

Załącznik 1 do OPZ



Szczegółowy Opis Techniczny Systemu C2.6 – Tom 4. Architektura techniczna - Warstwa fizyczna systemów i baz danych



UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ
ROZWOJU REGIONALNEGO



*Projekt: Informatyczny system ochrony kraju przed nadzwyczajnymi zagrożeniami
Nr Projektu: POIG.07.01.00-00-025/09*

Pakiet C2.6		
	Szczegółowy Opis Techniczny Systemu	

Szczegółowy Opis Techniczny Systemu

Tom 4

Architektura techniczna

Warstwa fizyczna systemów i baz danych

C2.6. Wdrożenie systemu weryfikacji jakości pomiarów H-M i prognoz hydrologicznych, rozszerzenie funkcjonalności Systemu Obsługi Klienta (SOK) i wdrożenie Centralnej Bazy Danych Historycznych.

Metryka dokumentu

Nazwa projektu:	Pakiet C2.6.		
Numer wersji dokumentu:	1.60	Data wersji dokumentu:	2012-06-12
Metoda kontroli jakości:	Przegląd	Data sprawdzenia:	2012-06-12
Opracował (a):	Zespół projektowy Dostawcy		
Sprawdził (a):	Maciej Skalski		

Historia zmian dokumentu

Nr wersji	Data wersji	Zmiany wprowadził (a)	Opis
1.00	2012-04-26	Zespół Projektowy Dostawcy	Utworzenie dokumentu.
1.10	2012-05-11	Zespół Projektowy Zamawiającego	Uwagi i edycja w trybie rejestracji zmian do wersji 1.00.
1.20	2012-05-18	Zespół Projektowy Dostawcy	Uwzględnienie wybranych uwag zgłoszonych przez Zamawiającego w wersji 1.10.
1.30	2012-04-26	Zespół Projektowy Zamawiającego	Uwagi i edycja w trybie rejestracji zmian do wersji 1.20.
1.40	2012-06-01	Zespół Projektowy Dostawcy	Uwzględnienie wybranych uwag zgłoszonych przez Zamawiającego w wersji 1.30.
1.50	2012-06-05	Zespół Projektowy Zamawiającego	Uwagi i edycja w trybie rejestracji zmian do wersji 1.40.
1.60	2012-06-12	Zespół Projektowy Dostawcy	Wprowadzenie modyfikacji określonych w protokole odbioru warunkowego.

Spis treści

Spis treści.....	2
1 Opis dokumentu	4
1.1 Cel dokumentu	4
1.2 Organizacja dokumentu	4
2 Architektura systemu	5
2.1 Modele logiczne warstwy fizycznej	5
2.1.1 Serwery kasetowe	6
2.1.2 Węzeł bazodanowy	6
2.1.3 System kopii zapasowych	7
2.1.4 Sieciowa pamięć masowa	7
2.1.5 Infrastruktura sieciowa	8



2.2	Modele logiczne warstwy systemów operacyjnych i baz danych	11
2.2.1	Model logiczny systemów operacyjnych	11
2.2.2	Model logiczny systemu składowania danych	13
2.2.3	Model logiczny systemu kopii zapasowych.....	14

1 Opis dokumentu

1.1 Cel dokumentu

Celem dokumentu jest prezentacja architektury technicznej systemu C2.6 na poziomie warstwy fizycznej systemów i baz danych. Opis obejmuje infrastrukturę całego systemu na ogólnym poziomie szczegółowości. W kolejnym etapie – zgodnie z harmonogramem projektu – będzie utworzony szczegółowy projekt implementacji infrastruktury sprzętowej oraz Standard Software.

1.2 Organizacja dokumentu

Rozdział 2.1 opisuje następujące komponenty infrastruktury fizycznej systemu C2.6:

- Serwery kasetowe
- Węzeł bazodanowy
- System kopii zapasowej
- Sieciowa pamięć masowa
- Infrastruktura sieciowa

