



Najważniejsze informacje

- Bardzo krótki czas wdrożenia – instalacja serwera w 30 minut a tysięcy agentów w kilka godzin.
- Skalowalność do 250 000 agentów obsługiwanych z poziomu jednego (!) serwera.
- Małe wymagania sprzętowe dla serwera i agentów.
- Wysoka skuteczność instalowania poprawek systemowych i aplikacyjnych – 95%+ w pierwszym przebiegu.
- Ciągła widoczność statusu środowiska – każda zmiana na zarządzanej końcówce natychmiast raportowana do serwera i widoczna na konsoli.
- Zarządzanie oparte o polityki egzekwowane na komputerach mobilnych również poza siecią korporacyjną.
- Hierarchiczna architektura pozwalająca na efektywną obsługę zdalnych placówek przy słabych łączach.
- Łatwość utrzymania i rozwoju platformy dzięki funkcji automatycznej aktualizacji.

IBM Tivoli Endpoint Manager

Tivoli Endpoint Manager to nowoczesna platforma zarządzania konfiguracją i bezpieczeństwem stacji roboczych i serwerów, cechująca się nowatorską architekturą, niezwykłą skalowalnością oraz wysoką szybkością działania.

Funkcjonalność

Tivoli Endpoint Manager to elastyczna platforma zarządzania, która w zależności od potrzeb danego środowiska może być wyposażona w konkretne funkcjonalności – podzielone na 4 kategorie:



Tivoli Endpoint Manager for Lifecycle Management



Tivoli Endpoint Manager for Security and Compliance



Tivoli Endpoint Manager for Power Management



Tivoli Endpoint Manager for Patch Management

- Tivoli Endpoint Manager for Lifecycle Management to jeden z głównych modułów rozwiązania adresowany do działów wsparcia, odpowiedzialnych za utrzymanie środowiska stacji roboczych i serwerów.
- Tivoli Endpoint Manager for Security and Compliance zawiera funkcjonalność adresującą przede wszystkim wymagania departamentu bezpieczeństwa, zapewniając ciągłą i skuteczną kontrolę nad bezpieczeństwem konfiguracji stacji i serwerów.
- Tivoli Endpoint Manager for Power Management skierowany jest do tych odbiorców, którzy chcą zaoszczędzić na rachunkach za energię elektryczną i czując odpowiedzialność ekologiczną pragną wspierać „zielone” inicjatywy.
- Tivoli Endpoint Manager for Patch Management to pakiet zawierający tylko rozwiązanie do zarządzania poprawkami, skierowany przede wszystkim do tych organizacji, które posiadają inne narzędzia do zarządzania, a dla których wyzwanie stanowi właśnie ta sfera utrzymania środowiska.

W ramach poszczególnych modułów rozwiązanie zapewnia następującą funkcjonalność:



Wykrywanie zasobów w sieci. Jednym z podstawowych wyzwań w dużych rozproszonych środowiskach, w szczególności korzystających z sieci w technologii WiFi jest inwentaryzacja zasobów podłączonych do sieci korporacyjnej. Duża mobilność zasobów



powoduje, że typowe podejście polegające na centralnym okresowym skanowaniu sieci się nie sprawdza, ponieważ nie zapewnia aktualności danych. Aby sprostać temu wyzwaniu, Tivoli Endpoint Manager umożliwia zdefiniowanie wielu rozproszonych punktów skanowania, które dzięki temu, że skanują tylko lokalną podsieć mogą to robić często, a zebrane dane są natychmiast przesyłane do centralnego serwera – zapewniając ciągłą, aktualną listę wszystkich zasobów w sieci.

Inwentaryzacja sprzętu i oprogramowania. Dla zasobów, które posiadają zainstalowanego agenta platformy Tivoli Endpoint Manager, dostępny jest szeroki wachlarz analiz odpowiadających za zbieranie danych inwentaryzacyjnych o sprzęcie i oprogramowaniu. W odróżnieniu od innych rozwiązań, gdzie skanowanie odbywa się okresowo, np. raz na tydzień i za każdym razem cały wynik skanowania przesyłany jest na serwer w celu analizy i przygotowania raportów, agent Tivoli Endpoint Manager analizuje konfigurację w sposób ciągły, wysyłając do serwera tylko informację o wykrytych zmianach, co z jednej strony minimalizuje obciążenie sieci, z drugiej zaś zapewnia ciągłą aktualność danych na serwerze.

