

## Rozdział 3

# Budowa systemu e-matura



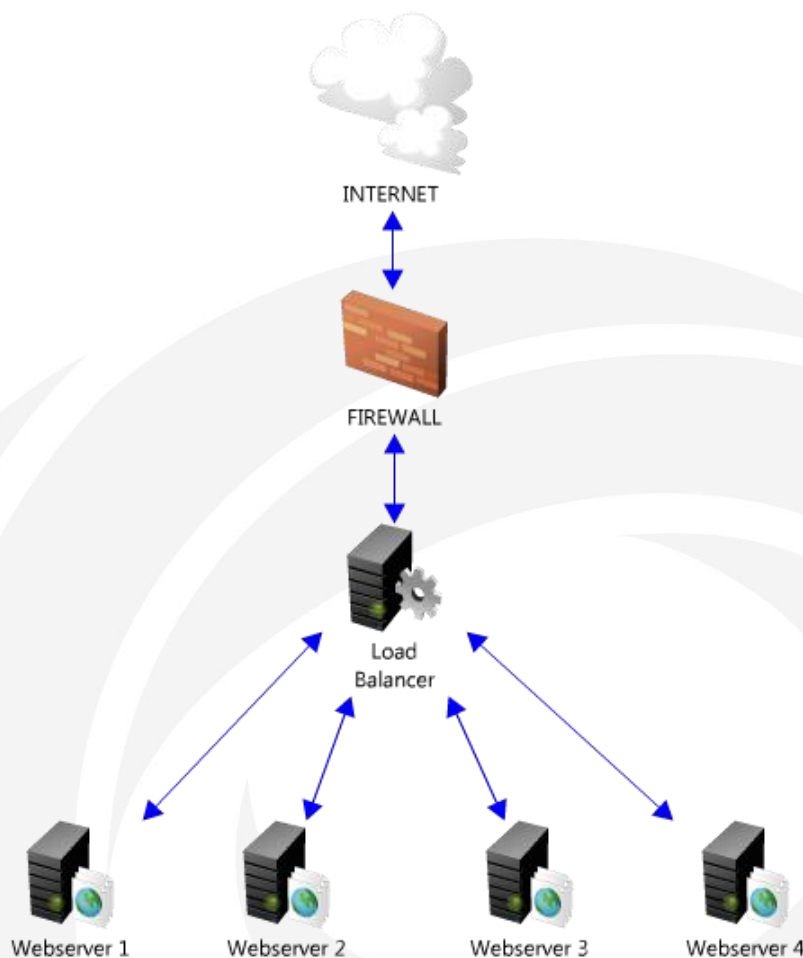
# Budowa systemu e-matura

Systemy informatyczne służące do egzaminowania na odległość muszą spełniać rygorystyczne wymagania dotyczące bezpieczeństwa i wysokiej dostępności zarówno od strony serwerów aplikacyjnych jak i serwerów baz danych. Aby sprostać tym wymaganiom w projekcie e-matura został wykorzystany cały wachlarz mechanizmów i funkcjonalności, które zapewniają wysoki poziom bezpieczeństwa danych. Niniejszy załącznik przedstawia listę mechanizmów zaimplementowanych w systemie e-matura.

## 1. Odpowiednie balansowanie ruchem

Jednym z podstawowych wyzwań, przed którymi stanęliśmy projektując system E-matura było zapewnienie wysokiej i nieprzerwanej dostępności egzaminu. Podczas pierwszej próby uruchomienia egzaminu udostępniliśmy nasz system około trzem tysiącom uczniów. Do tego celu wykorzystana została bardzo prosta architektura składająca się z jednego serwera aplikacyjnego i jednego serwera bazodanowego. Była to wtedy wystarczająca konfiguracja jednak nie jest ona wystarczająca, aby przeegzaminować wszystkich maturzystów w Polsce. W przypadku, w którym jednocześnie do jednego serwera może odwoływać się kilkaset tysięcy osób, każde połączenie do serwera musi mieć przydzieloną pewną liczbę pamięci oraz czasu procesora. Aby sprostać wymogowi wysokiej dostępności egzaminu zastosowano rozwiązanie opierające się o mechanizm zarządzania obciążeniem (ang. Load Balancing). Rozwiązanie to polega na zbudowaniu klastra serwerów, w którym można wyróżnić dwie zasadnicze części (serwer pełniący rolę Load Balancera oraz serwery aplikacyjne).

# Budowa systemu e-matura



*Rys. 1 Zasada działania Load Balancera*

Klasyczna aplikacja działająca w środowisku internetowym uruchamiana jest na pojedynczym serwerze www, który obsługuje cały ruch generowany przez zainstalowane na nim aplikacje. Rozwiązanie takie sprawdza się w większości przypadków, ponieważ średnia ilość osób korzystających w danym czasie z serwera www nie jest w stanie przeciążyć jego zasobów. W przypadku egzaminu, gdy jednocześnie do jednego serwera może odwoływać się kilkaset tysięcy osób, taka sytuacja jest niedopuszczalna ze względu na fakt, że każde połączenie do serwera musi mieć przydzieloną określoną wielkość pamięci oraz czasu procesora. Aby sprostać stawianym przed projektem e-matura wymagom zastosowany został mechanizm zarządzania obciążeniem (ang. Load Balancing). Rozwiązanie to polega na zbudowaniu klastra serwerów, w których można wyróżnić 2 zasadnicze części. Pierwszą część stanowi serwer stanowiący punkt dostępowy do egzaminu. Wszystkie połączenia kierowane są do tego serwera, jednak nie są one bezpośrednio obsługiwane, tylko

# Budowa systemu e-matura

przekazywane do serwerów aplikacyjnych w klastrze. Na podstawie wybranego algorytmu zarządzania obciążeniem serwer ten przekierowuje ruch do najmniej obciążonego serwera aplikacyjnego w klastrze. Rozwiązanie to jest w pełni skalowalne i pozwala na duże możliwości rozbudowy klastra – ograniczeniem szybko może stać się łącze sieciowe, po którym odbywa się komunikacja. Dodatkową cechą, jaką może spełniać ten serwer jest odkodowanie zaszyfrowanej wiadomości SSL i przekazywanie jej dalej w postaci odszyfrowanej, co powoduje zmniejszenie obciążenia serwerów docelowych, jednak przy dużej liczbie połączeń może spowodować przeciążenie serwera balansującego ruch.

