



Zwiększanie bezpieczeństwa usług sieciowych poprzez wirtualizację systemu operacyjnego

Ireneusz Tarnowski

Wrocławskie Centrum Sieciowo-Superkomputerowe
Poznań, 5 listopada 2009

Plan wystąpienia



Co to jest wirtualizacja?

Motywacja ... czyli po co wirtualizować?

Wykorzystanie wirtualizacji

Kontenery systemu operacyjnego

Kontener vs. system rzeczywisty

Nasza rzeczywistość

- konsolidacja zasobów

- alokacja usług (poczta elektroniczna)

- alokacja usług (multihosting)

- HA usług w oparciu o kontener

Co to jest wirtualizacja



Jednym z najważniejszych kierunków rozwoju technologii serwerowych, mającym na celu optymalizację i racjonalizację infrastruktury jest obecnie wirtualizacja zasobów serwerowych. Dzięki takiemu podejściu na jednym fizycznym urządzeniu możliwa jest instalacja wielu w pełni funkcjonalnych, wirtualnych komputerów.

Wirtualizacja umożliwia efektywniejsze wykorzystanie istniejących zasobów sprzętowych środowiska informatycznego poprzez dowolne (w ramach możliwości sprzętowych, programowych oraz założeń projektowych) modyfikowanie cech wirtualizowanych zasobów, dostosowując je do wymagań użytkownika.

Po co wirtualizować?

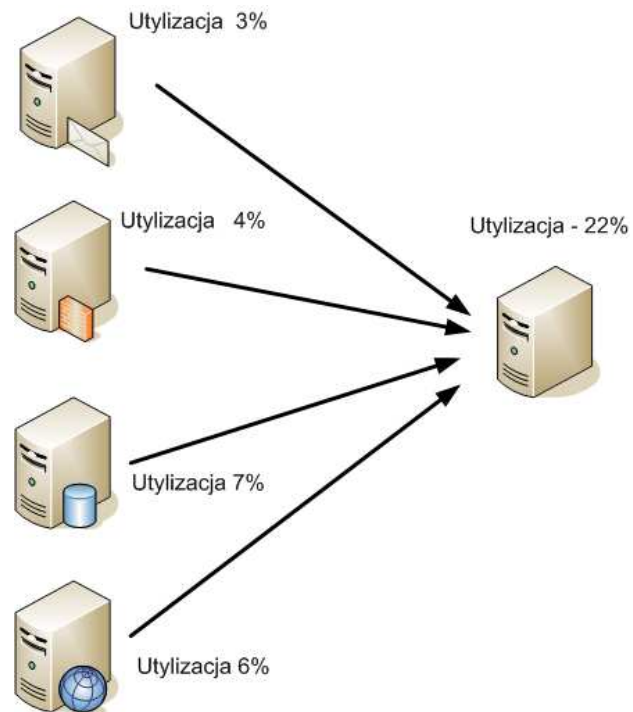


- ✓ większa utylizacja zasobów sprzętowych komputera (data center),
- ✓ redukcja kosztów infrastruktury informatycznej,
- ✓ uproszczenie procesu zmian oraz redukcja kosztów zarządzania,
- ✓ zwiększenie elastyczności - łatwiejsza możliwość wdrożeń i szybsza reakcja na zmiany w biznesie,
- ✓ podniesienie poziomu serwisu,
- ✓ zwiększona niezawodność - między innymi dzięki wspólnej polityce bezpieczeństwa,
- ✓ zwiększenie bezpieczeństwa
- ✓ oszczędność energii i miejsca

