PROJEKT KONCEPCYJNY

Temat zadania: **Zintegrowany System Miejskiego Transportu Publicznego – Zaprojektowanie i Budowa Systemu Zarządzania Ruchem w Lublinie w ramach zadania pt. "Zintegrowany System Miejskiego Transportu Publicznego w Lublinie" współfinansowany w ramach Programu Operacyjnego Rozwój Polski Wschodniej 2007 – 2013**

Temat projektu: **Podsystem TI.**

ZAMAWIAJĄCY:	**Gmina Lublin** **Zarząd Dróg i Mostów w Lublinie** ul. Krochmalna 13j 20-401 Lublin
GENERALNY WYKONAWCA:	**Aeronaval de Construcciones e Instalaciones S.A.** Ul. Dekerta 24 30-703 Kraków

Funkcja	Imię i nazwisko autora	Data	Podpis
Autor	D. Gustavo A. Molina Méndez *Dyrektor Techniczny ACISA S.A.*	21/02/2013	
Dyrektor Projektu	Carlos Blázquez Alonso *Dyrektor Projektu ACISA S.A*	21/02/2013	

SPIS TREŚCI

1.- HARDWARE 5

1.1.- CELE 5
1.2.- SZAFA RACK 5
1.2.1 WYMIARY 5
1.2.2 CZĘŚCI SKŁADOWE 6
1.2.3 SYSTEM KONTROLI STANU SZAF RACK W CPD. 6
1.2.3.1 Wspólny czujnik magnetyczny otwartych drzwi: 7
1.2.3.2 Czujnik temperatury w szafie rack. 7
1.2.3.3 Czujniki utraty napięcia i wentylatorów. 8
1.3.- SERWERY 10
1.3.1 WYMIARY 10
1.3.2 CZĘŚCI SKŁADOWE 10
1.4.- PRZECHOWYWANIE 11
1.4.1 KONFIGURACJA 11
1.4.1.1 Macierz Główna i Dodatkowa 11
1.4.1.1.1 DANE KONFIGURACJI SYSTEMU ITS 11
1.4.1.1.2 Wielkość DANYCH HISTORYCZNYCH + PODSYSTEMÓW 11
1.4.1.1.3 Streszczenie obliczonych danych 13
1.4.1.2 Matryca Backup'u 14
1.4.2 ISCSI 14
1.4.2.1 Działanie iSCSI 14
1.4.3 WYMIARY 14
1.4.4 KOMPONENTY 14
1.5.- BIBLIOTEKA TAŚMOWA 15
1.5.1 WŁAŚCIWOŚCI 15
1.5.2 KOMPONENTY 15
1.6.- KOMPUTERY / PC 15
1.6.1 CZĘŚCI SKŁADOWE 16
1.7.- ARCHITEKTURA 16
1.7.1 PROPONOWANA ARCHITEKTURA 16
1.7.2 SCHEMAT RAMY 17

2.- SOFTWARE 19

2.1.- OTWARTOŚĆ SYSTEMU - CELE 19
2.2.- INTERFEJS - CELE 20
2.3.- DATEX II 21
2.4.- SYSTEMY OPERACYJNE 21
2.4.1 DEFINICJA 21
2.4.2 SERWERY 21
2.4.2.1 Windows Server 2008 21
2.4.2.1.1 Charakterystyki 22
2.4.2.1.2 Licencja 23
2.4.2.2 Red Hat Cluster Suite 23
2.4.2.2.1 Podstawowe informacje o klastrze 23
2.4.2.2.2 Omówienie Red Hat Cluster 24
2.4.2.2.3 Infrastruktura klastra 26
2.4.2.2.4 Administracja usługami o wysokiej dostępności 27
2.4.2.2.5 Red Hat GFS 29
2.4.2.2.6 Menedżer wolumenów logicznych klastra 32