Dzięki zastosowaniu technologii zarządzania obciążeniem projekt e-matura zyskał możliwość łatwej i szybkiej skalowalności. Zastosowanie klastra pozwala także na zapewnienie stałej dostępności aplikacji, ponieważ awaria któregośkolwiek z elementów klastra nie ma wpływu na działanie systemu, gdyż cała architektura jest redundantna i rolę uszkodzonego serwera automatycznie przejmuje inny serwer w strukturze.

## 2. Buforowanie danych pobieranych z bazy danych

Bardzo często dane pobierane z serwera bazodanowego do serwera aplikacji dublują się dla poszczególnych klientów. Przykładowo pytania egzaminacyjne dla danej grupy egzaminowanych są takie same. Możliwa jest więc optymalizacja procesu dostępu do bazy danych poprzez odpowiednie zbuforowanie danych po stronie serwera aplikacji. W systemie e-matura dane są pobierane tylko raz podczas pierwszego zapytania do aplikacji, a następnie przechowywane są w tablicy asocjacyjnej, w której klucz jednoznacznie identyfikujący buforowane dane. Przy każdej operacji pobierania danych sprawdzana jest ta tablica i gdy okaże się, że zostały one już zbuforowane, zapytanie do bazy danych może być zastąpione szybkim pobraniem danych z bufora. Ważnym jest, żeby przechowywane dane nie zajmowały zbyt dużo miejsca w pamięci operacyjnej komputera, gdyż może spowodować to jego spowolnienie lub unieruchomienie.

## 3. Ograniczona wielkość wymiany informacji /Kompresja wymienianych informacji/Stosowanie wydajnych protokołów komunikacyjnych

Ostatnim etapem optymalizacji wydajności aplikacji jest zmniejszenie do minimum ilości oraz wielkości wymienianych informacji. Nasz system realizuje ten cel poprzez

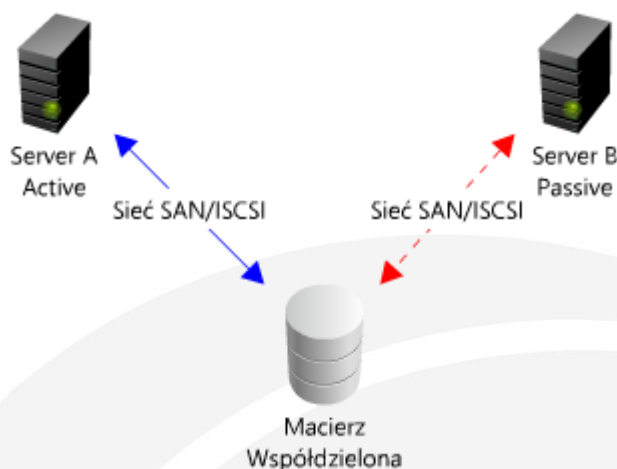
# Budowa systemu e-matura

zastosowanie kilku metod optymalizacyjnych. Wszystkie dane przesyłane pomiędzy klientem a serwerem kodowane są w postaci binarnej. W odróżnieniu od klasycznej implementacji protokołu SOAP, w którym dane przesyłane są w postaci zwykłego tekstu, to rozwiązanie pozwala na zmniejszenie rozmiaru wiadomości aż do 40% jej pierwotnego rozmiaru.

## 4. Budowa klastra wysokiej dostępności bazy danych

W celu zapewnienia wysokiej dostępności systemu egzaminacyjnego należy zadbać o serwery aplikacyjne, które serwują aplikację do użytkowników, a także o serwery bazodanowe, które są odpowiedzialne za przechowywanie danych. W projekcie e-matura serwery baz danych zostały połączone w klaster wysokiej dostępności zbudowany w oparciu o mechanizm Failover Clustering wbudowany w system operacyjny Windows Server 2008 R2. Infrastruktura sprzętowa obydwu serwerów bazodanowych jest identyczna i została zbudowana w oparciu o serwery IBM Blade Server. Serwery te zostały podłączone do współdzielonej macierzy dyskowej poprzez sieć SAN (ang. Storage Area Network). Klaster został skonfigurowany w trybie Active-Passive, co oznacza, że tylko jeden z węzłów klastra jest w danej chwili odpowiedzialny za obsługę połączeń od użytkowników, drugi węzeł jest cały czas w trybie gotowości. Jeśli wystąpią problemy z aktywnym węzłem klastra np. awaria sprzętowa, drugi węzeł automatycznie przejmuje jego rolę i rozpoczyna obsługę połączeń użytkowników. Ponieważ baza danych przechowywana jest na, współdzielonej dla obydwu serwerach, przestrzeni dyskowej nawet w przypadku awarii jednego z węzłów klastra nie następuje utrata danych i drugi węzeł pracuje od razu z takim samym zestawem danych, z jakim pracował pierwszy węzeł.

