



TIVOLIDAY2010

Pulse Comes To You

12 października 2010, Hotel Sheraton

Urządzenia sieciowe pod kontrolą, czyli jak uporządkować środowisko sieciowe za pomocą Tivoli Netcool Configuration Management.

Maciej Szulc, maciej.szulc@pl.ibm.com

© 2010 IBM Corporation



Problem – wzrastająca złożoność sieci

Złożoność sieci...

- Dynamicznie zwiększająca się ilość urządzeń
- Heterogeniczność środowiska IT
- Plik konfiguracyjny wielkości książki

Wzrastająca dynamika zmian

- Tysiące zmian w konfiguracji i coraz krótsze okna na ich wprowadzenie
- Częste aktualizacje firmware urządzeń

... i ilość powiązanych z nią informacji

- Coraz więcej danych niez...
- Niez...
- „Tyn...

Obciążenie

- Niew...
- Śred...
- ~21k...
- światła

Nacisk na zgodność

- Wzrastające koszty



Handwritten mathematical notes and calculations:

$$\begin{aligned} & \cdot (-8) \\ & -32 \\ & 11. (-6) + [6 + (-1)] \\ & = (-9) \\ & + 9x \\ & + x^2 \\ & 11x(2x-7) - 57(6x-7) \\ & x^2 = 12xy - 170y + 39y^2 \\ & x^2 = 27x^2y + 35y^2 \\ & + \frac{18}{5} = -\frac{4}{5} \\ & = -12 \\ & = -3 \\ & -2(x-2) = 2(8-x)15x \\ & 2x+12 = 6-2x+6x \\ & 4+12 = 6+6x \\ & 12 = 6+6x \\ & 6 = 6x \\ & 6 = 2x \\ & x = 3 \\ & 4-6x \\ & 4-6x \\ & 6x \\ & 6x \\ & \text{No. EA VALUES} \\ & \begin{array}{|c|c|c|} \hline x & 25 & 25x \\ \hline 20x & 10 & 10(50-x) \\ \hline & & 500 \\ \hline \end{array} \\ & 25x + 10(50-x) = 590 \\ & 25x + 500 - 10x = 590 \\ & 15x + 500 = 590 \\ & 15x = 90 \\ & x = 60 \\ & 50 - x = 44 \end{aligned}$$

Sources: Cisco, EMA, Gartner, Juniper Networks, Network World

Złożoność generuje koszty...

Błędy najczęstszą
przyczyną przestoju
sieci

60%

awarii spowodowane
błędami operatorów
podczas konfiguracji

Złożoność sieci
wyrządza
oskrytowanie

30

Średnia ilość błędów w
konfiguracji na
urządzenie

Rutynowe zadania
zużywają zasoby

45%

Czasu inżynierów zużyta
na ręczną konfigurację

Niepoprawny
provisioning i brak
zasobów sprzętowych

35%

Zasobów sieciowych
uruchomionych
nieprawidłowo

Niespójność
bezpieczeństwa to
otwarcie na atak

80%

ataków na urządzenia
skonfigurowanie
niezgodnie z polityką

Sources: Dataquest, EMA, Yankee, Infonetics Research



Co można zrobić?

Poczekać

Ale zmian nie da się zatrzymać, będzie tylko gorzej

Zautomatyzować

Jedyny rozsądny sposób na poprawę stanu





IBM przejął Intelliden!

- Intelliden to wiodący dostawca najwyższej klasy narzędzi automatyzujących nadzór heterogenicznych sieci
- Rozwiązanie staje się częścią oprogramowania rodziny Tivoli; uzupełnia istniejącą dotąd funkcjonalność dla zarządzania i monitorowania IT
- Rozwiązanie sprawdzone w praktyce i zintegrowane z narzędziami Tivoli

“By leveraging Intelliden, we have added a critical layer of automation to the activation and configuration of our new service offerings. Intelliden gives us a common data plane and complete understanding and control of device configuration. This allows TELUS to roll out new services, improve standardization and ultimately customer satisfaction, as well as reduce operating expenses and errors.”

Ibrahim Gedeon, CTO, TELUS



Tivoli Netcool Configuration Manager = Intelliden R-Series

Bezpieczeństwo i administracja

Precyzyjna kontrola uprawnień

Zarządzanie konfiguracją i zmianą

Zawsze aktualna konfiguracja

Zgodność i audyt

Bezpieczeństwo

Provisioning sieci

Bezskryptowe uruchamianie usług

The screenshot displays the Intelliden software interface. On the left, a tree view shows the 'Intelliden' resource browser with folders like 'Command Sets', 'Content', 'DuplicateTest', 'Emus', 'IDT-Test-Lab', 'lab', 'OS Upgrades', 'Production', and 'Scale'. The main area shows a table of configurations:

Name	Vendor	Type
10.216.1.53	Cisco	Router
10.216.1.234	Cisco	Router
10.216.1.235	Cisco	Router
10.216.1.40	Cisco	Switch
10.216.1.208_old	Cisco	Router

Below the table, a 'Configurations' list shows items like 'Configuration Synchronization' and 'Imported Configuration' with their respective authors (adrien, earcuri, sbond). A 'Native Differences' window is open, comparing two configurations for 'Intelliden/lab/10.216.1.235'. It shows a side-by-side comparison of configuration lines, with changes highlighted in yellow. The legend indicates: Deleted (red), Added (green), Changed (yellow), and No Change (black).