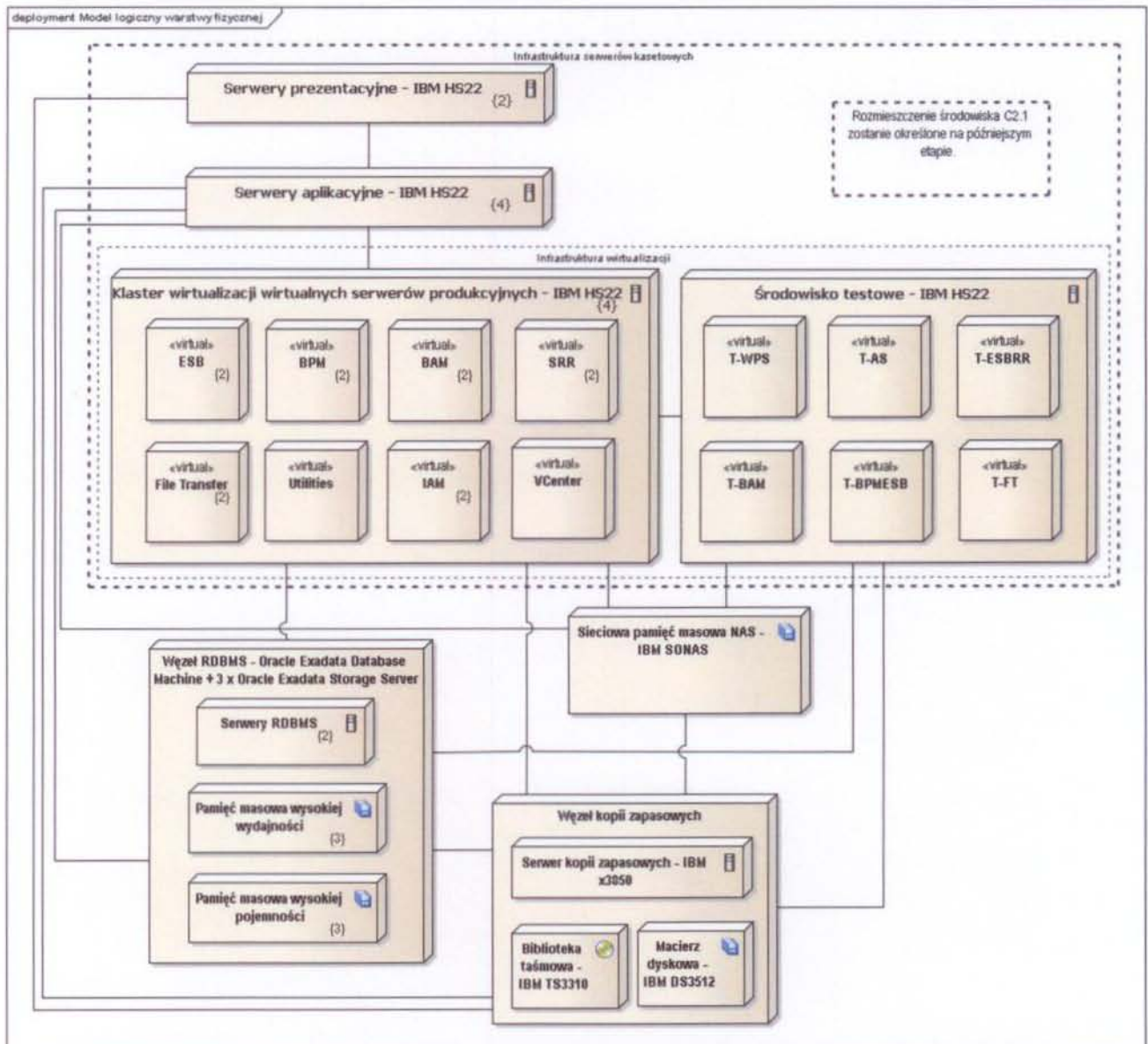
Rozdział 2.2 przedstawia modele logiczne rozmieszczenia systemów operacyjnych, systemu składowania danych oraz systemu kopii zapasowych systemu C2.6.

Liczby w nawiasach klamrowych umieszczone na rysunkach, np. {2} oznaczają liczbę wystąpień danego komponentu. Jeśli komponent występuje pojedynczo, nie jest dodatkowo oznaczany.

2 Architektura systemu

2.1 Modele logiczne warstwy fizycznej

Poniższy rysunek przedstawia model logiczny warstwy fizycznej środowiska produkcyjnego i testowego z pominięciem topologii sieci. Rozmieszczenie środowiska C2.1 zostanie określone na późniejszym etapie.



Rysunek 1. Model logiczny warstwy fizycznej.

2.1.1 Serwery kasetowe

Wszystkie systemy aplikacyjne zostaną zainstalowane na serwerach kasetowych (blade) zamontowanych w dedykowanej obudowie. Obudowa integruje ze sobą poszczególne elementy infrastruktury: serwery, przestrzeń dyskową, sieć, I/O i oprogramowanie zarządzające, umożliwiając budowę w pełni elastycznej infrastruktury IT. Obudowa zapewni również redundancję wszystkich kluczowych elementów eliminując pojedynczy punkt awarii.

Obudowa zastosowana w tym rozwiązaniu będzie zawierać:

- 11 serwerów kasetowych,
- napęd DVD +/-RW dostępny dla wszystkich serwerów,
- redundantną parę modułów przełączników 1Gb Ethernet,
- redundantną parę modułów przełączników 10Gb Ethernet,
- redundantną parę modułów zarządzających.

Karty zarządzające obudową posiadają wbudowanego agenta SNMP umożliwiającego pobieranie informacji o urządzeniu oraz wysyłanie komunikatów trap, dzięki czemu możliwy będzie monitoring.

Odbiorcą komunikatów SNMP będzie system, który jest własnością IMGW: HP Operations.

Na dwóch serwerach kasetowych zostaną zainstalowane serwery WWW. Utworzą one klaster serwerów prezentacyjnych.

Następne cztery serwery kasetowe zostaną przeznaczone na zainstalowane w klastrze serwery aplikacyjne.

Kolejne cztery serwery będą działały jako klaster wirtualizacji i na nich uruchomione zostaną serwery wirtualne na potrzeby platformy integracyjnej i usług dodatkowych.

Ostatni serwer kasetowy zostanie również użyty jako host wirtualny i wykorzystany zostanie do obsługi środowiska testowego.

W zależności od rodzaju produktów dostarczonych przez pakiet C2.1 zostaną one zainstalowane na serwerach aplikacyjnych lub produkcyjnym klastrze wirtualizacji. Na potrzeby C2.1 zostanie zarezerwowanych 8 rdzeni w serwerach kasetowych.

