Wyższa Szkoła Technologii Informatycznych w Katowicach

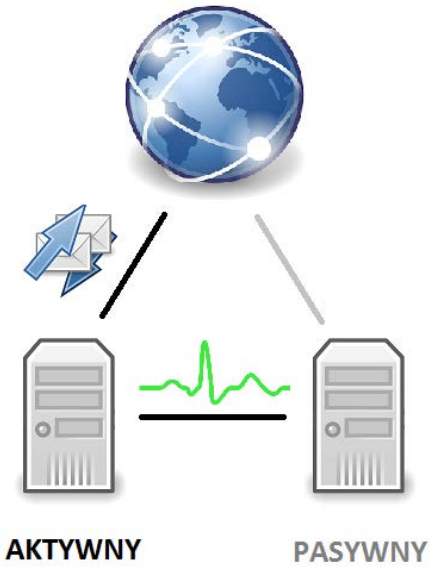
REFERAT O PRACY DYPLOMOWEJ

Temat pracy: Wdrożenie usługi poczty elektronicznej opartej na aplikacji Postfix dla średniego przedsiębiorstwa ze szczególnym uwzględnieniem aspektów wysokiej dostępności

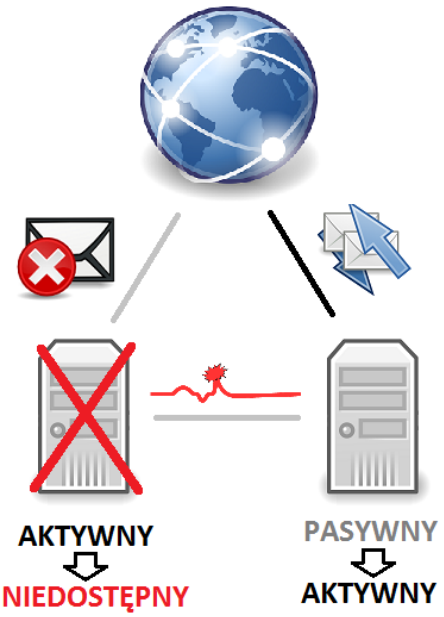
Autor: Dominik Oleś

W ramach pracy dyplomowej rozważano sytuację, w której przedsiębiorstwo branży handlowej podjęło decyzję o konieczności wdrożenia własnego serwera poczty elektronicznej. Głównym powodem takiej zmiany była częsta niedostępność usługi spowodowana awariami po stronie dotychczasowego usługodawcy, oraz niska pojemność skrzynek pocztowych. Projektując własne rozwiązanie usługi poczty elektronicznej istotnym kryterium, jakie należało wziąć pod uwagę, była minimalizacja kosztów związana ze zwiększającą się ilością użytkowników serwera pocztowego, co wynika z dość dynamicznego rozwoju firmy. Podjęto decyzję, aby w ramach rozwiązania wykorzystane zostało oprogramowanie Open Source, tj. serwer SMTP Postfix wraz z dodatkowym oprogramowaniem realizującym m.in. funkcję skanera antywirusowego i filtra antyspamowego.

Dla zapewnienia wysokiej dostępności usługi poczty elektronicznej zdecydowano się na wdrożenie prostego klastra typu "active-passive" składającego się z dwóch serwerów. Jeden z serwerów (aktywny) przetwarza żądania związane z usługą poczty elektronicznej (obsługuje połączenia od innych serwerów SMTP, oraz klientów poczty), podczas gdy drugi serwer (pasywny) monitoruje jego dostępność. Schemat działania przedstawiony został na Ilustracji 1. W razie niedostępności aktywnego serwera, pasywny przejmuje jego rolę, co zostało zaprezentowane na Ilustracji 2.

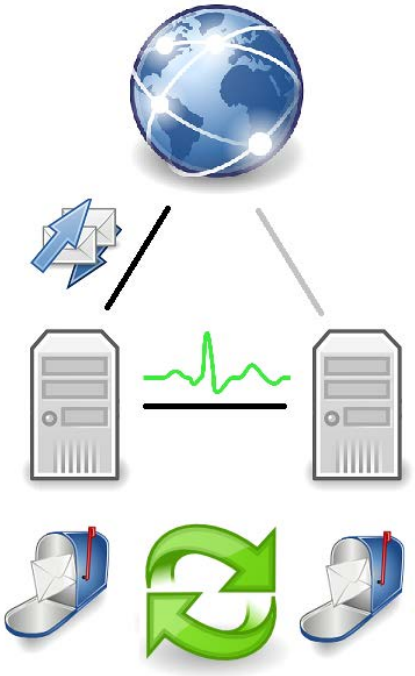


Ilustracja 1: Schemat obrazujący sposób działania klastra active-passive
Źródło: Opracowanie własne



Ilustracja 2: Schemat obrazujący reakcję klastra active-passive na wystąpienie awarii jednego z jego węzłów
Źródło: Opracowanie własne