Tivoli Netcool Configuration Manager

Bezpieczeństwo i administracja

Precyzyjna kontrola uprawnień

Kontrola dostępu do urządzeń na bazie użytkownika lub grup

Kontrola dostępu aż do poziomu parametrów wydawanych komend

Autentykacja na bazie wewnętrznej bazy lub usług zewnętrznych (np. Radius)

Logiczna organizacja urządzeń w grupy – np. geograficzne, funkcjonalne, związane z konkretnym klientem

Polityki bezpieczeństwa mogą dotyczyć zarówno użytkowników, jak i grup urządzeń

Powiadamianie o nieudanych próbach logowania

Centralne zarządzanie użytkownikami, grupami i uprawnieniami

Rejestrowanie wykonywanych akcji

Śledzenie aktywności użytkowników – również jeśli zmiany są wykonywane poza systemem

Zarządzanie konfiguracją i zmianą

Zawsze aktualna konfiguracja

Automatyzacja zatwierdzania zmian, roll-out, raportowania

Zarządzanie konfiguracją działające w czasie rzeczywistym, z analizą aktualnej konfiguracji

Walidacja zmian – kolejność, składnia, semantyka

Wsparcie dla komunikacji poprzez Telnet / SSH / FTP / SNMP

Synchronizacja konfiguracji: automatyczna po wykryciu zmiany, ręczna, okresowa etc.

Pełna archiwizacja konfiguracji – wersjonowanie, filtrowanie

Wsparcie dla odwracania zmian: roll-back, reload i reset

Detekcja zmian wykonywanych poza systemem

Przeszukiwanie konfiguracji, wskazywanie różnic pomiędzy poszczególnymi ich wersjami

Interfejs graficzny i CLI



Tivoli Netcool Configuration Manager

Zgodność i audyt

Bezpieczeństwo

Mechanizmy definiowania i egzekwowania polityki operacyjnej, bezpieczeństwa i regulacyjnej.

Automatyczne, zawsze aktywne nadzorowanie zgodności

Centralne repozytorium polityk

Graficzna definicja reguł i polityk

Inteligentne akcje w razie wykrycia niezgodności

Pełne logowanie wydawanych komend i odpowiedzi urządzenia

Audyt historii zmian w konfiguracji

Dostarczane z produktem polityki i przykłady

Automatyczne raportowanie niezgodności

Provisioning sieci

Bezskryptowe uruchamianie usług

Funkcjonalność provisioningu opartego na aktualnej konfiguracji, z pełnym sprawdzaniem zależności

Weryfikacja zmian przed ich wykonaniem w zakresie poleceń, kolejności i zgodności

Wzorce provisioningu dostępne zarówno w interfejsie operatorskim, jak i poprzez API

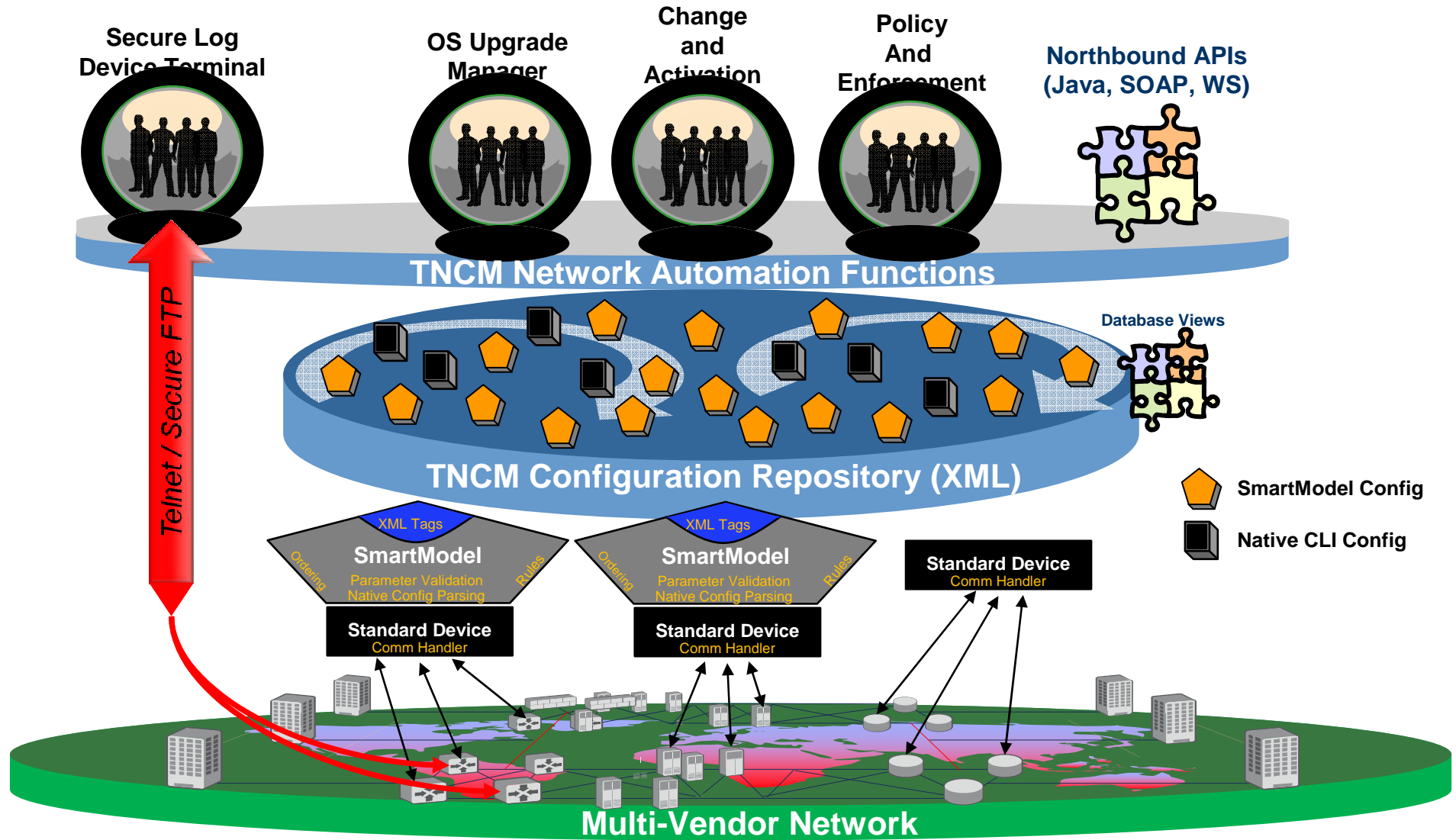
Wsparcie dla parametrów podawanych/definiowanych w trakcie wykonywania operacji

Pełne wsparcie cyklu zmian: Move, Add, Change, Delete

Automatyczna obsługa błędów i wyjątków

Rozbudowane API dla integracji z narzędziami Service Provisioning i Inventory

TNCM - architektura





Dlaczego klienci kupują Tivoli Netcool Configuration Manager?

