Załącznik nr 3 do SIWZ

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2007-2013 oraz z budżetu państwa.

Spis treści

I. Przedmiot zamówienia

Zaprojektowanie, dostarczenie, wykonanie i uruchomienie „Systemu zarządzania zasobami IT wraz ze sprzętową infrastrukturą serwerową, systemem archiwizacji i backupu".

Niniejszy projekt jest częścią projektu „e-Policja – w służbie społeczeństwu województwa śląskiego", działanie 2.2. Rozwój Elektronicznych Usług Publicznych, Priorytet II. Społeczeństwo Informacyjne, realizowanego w ramach Regionalnego Programu Operacyjnego Województwa Śląskiego Na Lata 2007 – 2013.

II. Wstęp

Zakres zadania obejmuje zakup, instalację i uruchomienie wszystkich elementów niezbędnych do stworzenia „Systemu do zarządzania zasobami IT wraz ze sprzętową infrastrukturą serwerową, systemem archiwizacji i backupu" zwany dalej SYSTEMEM, a także dostarczenie wszelkich niezbędnych licencji do zaprojektowanego rozwiązania sprzętowo-programowego. Zbudowane środowisko usług katalogowych z uwagi na dwie odseparowane od siebie sieci komputerowe stworzone zostanie w postaci dwóch osobnych domen. Ze względu na ten podział, w ramach prac konieczne jest wykonanie dwóch projektów logowania i procedur migracji danych. Całość infrastruktury sprzętowo-programowej zostanie podzielona na dwie lokalizacje: Podstawowe Centrum Przetwarzania Danych (PCPD) oraz Zapasowe Centrum Przetwarzania Danych (ZCPD). W PCPD zostaną zlokalizowane serwery typu blade, podstawowa macierz dyskowa oraz podstawowy system backupu. ZCPD obejmuje zapasową macierz dyskową oraz zapasowy system backupu.

System zarządzania zasobami IT obejmie wszystkich użytkowników (ok. 13.000 użytkowników) w obecnie istniejących dwóch sieciach (PSTD i CWI), wszystkie stacje robocze (8000 komputerów w obu powyższych sieciach), system zarządzania wydrukiem oraz konieczną infrastrukturę sprzętową przechowywania danych i ich archiwizację.

III. Architektura docelowa SYSTEMU

1. Podstawowe Centrum Przetwarzania Danych i Zapasowe Centrum Przetwarzania Danych.

Wymagane jest, aby SYSTEM funkcjonował na podstawie technologii centralnego przetwarzania danych. SYSTEM ma zagwarantować spójne zarządzanie danymi, ułatwioną kontrolę oraz administrację.

Koncepcja zakłada następujące elementy, które zostały podzielone ze względu na fizyczną lokalizację:

- Podstawowe centrum przetwarzania danych:
  - serwer typu blade składający się z 8 modułów serwerowych
  - oprogramowanie do wirtualizacji
  - oprogramowanie zarządzające
  - podstawowa macierz dyskowa
  - system backupu
- Zapasowe centrum przetwarzania danych:
  - zapasowa macierz dyskowa
  - zapasowy system backup

Środowisko zostanie zbudowane przy użyciu serwera typu blade składającego się z 8 modułów serwerowych. Architektura oparta o technologię blade charakteryzuje się wysokim stopniem zagęszczenia serwerów przy jednoczesnej minimalizacji kosztów okablowania, zasilania i klimatyzacji. W ramach jednej obudowy powstanie kompletne środowisko sprzętowe wraz z infrastrukturą sieciową Ethernet oraz Fibre Channel. Obudowa powinna umożliwiać późniejsze doposażenie o kolejne moduły serwerowe oraz moduły komunikacyjne.

Na każdym serwerze zostanie preinstalowany na redundantnych kartach flash system operacyjny, tzw. hypervisor, który stanowi podstawę pracy serwera w środowisku wirtualnym. Całe środowisko wirtualne będzie zarządzane przy pomocy konsoli zarządzającej. Każdy z serwerów będzie miał dostęp do macierzy dyskowych, które udostępnią (współdzielone między serwerami) zasoby pod przyszłe maszyny wirtualne. Przy pomocy oprogramowania do wirtualizacji, środowisko serwerowe zostanie zabezpieczone przed awariami fizycznymi serwerów oraz zostaną ustawione priorytety umożliwiające relokację maszyn wirtualnych w przypadku nadmiernego

obciążenia SYSTEMU. Technologia proponowanych macierzy dyskowych pozwoli na pełną współpracę ze środowiskiem wirtualizacji serwerów tak, aby administrator dysponował pojedynczą konsolą do środowiska wirtualnego i dyskowego (storage). Same macierze dyskowe wyposażone zostaną w funkcjonalności umożliwiające dynamiczną zmianę parametrów pracy w zależności od warunków obciążenia środowiska (thin provisioning, virtual provisioning, tiering itp.).