# Budowa systemu e-matura



Rys. 2 Macierz współdzielona

## 5. Zapewnienie bezpieczniej komunikacji

Aplikacja kliencka, uruchamiana na komputerze zdającego, komunikuje się z częścią serwerową poprzez usługę sieciową opartą o technologię Windows Communication Foundation w wersji 4.0. Technologia ta wykorzystując otwarte standardy takie jak HTTP oraz SOAP udostępnia funkcjonalność aplikacjom klienckim. W celu zapewnienia bezpiecznej komunikacji pomiędzy klientem a serwerem wykorzystano technologię SSL, która pozwoliła na zabezpieczenie systemu w dwóch płaszczyznach:

- Weryfikacja serwera aplikacji
- Szyfrowanie przesyłanych danych

Weryfikacja serwera opiera się na systemie certyfikatów, na podstawie których możliwa jest weryfikacja podmiotu identyfikującego się danym certyfikatem. Certyfikat wydawany jest przez centrum certyfikacji na wniosek osoby ubiegającej się o niego. Każdy certyfikat jest przypisany do konkretnej nazwy domeny internetowej, z którą jest nieodłącznie powiązany oraz nazwą firmy lub osoby fizycznej, na która jest wystawiany. Certyfikat taki może zostać wydany jedynie przez ośrodek do tego autoryzowany, dzięki czemu nie może on zostać wydany przez oszusta, czy osobę trzecią niemającą takich uprawnień. Każde centrum jest dodatkowo sprawdzane przez centrum nadrzędne w celu dodatkowej weryfikacji i zachowaniu tak zwanej ścieżki certyfikacji polegającej na weryfikacji każdego szczebla łańcucha wydawania certyfikatu. Każdy certyfikat zawiera informację o całym łańcuchu



# Budowa systemu e-matura

certyfikacji w certyfikacie docelowym, dzięki czemu informacje te mogą zostać zawsze zweryfikowane.

Co więcej, każdy certyfikat zawiera klucz prywatny i publiczny, dzięki czemu możliwe jest asymetryczne szyfrowanie przesyłanych danych pomiędzy klientem a serwerem.

## **6. Autentykacja aplikacji klienckiej poprzez użycie tokenu o ograniczonym czasie życia**

Szyfrowanie połączenia oraz identyfikacja serwera poprzez certyfikat wystawiony przez zaufane centrum certyfikacji nie zapewnia jednak całkowitej ochrony systemu. Użytkownik wie, że komunikuje się z oryginalnym serwerem, a dane, które wprowadzi nie dostaną się w ręce osób trzecich, jednak sam klient musi zostać odpowiednio zweryfikowany, aby zdecydować czy i do jakich zasobów powinien mieć dostęp. W celu poprawnego zidentyfikowania użytkownika przeprowadzona zostać musi jego autentykacja oraz autoryzacja. Autentykacja polega na sprawdzeniu czy osoba jest tym, za kogo się podaje, a więc sprawdzana jest jej nazwa użytkownika oraz hasło. W następnej kolejności przeprowadzany jest proces autoryzacji, czyli sprawdzanie, do jakich zasobów/funkcjonalności użytkownik ma prawo dostępu. W systemie e-matura autentykacja do systemu opiera się na podaniu nazwy użytkownika oraz hasła, które jest sprawdzane przy logowaniu do systemu. Jeśli użytkownik poda poprawne dane otrzymuje w wyniku tej operacji specjalnie wygenerowany numer zwany tokenem, który przypisany jest do bieżącej sesji logowania. Token ten jest wykorzystywany do autoryzacji we wszystkich metodach usługi sieciowej, która stanowi jedyną warstwę komunikacyjną pomiędzy klientem a serwerem. Dzięki zastosowaniu tokenu nazwa użytkownika oraz jego hasło nie są przesyłane przy każdym zapytaniu do usługi sieciowej, dzięki czemu zwiększa się bezpieczeństwo poprzez zmniejszenie do minimum przesyłania poufnych danych użytkownika. Dodatkowe zabezpieczenie stanowi licznik czasu życia tokenu. Każdy token ma ustawiony swój czas życia, który zwiększany jest przy każdym odwołaniu się do serwisu. Jeśli przez określony czas nie nastąpi odwołanie do serwisu z użyciem wygenerowanego tokenu jego ważność ulega przedawnieniu i każde następne odwołanie do serwisu powoduje zwrócenie błędu i przekierowanie na stronę logowania. Dzięki takiemu podejściu token przechwycony na komputerze ofiary ataku hackerskiego nie może być użyty na innym komputerze lub tym samym komputerze w innej sesji.

## 7. Zamknięta procedura rejestracji

Dzięki temu, że system e-matura nie jest systemem otwartym, w którym konto do systemu może mieć każda osoba znająca adres serwisu, możliwe było zapewnienie dodatkowej warstwy bezpieczeństwa. Proces rejestracji rozpoczyna się od osobistego lub telefonicznego kontaktu osoby rekrutującej z przedstawicielem jednostki - szkoły, która chce przystąpić do projektu i otrzymać konto w systemie. Następnie osoba wybrana na stanowisko koordynatora po stronie szkoły otrzymuje papierowy formularz stanowiący wniosek o przystąpienie do udziału w projekcie. Dzięki zastosowaniu tradycyjnej metody weryfikacji na tym etapie wyeliminowano wszystkie osoby, które mogłyby chcieć uzyskać konto do systemu w celu jego penetracji. Po weryfikacji przesłanych danych koordynator otrzymuje drogą elektroniczną, na wskazany przez siebie adres, informacje potrzebne do zalogowania się do systemu. Osoba otrzymująca takie konto posiada uprawnienia do zakładania kont dla użytkowników w ramach swojej jednostki.

Rejestracja uczniów do egzaminu przebiega w sposób kontrolowany przez koordynatorów po stronie szkół. W celu umożliwienia uczniom przystąpienia do egzaminu koordynator musi wprowadzić jego dane osobowe do bazy danych przy użyciu aplikacji e-. Następnym zadaniem koordynatora jest wydruk dokumentu zawierającego dane ucznia, podpisanie go oraz odesłanie do biura projektu e-matura. W biurze projektu każdy formularz jest sprawdzany i zatwierdzany w systemie. Tak zweryfikowany uczeń może przystąpić do udziału w egzaminie.