Skalowalność

- Skalowalność od dziesiątek do setek tysięcy heterogenicznych urządzeń przy zapewnieniu najwyższej jakości obsługi

Pełna automatyzacja sieci

- Wykrywanie i synchronizacja konfiguracji, nadzór nad bezpieczeństwem, zarządzanie konfiguracją i jej zmianą, nadzór nad zgodnością, provisioning

Dokładność

- Unikalne moduły SmartModels™ wymuszają odpowiednią składnię i kolejność poleceń
- Moduł wprowadzania zmian analizujący stan urządzeń – nie działający w trybie “fire and forget”

Bezpieczeństwo

- Możliwość kontroli dostępu do urządzeń a nawet specyficznych poleceń konfiguracyjnych



Dlaczego klienci kupują Tivoli Netcool Configuration Manager?

Różne tryby automatyzacji

- Wsparcie dla różnorodnych potrzeb i poziomów wiedzy:
 - Terminal dla ekspertów i zastosowań „ad-hoc”
 - Zaawansowane mechanizmy dla mniej doświadczonych oraz do zadań powtarzalnych

Nadzór nad zgodnością

- Wsparcie dla różnorodnych typów polityk
- Inteligentne czynności zaradcze
- Raportowanie

Otwarta architektura

- Szybka integracja z narzędziami firm trzecich
- Otwarte API
- Wsparcie dla standardów

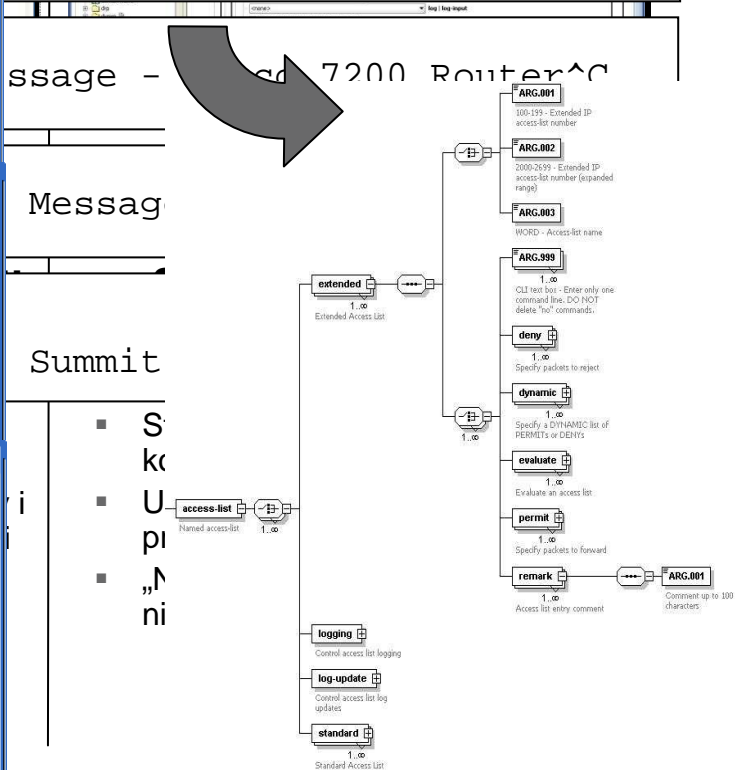


TNCM – Siła SmartModels™

The screenshots show the Intelligent Configuration GUI for various devices:

- Juniper Router (1410/5.1.1):** Configuration for a login banner with the text: `\n\n\n\nThis router is for the exclusive use of TELUS.\nAll unauthorized access or`
- Cisco Router (7206/C7200-IK95-M-12.3(12a)):** Configuration for a Message of the Day (MOTD) banner with the text: `* LINE - banner-text`
- Cisco Switch (4006/6.3(6)):** Configuration for a system banner with the text: `* Message text`
- Juniper Router (M10/7.4R2.6):** Configuration for a system login message with the text: `smokemet`

```
intelliden:~$ show access-list extended remote-offices
Remark: 192.209.5.57 any eq smtp
Deny IP host 192.209.5.57 any eq smtp
Deny IP host 82.72.184.196 any eq smtp
Deny IP host 82.72.184.196 any eq telnet
Deny IP host 15.41.184.182 any eq ftp
Deny IP host 19.29.66.34 any eq ftp
Deny IP host 192.168.32.52 any eq ftp
Deny IP host 65.173.211.71 any eq ftp
Deny IP host 192.209.5.56 any eq smtp
Deny IP host 192.168.32.99 any eq ftp
Deny IP host 192.168.32.99 any eq smtp
Deny IP host 191.169.211.71 any eq ftp
Deny IP host 192.209.5.55 any eq ftp
Deny IP host 192.209.5.58 any eq smtp
Deny IP host 15.41.184.221 any eq ftp
Deny IP host 191.169.211.71 any eq telnet
Deny IP host 192.209.5.55 any eq ftp
Deny IP host 191.169.211.71 any eq ftp
Deny IP host 191.169.211.71 any eq telnet
Deny IP host 82.72.184.192 any eq telnet
Deny IP host 19.29.66.34 any eq smtp
```

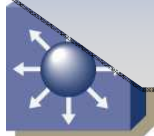


Szerokie wsparcie dla różnorodnych urządzeń

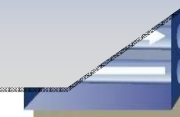


Bezpośrednie wsparcie dla ponad 850 typów urządzeń i tysięcy wersji firmware. Wsparcie dla dowolnych urządzeń w trybie „Native Command”