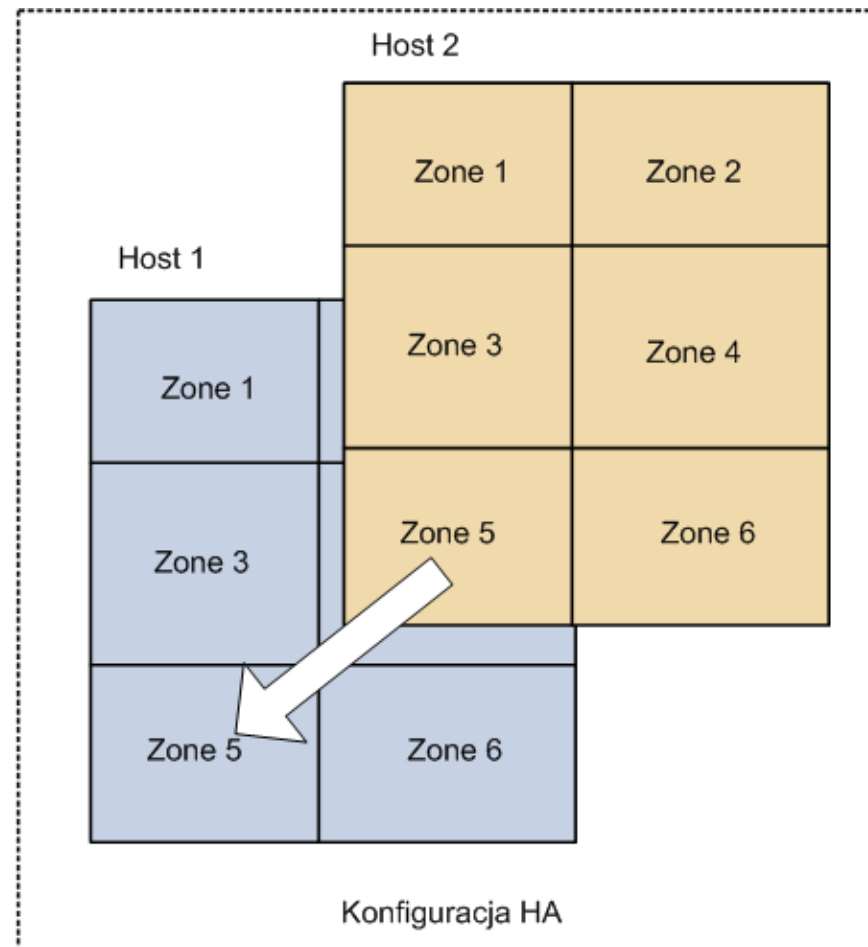
Wykorzystanie wirtualizacji (1)



Konsolidacja



Dynamiczna alokacja



Wykorzystanie wirtualizacji (2)



2 aspekty: konsolidacja vs. alokacja

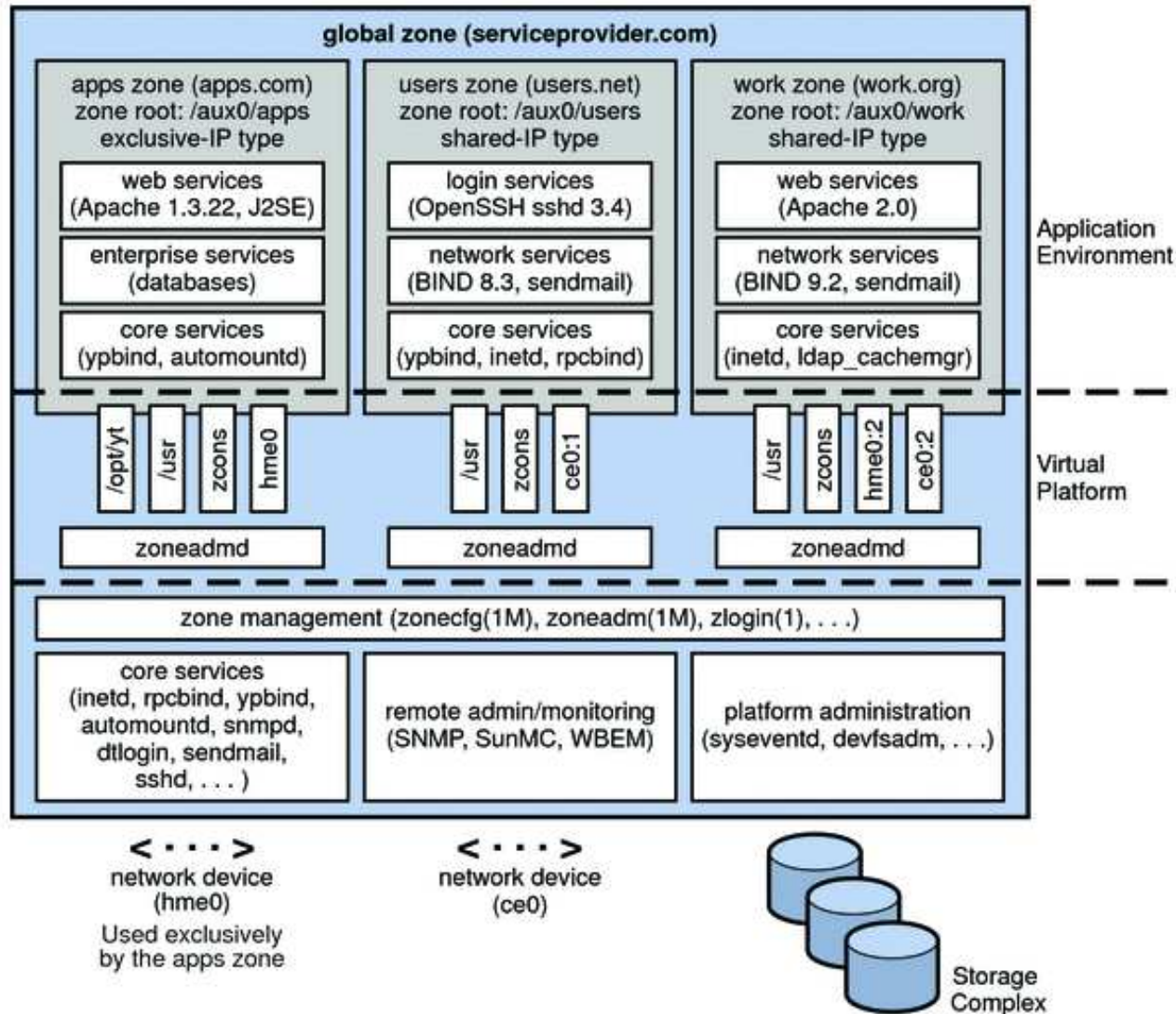
zwiększenie bezpieczeństwa:

- separacja usług
- separacja użytkowników
- separacja zasobów

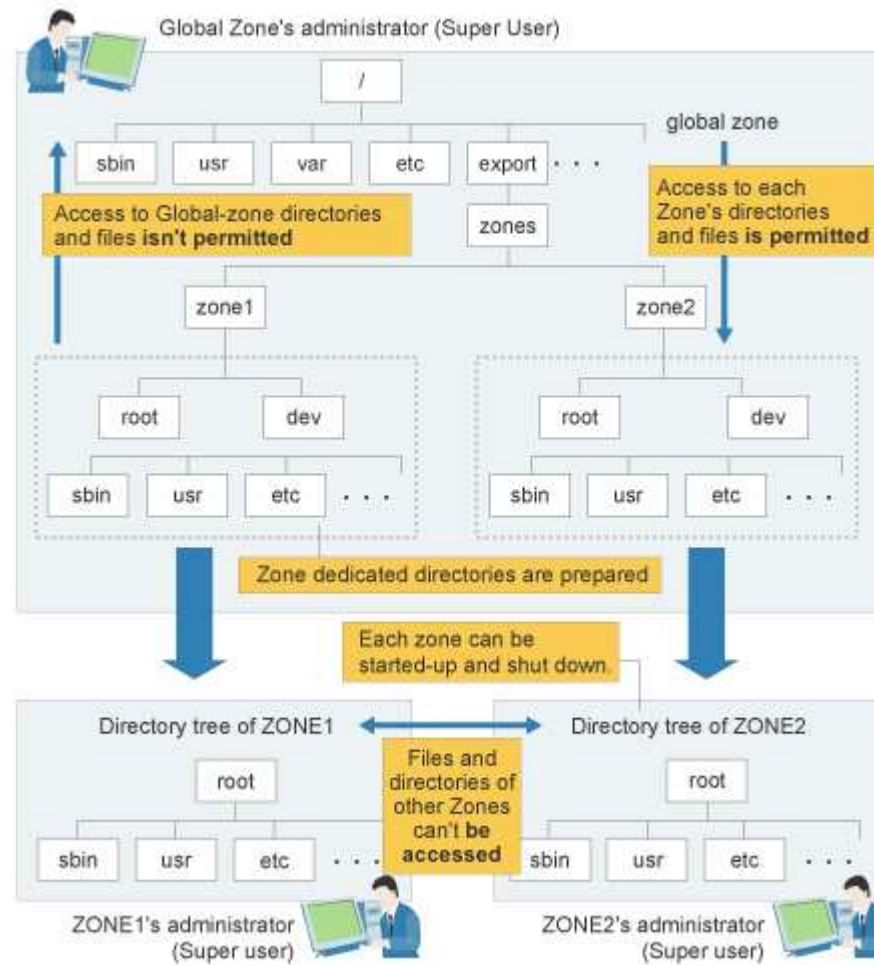
zwiększenie niezawodności:

- przyspieszenie procesu odtwarzania systemu lub danych
- ułatwienie procesu archiwizacji

Kontenery OS – idea (1)



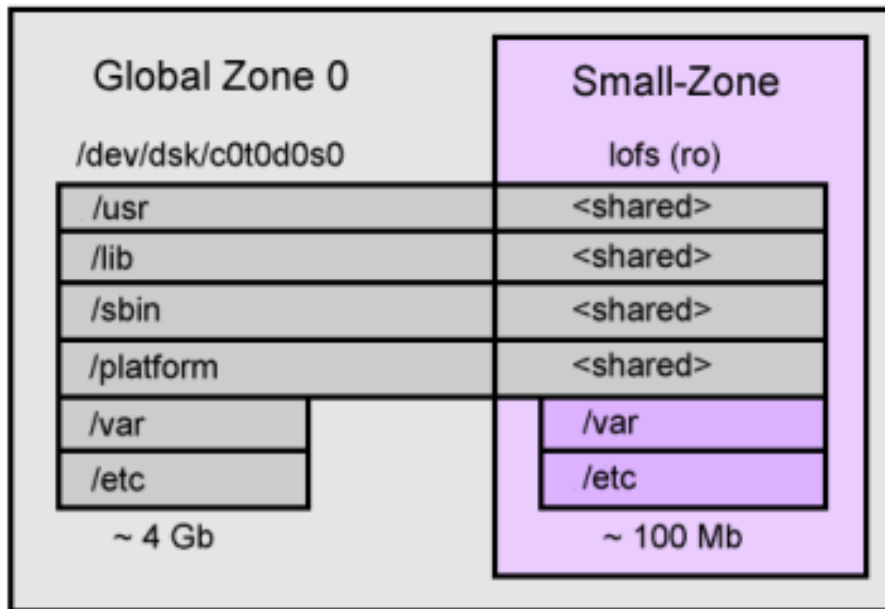
Kontenery OS – idea (2)



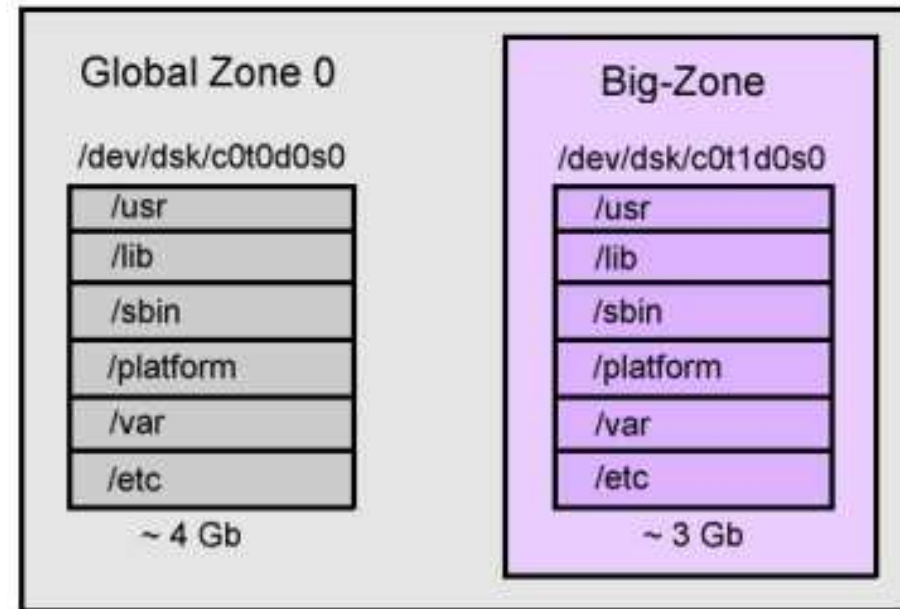
Kontenery OS – idea (3)



Kontener współdzielony



Kontener samodzielny



Kontenery OS – podstawowe cechy



Separowalność (procesów, użytkowników)