Zarządzanie poprawkami systemowymi i aplikacyjnymi. Kolejnym dużym wyzwaniem w zarządzaniu stacjami roboczymi i serwerami jest konieczność ciągłej aktualizacji zarówno systemów operacyjnych jak i różnych aplikacji ze względu na wykrywane w nich luki bezpieczeństwa. Zadanie to, choć pozornie jest proste, jeśli dana platforma zapewnia mechanizm automatycznej aktualizacji w praktyce spędza sen z powiek wielu administratorom, gdyż mechanizmy automatycznej aktualizacji nie gwarantują udanej instalacji i nie zapewniają spójnego raportowania statusu. Tivoli Endpoint Manager oferuje automatyczne pobieranie najnowszych poprawek dla różnych systemów operacyjnych i typowych aplikacji Windows, wkrótce po tym jak dana poprawka zostanie wydana przez producenta. Poprawki są rozprowadzane w postaci paczek dystrybucyjnych, tak że administrator może od razu przystąpić do testowania ich w swoim środowisku i po akceptacji zlecić dystrybucję na wszystkie systemy, które danej poprawki wymagają. Rozwiązanie zapewnia również mechanizm ciągłego raportowania postępu aktualizacji środowiska z dokładnością do pojedynczej stacji czy serwera.

Zdalna dystrybucja oprogramowania. Tivoli Endpoint Manager posiada moduł odpowiedzialny za zdalną instalację oprogramowania na stacjach roboczych i serwerach. Dzięki hierarchicznej architekturze dystrybucji paczki instalacyjne są przesyłane po łączach WAN do zdalnych oddziałów tylko raz, a wbudowane mechanizmy kontroli wykorzystania pasma zapewniają, że zdalna instalacja nie zakłóca normalnej pracy sieci.

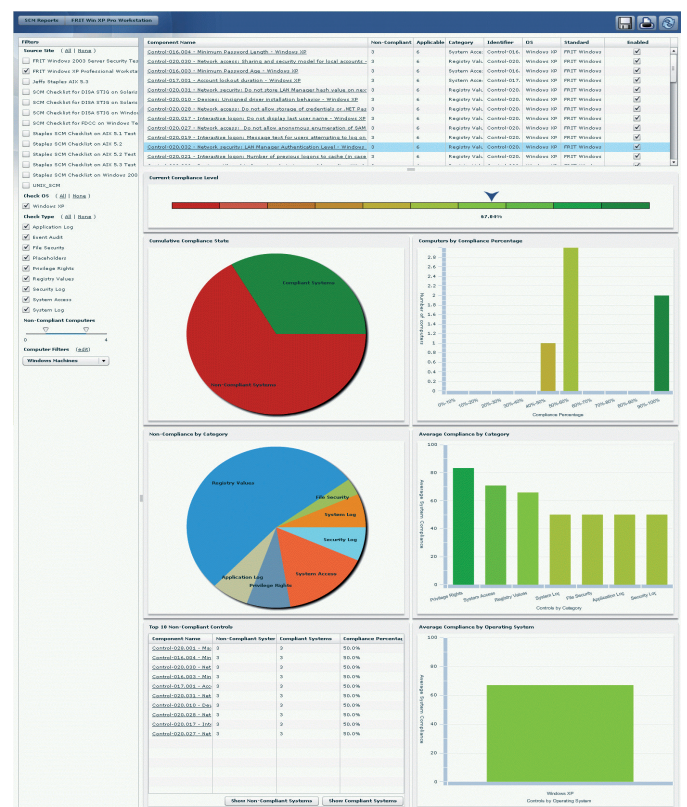
Zdalna instalacja systemów operacyjnych. Tivoli Endpoint Manager for Lifecycle Management oferuje funkcjonalność zdalnej instalacji, reinstalacji i migracji systemów operacyjnych. Dostępne są mechanizmy zdalnej nie