Multi-service Switches

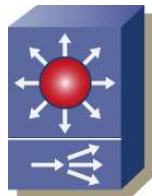


VPN Concentrators

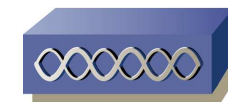


Tivoli Netcool Configuration Manager

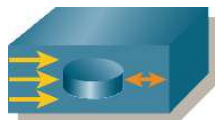
Content Switches



Wireless Access Points



WAN Optimization



Session Border Controllers



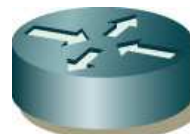
LAN Switches



Firewalls



Routers





Zarządzanie konfiguracją i zmianą

- **Działające w czasie rzeczywistym, oparte na aktualnym stanie urządzeń zarządzanie konfiguracją**
 - Grupowanie urządzeń, wraz z przypisywaniem:
 - Metod dostępu
 - Uprawnień
 - Serwerów wykonujących rekonfigurację
 - Różne tryby automatyzacji
 - Telnet (Intelliden Device Terminal)
 - CLI (native commands)
 - Modelowany za pomocą SmartModels™
 - Zestawy poleceń – do przyszłego wykorzystania
 - Rollback zmian nie powodujący przerwy w świadczeniu usług
 - Zarządzanie zmianami dokonywanymi poza systemem
 - Porównywanie konfiguracji
 - Przeszukiwanie konfiguracji
- **Zarządzanie zmianą**
 - Wbudowany workflow wprowadzania zmian, z możliwością dowolnej modyfikacji
- **Śledzenie, raportowanie, otwarte API**

Configuration/
Change Mgmt.

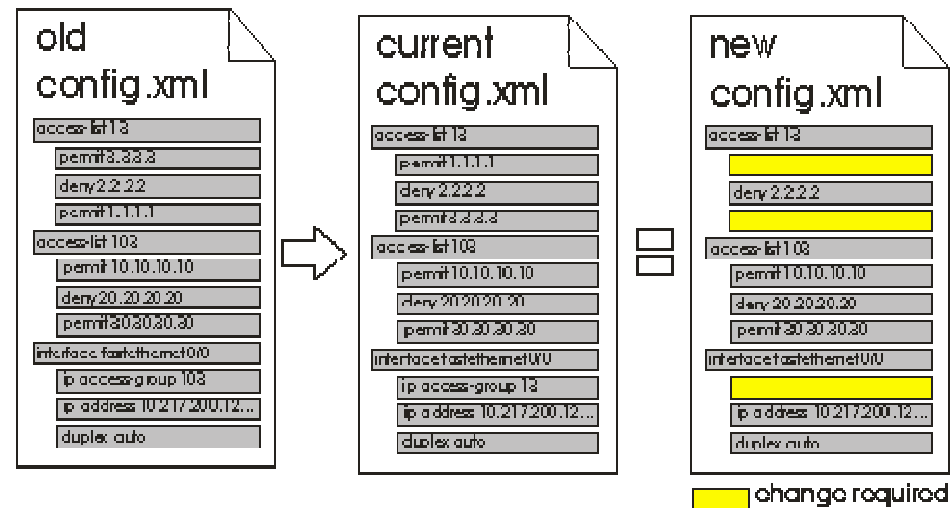
Automatyzuje konfigurację urządzeń w skali całej sieci z niespotykanym u konkurencji poziomem standaryzacji, dokładności i kontroli



W odróżnieniu od rozwiązań skryptowych, mechanizmy SmartModels zapewniają iż każda wprowadzana zmiana jest składniowo i semantycznie poprawna i bazuje na rzeczywistym stanie urządzenia

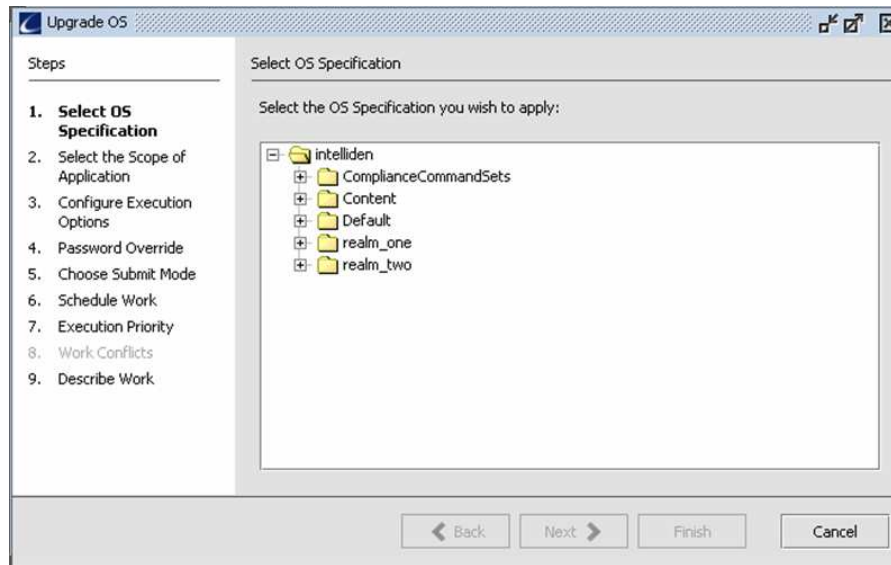
Inteligentny roll-back

- Każda wersja konfiguracji jest przechowywana jako oddzielny dokument XLS zawierający całą konfigurację urządzenia (włącznie z ukrytymi komendami)
- Inteligentny roll-back aplikuje jedynie niezbędne komendy, bez konieczności przeładowania całego pliku



```
Native Commands of IntelIdea/sales_lab_2600-3...
no access-list 13 permit 1.1.1.1
access-list 13 permit 3.3.3.3
access-list 13 deny 2.2.2.2
access-list 13 permit 1.1.1.1
interface FastEthernet 0/0
  no ip access-group 13 in
  ip access-group 103 in
end
```

OS Manager



Automatyzacja aktualizacji firmware

- Aktualizuje oprogramowanie lub aplikuje poprawkę
- Pozwala na dostosowanie procesu aktualizacji do wymogów biznesowych, przyjętych praktyk lub wewnętrznych polityk
- Automatyczna rekonfiguracja urządzenia po aktualizacji
- Przechowuje historię dokonanych zmian dla potrzeb raportowania
- Wspiera różnorodne tryby aktualizacji