Zarządzanie zasobami (pamięć, procesor)

Rozdzielony stos IP

Uruchamianie innych systemów wewnątrz zony (BrandZ)

Rzeczywisty OS, a kontener OS



Z punktu widzenia administratora kontenera różnica bywa niedostrzegalna

Przy niektórych konfiguracjach można spostrzec ograniczenie uprawnień:
do plików,
do funkcji systemowych,
do konfiguracji (np. IPF),

Brak możliwości zarządzania na niskim poziomie (poweroff)

Brak plików mających bezpośredni wpływ na kernel (/etc/system ... istotne np. dla DB ORACLE)

Planowanie



Jaki jest cel wirtualizacji?

Jakie usługi będą uruchamiane w zonie?

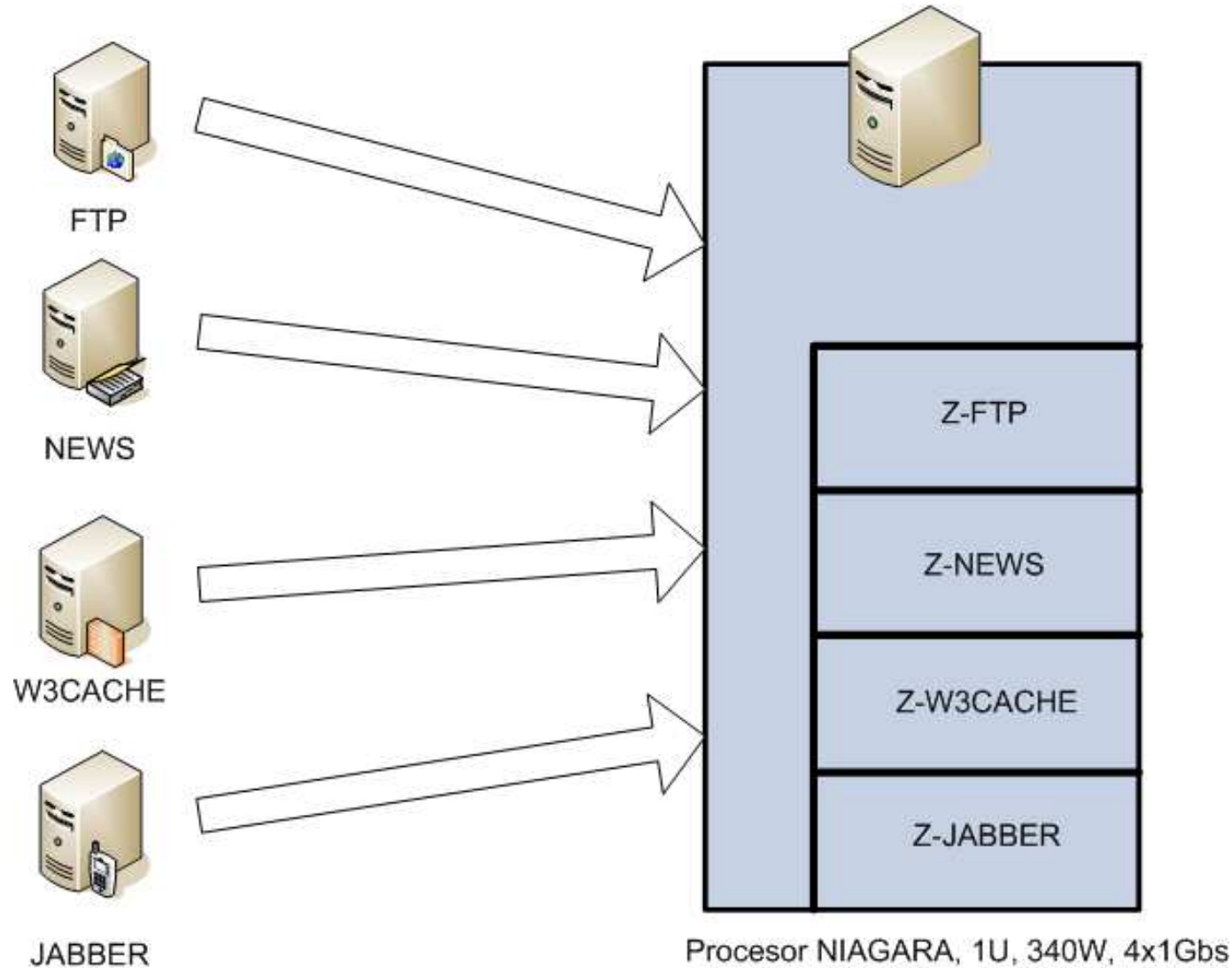
Kto (użytkownicy) będzie pracować w zonie?