Cała architektura będzie w pełni redundantna, czyli będzie posiadać co najmniej podwójne moduły komunikacyjne, interfejsy do serwerów, dwie macierze dyskowe oraz podwójny system backupu dyskowego. W ramach projektu wydzielona zostanie zapasowa fizyczna lokalizacja, która posłuży do replikacji danych. W przypadku awarii podstawowej macierzy dyskowej jej rolę przejmie zapasowa macierz dyskowa (do czasu usunięcia awarii). Dopełnieniem całej architektury będzie również zastosowanie wydajnego systemu kopii zapasowych i archiwizacji z deduplikacją. Backup będzie odbywać się na medium dyskowe w postaci wydzielonej przestrzeni dyskowej RAID. System backupu będzie umożliwiał wykonanie kopii plików, aplikacji (usługi katalogowe, bazy danych itp.) oraz całych maszyn wirtualnych. Będzie to rozwiązanie kompletne i zarządzane z jednej konsoli administracyjnej. System tworzenia kopii zapasowych będzie pozwalał na granularne odtwarzanie danych na poziomie usług katalogowych (odtwarzania pojedynczych obiektów) lub pojedynczych plików całych maszyn wirtualnych (nawet jeśli maszyna jest wyłączona). System backupu musi umożliwiać wykonanie kopii zapasowych dowolnej ilości maszyn wirtualnych. W założeniach proponowanej architektury, system backupu będzie się znajdować w PCPD, natomiast w ZCPD będzie jego replika. Dane synchronizowane będą na bieżąco, a przez zastosowane algorytmy deduplikacji system w sposób minimalny obciąży sieć.

Projektowane środowisko zapewni bezpieczeństwo, skalowalność, możliwość rozbudowy, oszczędność, a ponadto neutralność technologiczną, dzięki czemu umożliwi instalację wszelkiego rodzaju rozwiązań m.in. systemów operacyjnych czy aplikacji.

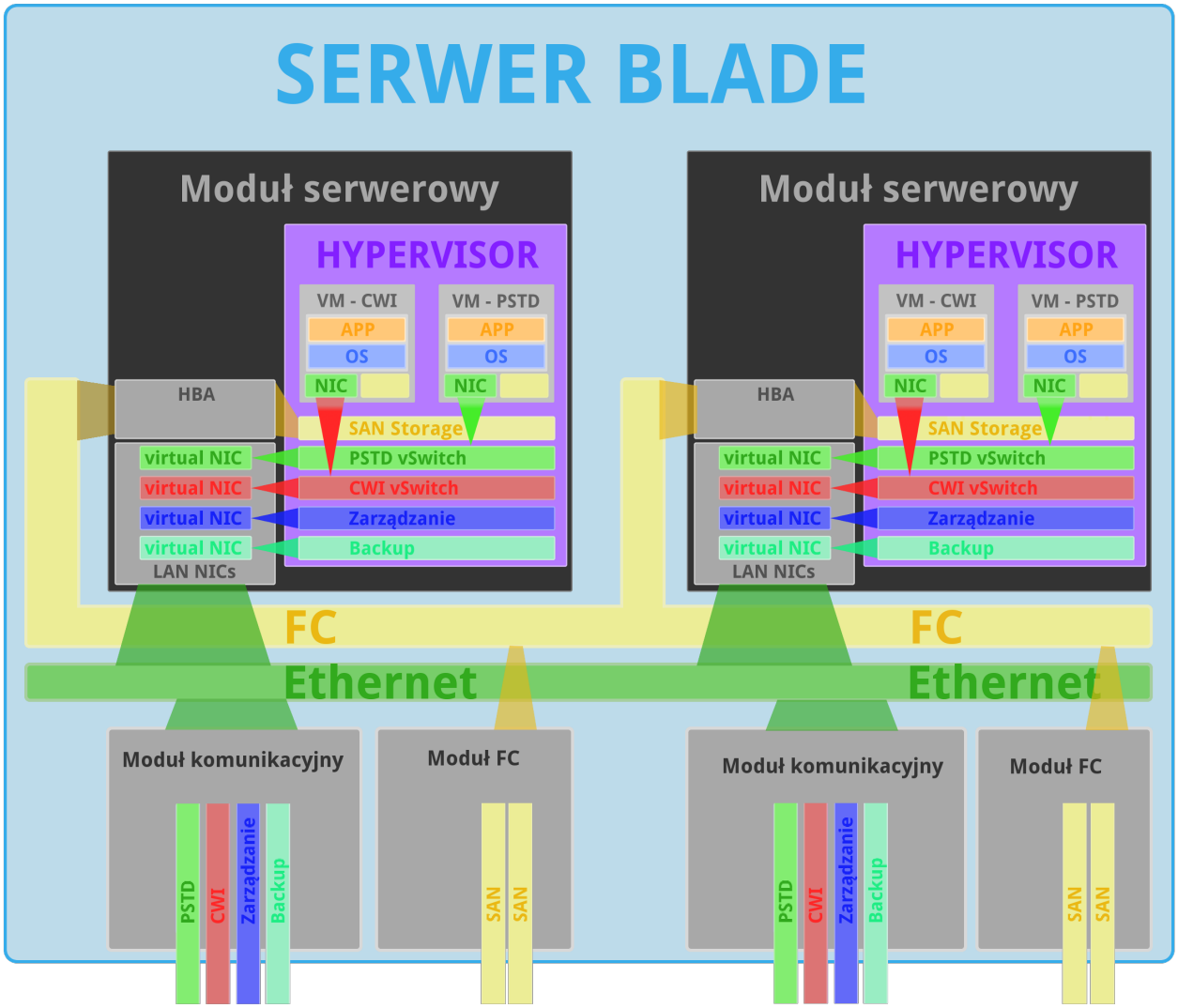
2. Warstwa techniczna

2.1. Serwer blade

Wymagane jest zastosowanie serwera typu blade, który zostanie umieszczony w PCPD.