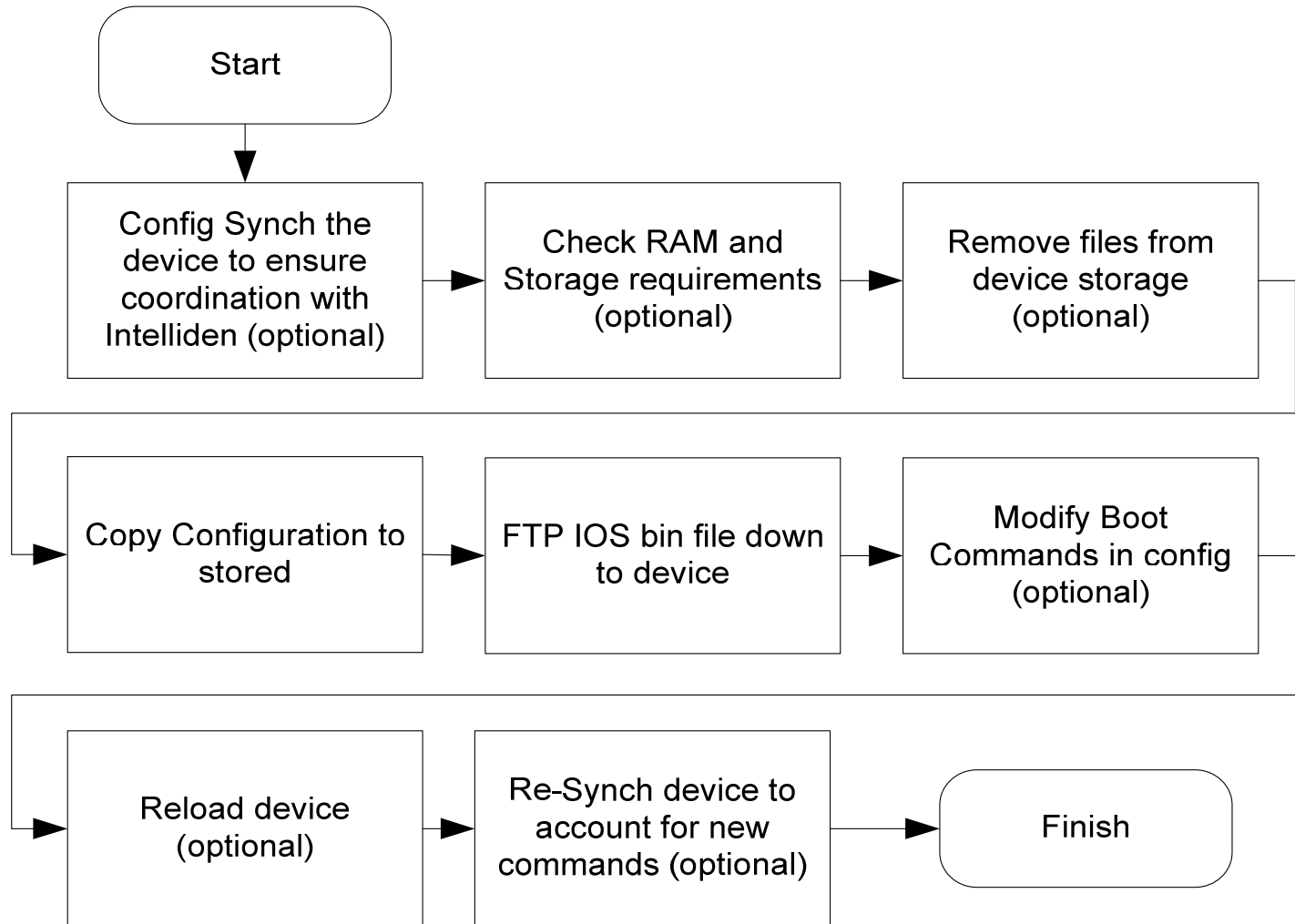
OS Manager



- Z produktem dostarczane są wykonywane przed aktualizacją procedury sprawdzające, istnieje możliwość ich dostosowywania
- Wspierane są niuanse związane ze specyfiką urządzenia – np. Skopiowanie konfiguracji i vlan.dat z urządzeń CatOS przed wyczyszczeniem pamięci flash i ich przywrócenie przed wgraniem nowego firmware.
- Możliwość dodawania nowych rodzajów urządzeń bez konieczności konsultacji z IBM



OS Manager - proces





Zgodność i audyt

- „Zamknięta pętla”
 - Wspiera cały cykl zapewniania zgodności
- **Centralne repozytorium polityk i niezawodny silnik nadzorujący**
 - Wsparcie dla dowolnej ilości kombinacji polityk i urządzeń
 - Zapewnia ciągłą weryfikację zgodności
- **Inteligentne działania zaradcze**
 - Rozwiązywanie wykrytych niezgodności
 - Możliwość dostosowania procesu – np. wprowadzenie ręcznej autoryzacji czynności zaradczych
- **Rozbudowane raportowanie**
 - Pełna informacja audytowa dla odbiorców technicznych i biznesowych
- **Łatwość użycia**
 - Interfejs typu Drag-and-drop
- **Niespotykana skalowalność**
 - > 1,000,000 walidacji na godzinę
- **Dostarczane z produktem przykładowe polityki**
 - NSA router guidelines; operational policies