## 8. Praca aplikacji w trybie offline (praca na pytaniach pobranych wcześniej)

Bezpieczeństwo to nie tylko zapewnienie poufności danych oraz weryfikacja uczestników. Dla pełnego bezpieczeństwa należy zapewnić ciągłość przeprowadzenia egzaminu w każdych warunkach. System e-matura został zaprojektowany z myślą o nieprzewidzianych przerwach w dostępie do Internetu, czy sieci zasilającej zarówno po stronie klienta jak i po stronie aplikacji serwerowej. Aplikacja kliencka po uruchomieniu egzaminu pobiera wszystkie pytania na komputer klienta i zapisuje je lokalnie w formie zaszyfrowanej. Podczas udzielania każdej odpowiedzi system najpierw zapisuje ją lokalnie w formie zaszyfrowanej, a następnie stara się wysłać odpowiedź do serwera. Jeśli odpowiedź



# Budowa systemu e-matura

nie może zostać wysłana od razu, trafia do kolejki odpowiedzi oczekujących. Kolejka ta jest cyklicznie sprawdzana i w przypadku odzyskania kontaktu z serwerem wszystkie odpowiedzi zostają wysłane. W przypadku, gdy awaria się przedłuża system zamyka egzamin bez podania wyniku jednak wszystkie odpowiedzi w bezpiecznej formie przechowane są na dysku lokalnym i mogą zostać wysłane, gdy tylko awaria zostanie usunięta.

## 9. Polityka dostępu do danych (procedury składowane)

Projekt e-matura zapewnia bezpieczeństwo nie tylko na poziomie aplikacji, ale też na poziomie bazy danych. Komunikacja serwera aplikacyjnego z serwerem bazodanowym odbywa się przy użyciu konta w bazie danych, które ma bardzo ograniczone uprawnienia do obiektów znajdujących się na serwerze baz danych. Użytkownik, przy użyciu którego serwer aplikacyjny loguje się do serwera baz danych ma prawo tylko i wyłącznie do wykonywania wybranych procedur składowanych. Nie ma możliwości, aby serwer aplikacyjny odwołał się bezpośredni do tabel, w których znajdują się dane. Cała komunikacja odbywa się poprzez procedury składowane, dzięki czemu system stał się odporny na wiele rodzajów ataków hackerskich jak np. SQL Injection (atak polegający na wprowadzeniu w formularzu aplikacji klienckiej kawałka kodu SQL, który ma być wykonany po stronie serwera baz danych). Wykorzystanie procedur składowanych do pełnej komunikacji aplikacji z bazą danych pozwoliło też zaimplementować część logiki biznesowej aplikacji po stronie serwera baz danych, co z kolei przełożyło się na wzrost wydajności systemu e-matura.

### 9.1. Szyfrowanie danych osobowych i niejawnych

Bardzo istotnym elementem systemu e-matura jest zbieranie pełnych danych osobowych uczestników biorących czynny udział w projekcie, aby możliwa była ich jednoznaczna identyfikacja w celu np. ewaluacji przez organ finansujący projekt. Informacje te są zbierane i zapisywane w bazie danych, w której są też przechowywane pytania egzaminacyjne. W celu zapewnienia pełnego bezpieczeństwa zbieranych danych osobowych oraz danych niejawnych w systemie e-matura, zostało wprowadzone szyfrowanie na poziomie konkretnych tabel. Dzięki temu wszystkie dane, które nie mogą trafić w niepowołane ręce są zaszyfrowane i bezpośrednie odwołanie do tabeli nie pozwoli na dostęp do danych. Dostęp do zaszyfrowanych danych możliwy jest jedynie poprzez procedury składowane po wylegitymowaniu się certyfikatem. Zastosowanie mechanizmu szyfrowania tylko do tych

tabel, w których faktycznie przechowywane są dane osobowe i niejawne, pozwoliło zwiększyć znacząco bezpieczeństwo danych bez generowanie niepotrzebnego obciążenia serwerów, powodowane np. przez szyfrowanie danych, które nie wymagają takiego bezpieczeństwa.

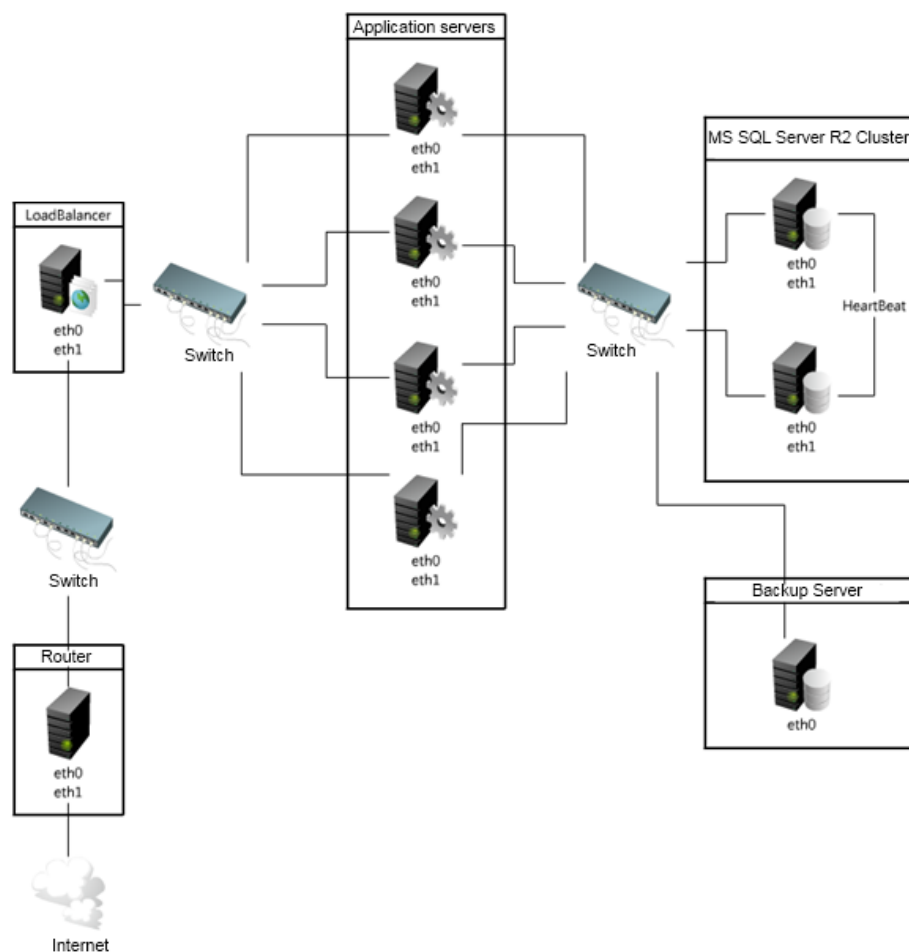
Oprócz zabezpieczenia przed bezpośrednim dostępem do danych z poziomu serwera baz danych, wprowadzenie szyfrowania zapewniło większe bezpieczeństwo kopii zapasowych bazy danych. W przypadku uzyskania dostępu do plików kopii zapasowych przez nieuprawnionego użytkownika nie będzie on w stanie odzyskać bazy danych z takiego pliku bez posiadania certyfikatu oraz hasła do certyfikatu, które przechowywane są w ściśle strzeżonym miejscu.