nadzorowanej instalacji w oparciu o plik odpowiedzi, klonowania przygotowanego wcześniej obrazu wzorcowego jak i migracja systemu do nowszej wersji (np. z Windows XP do Windows 7) z zachowaniem ustawień użytkownika. Instalacja przez klonowanie obrazu wzorcowego wspomaga standaryzację konfiguracji końcówek, a funkcja automatycznej instalacji w obrazie właściwych sterowników umożliwia wykorzystanie jednego obrazu systemu dla różnych konfiguracji sprzętu.

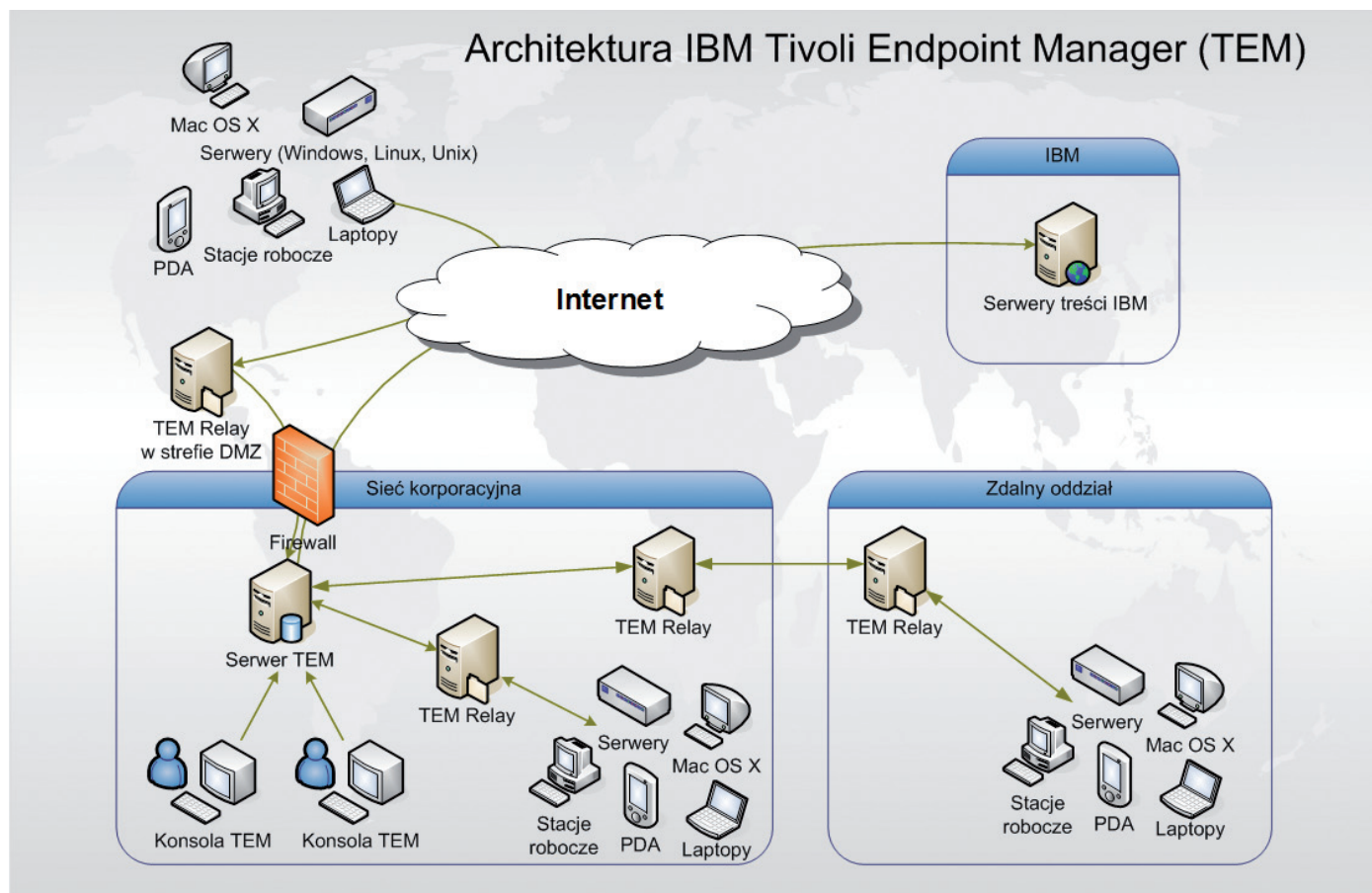
Przejmowanie zdalnego pulpitu. Oprogramowanie Tivoli Endpoint Manager zapewnia mechanizm przejmowania zdalnego pulpitu użytkownika dla systemów Windows i Linux (w oparciu o technologię Tivoli Remote Control) jak również umożliwia integrację z mechanizmami zdalnej pomocy systemu Microsoft® Windows lub innymi narzędziami zdalnej pomocy, które mogą być już wykorzystywane w przedsiębiorstwie.