Jaki poziom bezpieczeństwa zapewnić?

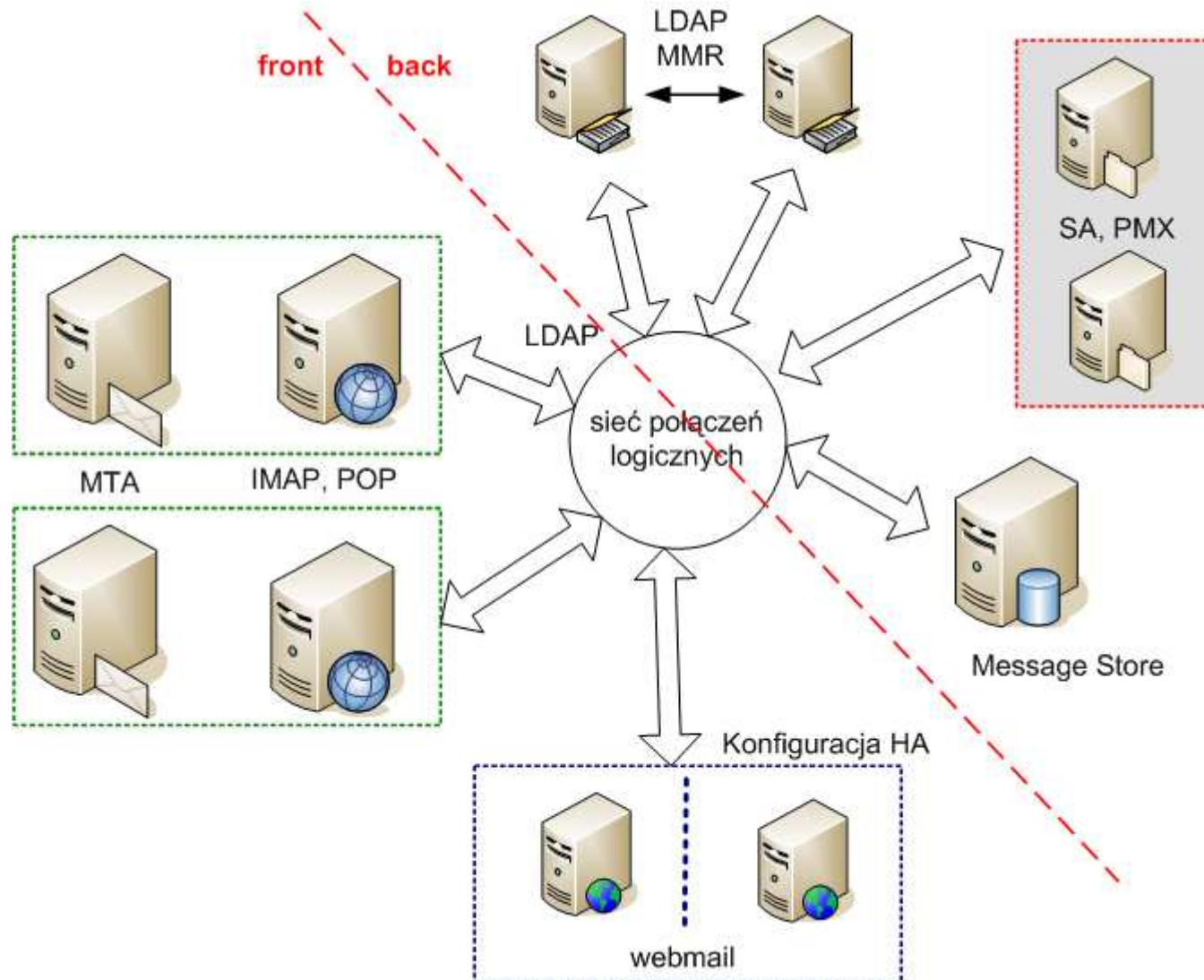
Jakie narzędzia i biblioteki zapewnić?

