
- Podpora technologií Cisco Flexible Netflow NBAR pro inteligentní kategorizaci aplikací (vrstva 7 OSI) na základě hloubkové analýzy balíčků
- Podpora pro SNMPv3 a Cisco ASA
- Technologie Continuous Stream Mining Engine™ v modulu ASAM
- Tvorba výkazů Cisco CBQoS
- Podpora pro technologie Cisco WAAS, Medianet a IPSLA
- Analýza a tvorba výkazů propustnosti sítě
- Monitorování provozu mezi oddělenými lokacemi
- Výkazy plánování kapacity s analýzou nárůstu provozu aplikace
- Vyspělé úložiště dat: všechny záznamy ze zařízení jsou uchovávány v aplikaci až jeden měsíc. Agregovaná data jsou uchovávána pro potřeby historických výkazů



Grafické diagramy NetFlow Analyzer znázorňují detaily spotřeby síťového pásma pro různá časová období, v závislosti na rychlosti přenosu, objemu dat, procentuálním využití spojení a množství packetů.



Díky použití technologie Continuous Stream Mining Engine™ je modul ASAM v NetFlow Analyzer prakticky jediným účinným nástrojem pro detekci a klasifikaci útoků zero-day v reálném čase. ASAM nabízí inteligentní systém detekce širokého spektra vnitřních i vnějších hrozeb a kontinuální hodnocení bezpečnosti v síti.

ESSENTIAL EDITION

- Jednoduchá instalace s integrovaným kolektorem dat a systémem pro generování výkazů
- Vhodná pro monitorování až 5000 rozhraní (až 100.000 flows/sec)
- Výkazy provozu sítě v reálném čase
- Geolokalizace IP adres
- Vyspělý modul analýzy hrozeb

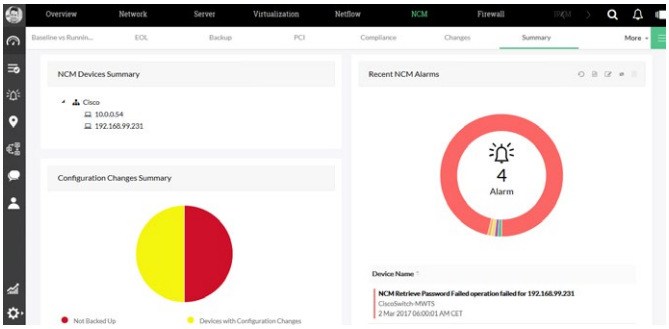
DISTRIBUTED EDITION

- Rozptýlený sběr dat NetFlow a centralizovaná tvorba výkazů
- Monitorování neomezeného množství rozhraní
- Obsahuje všechny funkce verze Professional
- Bezpečná komunikace HTTPS mezi centrálním serverem a datovými kolektory
- Analýza NBAR, CBQoS, ASAM a mnoho jiných.

Správa konfigurace sítě

Network Configuration Manager

Network Configuration Manager je systém podporující správu konfigurací síťových zařízení typu switche a routery. Při využití tohoto systému v IT prostředí lze definovat harmonogram zálohování konfiguračních souborů, porovnávat dvě konfigurace, tvořit základní a aktuální konfigurace a distribuovat vybrané řádky konfigurace na mnoho zařízení současně.

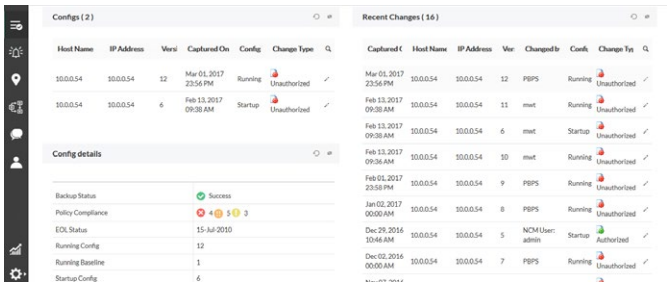


Bohatá funkčnost nástroje, která obsluhuje automatickou detekci zařízení, šifrované součásti konfigurace, verzování, definování harmonogramů zálohování konfigurací a jiných úkolů a modelování přístupu do systému na základě rolí uživatelů, umožňuje bezpečnou, ergonomickou a účinnou centralizaci správy konfigurace síťových zařízení.

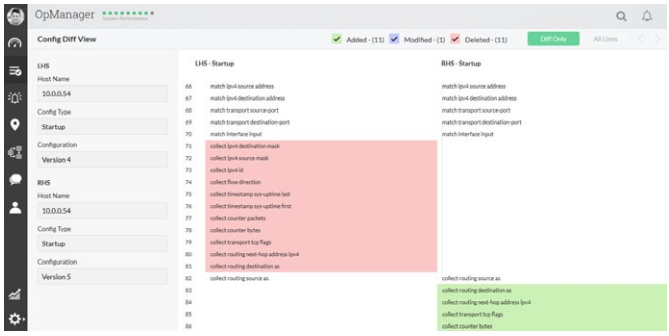
Mechanismus potvrzování konfigurací před implementací na výrobní verzi garantuje stabilitu práce síťových zařízení a kontrolu změny, verzování konfigurací umožňuje rychlou obnovu správného nastavení. Systém obsahuje také mnoho výkazů, které ověřují aktuální konfiguraci z hlediska shody, dobré praxe nebo standardů. Takové výkazy garantují udržení kvality a bezpečnosti konfigurace na vysoké úrovni.

NEJDŮLEŽITĚJŠÍ VLASTNOSTI:

- Podpora pro síťová zařízení nezávisle na výrobci
- Šifrované úložiště konfigurací
- Verzování a porovnávání konfigurací
- Režim základní konfigurace a práce na základě štítků
- Harmonogramy záloh konfigurací a jiných úkolů
- Přístup na základě role
- Mechanismus potvrzování a detekce konfigurací
- Sledování změn konfigurace v reálném čase
- Monitoring shody konfigurace s politikou a standardy
- Automatizace konfiguračních úkolů



Náhled inventarizovaného síťového zařízení umožňuje pohodlnou správu jeho konfigurace. Z tohoto místa je umožněn rychlý přístup do základní a aktuální konfigurace, vyhledávání změn, hardwarových parametrů nebo pravidel správy změn.



Náhled srovnání dvou konfigurací je ideální místo pro ověření změn. Jednotlivé řádky jsou označeny barvami jako změněné, přidané nebo odstraněné. Volitelný režim SyncScroll navíc umožňuje navigaci po obou konfiguracích současně.

POWERING IT AHEAD

ManageEngine

www.manageengine.com