Compliance & Audit

Zautomatyzowane, kompleksowe rozwiązanie do nadzoru zgodności w sieci

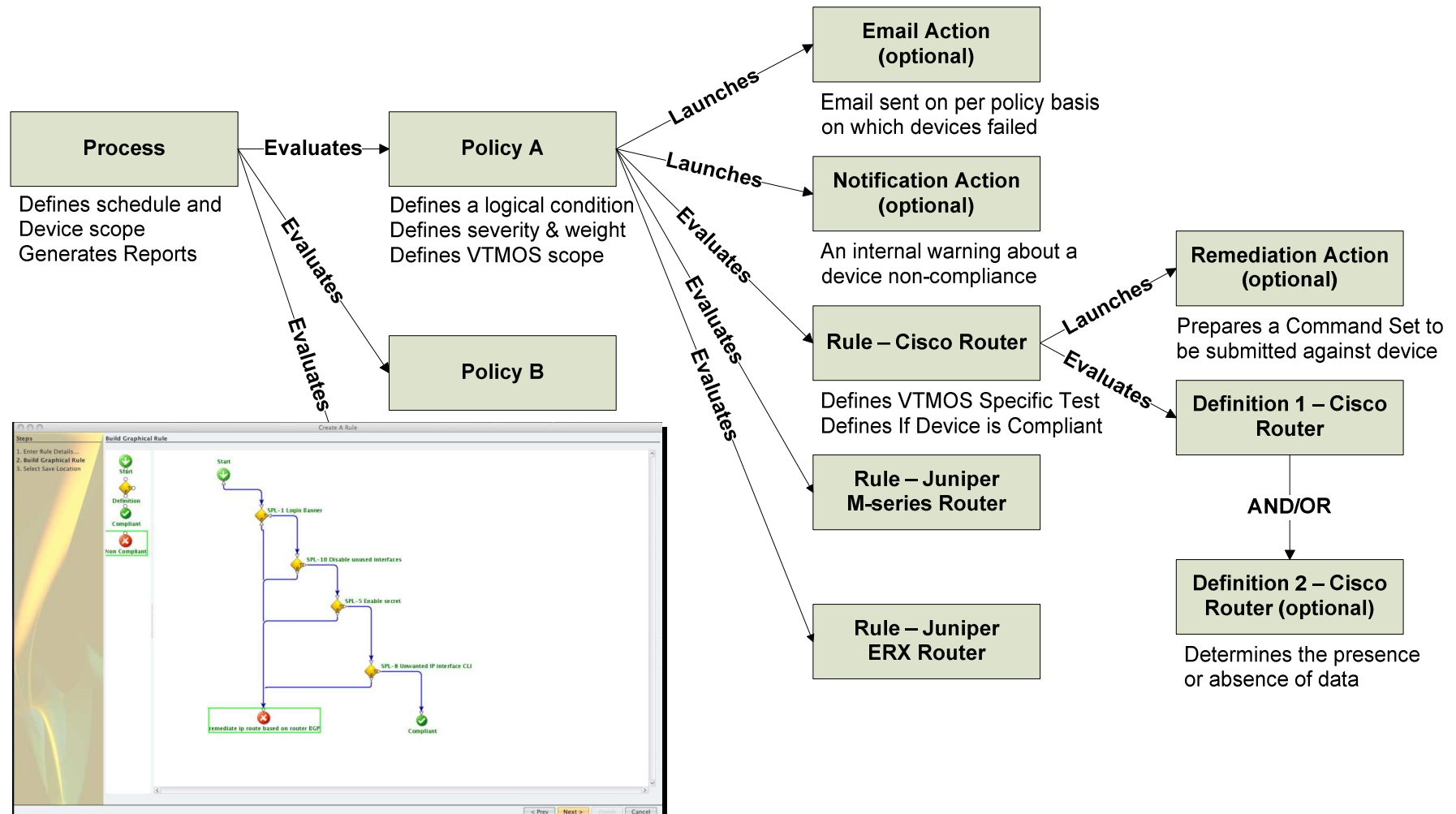


- W sposób ciągły weryfikuje konfigurację sieci na zgodność z normami regulacyjnymi, bezpieczeństwa o operacyjnymi, inteligentne czynności zaradcze
- Pozwala na czasowe lub stałe wyłączenie niektórych urządzeń z działania procesu



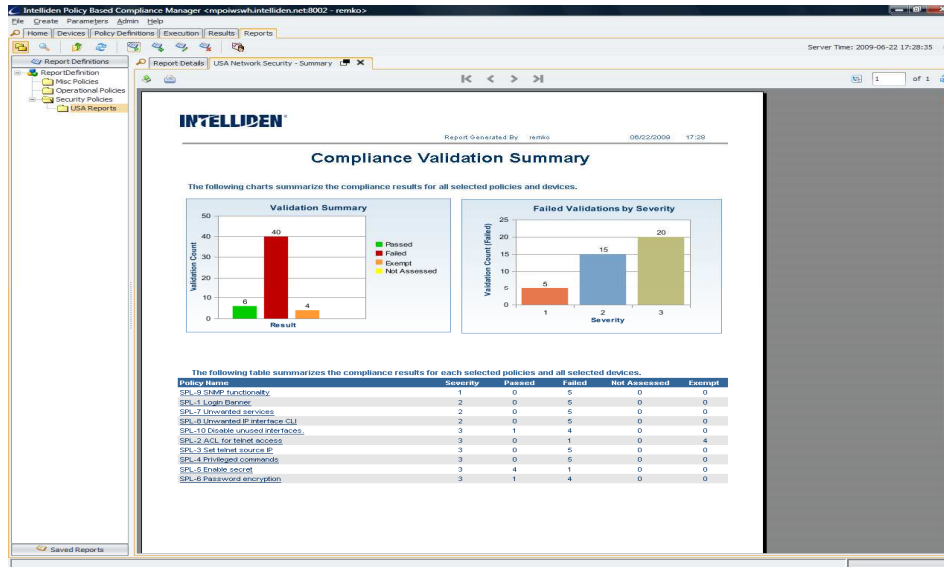
Zgodność i audyt - proces

Compliance
& Audit





Zgodność i audyt - raportowanie



Zawsze aktywne automatyczne logowanie informacji audytowej

- Sumaryzacja danych o zgodności w skali całej sieci
- Szybkie wyszukiwanie rezultatów dla wskazanych urządzeń
- Raporty: Dashboard, Summary, Policy, Device, Validation Detail
- Dane aktualne oraz wyliczony trend
- Aktywne raportowanie – nawigacja od podsumowania aż do specyficznych naruszeń polityki
- Możliwość definiowania własnych raportów, ich zapisywania i przesyłania.