## 9.2. Odseparowanie logiczne serwera baz danych

Zapewnienie pełnego bezpieczeństwa systemu egzaminacyjnego to nie tylko zabezpieczenia na poziomie aplikacyjnym, to również zapewnienie odpowiednio zaprojektowanej infrastruktury serwerowej. W projekcie e-matura w celu zapewnienia jak najlepszego bezpieczeństwa infrastruktura serwerowa została zaprojektowana w taki sposób, aby wyeliminować wszystkie pojedyncze punkty awarii. Wszystkie elementy składające się na infrastrukturę zostały zdublowane, serwery aplikacyjne i bazodanowe zostały połączone w klastry, dyski twarde zostały połączone w macierze RAID, a poszczególne serwery zostały wydzielone do odrębnych podsieci.

Podział infrastruktury na kilka odseparowanych od siebie podsieci znacząco zwiększył bezpieczeństwo danych przechowywanych w bazie danych. Serwery aplikacyjne, serwujące aplikację użytkownikom podłączone są do sieci Internet poprzez serwery zarządzające obciążeniem. Są też podłączone przy użyciu osobnych interfejsów sieciowych do sieci LAN, do której podłączone są również serwery baz danych. Sieć LAN, w której pracują serwery baz danych jest odseparowana od sieci Internet i nie ma możliwości dostępu do tych serwerów w inny sposób niż poprzez serwery aplikacyjne. Zastosowanie takiej infrastruktury powoduje, że potencjalny włamywacz, który chciałby wykraść dane np. o pytaniach egzaminacyjnych z serwera baz danych musiałby najpierw włamać się na serwer zarządzający obciążeniem, później włamać się na serwer aplikacyjny i dopiero z niego włamać się na serwer baz danych. Tak długa ścieżka byłaby bardzo czasochłonna i trudna do przejścia przez nieuprawnionego użytkownika, co znacząco zwiększa bezpieczeństwo danych przechowywanych w systemie.

# Budowa systemu e-matura



Rys. 3 Architektura aplikacji

## 10. Mechanizmy kopii zapasowych w serwerze baz danych (backup, log shipping)

Kolejnym bardzo ważnym aspektem budowy projektu e-matura było zapewnienie infrastruktury, która zabezpiecza przed utratą danych przechowywanych w bazie danych.

Aby sprostać tym wymaganiom, kopie zapasowe baz danych wykonywane są każdej nocy na odseparowany serwer znajdujący się w odrębnej podsieci podpiętej bezpośrednio do serwera baz danych. Serwer kopii zapasowych nie jest widoczny dla pozostałych serwerów znajdujących się w infrastrukturze takich jak serwery aplikacyjne, czy też serwery zarządzania obciążeniem. Ma to na celu zwiększenie bezpieczeństwa kopii zapasowych przed nieuprawnionym dostępem.

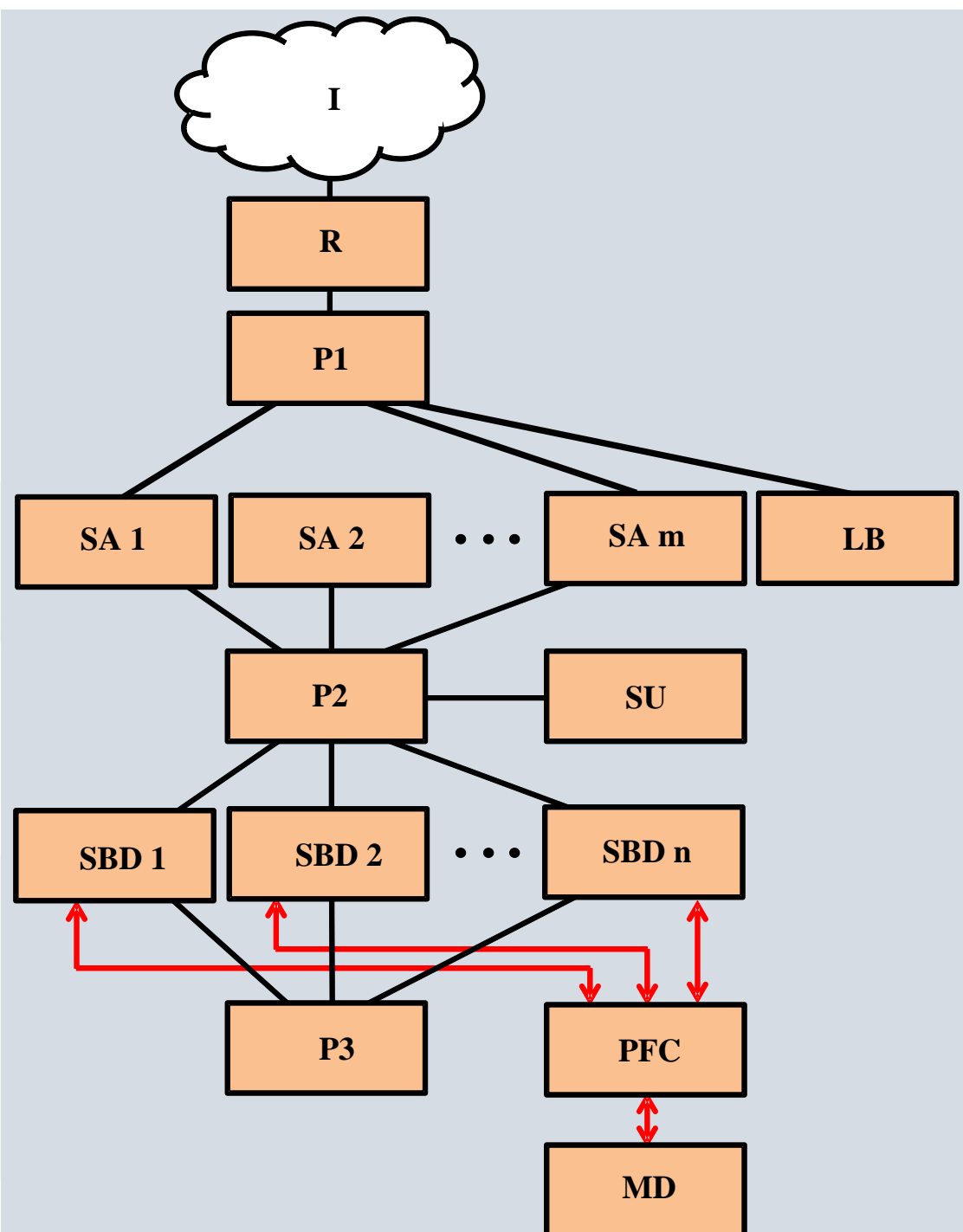
Dodatkowo, aby jeszcze bardziej zwiększyć bezpieczeństwo danych przechowywanych na serwerze baz danych, wykorzystany został mechanizm Log Shippingu polegający na cyklicznym odkładaniu kopii zapasowej dziennika transakcji. Kopia zapasowa loga transakcji jest odkładana w 15 minutowych odstępach umożliwiając tym samym wycofanie zmian w bazie danych do konkretnego momentu w czasie (ograniczając się do odstępów, w jakich jest wykonywana kopia zapasowa). Piętnastominutowe odstępy zapewniają wystarczającą granulację kopii zapasowych bez powodowania nadmiernego obciążenia serwerów.