1. Obudowa blade powinna spełniać warunki określone w Załączniku nr 4 do SIWZ.
2. Dostarczona obudowa serwerowa powinna zostać obsadzona redundantnymi modułami komunikacyjnymi, zasilaczami i wentylatorami.
3. Zamawiający wymaga funkcji wirtualizacji połączeń Ethernet na poziomie modułów zainstalowanych w obudowie serwerowej.

4. Zamawiający dopuszcza funkcję wirtualizacji połączeń FC na poziomie modułów zainstalowanych w obudowie serwerowej.
5. Serwer blade – co najmniej 8 modułów serwerowych rozłożonych w jednej obudowie spełniających warunki określone w Załączniku nr 4 do SIWZ. Moduły te nie będą posiadały wewnętrznych dysków twardych, dostarczony przez Wykonawcę hypervisor uruchamiany będzie bezpośrednio z dedykowanych kart pamięci typu flash. Moduły serwerowe będą tworzyły platformę wirtualizacyjną do uruchamiania maszyn wirtualnych i będą stanowiły wydajny, elastyczny i skalowalny trzon całości SYSTEMU. Dostarczone licencje muszą zapewnić możliwość uruchomienia dowolnej ilości maszyn wirtualnych na każdej z maszyn fizycznych (modułów serwerowych). Moduły muszą posiadać co najmniej dwa procesory (min. 8 rdzeni każdy) oraz co najmniej 128GB pamięci RAM. Na dostarczonej platformie wirtualizacyjnej wymaga się zbudowania całego nowego i pełnego środowiska Systemu Zarządzania Zasobami IT w tym usługi katalogowe.



Rys. 1. Schemat połączeń LAN i SAN wewnątrz serwera blade.

2.2. System wirtualizacji

System wirtualizacji musi spełniać warunki opisane w Załączniku nr 4 do SIWZ.

2.3. System backupu dyskowego

W założeniach proponowanej architektury, system backupu będzie się znajdować w PCPD, natomiast w ZCPD będzie jego replika. Dane synchronizowane będą na bieżąco, a przez zastosowane algorytmy deduplikacji system w sposób minimalny obciąży sieć. System zbudowany zostanie przy pomocy wydajnej architektury, pozwalającej na wymianę danych bezpośrednio pomiędzy macierzami a systemem backupu. Backup będzie odbywać się na medium dyskowe w postaci wydzielonej przestrzeni dyskowej RAID. System backupu będzie umożliwiał wykonanie kopii plików, aplikacji (usługi katalogowe, bazy danych itp.) oraz całych maszyn wirtualnych. Będzie to rozwiązanie kompletne i zarządzane z jednej konsoli administracyjnej. System tworzenia kopii zapasowych będzie pozwalał na granularne odtwarzanie danych na poziomie usług katalogowych (odtwarzania pojedynczych obiektów) lub pojedynczych plików całych maszyn wirtualnych (nawet jeśli maszyna jest wyłączona). System backupu musi umożliwiać wykonanie kopii zapasowych dowolnej ilości maszyn wirtualnych.

Architektura środowiska backupu powinna składać się dwóch serwerów (lub serwer wraz z urządzeniem rozszerzającym przestrzenią dyskową – np. półka dyskowa), po jednym w każdej lokalizacji. Na serwerze w lokalizacji podstawowej (PCPD) pracuje równocześnie serwer zarządzający, jak i serwer zapisujący dane(media-agent). W lokalizacji zapasowej (ZCPD) serwer pełni jedynie rolę media-agenta. Całość środowiska zarządzana jest poprzez serwer w lokalizacji podstawowej. Oprogramowanie zarządzając musi zapewniać pełne zarządzanie całym środowiskiem z poziomu jednej konsoli administracyjnej.

Każdy z serwerów przechowuje zdeduplikowane dane backupowe na wewnętrznych dyskach serwera. Serwery powinny być wyposażone również w dodatkowe szybkie dyski na potrzeby przechowywania wewnętrznych baz i indeksów oprogramowania backupowego.

Backupowane dane w pierwszej kolejności zapisywane będą w formie zdeduplikowanej na serwerze w lokalizacji podstawowej. Następnie zostanie wykonana dodatkowa kopia danych do lokalizacji zapasowej (replikacja). Dodatkowo do lokalizacji zapasowej będzie przesyłana kopia wewnętrznej bazy oprogramowania backupowego tak, aby w razie awarii serwer zapasowy przejął funkcje serwera zarządzającego. Serwer zapasowy w razie awarii serwera podstawowego musi przejąć wszystkie jego zadania tak, aby było możliwe wykonywanie backupów z serwera blade, jak i procesu odtwarzania danych.

Transmisja danych powinna odbywać się w większości przy pomocy połączeń typu FC - SAN (tam gdzie to możliwe) lub przy pomocy Ethernet (LAN).

Przykładowy(poglądowy) przebieg podstawowego backupu:

- Oprogramowanie backupowe we współpracy z oprogramowaniem do wirtualizacji uruchamia wykonanie snapshotu dla każdej wirtualnej maszyny.

- Po stworzeniu snapshotów wirtualnych maszyn, na macierzy wykonywany jest snapshot SAN.
- Po utworzeniu snapshotu SAN snapshoty maszyn wirtualnych stworzone przy pomocy oprogramowania do wirtualizacji są usuwane.
- Snapshot macierzy SAN podmontowywany jest do serwera backupu.
- Teraz następuje proces tworzenia kopii bezpieczeństwa danych maszyn wirtualnych na dyski w serwerze backupowym. W tym procesie mogą zostać wykorzystane specjalnie stworzone do tego celu tymczasowe wirtualne maszyny typu offline z wykorzystaniem danych wcześniej stworzonego snapshotu SAN.
- Snapshot SAN usuwany jest od razu po zakończeniu procesu backupu lub zgodnie z przyjętą polityką w późniejszym terminie.