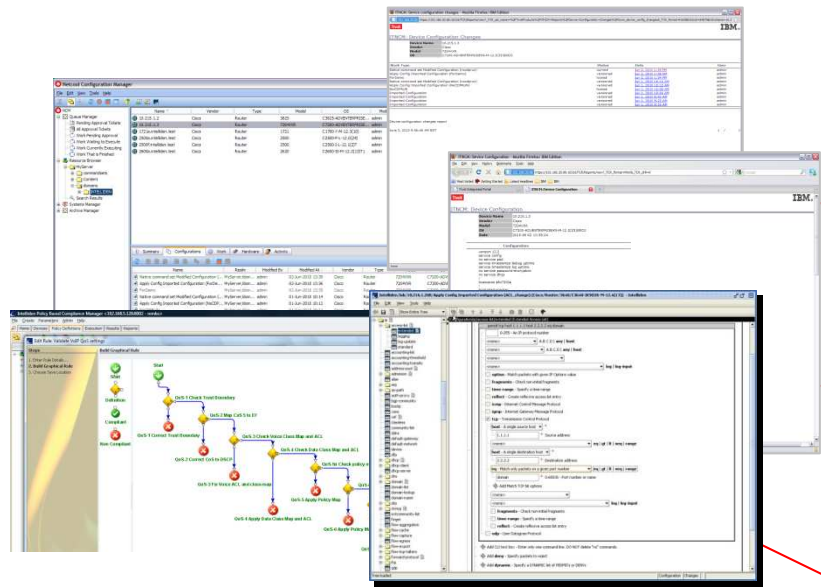
Compliance & Audit



- Oparty na rolach i uprawnieniach model autoryzacji dostępu do logów i raportów
- Możliwość definiowania spersonalizowanych raportów – np. obejmujących wyłącznie wskazane polityki czy też urządzenia
- Wskaźnik „Network Compliance Score” może agregować tysiące rezultatów walidacji polityk w pojedynczą liczbę obrazującą aktualny stan sieci a wskaźnik trendu pozwala na obserwację zmian w czasie



TNCM: Użytkownicy oprogramowania



CTO / CIO



- Ustala obowiązujące zalecenia i potrzebuje narzędzi do ich weryfikowania
- Musi uruchomić nowe usługi – niezbędna jest mu wiedza o urządzeniach i ich możliwościach
- Odpowiedzialny za audyt i zgodność sieci z normami

Chief Security Officer



- Odpowiada za procedury w zakresie bezpieczeństwa
- Potrzebuje automatycznych narzędzi wymuszających przestrzeganie zaleceń
- Potrzebuje raportowania incydentów i śledzenia zmian

Chief Operations Officer



- Odpowiada za diagnozę i usuwanie awarii we współpracy z NOC
- Odpowiada za przestrzeganie standardów przy zapewnieniu odpowiedniego poziomu produktywności personelu
- Potrzebuje automatyzacji działań aby poprawić efektywność i wprowadzać nowe usługi
- Potrzebuje narzędzi do automatycznego provisioningu

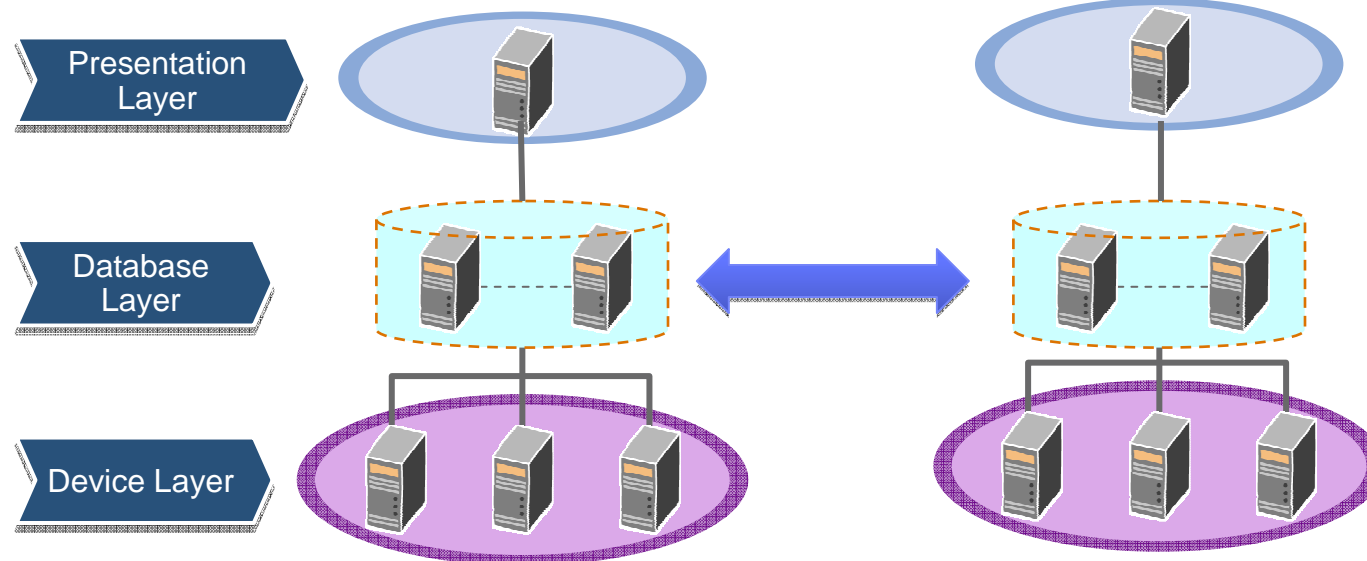
Inżynier NOC



- Musi szybko zaradzić pojawiającym się problemom
- Potrzebuje precyzyjnej informacji o urządzeniach i ich konfiguracji
- Potrzebuje narzędzi pozwalających na szybkie realizowanie napływających zleceń rekonfiguracji

TNCM: skalowalność i odporność na awarie

- ▶ Możliwość implementacji każdej z warstw na wielu fizycznych serwerach
 - ▶ Awaria serwera nie zmniejsza dostępności narzędzi
 - ▶ Nadmiarowe serwery mogą być w pełni aktywne i dostępne
- ▶ Rozproszenie geograficzne
 - ▶ Nawet awaria całej serwerowni nie wyłączy systemu!