2.4.2.2.7 Globalne sieciowe urządzenie blokowe (GNBD) 33
2.4.2.2.8 Serwer wirtualny Linux 34
2.4.2.2.9 Narzędzia administracyjne klastra 40
2.4.3 PC 43
2.4.3.1 Windows 7 43
2.4.3.1.1 Charakterystyki 43
2.4.3.1.2 Interfejs 44
2.4.3.1.3 Licencje 45
2.5.- OPROGRAMOWANIE BIUROWE 45
2.5.1 APACHE OPEN OFFICE 45
2.5.1.1 Charakterystyki 46
2.5.1.2 Pakiety Apache OpenOffice 46
2.5.1.2.1 WRITER 46
2.5.1.2.2 CALC 46
2.5.1.2.3 IMPRESS 46
2.5.1.2.4 DRAW 46
2.5.1.2.5 BASE 47
2.5.1.2.6 MATH 47
2.5.2 IZARC 47
2.5.2.1 Charakterystyki 48
2.5.3 FILEZILLA CLIENT 48
2.5.3.1 Charakterystyki 49
2.6.- NARZĘDZIA CAD 49
2.6.1 AUTOCAD 49
2.6.1.1 Charakterystyka 49
2.7.- GIS 50
2.8.- WIRTUALIZACJA 51
2.8.1 CO TO JEST WIRTUALIZACJA 51
2.8.2 ZMNIEJSZENIE KOSZTÓW POSIADANIA (TCO) 52
2.8.3 ZWIĘKSZENIE DOSTĘPNOŚCI I CIĄGŁOŚCI PRACY PRZEDSIĘBIORSTWA 52
2.8.4 CHARAKTERYSTYKI 52
2.8.5 MASZYNY WIRTUALNE GUEST 53
2.8.6 OGÓLNE PRZEDSTAWIENIE ROZWIĄZANIA 54
2.8.7 SERWERY 55
2.8.8 MAGAZYNOWANIE 55
2.8.9 GŁÓWNE ZABEZPIECZENIA NA WYPADEK AWARII 56
2.8.10 LICENCJE 56
2.9.- SYSTEM KOPII ZAPASOWYCH 56
2.9.1 CO TO JEST KOPIA ZAPASOWA 56
2.9.2 SYMANTEC BACKUP EXEC 2010 56
2.9.2.1 Główne funkcje 57
2.9.2.2 Procedura tworzenia kopii zapasowych 57
2.9.3 LICENCJA 58
2.10.- BAZY DANYCH BBDD 58
2.10.1 MICROSOFT SQL SERVER 2012 ENTERPRISE EDITION 58
2.10.1.1 - Microsoft SQL Server Enterprise 2012 Edition 58
2.10.1.2 Charakterystyka 58
2.10.1.3 Licencje 59
2.11.- FIREWALL 59
2.11.1 NETFILTER/IPTABLES 59
2.11.1.1 iptables 60
2.11.1.2 Tabele 61
2.11.1.3 Cel reguły 62
2.11.1.3.1 ACCEPT (akceptuj) 62
2.11.1.3.2 DROP (odrzuć) 63
2.11.1.3.3 QUEUE (kolejkuj) 63

2.11.1.3.4 RETURN (zwróć) 63
2.11.1.3.5 REJECT (odrzuć) 63
2.11.1.3.6 LOG (loguj) 63
2.11.1.3.7 ULOG 64
2.11.1.3.8 DNAT 64
2.11.1.3.9 SNAT 64
2.11.1.3.10 MASQUERADE 64
2.11.1.4 Diagram Netfilter/Iptables 65

3.- FACILITY MANAGEMENT 65

3.1.- CELE 65
3.2.- USŁUGI 65
3.2.1 SERWER POCZTY 65
3.2.1.1 Qmail 66
3.2.1.2 Działanie 66
3.2.2 SERWER WWW 68
3.2.2.1 Wyjaśnienie 68
3.2.2.2 Apache 68
3.2.2.3 Charakterystyki 69
3.2.2.4 Działanie 69
3.2.3 SERWER FTP 69
3.2.3.1 Wyjaśnienie 70
3.2.3.2 Opis 70
3.2.3.3 Działanie 70
3.2.3.4 Filezilla 71
3.2.4 SERWER LDAP 71
3.2.4.1 Opis LDAP 71
3.2.4.2 Zalety w stosowania LDAP 73
3.2.5 OPENLDAP 73
3.2.6 SERWER RADIUS 73
3.2.6.1 Wyjaśnienie 73
3.2.6.2 Free Radius 74
3.2.6.3 Charakterystyki 75
3.2.7 SERWER VPN 75
3.2.7.1 OpenVPN 75
3.2.7.2 Opis 75
3.2.7.3 Uwierzytelnianie OpenVPN 77
3.2.7.4 Uwierzytelnianie oparte na statycznych kluczach wstępnie współdzielonych 78
3.2.7.4.1 Zalety 78
3.2.7.4.2 Wady 78
3.2.7.5 Uwierzytelnianie oparte na certyfikatach X.509 78