W kolejnym rozdziale zostanie opisana fizyczna budowa infrastruktury informatycznej projektu e-matura.

## **11. Opis infrastruktury informatycznej projektu e-matura**

Schemat blokowy zasadniczej części struktury informatycznej projektu e-matura przedstawiono na rys. 4. Nie uwzględniono na nim zasilania, które zostanie omówione osobno oraz komputerów biura i innych składników niemających bezpośredniego wpływu na działanie systemu.

# Budowa systemu e-matura



Rys.4. Schemat blokowy infrastruktury informatycznej projektu e-matura. Objasnienia w tekście.

Zasadniczymi elementami infrastruktury projektu są serwery bazy danych SBD i serwery aplikacji SA oraz serwer równoważenia obciążenia sieciowego LB (load balancer).

Serwery bazy danych tworzą klaster niezawodnościowy. W jego skład powinny wchodzić co najmniej dwa serwery mogące przejąć nawzajem swoje zadania w przypadku awarii któregośkolwiek z nich. W modelowym rozwiązaniu zastosowano dwa serwery ( $n=2$ ).

# Budowa systemu e-matura

Serwery klastra są połączone między sobą separowaną siecią Ethernet o prywatnych numerach IP np. 192.168.10.yy przez przełącznik P3.

Przełącznik P2 łączy serwery bazy danych z serwerami aplikacji oraz serwerem uwierzytelniania również przez sieć o adresach prywatnych, innych niż w sieci P3, np. 192.168.20.xx.

W bazie danych są przechowywane wszystkie dane w tym:

- dane uczestników projektu,
- zadania egzaminacyjne,
- odpowiedzi zdających na pytania egzaminacyjne – przebieg egzaminów.

Serwery bazy danych powinny mieć wspólne miejsce przechowywania danych – macierz dyskową MD. Jest to potrzebne do utworzenia klastra niezawodnościowego. W modelowym rozwiązaniu zastosowano macierz IBM DS3400 wyposażoną w dyski z interfejsem typu SAS połączone w wolumin RAID. Na woluminie tym utworzono partycje dyskowe. Macierz dołączono do serwerów za pomocą światłowodów przez interfejs Fibre Channel za pośrednictwem przełącznika PFC (rys. 4).

Wymagania dotyczące serwerów klastra bazy danych są następujące:

- Wydajne serwery wielordzeniowe z pamięcią RAM 32-64GB. W projekcie zastosowano serwery modułowe IBM HS22.
- Serwery wyposażone w interfejs do podłączenia macierzy dyskowej np. interfejs Fibre Channel.
- Serwery pod kontrolą systemów operacyjnych rodziny Windows, co najmniej Windows 2008 R2.
- Program bazy danych MS SQL Server, w wersji co najmniej 2008 Standard.
- Serwery wyposażone w dwa niezależne interfejsy sieciowe.

Grupa serwerów aplikacji składa się z co najmniej dwóch serwerów w celu zapewnienia niezawodności i wysokiej wydajności. Liczba serwerów zależy od planowanego obciążenia. W modelowym rozwiązaniu zastosowano cztery serwery ( $m=4$ ). Serwery te mogą dzielić między siebie zadania, mogą też przejmować nawzajem swoje funkcje w razie awarii.

Ich rolą jest obsługa witryny projektu – komunikacja z uczestnikami projektu. Pobierają one i składują dane w bazie danych, z którą łączą się za pomocą sieci Ethernet o prywatnych numerach IP przez przełącznik P2. Serwery aplikacji komunikują się



# Budowa systemu e-matura

z Internetem „I” za pośrednictwem sieci o publicznych numerach IP przez przełącznik P1, serwer równoważenia obciążenia sieciowego LB i router-zaporę sieciową R.

Serwer równoważenia obciążenia sieciowego do komunikacji z Internetem i z serwerami aplikacji wykorzystywał ten sam interfejs sieciowy o adresie publicznym. Dlatego na rys. 4. jest przedstawiony na tym samym poziomie co serwery aplikacji ponieważ tak wyglądała struktura fizyczna.