Repozytorium plików wszystkich komponentów systemu znajdzie się na wielkoskalowym systemie sieciowej pamięci masowej (NAS).

2.1.2 Węzeł bazodanowy

Bazy danych środowiska produkcyjnego oraz baza danych środowiska testowego zostaną zainstalowane na rozwiązaniu Oracle Exadata Database Machine składającym się z dwóch serwerów bazodanowych pracujących w klastrze oraz korzystając będą z dwóch zestawów pamięci masowej (każdy składający się z trzech serwerów fizycznych):

- pamięć masowa o wysokiej pojemności (Exadata Storage Server High Capacity) – przeznaczona do obsługi bazy CBDH
- pamięć masowa o wysokiej wydajności (Exadata Storage Server High Performance) – przeznaczona do obsługi bazy CBDO.

Oracle Exadata Database Machine posiada agenta SNMP umożliwiającego monitoring.

Odbiorcą komunikatów SNMP będą systemy, które są własnością IMGW: HP Operations i 'HP Network Node Manager i'.

Bazy danych Oracle będą monitorowane za pomocą Oracle Enterprise Manager Console.

2.1.3 System kopii zapasowych

Do obsługi systemu kopii zapasowych przeznaczony zostanie dedykowany serwer. Serwer kopii zapasowych podłączony będzie poprzez redundantne połączenia FC z zewnętrzną macierzą dyskową, na której składowana będzie baza danych oprogramowania kopii zapasowych. Kopie zapasowe składowane będą w bibliotece taśmowej połączonej z serwerem przez redundantne połączenia FC.

Komponenty systemu kopii zapasowych (karta zarządzająca serwerem, system operacyjny serwera, biblioteka taśmowa, przełączniki Fibre Channel) posiadają agentów SNMP umożliwiających monitoring.

Odbiorcą komunikatów SNMP będą systemy, które są własnością IMGW: HP Operations i 'HP Network Node Manager i'.

2.1.4 Sieciowa pamięć masowa

Repozytoria plików wszystkich systemów włączając pliki z CBDO i CBDH, będą składowane w wielkoskalowym systemie NAS.

Zastosowany będzie wysoko wydajny, globalnie klastrowalny systemem NAS, zapewniający globalną ciągłość przestrzeni nazw, co umożliwi skalowanie infrastruktury pamięci masowej do dużych ilości danych dzięki architekturze GRID.

NAS zawiera klienta HSM (Hierarchical Storage Management) pozwalającego na niezauważalne migracje danych nie tylko w obrębie zasobów użytkowanych na zasobach NAS ale także na zewnętrzne nośniki oraz biblioteki taśmowe. HSM migruje dane z rzadko używanych plików do podsystemów kopii zapasowych. Przeniesione pliki są wciąż dostępne dla użytkowników lub aplikacji, a w razie potrzeby dane są automatycznie przywracane.

NAS zawiera także wbudowanego agenta SNMP umożliwiającego monitoring tego komponentu.

Odbiorcą komunikatów SNMP będzie system, który jest własnością IMGW: HP Operations.