Zamawiający wymaga, aby kopie środowisk wirtualnych były wykonywane bez zatrzymywania z możliwością odtwarzania pojedynczych plików (np. dla serwerów Microsoft Windows).

Do wykonywania kopii zgodnie z powyższymi wymaganiami konieczne jest dostarczenie wszystkich i kompletnych licencji nieograniczonych czasowo. Jeżeli jakakolwiek z wymaganych licencji jest limitowana w zależności od pojemności to powinna ona zapewniać obsługę co najmniej 20 TB danych źródłowych.

Wymagane licencje:

Licencje na deduplikację co najmniej 20 TB danych źródłowych

Model licencjonowania musi pozwalać na backupowanie nieograniczonej ilości serwerów wirtualnych, a także aplikacji zainstalowanych na tych serwerach.

Każde dostarczane oprogramowanie kopii zapasowych musi być dostarczone w najnowszej dostępnej wersji wraz ze wsparciem na to oprogramowanie.

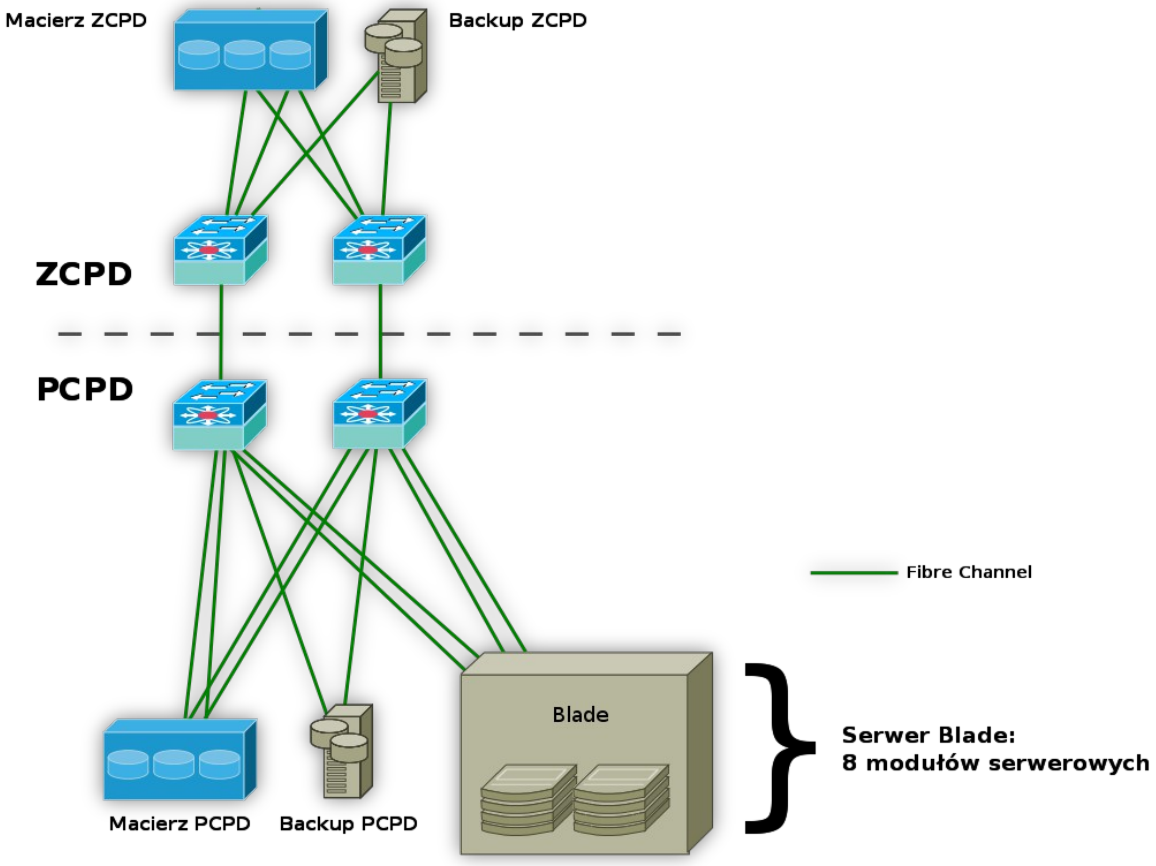
System backupu dyskowego należy dostarczyć zgodnie z minimalnymi wymaganiami opisanymi w Załączniku nr 4 do SIWZ.

2.4. Macierze dyskowe

Zamawiający wymaga, aby system składowania danych oparty został na dwóch macierzach dyskowych zlokalizowanych w PCPD i ZCPD oraz sieć SAN w technologii Fibre Channel z wykorzystaniem włókien optycznych pomiędzy lokalizacjami (łącze o długości około 4 km

zapewnia Zamawiający). W tym celu wykorzystane zostaną wkładki optyczne SFP Long Wave oraz 2 dedykowane światłowody. Wymagane jest zastosowanie tych samych macierzy dyskowych (inna liczba dysków i ich rodzaj), tego samego producenta w obu centrach danych zgodnych z opisem w Załączniku nr 4 do SIWZ.