W związku z faktem, że w firmie do obsługi poczty wykorzystywany jest protokół IMAP wszystkie wiadomości w skrzynkach użytkowników znajdować się muszą na serwerze. Istotne jest więc, aby przełączenie aktywnego serwera nie spowodowało zmiany zawartości skrzynek. W celu zapewnienia możliwości dostępu do skrzynek pocztowych przez obydwa serwery zastosowano replikację na poziomie partycji. Na każdym z węzłów klastra tworzona jest dodatkowa partycja dedykowana na skrzynki pocztowe użytkowników, na której wszystkie zmiany są synchronizowane w czasie rzeczywistym pomiędzy replikami. W związku z tym, że zastosowanie macierzy dyskowych wspierających replikację znacznie podniosłoby koszt całego rozwiązania, proces ten jest realizowany przez oprogramowanie DRBD zainstalowane na serwerach. Odpowiada ono za synchronizację danych i zarządzanie replikowanym wolumenem (np. podmontowanie wolumenu na jednym z węzłów klastra, reagowanie na problemy z komunikacją pomiędzy replikami). Schemat rozwiązania uwzględniający lokalizację skrzynek użytkowników został przedstawiony na Ilustracji 3.

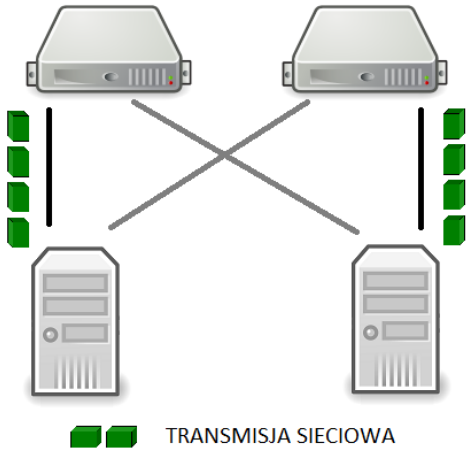


Ilustracja 3: Schemat rozwiązania uwzględniający lokalizację skrzynek pocztowych.
Źródło: Opracowanie własne

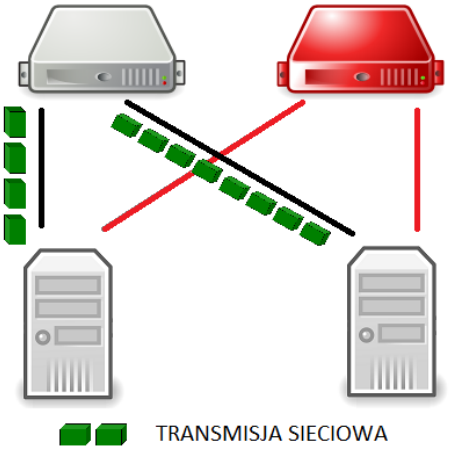
Poza skrzynkami pocztowymi użytkowników, na replikowanej partycji znajduje się również kolejka serwera Postfix, w której przechowywane są wiadomości przeznaczone do wysyłki do momentu pomyślnego ich dostarczenia do serwera docelowego. Często zdarza się, że z jakiegoś powodu następuje konieczność retransmisji wiadomości (np. wskutek działania mechanizmu szarych list). W związku z tym, że ponowna próba wysłania nie następuje natychmiast, wiadomość może znajdować się w kolejce przez dłuższy czas. Wystąpienie awarii serwera i przełączenie na drugi węzeł klastra spowodowałoby utratę wszystkich wiadomości znajdujących się w kolejce. Umieszczenie kolejki serwera Postfix na replikowanej partycji rozwiązuje ten problem.

Dotychczas opracowane rozwiązanie problemu wysokiej dostępności serwera poczty elektronicznej i skrzynek pocztowych użytkownika nic nie da, jeżeli awarii ulegnie przełącznik łączący serwery z resztą sieci. W celu rozwiązania tego problemu zdecydowano się na zastosowanie mechanizmu agregacji połączeń, która opiera się na skonfigurowaniu redundantnych połączeń fizycznych w ramach tzw. interfejsu logicznego. Za realizację opisanego

mechanizmu we wdrożonym serwerze poczty odpowiada wbudowany w system CentOS moduł bond. Schematy obrazujące zasadę działania oraz reakcję na awarię przełącznika zostały przedstawione na Ilustracjach 4 i 5.



Ilustracja 4: Schemat przedstawiający agregację połączeń.
Źródło: Opracowanie własne



Ilustracja 5: Przełączenie transmisji na redundantny interfejs na wypadek awarii jednego z przełączników.
Źródło: Opracowanie własne

Dodatkowo w ramach zaprojektowanego rozwiązania założono, iż oprogramowanie klastra musi być skonfigurowane w taki sposób, aby w razie utraty połączenia z określonymi adresami w sieci sprawdzić czy pasywny serwer takowe posiada (w takim wypadku powinno nastąpić przełączenie na serwer, który ma kontakt z wymienionymi adresami). Opisane zachowanie serwera poczty osiągnięto dzięki zastosowaniu modułu „ipfail" wchodzącego w skład oprogramowania Heartbeat. Wymieniony mechanizm zaimplementowany został w ten sposób, aby badać łączność z kilkoma adresami sieciowymi (dopiero niedostępność wszystkich zdefiniowanych adresów na aktywnym węźle powoduje reakcję). Jest to o tyle istotne, że nie powoduje destabilizacji pracy serwera na skutek awarii jednego adresu sieciowego (co może być wynikiem awarii urządzenia posiadającego ten adres, a nie utraty łączności serwera z siecią lokalną).