Platform

solution

- Klient decyduje o wymaganym poziomie nadmiarowości i sumarycznej wydajności rozwiązania, zgodnie z potrzebami biznesowymi



TNCM: raportowanie

Ostatnie zmiany – kto i kiedy ich dokonał?

Status konkretnej konfiguracji

Widok szczegółów konfiguracji

Czas ostatniej aktualizacji – możliwość kliknięcia na dacie aby zobaczyć szczegóły

Log audytowy – widok interakcji z urządzeniem

Szczegóły urządzenia

Podsumowanie wykonanego zadania (Unit of Work)

Przebieg wykonania i zakończenia oraz rezultat wykonania zadania na urządzeniu

Raport zgodności

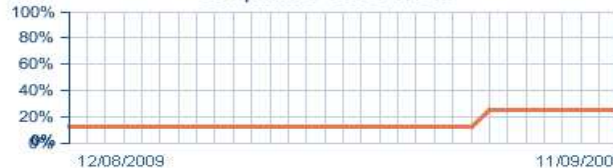
Selected Policy Realm: CIS-Level-1-Benchmark/Management Plane Level 1/Access Rules
Selected Device Realm: Intelligen/virtual-canadian-customer/alberta

Compliance Score

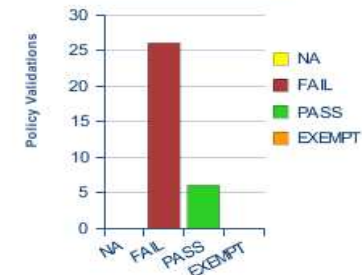
18.75%

0% 20% 40% 60% 80% 100%

Compliance Score Trend



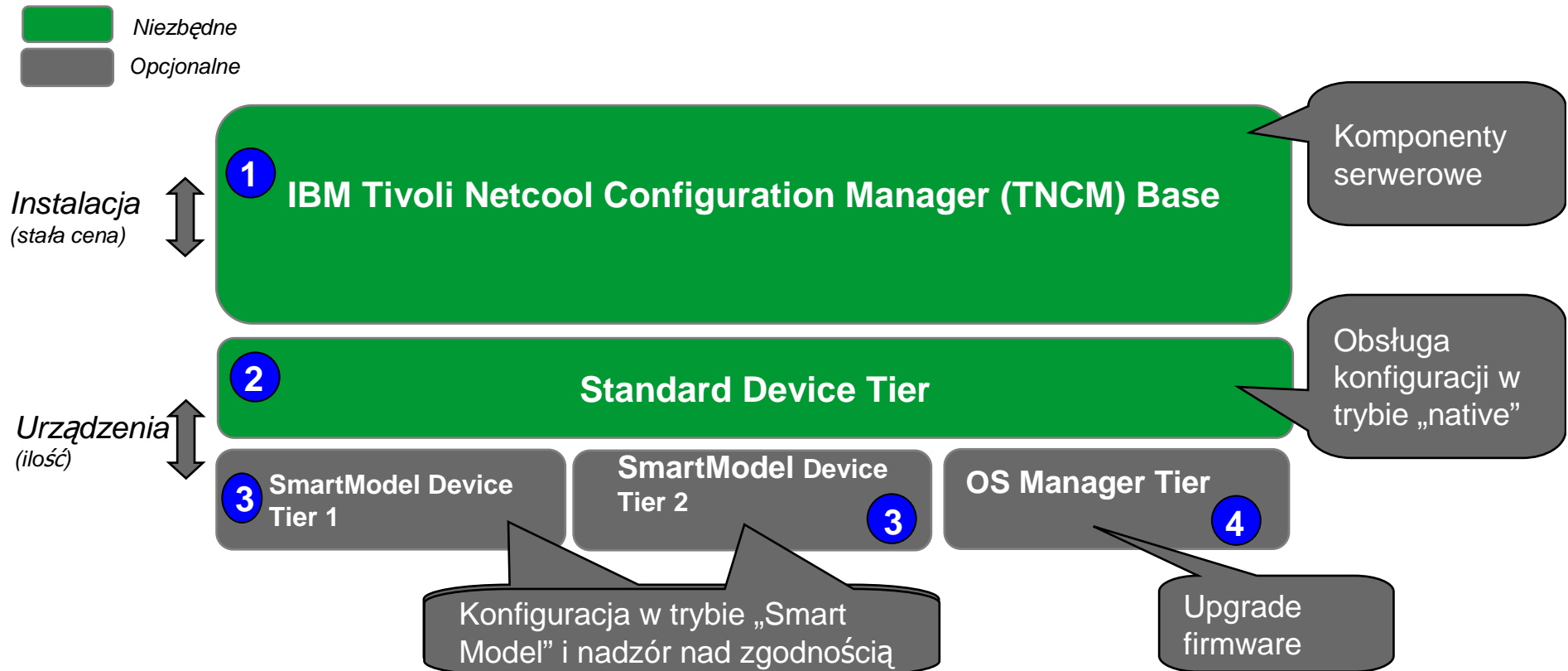
Validation Summary



Name	Weight	Passed	Failed	Exempt	Not Assessed	Score
3.1.20 disable AUX	25	0	4	0	0	0.0%
3.1.24 enable VTY password	25	0	4	0	0	0.0%
3.1.21 enable VTY login authentication default	25	4	0	0	0	100.0%
3.1.17 enable VTY transport telnet	25	0	4	0	0	0.0%
3.1.18 enable VTY exec timeout on lines	25	0	4	0	0	0.0%
3.1.28 enable VTY access class	25	0	4	0	0	0.0%
3.1.25 enable a local enable password	25	2	2	0	0	50.0%



TNCM: sposób licencjonowania





Tivoli Netcool Configuration Manager – Sprawdzony w akcji, dostępny już dziś dla Ciebie!