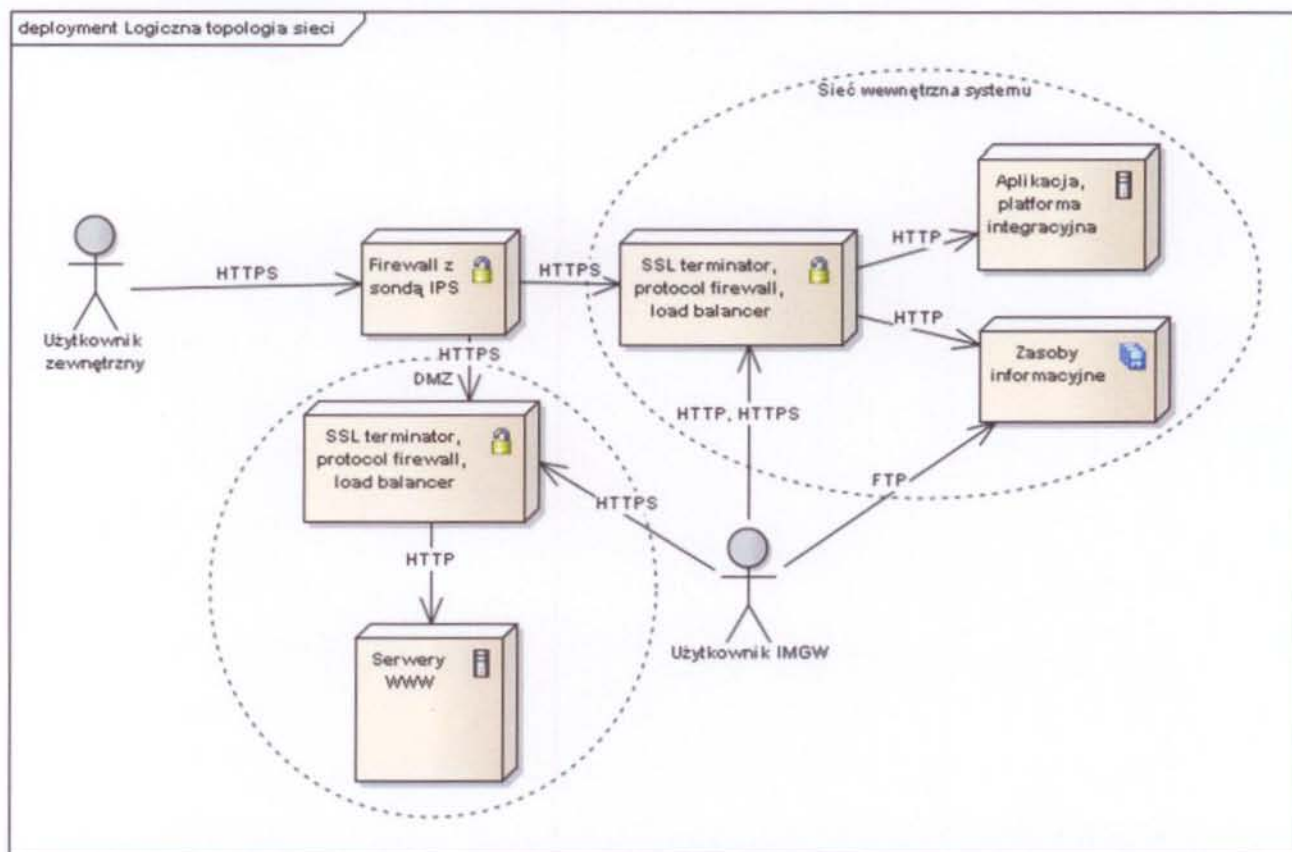
2.1.5 Infrastruktura sieciowa

Architektura infrastruktury sieciowej systemu zapewni następujące właściwości:

- łączność sieciową pomiędzy użytkownikami i serwerami,
- skalowalną wydajność,
- mechanizmy wysokiej dostępności i bezpieczeństwa.

Wszystkie urządzenia będą pracowały w funkcjonalnych parach w celu zapewnienia wysokich: dostępności, bezpieczeństwa oraz przepustowości. Analogicznie wszystkie elementy modelu logicznego warstwy fizycznej (Rysunek nr 2) będą komunikowały się ze sobą za pomocą szybkiej sieci LAN o prędkości 10Gb/s.

Poniższy rysunek przedstawia topologię logicznych komponentów sieci.



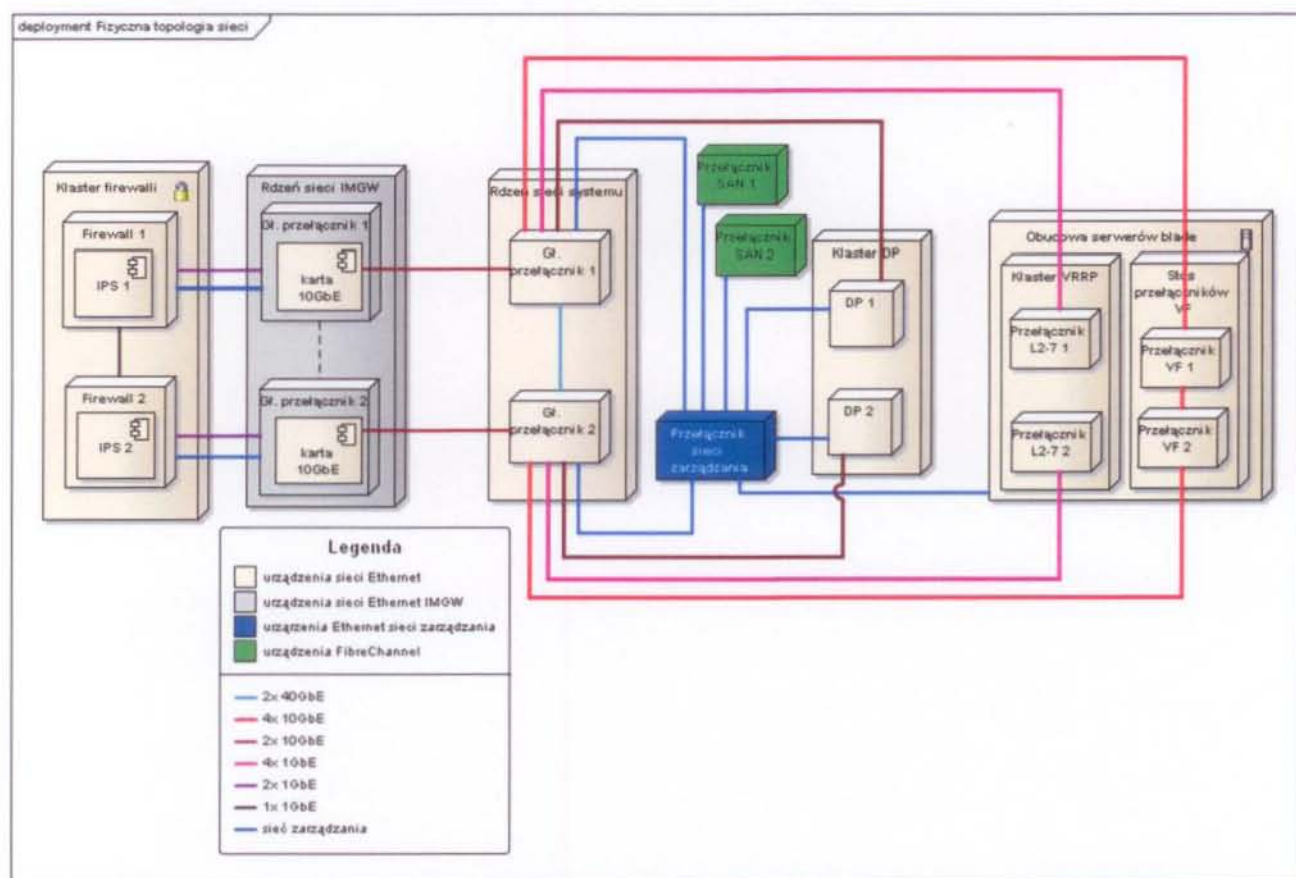
Rysunek 2. Logiczna topologia sieci.