Wymagania dotyczące serwerów aplikacji są następujące:

- Wydajne serwery wielordzeniowe z pamięcią RAM 32-48GB. W projekcie zastosowano serwery modułowe IBM HS22.
- Serwery pod kontrolą systemów operacyjnych rodziny Windows, co najmniej Windows 2008 R2 Web Server.
- Serwery wyposażone w dwa niezależne interfejsy sieciowe.
- Wymagania dotyczące serwera obciążenia sieciowego są podobne, jednak nie są potrzebne dwa interfejsy sieciowe.

Do poprawnej pracy całości potrzebny jest serwer uwierzytelnienia SU. W projekcie wykorzystano usługę katalogową Active Directory funkcjonującą w siedzibie projektu.

Przełączniki P1, P2 i P3 mogą być osobnymi urządzeniami lub pojedynczym przełącznikiem zarządzanym, mogącym za pomocą sieci wirtualnych (VLAN) odwzorować strukturę logiczną przedstawioną na rys. 1. Z punktu widzenia bezpieczeństwa i poprawności działania konieczne jest separowanie sieci P2 i P3 od Internetu lub innych sieci. Wymiana danych między użytkownikami i projektem powinna się odbywać za pośrednictwem serwerów aplikacji.

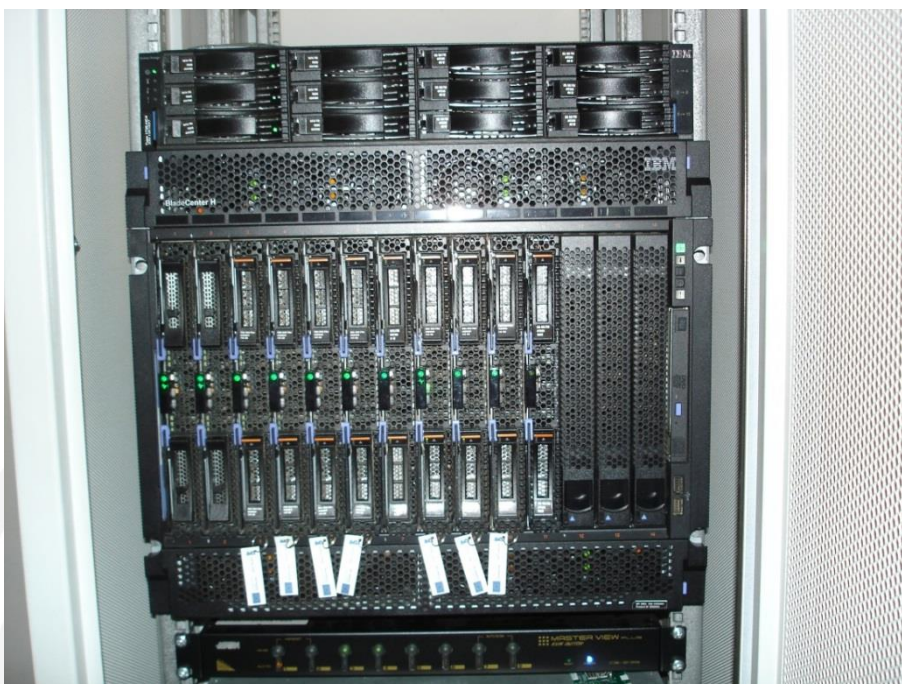
Szybkość przełączników powinna wynosić 1Gb/s. W modelowym rozwiązaniu zastosowano dwa przełączniki modułowe IBM 32R1860. Na jednym z nich zrealizowano funkcje przełącznika P2, na drugim P1 i P3.

Router-zapora sieciowa R o wydajności 1Gb/s powinien zapewniać filtrowanie przesyłanych danych tak, aby dopuścić tylko wybrane usługi lub protokoły i zablokować pozostałe. W modelowym rozwiązaniu wykorzystano D-Link DFL-1600.

System realizujący opisane założenia można zbudować na kilka sposobów np.:

- przy użyciu osobnych serwerów i przełączników w obudowach przemysłowych,
- na serwerach wirtualnych,
- z wykorzystaniem serwerów modułowych.

# Budowa systemu e-matura



*Rys. 5 Serwery wykorzystywane w projekcie. Wspólna obudowa (klatka) zawiera serwery (widoczne na zdjęciu pionowe wsuwki z etykietkami), zasilacze, napęd DVD. Z tyłu obudowy są, tutaj niewidoczne, przełączniki, wentylatory i moduł zarządzania. Na górze jest macierz dyskowa na 12 dysków twardych, które można, w razie awarii, wymienić bez przerywania pracy systemu.*

W projekcie do budowy systemu o strukturze z rys. 4 zastosowano trzecie rozwiązanie - komputery modułowe (rys. 5). Rozwiązanie takie polega na tym, że jest jedna duża obudowa zawierająca w sobie większość niezbędnych komponentów:

- redundantne (nadmiarowe) zasilacze,
- układy zarządzające,
- wentylatory,
- przełączniki sieciowe,
- przełącznik Fibre Channel,
- komputery (serwery),
- połączenia wewnętrzne,
- napęd DVD wspólny dla wszystkich serwerów,
- porty USB,
- przełącznik KVM (konsoli).

# Budowa systemu e-matura



*Rys. 6. Szafa teleinformatyczna mieszcząca m. in. serwery projektu*

Takie podejście ma wiele zalet:

- kompaktowa budowa – małe gabaryty (np. obudowa na rys. 5 może pomieścić 14 serwerów, w chwili obecnej jest 11, w tym 7 projektu e-matura),
- niezawodne nadmiarowe zasilanie,
- jednolite zarządzanie wszystkimi składnikami systemu,
- możliwość zdalnego zarządzania,
- możliwość zarządzania lokalnego za pomocą jednej konsoli (monitor, klawiatura i mysz),
- krótkie, niezawodne wewnętrzne połączenia między elementami systemu,
- wspólne korzystanie z niektórych urządzeń np. z napędu DVD lub portów USB,
- łatwość ulokowania urządzeń w szafach serwerowych,
- możliwość wymiany niektórych komponentów bez wyłączania napięcia.