W celu zwiększenia bezpieczeństwa SYSTEMU Zamawiający wymaga, aby dane zgromadzone na macierzy w PCPD były replikowane na drugą macierz, zlokalizowaną w ZCPD. Wymagane jest, aby replikacja została oparta o wbudowany mechanizm sprzętowy producenta (bez udziału hosta) w trybie asynchronicznym.

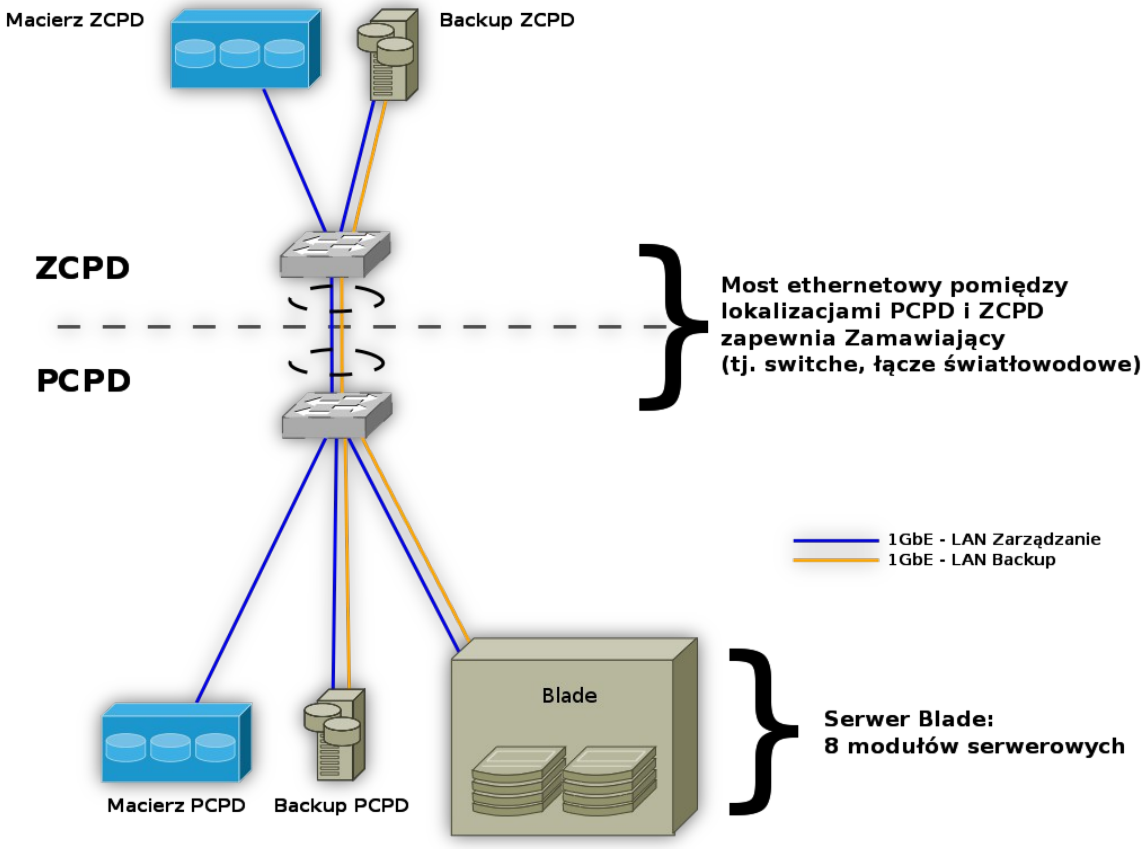


Rys. 2. Schemat wymaganych połączeń systemu składowania danych oraz systemu backupu

2.5. Warstwa sieciowa

Zamawiający posiada dwie niezależne i odseparowane sieci komputerowe (PSTD i CWI). Powyższe sieci są odseparowane galwanicznie na poziomie KWP w Katowicach. Proponowane rozwiązanie sprzętowo-programowe musi uwzględniać maksymalną separację sieci PSTD i CWI celem zapewnienia odpowiedniego poziomu bezpieczeństwa wymaganego przez wewnętrzne przepisy. Zamawiający dopuszcza separację logiczną sieci PSTD i CWI tylko w ramach infrastruktury serwera blade (tj. wirtualne połączenia pomiędzy modułami komunikacyjnymi a serwerami wirtualnymi). W pozostałych przypadkach wymagana jest tylko i wyłącznie separacja galwaniczna obu sieci.

Proponowane rozwiązanie sprzętowo-programowe musi zawierać wydzieloną sieć zarządzającą (wydzielenie na poziomie modułów komunikacyjnych) przeznaczoną do administrowania infrastrukturą serwerową oraz konsolą hypervisora. Dodatkowo należy wydzielić niezależną sieć backupową przeznaczoną do komunikacji hypervisora z systemem backupu dyskowego.



Rys. 3. Schemat wymaganych połączeń Ethernet w ramach SYSTEMU

3. Oprogramowanie do zarządzania zasobami IT

System zarządzania zasobami IT obejmuje zaprojektowanie, dostarczenie licencji serwerowych i dostępowych oraz wdrożenie i uruchomienie 2 odseparowanych od siebie redundantnych usług katalogowych Active Directory Domain Services lub równoważnych wraz z usługami towarzyszącymi obejmującymi swoim zasięgiem całość infrastruktury Zamawiającego.