Poza rozwiązaniami mającymi na celu zapewnienie wysokiej dostępności wdrożone zostały również mechanizmy bezpieczeństwa takie jak skaner

antywirusowy, autoryzacja SMTP, oraz odpowiednio połączone mechanizmy antyspamowe – greylisting, listy RBL, oraz skaner treści Spamassassin. W związku z tym, że kontrahentami przedsiębiorstwa są zwykle mniejsze firmy, w których nierzadko kwestie takie jak poprawna konfiguracja serwera pocztowego są zaniedbywane, zabezpieczenia antyspamowe zostały skonfigurowane w ten sposób, aby ograniczyć ryzyko odrzucenia wiadomości nie będącej spamem. W tym celu mechanizm list RBL ustawiono w ten sposób, aby w razie potwierdzenia obecności nadawcy na takiej liście nie odrzucać wiadomości, ale poddać przesyłkę działaniu mechanizmu greylistingu. Dodatkowo, wszystkie wiadomości, które pomyślnie przejdą weryfikację w mechanizmach czarnych i szarych list, są analizowane przez skaner treści Spamassassin, w którym progi punktowe skonfigurowano mniej restrykcyjnie w stosunku do ustawień domyślnych.

Wiadomości przesyłane wewnątrz firmy często zawierają informacje ściśle poufne, dlatego w ramach rozwiązania przewidziano wymuszenie szyfrowania połączeń dla użytkowników autoryzowanych. Sam proces autoryzacji użytkowników serwera pocztowego następuje w oparciu o ich poświadczenia w usłudze Active Directory. Eliminuje to konieczność posługiwania się odrębnym hasłem do poczty elektronicznej, co w pewien sposób ułatwia użytkownikom korzystanie z usługi. Dzięki zintegrowaniu serwera pocztowego z zewnętrzną bazą użytkowników, rozwiązany został również problem synchronizacji użytkowników i haseł pomiędzy dwoma serwerami w klastrze.

Testy rozwiązania przeprowadzone po jego zaimplementowaniu w środowisku laboratoryjnym wykazały, że zastosowane mechanizmy wysokiej dostępności działają poprawnie. System pocztowy reaguje na awarie pojedynczych komponentów zgodnie z oczekiwaniami. W przypadku awarii interfejsu sieciowego, skutki dla użytkownika są praktycznie niezauważalne (przełączenie następuje na tyle szybko, że nawiązane sesje nie są zrywane). W przypadku awarii całego serwera przełączenie na pasywny węzeł klastra powoduje zerwanie trwających sesji, natomiast czas niedostępności jest na tyle krótki, że nie stanowi dyskomfortu dla użytkowników (oprogramowanie klienta poczty zwykle samo ponawia próby połączenia z serwerem, a w niektórych przypadkach łączy się do serwera raz na jakiś czas). Charakterystyka zastosowanych rozwiązań wysokiej dostępności przedstawiona została w Tabeli 1.

RODZAJ AWARII	USZKODZENIE FIZYCZNEGO POŁĄCZENIA	AWARIA AKTYWNEGO SERWERA
MECHANIZM	*AGREGACJA POŁĄCZEŃ*	*KLASTER ACTIVE-PASSIVE*
REAKCJA	*PRZEŁĄCZENIE TRANSMISJI NA REDUNDANTNY INTERFEJS*	*DRUGI Z SERWERÓW PRZEJMUJE ROLĘ AKTYWNEGO*
CZAS NIEDOSTĘPNOŚCI	PONIŻEJ 1 SEKUNDY	OKOŁO 25-30 SEKUND
ROZŁĄCZENIE SESJI SMTP	NIE	TAK
UTRATA DANYCH	*BRAK UTRATY DANYCH*	*W PRZYPADKU POCZTY ELEKTRONICZNEJ PRAKTYCZNIE BRAK UTRATY DANYCH*

Tabela 1: Charakterystyka zastosowanych rozwiązań wysokiej dostępności w zależności od zaistniałej awarii.
Źródło: Opracowanie własne.

Jak można zauważyć, osiągniętym efektem pracy było kompleksowe wdrożenie usługi poczty elektronicznej, uwzględniające kryteria i uwarunkowania dla konkretnego przedsiębiorstwa. Rozwiązanie zostało dopasowane do potrzeb firmy, a przy jego projektowaniu uwzględniono możliwość integracji systemu z istniejącą infrastrukturą.

W ramach kierunków dalszych prac przewiduje się wdrożenie systemu monitorującego infrastrukturę informatyczną, co pozwoli na usprawnienie procesu monitorowania infrastruktury IT i szybką detekcję źródeł awarii nie tylko dla wdrożonego serwera pocztowego, ale również pozostałych systemów informatycznych.