Sekcja firewalla z sondą IPS będzie odpowiedzialna za mechanizmy bezpieczeństwa: filtrowanie ruchu sieciowego i wykrywanie ataków. Firewall będzie dzielił sieć na strefy. Sonda IPS da możliwość inspekcji wszystkich pakietów z danymi przesyłanych do i z serwerów i sprawdzenia zawartości pakietów pod kątem typowych ataków.

Kolejna sekcja będzie odpowiedzialna za kontrolę i dystrybucję ruchu sieciowego do i z serwerów. Dodatkowo wszystkie połączenia SSL będą terminowane na tym urządzeniu w celu odciążenia serwerów od obciążającego procesory procesu szyfrowania. Ponieważ dane przesyłane od urządzenia do serwerów nie będą zaszyfrowane da to możliwość kontroli tych danych za pomocą zapory aplikacji WWW (web application firewall) w celu ochrony przed atakami typu cross-site scripting, SQL injection i atakami na dane XML. Komunikacja między serwerami C2.6 a serwerownią IMGW również będzie realizowane bez użycia protokołu SSL.

Każdy komponent architektury sieci będzie korzystał z sieci i usług dostarczanych przez główne przełączniki sieciowe. Wszystkie komponenty sieciowe będą fizycznie podłączone do pojedynczego, centralnego „urządzenia”, natomiast połączenia logiczne między komponentami w postaci podsieci będą tworzone w technologii wirtualnych sieci (VLAN), co pozwoli na elastyczne konfigurowanie sieci.

Poniższy rysunek przedstawia topologię fizycznych komponentów sieci.



Rysunek 3. Fizyczna topologia sieci.

Sieć lokalna systemu będzie bazowała na dwóch głównych przełącznikach 10/40Gb Ethernet. Przełączniki te będą oferowały przełączanie z pełną prędkością, filtrowanie i kolejkowanie ruchu. Przełączniki będą zawierały redundantne zasilacze, wentylatory oraz funkcje zapewniające wysoką dostępność. Przełączniki będą zgodne z CEE/DCB oraz będą obsługiwały ruch sieciowy w warstwach drugiej i trzeciej modelu sieci ISO/OSI.

Firewall systemu będzie oparty na klastrze dwóch urządzeń z zainstalowanymi sondami IPS. Firewall będzie filtrował ruch sieciowy w celu zablokowania nieuprawnionych połączeń. Sondy IPS będą analizować zawartość pakietów i chronić system przed znanymi atakami i wirusami.

Funkcje terminowania SSL, XML gateway i firewall oraz load balancingu będą realizowane przez klaster urządzeń DP (Data Power), które będą pracowały jako XML proxy i wykonywały sprawdzenia poprawności formatu i danych w dokumentach XML, kontroli dostępu (AAA), szyfrowania i podpisywania dokumentów XML lub wybranych pól w tych dokumentach, weryfikacji zgodności dokumentów z DTD, filtrowania XML oraz ochrony przed atakami. Poza funkcjami związanymi z przetwarzaniem XML urządzenia te będą terminowały połączenia SSL przy użyciu wbudowanych modułów HSM (Hardware Security Module).

Połączenie do sieci IMGW będzie bazowało na dwóch kartach liniowych z czterema portami 10 Gigabit Ethernet każda, które zostaną dostarczone w celu zainstalowania w głównych przełącznikach sieciowych IMGW.

Sieć SAN oparta będzie na parze przełączników FC.

Sieć zarządzania będzie oparta na wydzielonym przełączniku Gigabit Ethernet, do którego podłączone zostaną interfejsy zarządzania dostarczonych urządzeń.