Oprogramowanie serwerowe i dostępowe oraz oprogramowanie do zarządzania środowiskiem serwerowym należy dostarczyć zgodnie z minimalnymi wymaganiami opisanymi w Załączniku nr 4 do SIWZ.

System zarządzania zasobami IT zostanie stworzony z wykorzystaniem usług katalogowych i będzie obejmował:

- Wszystkie stacje robocze Zamawiającego wyposażone w systemy operacyjne MS Windows XP Professional lub nowsze.
- Scentralizowane zarządzanie wszystkimi usługami i komputerami – zrealizowanie zaleceń w zakresie polityki bezpieczeństwa dotyczących użytkowników sieci komputerowej, sprzętu i oprogramowania komputerowego.
- Kompleksowe zarządzanie infrastrukturą komputerową, a tym samym usprawnienie przeprowadzenia cyklicznych audytów bezpieczeństwa obejmujących zasoby teleinformatyczne całego garnizonu śląskiej Policji
- Zminimalizowanie strat wywołanych przez awarie sprzętu.
- Sprzętową i programową ochronę danych.
- Udostępnienie do pracy grupowej zasobów IT (pliki, urządzenia wielofunkcyjne, drukarki).
- Pełną kontrolę dostępu wraz z historią działań.
- Ujednolicenie procesu logowania i związaną z tym redukcję czasowo - kosztową zarządzania kontami.
- Ograniczenie liczby interwencji serwisu.
- Spójną administrację zasobami.
- Automatyzację procesów instalacji nowych zasobów i użytkowników.
- Możliwość zdalnego i automatycznego instalowania i aktualizowania oprogramowania.

- Możliwość instalowania centralnych systemów teleinformatycznych, które w połączeniu z nowoczesną strukturą łączności światłowodowej między jednostkami, pozwolą na szybką i pełną reakcję.

Projekt wykonania struktury logowania obejmie:

Opracowanie konwencji nazewniczej dla całej organizacji uwzględniającej dopuszczalne standardy nazw dla:

- Oddziałów
  - Jednostek organizacyjnych,
  - Zasad grup (GPO),
  - Kont użytkowników, komputerów (stacji roboczych, serwerów),
  - Grup administracyjnych i zasobowych,
  - Kont funkcyjnych i serwisowych,
  - Zasobów,
  - Drukarek i urządzeń peryferyjnych.
- Opracowanie zasad tworzenia i stosowania grup do zarządzania systemem oraz zasobami.
- Projekt struktury logicznej domeny
  - Architektura i poziom funkcjonalności domen,
  - Struktura kontenerów domeny grupująca obiekty tj. konta komputerów,użytkowników, grupy,
  - Określenie sposobu zarządzania kontami użytkowników, komputerów,
  - Konfiguracja uprawnień administracyjnych dla jednostek organizacyjnych w domenie.
- Projekt topologii (struktury fizycznej) domeny
  - Topologia siedzib usług katalogowych,
  - Rozmieszczenie i funkcje kontrolerów domenowych,
  - Konfiguracja replikacji domeny,
  - Synchronizacja czasu,
  - Konfiguracja serwerów.

- Konfiguracja ustawień bezpieczeństwa.
  - Ustawienia Zasady Grup (GPO) dla domeny,
  - Ochrona antywirusowa,
  - Zarządzanie poprawkami,
  - Audyt zmian w konfiguracji domeny.
- Projekt usług sieciowych
  - Konfiguracja usług DHCP i DNS.
- Zarządzanie środowiskiem pracy użytkownika
  - Zasady Grup – Group Policy,
  - Uprawnienia do zarządzania stacjami roboczymi.
- Koncepcja zarządzania zasobami plikowymi
  - Organizacja zasobów sieciowych (folder domowy, repozytoria).
- Model administrowania dla Systemu Zarządzania Zasobami IT
  - Administrowanie domeną,
  - Administrowanie systemem,
  - Role administracyjne,
  - Zadania i zakres uprawnień administratorów.

Dla zapewnienia wymaganego poziomu bezpieczeństwa użytkownicy obu sieci zostaną objęci systemem silnego uwierzytelniania opartego o karty inteligentne, na których będą zapisane certyfikaty X509. Zamawiający wymaga, aby w okresie przejściowym istniała możliwość logowania przy wykorzystaniu loginu i hasła, pomijając kartę inteligentną.

System silnego uwierzytelniania zostanie zaprojektowany w taki sposób, aby maksymalnie wykorzystać produkty i rozwiązania informatyczne obecnie eksploatowane w KWP w Katowicach i w Komendzie Głównej Policji. W skład systemu uwierzytelniania wejdą wykorzystywane już:

1. Centrum Certyfikacji Kluczy Centaur CCK, który będzie odpowiedzialny za wystawianie, zawieszanie i unieważnianie certyfikatów X509 v3 dla użytkowników kart inteligentnych. System zarządzany przez KGP Warszawa.
2. Sprzętowy moduł kryptograficzny CompCrypt Delta-1 służący do bezpiecznego generowania i przechowywania materiału kryptograficznego.
3. Karty mikroprocesorowe CryptoCard multiSIGN (CryptoCard multiSIGN jest

specjalizowaną kryptograficzną kartą mikroprocesorową przeznaczoną do realizacji kwalifikowanego i niekwalifikowanego podpisu elektronicznego oraz funkcji identyfikacji i silnego uwierzytelniania użytkowników).