Analiza wykorzystania oprogramowania. Opcjonalny dodatek Tivoli Endpoint Manager for Software Use Analysis umożliwia monitorowanie wykorzystania oprogramowania na stacjach roboczych z systemem Windows, jak również zarządzanie posiadanymi licencjami i przygotowywanie raportów zgodności, weryfikujących legalność używanego oprogramowania.

Zarządzanie bezpieczeństwem konfiguracji. Większość firm posiada jasno określoną politykę bezpieczeństwa konfiguracji, jednak jej egzekwowanie w dużym, rozproszonym środowisku nie jest zadaniem łatwym. Z pomocą



Konsola Tivoli Endpoint Manager raportująca status zgodności zarządzanych komputerów z polityką bezpieczeństwa.



Architektura IBM Tivoli Endpoint Manager.

przychodzi Tivoli Endpoint Manager, umożliwiającą automatyczne wykrywanie naruszeń polityki bezpieczeństwa jak i szybkie zaaplikowanie niezbędnych zmian. Dzięki nowatorskiej architekturze, w której to agent jest odpowiedzialny za ciągłą realizację przypisanych polityk bezpieczeństwa, możliwe jest skuteczne przestrzeganie reguł również, kiedy stacja robocza znajduje się poza siecią korporacyjną. Z drugiej strony mechanizm ciągłego monitorowania zgodności i szybkiego aktualizowania danych na serwerze zapewnia administratorom odpowiedzialnym za bezpieczeństwo ciągły podgląd statusu zgodności w całym środowisku.

Zarządzanie podatnościami. W produkcyjnym środowisku, w szczególności w odniesieniu do serwerów wypełnienie zaleceń polityki bezpieczeństwa wymaga odpowiedniego okresu testowania, a czasem nie jest możliwe bez zmian w aplikacjach. Tivoli Endpoint Manager przychodzi z pomocą administratorom bezpieczeństwa pozwalając precyzyjnie śledzić, które systemy są podatne na jakie zagrożenia i sukcesywnie te zagrożenia eliminować.

Izolacja sieciowa niezgodnych komputerów. Tivoli Endpoint Manager umożliwia zdefiniowanie polityk ograniczających dostęp do zasobów sieci korporacyjnej, jeżeli stacja robocza nie spełnia krytycznych wymogów polityki bezpieczeństwa. Dzięki temu komputery, które nie posiadają np. działającego, zaktualizowanego systemu antywirusowego

mogą być odizolowane, dopóki nie przejdą kwarantanny, co chroni zasoby przedsiębiorstwa.