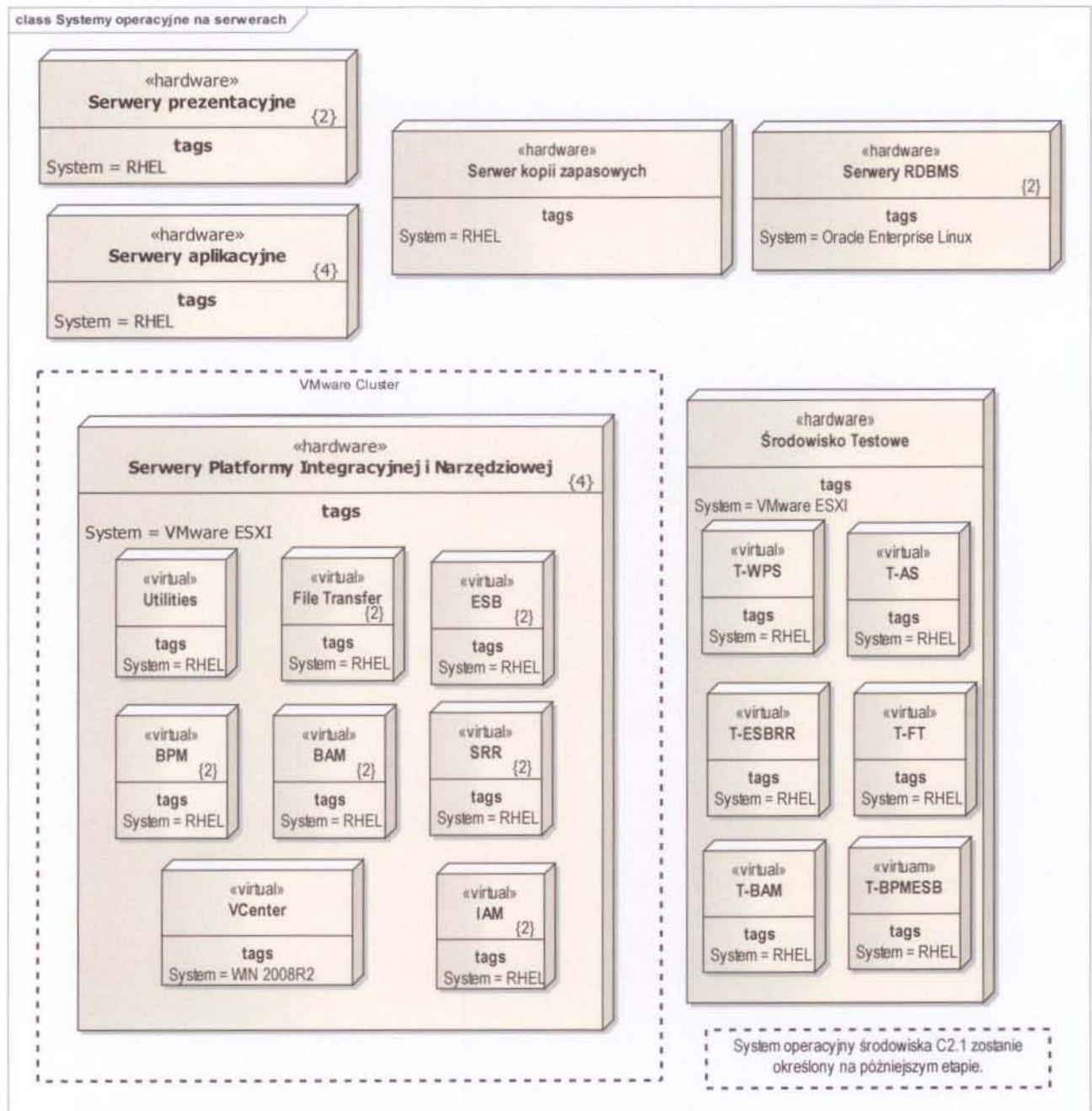
Wszystkie urządzenia sieciowe będą posiadały wbudowanego agenta SNMP umożliwiającego pobieranie informacji o urządzeniu oraz wysyłanie komunikatów trap, dzięki czemu możliwy będzie monitoring tych urządzeń.

Odbiorcą komunikatów SNMP będzie system, który jest własnością IMGW: 'HP Network Node Manager i'.

2.2 Modele logiczne warstwy systemów operacyjnych i baz danych

2.2.1 Model logiczny systemów operacyjnych

Poniższy rysunek przedstawia schemat wykorzystania systemów operacyjnych na środowiskach produkcyjnym i testowym. System operacyjny środowiska C2.1 zostanie określony na późniejszym etapie.



Rysunek 4. Systemy operacyjne na serwerach.

Na sześciu serwerach kasetowych, wchodzących w skład środowiska aplikacyjnego (czyli 2 serwery prezentacyjne i 4 serwery aplikacyjne) zainstalowany będzie system operacyjny Red Hat Enterprise Linux Server.

Informacje na temat zwymiarowania architektury zostaną przedstawione w ramach PROD-3. Jako dane wejściowe do wymiarowania zostaną uwzględnione wymagania z rejestru wymagań DSTD, wymagania z Technical Requirements, założenia przyjęte w ofercie, dane techniczne dotyczące zastosowanego sprzętu i oprogramowania, pozostałe zapisy DSTD.

Cztery serwery kasetowe będą użyte jako hosty wirtualizacji, pracujące jako klaster wirtualizacji, pod kontrolą oprogramowania VMware vSphere Enterprise Edition (zawierającego funkcje zapewniające wysoką dostępność i vMotion). Obsługiwać będą środowisko produkcyjne.

VMware HA nieprzerwanie monitoruje stan wszystkich serwerów fizycznych w ramach zdefiniowanych grup serwerów i w przypadku awarii jednego z nich restartuje jego maszyny wirtualne na pozostałych działających serwerach.

Natomiast VMware vMotion pozwala zapisać aktualny stan maszyny wirtualnej w postaci kilku plików udostępnionych na współdzielonych zasobach dyskowych (np. na macierzy). Jednocześnie dostęp do plików posiadają zarówno wirtualny serwer źródłowy, jak i docelowy, który w razie potrzeby przejmie rolę podstawowego po migracji. Dzięki temu, że w środowisku serwera ESX zwirtualizowana jest również sieć, po migracji serwer wirtualny utrzymuje parametry, adresację i konfigurację serwera migrowanego. Technologia ta pozwala przeprowadzać migrację serwerów wirtualnych pomiędzy maszynami fizycznymi bez najmniejszego przestoju.