4. CryptoCard Suite - oprogramowanie middleware do obsługi i zarządzania kartami elektronicznymi CryptoCard multiSIGN.
5. Czytniki kart mikroprocesorowych.

Zamawiający wymaga, aby Wykonawca opracował procedury importu wymaganych danych o użytkownikach z eksploatowanych środowisk LDAP (OpenLDAP oraz Lotus Domino). Dodatkowo Wykonawca musi utworzyć skrypty administracyjne, które pozwolą Zamawiającemu na okresowe synchronizowanie powyższych danych w obu domenach (PSTD i CWI).

Na podstawie opracowanego projektu Wykonawca wdroży usługi katalogowe poprzez instalację, konfigurację kompletnego środowiska domenowego zgodnie z powyższymi założeniami i funkcjonalnością wraz z przygotowaniem planów migracji i integracji istniejącego środowiska komputerowego.

Wprowadzenie systemu zarządzania zasobami IT pozwoli na:

- uruchomienie centralnego zarządzania infrastrukturą teleinformatyczną,
- automatyzację procesów administracyjnych,
- zapewnienie pełnego bezpieczeństwa zgodnego ze standardami,
- ograniczenie ilości i przyspieszenie interwencji serwisowych

IV. Gwarancja i Serwis Gwarancyjny

Zamawiający wymaga gwarancji oraz serwisu gwarancyjnego zgodnie z Załącznikiem nr 5 do SIWZ.

V. Dokumentacja SYSTEMU

Wymagane jest, aby Wykonawca opracował Dokumentację Projektową, Powykonawczą i Eksploatacyjną dla zaoferowanego i zbudowanego SYSTEMU.

Dokumentacja Projektowa SYSTEMU będzie tworzona etapami i będzie obejmowała w szczególności:

1. opis ogólny SYSTEMU.

2. opis funkcjonalny SYSTEMU.
3. schematy blokowe połączeń pomiędzy elementami SYSTEMU z opisem parametrów styku,
4. schematy blokowe połączeń wewnątrz poszczególnych elementów SYSTEMU z opisem krytycznych parametrów,
5. wykaz sprzętu, urządzeń, wykaz oprogramowań (licencji) i systemów operacyjnych wraz z ich wersjami,
6. szczegółowe informacje dotyczące instalacji i konfiguracji SYSTEMU,
7. procedury i wymagania uruchomieniowe,
8. opracowanie konwencji nazewniczej dla całej organizacji uwzględniającej dopuszczalne standardy nazw (usługi katalogowe),
9. opracowanie zasad tworzenia i stosowania grup do zarządzania systemem oraz zasobami (usługi katalogowe),
10. projekt struktury logicznej usług katalogowych,
11. projekt topologii (struktury fizycznej) usług katalogowych,
12. konfiguracja ustawień bezpieczeństwa (usługi katalogowe),
13. projekt usług sieciowych (usługi katalogowe),
14. zarządzanie środowiskiem pracy użytkownika (usługi katalogowe),
15. koncepcja zarządzania zasobami plikowymi (usługi katalogowe),
16. model administrowania dla systemu (usługi katalogowe),
17. procedury awaryjne,
18. wykaz Testów Akceptacyjnych,
19. dokumenty uzupełniające, uzgodnione przez Strony.

Dokumentacja projektowa SYSTEMU będzie uwzględniać rozwiązania organizacyjne funkcjonujące u Zamawiającego, wszystkie wymagane moduły funkcjonalne, sposoby realizowania wymagań funkcjonalnych, użytkowych i usługowych oraz zasady zarządzania SYSTEMEM, określać proponowane do zastosowania i wbudowania w SYSTEM mechanizmy programowe zapewniające jego bezpieczeństwo oraz bezpieczeństwo gromadzonych i przetwarzanych w nim danych, przedstawiać możliwości dalszej rozbudowy SYSTEMU w kierunku jego unowocześnienia.

Dokumentacja projektowa SYSTEMU będzie opracowana zgodnie z wymogami określonymi w

umowie, dokumentacji przetargowej, zasadami wiedzy technicznej, powszechnie obowiązującymi w tym zakresie normami, normatywami z uwzględnieniem obowiązujących przepisów.

Dokumentacja sporządzona będzie w języku polskim.

Dokumentacja powykonawcza powinna uwzględniać rozwiązania organizacyjne funkcjonujące u Zamawiającego, wszystkie wymagane moduły funkcjonalne, sposoby realizowania wymagań funkcjonalnych, użytkowych i usługowych oraz zasady zarządzania SYSTEMEM, określać wbudowane mechanizmy programowe i sprzętowe zapewniające jego bezpieczeństwo oraz bezpieczeństwo gromadzonych i przetwarzanych w nim danych, przedstawiać możliwości dalszej rozbudowy SYSTEMU w kierunku jego unowocześnienia.

Dokumentacja eksploatacyjna będzie podlegała akceptacji i odbiorowi przez Zamawiającego. Dokumentacja eksploatacyjna będzie w szczególności zawierać procedury postępowania na wypadek awarii i błędów krytycznych, instrukcje serwisowe dla administratorów i instrukcje dla użytkowników końcowych. Wykonawca jest zobowiązany do uwzględnienia w dokumentacji procedury przełączania rozwiązań redundantnych dla obu lokalizacji (PCPD i ZCPD), np. przełączenia macierzy, synchronizacji elementów systemu backupu dyskowego, środowiska wirtualnego, kontrolerów obu domen.