Jaką ilość zasobów (pamięć, procesor, sieć) zapewnić?

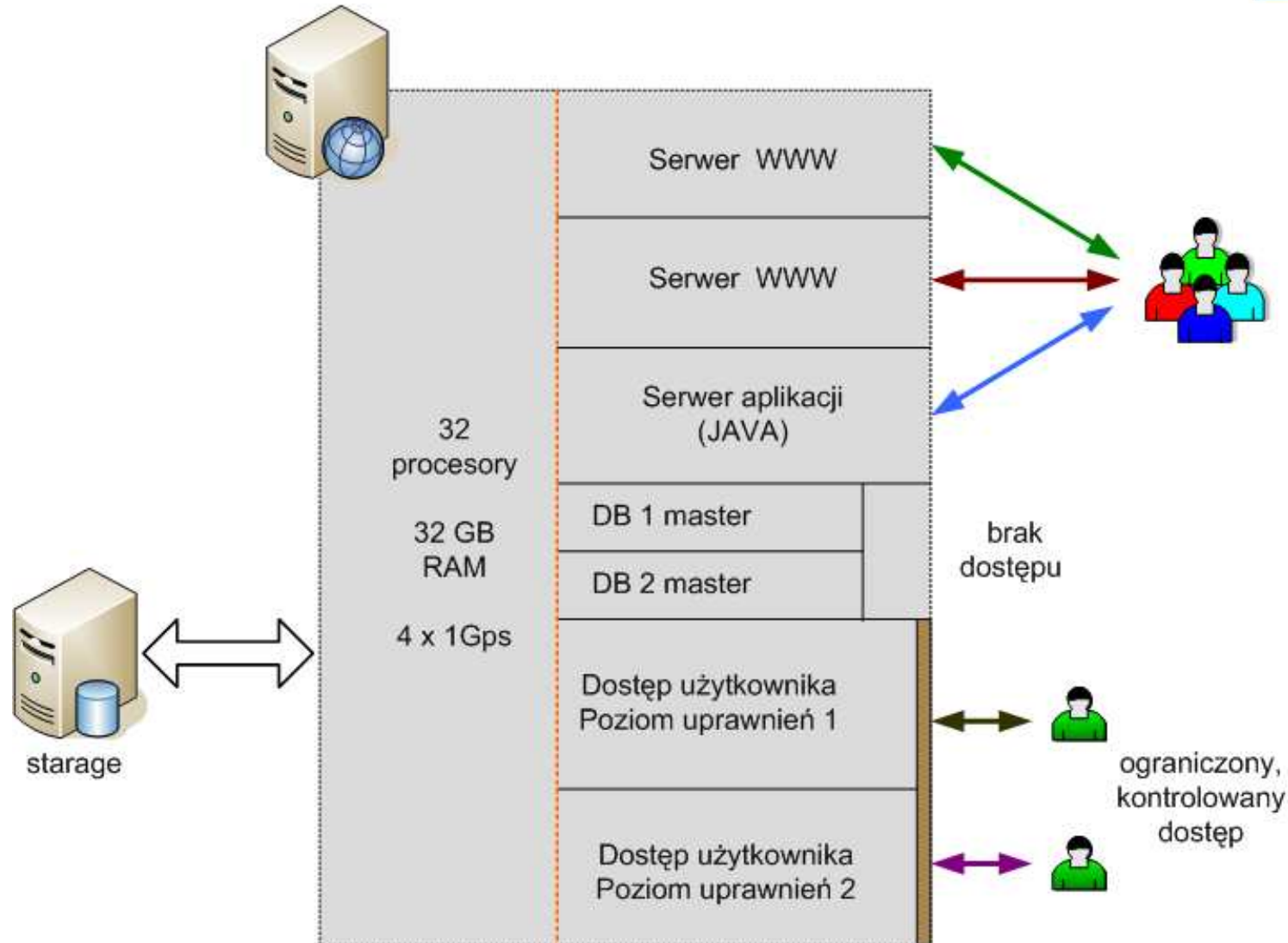
Nasza rzeczywistość - konsolidacja



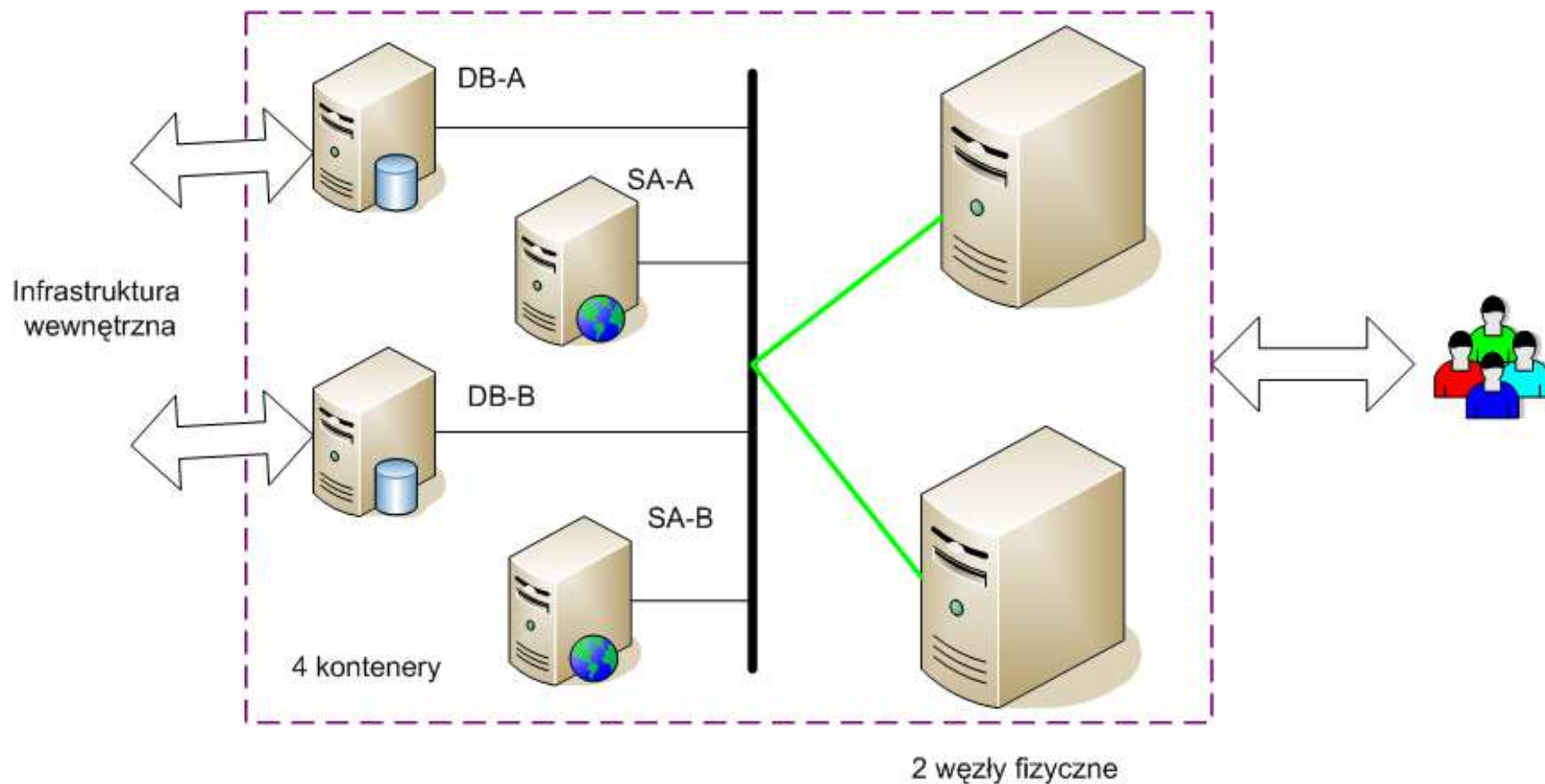
Nasza rzeczywistość - alokacja (poczta)



Nasza rzeczywistość - alokacja (WWW)



Nasza rzeczywistość – HA usług



Podsumowanie - pytania otwarte ...



Idea ...

Zagadnienia techniczne ...

Niebezpieczeństwa ...

Inne rozwiązania



Zwiększanie bezpieczeństwa usług sieciowych poprzez wirtualizację systemu operacyjnego

Ireneusz Tarnowski

Wrocławskie Centrum Sieciowo-Superkomputerowe
Poznań, 5 listopada 2009