Wszystkie serwery wirtualne środowiska produkcyjnego, poza VMware vCenter Management Server, pracować będą pod kontrolą systemu operacyjnego Red Hat Linux Enterprise Server. VMware vCenter wymaga systemu operacyjnego Windows Server 2008 R2 dlatego też serwer, na którym będzie zainstalowane vCenter pracować będzie pod kontrolą właśnie tego systemu. Ostatni serwer kasetowy posłuży za hosta dla stworzenia wirtualnego środowiska testowego, również w oparciu o oprogramowanie VMware. Wszystkie serwery wirtualne pracujące na tym środowisku korzystać będą z systemu Red Hat Linux Enterprise Server. Serwer kopii zapasowych również będzie mieć zainstalowany system operacyjny Red Hat Linux Enterprise Server.

Wymienione systemy operacyjne oraz hipernadzorcy (ang. hipervisor) posiadają oprogramowanie agenta SNMP. Agent SNMP umożliwia pobieranie informacji o urządzeniu oraz wysyłanie komunikatów trap, dzięki czemu możliwy będzie monitoring tych urządzeń. Odbiorcą komunikatów SNMP będzie system, który jest własnością IMGW: HP Operations.

Na serwerach platformy integracyjnej i narzędziowej zostaną zainstalowane następujące komponenty oprogramowania integracyjnego:

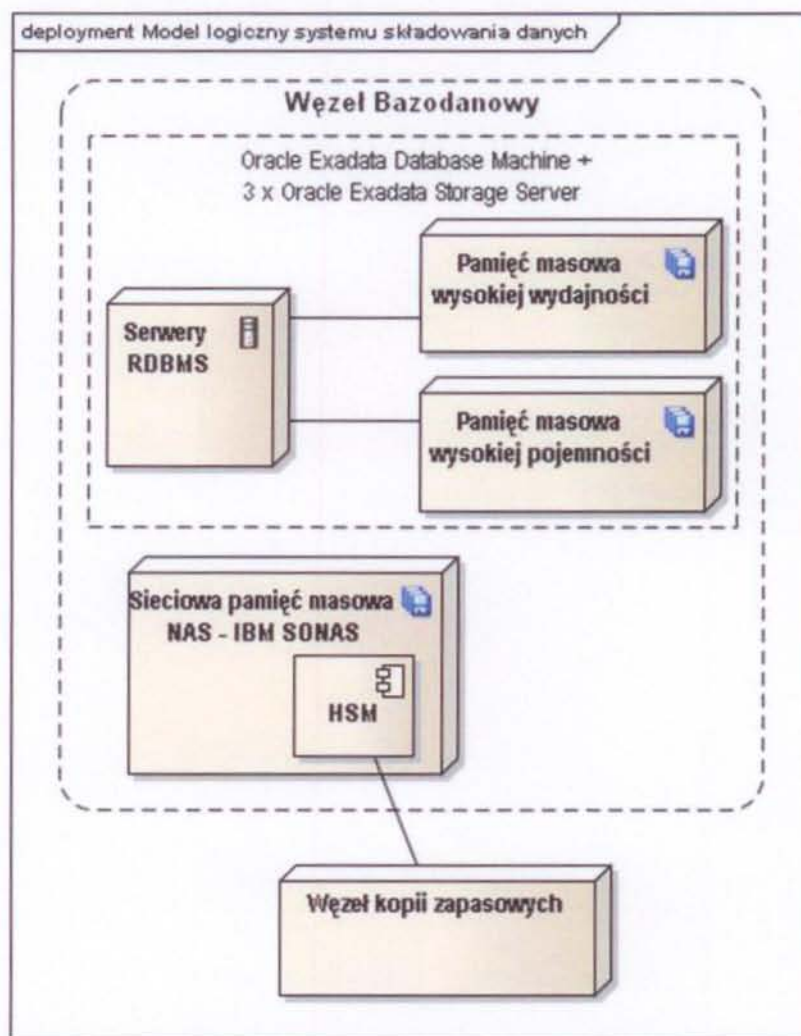
- IBM WebSphere Enterprise Service Bus,
- IBM WebSphere Enterprise Service Bus Registry Edition,
- IBM Process Server Advanced,
- IBM Tivoli Federated Identity Manager,
- IBM WebSphere MQ File Transfer Edition,

- IBM WebSphere Business Monitor.

Na serwerach aplikacyjnych zostanie zainstalowany JBoss Enterprise Application Platform.

2.2.2 Model logiczny systemu składowania danych

Poniższy rysunek przedstawia topologię systemu składowania danych.



Rysunek 5. Model logiczny systemu składowania danych.

Część relacyjna danych przechowywana będzie w bazach danych Oracle Database Enterprise Edition zainstalowanych na rozwiązaniu Oracle Exadata Database Machine składającym się z serwerów bazodanowych oraz serwerów pamięci masowej.