Wykonawca opracuje w 3 egzemplarzach i w wersji elektronicznej dokumentację powykonawczą i eksploatacyjną SYSTEMU zgodnie z wymogami określonymi w umowie, dokumentacji przetargowej, zasadami wiedzy technicznej, powszechnie obowiązującymi w tym zakresie normami, normatywami z uwzględnieniem obowiązujących przepisów.

Dokumentacja powykonawcza i eksploatacyjna będzie sporządzona zgodnie z przyjętymi standardami tak, aby możliwe było dokonanie jej oceny przez niezależny podmiot niebędący Stroną niniejszej UMOWY, co zastrzega sobie Zamawiający.

Wykonawca opracuje i w terminie 30 dni od zakończenia testu wdrożeniowego przekaże Zamawiającemu 3 egzemplarze dokumentacji powykonawczej, ponadto 3 nośniki z wersją elektroniczną. Dokumentacja powykonawcza będzie podlegała akceptacji i odbiorowi przez Zamawiającego.

Dokumentacja eksploatacyjna i powykonawcza sporządzone mają być w języku polskim.

Wykonawca dostarczy ponadto standardowe dokumentacje producentów urządzeń oraz dokumentacje producentów oprogramowania systemowego i oprogramowania narzędziowego.

Wykonawca opracowuje oraz uzupełnia na etapie realizacji dokumentację do SYSTEMU, która jest wymagana przez akty prawne wymienione w OPZ, a w szczególności wynikające z ustawy o ochronie danych osobowych i przepisach wykonawczych do tej ustawy, czyli - politykę

bezpieczeństwa i instrukcję zarządzania systemem przetwarzającym dane osobowe.

Polityka bezpieczeństwa systemu przetwarzającego dane osobowe, opisująca sposób ochrony przetwarzanych danych osobowych adekwatny do zagrożeń, powinna być traktowana jako polityka szczegółowa Systemu Zarządzania Bezpieczeństwem Informacji, zatem powinna uwzględniać postanowienia norm:

- ISO/IEC 27001:2007 Technika informatyczna – Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji.

- ISO/IEC 17799:2009 Technika informatyczna – Techniki bezpieczeństwa - Praktyczne zasady zarządzania bezpieczeństwem informacji.

- ISO/IEC 27005/2010 Technika bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.

VI. Testy odbioru SYSTEMU

Wymagane jest przeprowadzenie testów akceptacyjnych, określonych w Planie Testów Akceptacyjnych, który zostanie sporządzony przez Wykonawcę SYSTEMU i będzie podlegał akceptacji przez Zamawiającego. Plan Testów Akceptacyjnych musi uwzględniać rodzaje testów, kolejność ich wykonywania oraz metodykę, całokształt wymagań i kryteriów akceptacyjnych, algorytmy i procedury przeprowadzania testów, harmonogram przeprowadzania testów, a także sposób dokumentowania wyników testów.

Testy Akceptacyjne przeprowadzone zostaną przez przedstawicieli Wykonawcy i Zamawiającego dwuetapowo w terminie i kolejności wynikającej z Planu Testów Akceptacyjnych:

- I etap – testy systemu zarządzania zasobami IT wraz ze sprzętową infrastrukturą serwerową i systemu archiwizacji
- II etap – testy systemu backupu dyskowego.

Jeżeli przeprowadzenie testu akceptacyjnego może wiązać się z ryzykiem utraty danych, wówczas Wykonawca SYSTEMU jest zobowiązany do prawidłowego zabezpieczania danych przed rozpoczęciem testu akceptacyjnego.

Zamawiający zastrzega sobie prawo wyboru elementów SYSTEMU, które będą podlegać testom akceptacyjnym, przy czym wybór musi nastąpić przed uzgodnieniem Planu Testów Akceptacyjnych. W szczególności sporządzone plany testów akceptacyjnych muszą uwzględniać:

1. Testy środowiska wirtualizacyjnego.

2. Testy systemów składowania danych.
3. Testy środowiska usług katalogowych.
4. Testy przełączenia pomiędzy PCPD i ZCPD.
5. Testy centralnego zarządzania stacjami klienckimi (w tym m.in. wysyłanie jednej „polityki" na wszystkie stacje klienckie).
6. testy środowiska backupowego (odtwarzanie wybranych elementów SYSTEMU, Disaster Recovery)

Wymagane jest także zweryfikowanie prawidłowego wykorzystania redundantnej infrastruktury SYSTEMU. Wymagane jest testowe przejście na ZCPD, praca na ZCPD, przejście na PCPD, synchronizacja danych z ZCPD do PCPD.

Przystąpienie do testów systemu backupu dyskowego możliwe będzie tylko po pozytywnym zakończeniu testów systemu zarządzania zasobami IT wraz ze sprzętową infrastrukturą serwerową i systemu archiwizacji.

Odbiór końcowy SYSTEMU będzie możliwy tylko w przypadku pozytywnego zakończenia wszystkich uzgodnionych testów akceptacyjnych.

VII. Ogólne

Wykonawca dostarczy komplet wymaganych licencji dla projektowanego rozwiązania. Ponadto dostarczy na własny koszt wszelkie elementy, które są wymagane do wykonania wdrożenia, a nie zostały ujęte w SIWZ. W szczególności dotyczy to przyłączy patchcord do połączenia infrastruktury serwerowej oraz przewodów, kart lub innych do podłączenia infrastruktury Blade, macierzy, sieci SAN.