W projekcie wykorzystano wiele elementów będących w posiadaniu beneficjenta np.:

- obudowę,
- zasilacze,

# Budowa systemu e-matura

- przełączniki sieciowe,
- przełącznik światłowodowy (Fibre Channel),
- wentylatory,
- moduł zarządzający,
- macierz dyskową,
- szafy teleinformatyczne.



*Rys. 7. Zasilacz rezerwowy UPS zasilający serwery projektu z bateriami akumulatorów*



# Budowa systemu e-matura



*Rys. 8. Router wykorzystywany w projekcie oraz zasilacz rezerwowy UPS*

Ze środków projektu do budowy głównej infrastruktury informatycznej zakupiono:

- siedem serwerów,
- sześć dysków twardych,
- zasilacz rezerwowy z bateriami akumulatorów.

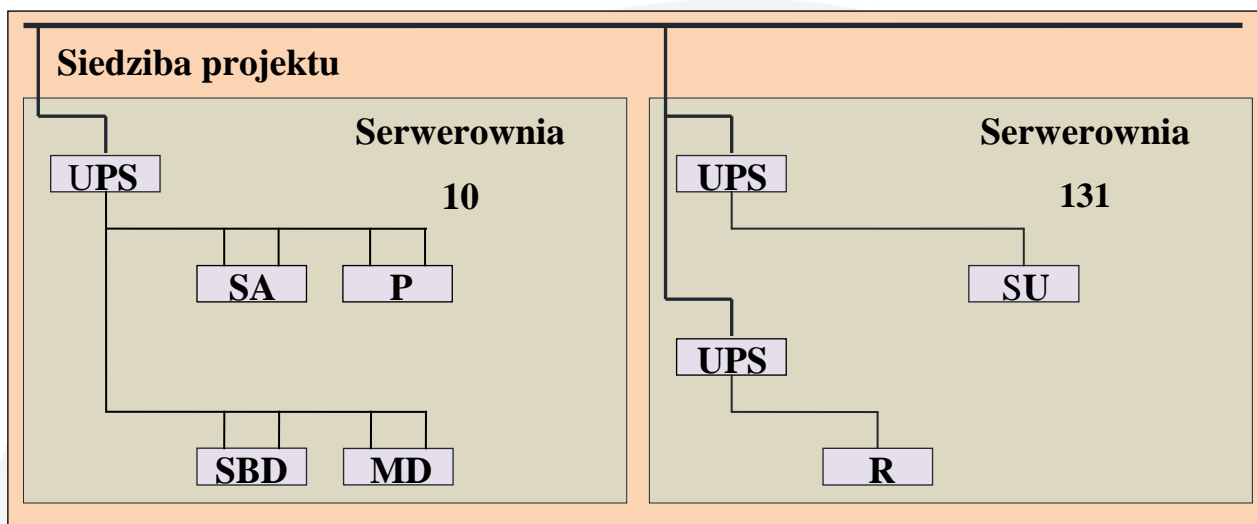
Ważnym elementem wpływającym na jakość pracy z serwisami www, zwłaszcza w przypadku egzaminów, jest ciągła bezawaryjna praca.

Ważnym czynnikiem przyczyniającym się to tego jest zasilanie rezerwowe. W projekcie e-matura zastosowano zasilacze rezerwowe wyposażone w baterie akumulatorów rys. 9. Rozwiązanie takie jest wystarczające dla zapewnienia około trzygodzinnej pracy w przypadku braku napięcia w sieci.

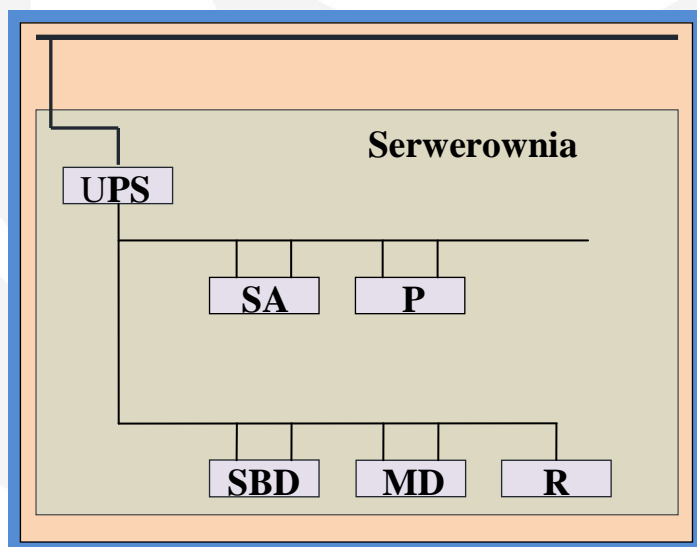
Ważne też jest, aby stosować urządzenia z redundantnym zasilaniem tj. wyposażonych w co najmniej dwa zasilacze. W przypadku takiego rozwiązania system byłby odporny nie tylko na zaniki napięcia ale również na awarie urządzeń będących składnikami systemu. W rozwiązaniu modelowym większość urządzeń miała takie zabezpieczenie. Na rys. 9 i 10 zaznaczono to symbolicznie dwiema kreskami.

# Budowa systemu e-matura

W projekcie elementy systemu były rozmieszczone w dwóch serwerowniach. Było to związane z wykorzystaniem istniejącej infrastruktury informatycznej w siedzibie beneficjenta projektu. Tworząc rozwiązanie docelowe można umieścić wszystkie serwery i pozostałe urządzenia w jednym pomieszczeniu rys. 10.



Rys.9 Schemat zasilania urządzeń wykorzystywanych w projekcie e-matura niezbędnych do przeprowadzenia egzaminu.



Rys.10 Schemat zasilania urządzeń skupionych w pojedynczym pomieszczeniu