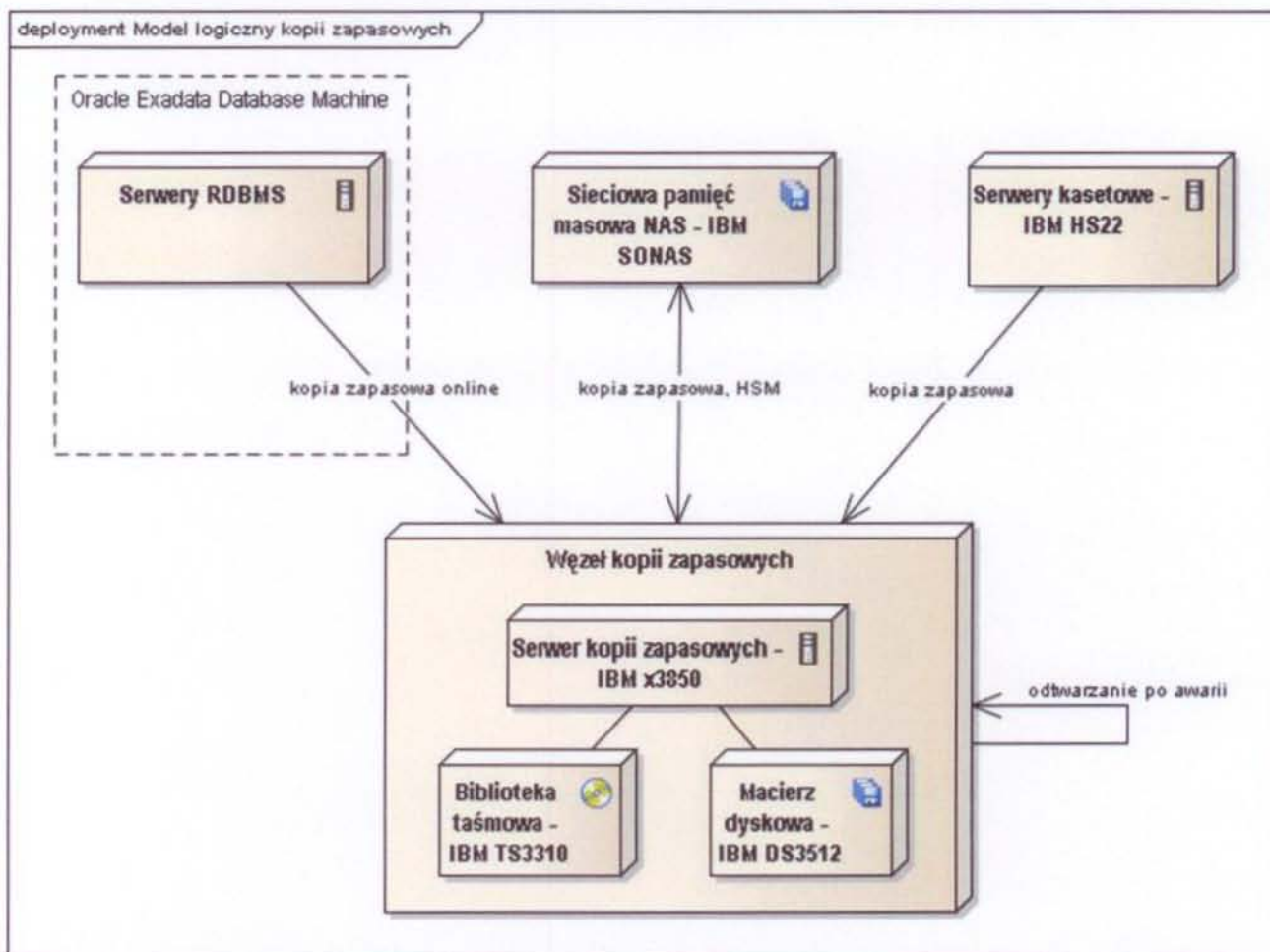
Serwery bazodanowe pracować będą pod kontrolą systemu operacyjnego Oracle Enterprise Linux, zainstalowanego i prekonfigurowanego fabrycznie.

Instancje baz danych pracować będą na dwóch serwerach bazodanowych skonfigurowanych do pracy w klastrze Oracle Real Application Clusters.

Część plikowa baz danych przechowywana będzie na urządzeniu sieciowej pamięci masowej (NAS). Część plikowa korzystać będzie z mechanizmu HSM (Hierarchical Storage Management) w celu zapewnienia optymalnego zagospodarowania dostępnych nośników danych.

2.2.3 Model logiczny systemu kopii zapasowych

Poniższy rysunek przedstawia schemat logiczny systemu kopii zapasowych.



Rysunek 6. Schemat systemu kopii zapasowych.

Węzeł kopii zapasowych składać się będzie z serwera kopii zapasowych połączonego siecią SAN z biblioteką taśmową oraz macierzą dyskową. Na macierzy dyskowej przechowywana będzie baza danych centralnego programu zarządzającego tworzeniem kopii zapasowych, natomiast same kopie zapasowe wykonywane będą na bibliotekę taśmową.

Serwer kopii zapasowych pracować będzie pod kontrolą Red Hat Enterprise Linux Server.

Kopie zapasowe wszystkich serwerów tworzone będą za pomocą oprogramowania klienckiego i za pośrednictwem serwera kopii zapasowych przesyłane będą na bibliotekę taśmową.

Na serwerach bazodanowych zainstalowane zostaną rozszerzenia do klienta kopii zapasowych, które umożliwią integrację z mechanizmami oprogramowania baz danych umożliwiającymi tworzenie kopii zapasowych bazy danych bez konieczności ich wyłączania (online backup).

Serwer kopii zapasowych będzie posiadał funkcje odtwarzania po awarii (disaster recovery).

Głównym oprogramowaniem przeznaczonym do realizacji funkcji tego węzła będzie IBM Tivoli Storage Manager.