Zarządzanie wykorzystaniem energii. Rosnące ceny energii powodują ciągły wzrost wydatków na elektryczność mimo tego, że nowoczesne komputery posiadają wiele funkcji pozwalających na oszczędności w tym zakresie. Niestety niewielu użytkowników z tych opcji korzysta, co w skali przedsiębiorstwa daje olbrzymi potencjał oszczędności. Tivoli Endpoint Manager for Power Management to dedykowana funkcjonalność pozwalająca śledzić zużycie energii przez stacje robocze rozproszone w całym środowisku, weryfikować i poprawiać ustawienia profilu energetycznego oraz w razie potrzeby hibernować stacje, które zostały włączone np. na noc a nikt z nich nie korzysta. Dodatkowo na centralnej konsoli w sposób ciągły prezentowane są dane zużycia energii z całego środowiska jak również oszczędności poczynione dzięki zastosowaniu oprogramowania Tivoli Endpoint Manager.

Funkcjonalność wszystkich opisanych modułów może być połączona w ramach jednej infrastruktury, jednego serwera i z wykorzystaniem jednego agenta instalowanego na stacji roboczej lub serwerze.

Architektura rozwiązania

Jedną z kluczowych cech wyróżniających oprogramowanie Tivoli Endpoint Manager od konkurencji są niewielkie wymaga-

nia sprzętowe. Nawet w środowisku liczącym 250 000 końcówek wymagany jest jeden centralny serwer, który pozwala zarządzać całym środowiskiem. Taka niezwykła skalowalność rozwiązania możliwa jest dzięki innowacyjnemu podejściu do roli serwera i agenta. W oprogramowaniu Tivoli Endpoint Manager to agent zainstalowany na stacji roboczej lub serwerze wykonuje większość pracy, a serwer odpowiada tylko za gromadzenie informacji o statusie w centralnej bazie danych.

Aby uniknąć nadmiernego obciążania stacji roboczych lub serwerów, agent Tivoli Endpoint Manager posiada wbudowany mechanizm kontroli, który sprawia, że wykorzystanie mocy procesora nie przekracza 2%. Nawet, jeśli agent ma przypisanych wiele polityk, które w sposób ciągły analizuje i wykonuje, próg ten jest zachowany i tylko pełny cykl ewaluacji wszystkich polityk trwa trochę dłużej.

Drugim elementem umożliwiającym taką skalowalność jest funkcja komponentu pośredniego Tivoli Endpoint Manager Relay, która sprawia, że zwykły agent zainstalowany na stacji roboczej może pełnić funkcję proxy komunikacyjnego i bufora treści dla innych agentów. Dzięki temu komponentowi, który nie wymaga dedykowanego sprzętu, ani serwerowego systemu operacyjnego komunikacja po łączach WAN do zdalnych oddziałów może być optymalizowana, tak aby np. pakiety instalacyjne oprogramowania lub poprawek były przesyłane tylko raz.



© Copyright IBM Corporation 2011

IBM Polska Sp. z o.o.
ul. 1 Sierpnia 8
02-134 Warszawa
tel. (+ 48 22) 878 67 77
faks (+ 48 22) 878 68 88
ibm.com/pl

Wydrukowano w Polsce
Wszelkie prawa zastrzeżone.

IBM i logo IBM są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy International Business Machines w Stanach Zjednoczonych i/lub innych krajach.

Pozostałe nazwy firm, produktów i usług mogą być znakami towarowymi lub znakami usług należącymi do innych podmiotów.

Wspierane platformy

Tivoli Endpoint Manager 7.2.1 wspiera poniższe platformy systemowe.

Wymagania dla serwera:

- Microsoft SQL Server 2005/2008
 - Microsoft Windows Server 2003/2008/2008 R2
-

Wymagania dla konsoli:

- Microsoft Windows XP/2003/Vista/2008/2008 R2/7
-

Wymagania dla agenta:

- Microsoft Windows, w szczególności wersje XP, 2000, 2003, Vista, 2008, 2008 R2, 7, CE, Mobile, XP Embedded i Embedded Point-of-Sale
 - Mac OS X
 - Solaris
 - IBM AIX®
 - Linux on IBM System z®
 - HP-UX
 - VMware ESX Server
 - Red Hat Enterprise Linux
 - SUSE Linux Enterprise
 - Oracle Enterprise Linux
 - CentOS Linux
 - Debian Linux
 - Ubuntu Linux
-