4.- ZUŻYCIE ENERGII 79

4.1.- ZASILACZ BEZPRZERWOWY (UPS) I GENERATOR 79

5.- LOKALIZACJA ELEMENTÓW 85

5.1.- OGÓLNIE 85
5.2.- RYSUNKI & WIZUALIZACJA 86

1.- Hardware

1.1.- Cele

W niniejszym rozdziale wyjaśnimy propozycję dostosowania hardware'u istniejącego na miejscu. Proponowane rozwiązanie jest kompatybilne z produktami najlepszych producentów na rynku, takich jak HP, Dell i Fujitsu. Opieramy się na gamie ich produktów oraz wydajnych rozwiązaniach serwerowych, które dostosowują się do potrzeb każdej firmy, takich jak zgodne ze standardami skuteczne działanie, zaprojektowane w celu osiągnięcia wysokiej wydajności, dyspozycyjności i niezawodności.

Ci 3 producenci przestrzegają zasad dobrowolnego programu wydajności energetycznej, któremu patronuje Agencja Ochrony Środowiska USA. Program ENERGY STAR® amerykańskiej Agencji Ochrony Środowiska został niedawno przyjęty w Australii, Unii Europejskiej, Japonii i Korei.

Ostatecznego wyboru urządzeń dokona ACISA wraz z Urzędem Miasta Lublina, zgodnie z kryteriami ustalonymi wcześniej w dokumencie Projekt i Budowa Systemu Zarządzania Ruchem w Lublinie.

1.2.- Szafa Rack

Szafa rack jest metalowym stojakiem, w którym umieszcza się sprzęt elektroniczny, informatyczny i łącznościowy. Wymiary szerokości są znormalizowane, tak by były kompatybilne ze sprzętem jakiegokolwiek producenta. Nazywana jest również szafą serwerową lub teleinformatyczną.

Szafy rack do montażu serwerów na zewnątrz mają standardową szerokość 600 mm i głębokość 800 lub 1000 mm. Szerokość 600 mm dla szaf serwerowych odpowiada standardowemu wymiarowi płyt centrum danych. W ten sposób w centrach danych (CPD) można bardzo łatwo rozporządzać przestrzenią. Dla serwerów używa się również szaf rack o szerokości 800 mm, gdy potrzeba więcej miejsca po boku na okablowanie.
W szafie umieszcza się serwery, macierze dyskowe oraz biblioteki taśmowe.

1.2.1 Wymiary

Właściwości fizyczne:

Obciążenie	840.00 kg Pay Load
Wysokość	2003.0 mm
Szerokość	605.0 mm
Głębokość	1070.0 mm
Form Factor	19" 42U Wall Mounted
Ciężar (około)	122.00 kg

1.2.2 Części składowe

Zainstalowana szafa rack będzie zawierała następujące części:

- 1x Drzwi przednie
- 2x Drzwi tylne
- 2x Ściany boczne
- 2x PDU (Power Distribution Unit) Basic, Half-Height, 1ph 16A 120-240V, In(C20) Out(14*C13), No input cord; For 2420/4220/4820 (& 4210 w/AP7400 bracket)
- 2x 3.7M PDU Input Power Cord (Wall to 16A 1ph PDU) IEC309-16A plug to IEC320 C19 socket, 250V
- 1x U LCD (17in) with rack rails
- 1x Set of 4 Fans for Rack, 230V – Kit

1.2.3 System kontroli stanu szaf rack w CPD.

W celu zapewnienia nieprzerwanej pracy proponuje się system kontroli stanu szaf rack.

System zawiera RTU (zdalne urządzenie końcowe), które zarządza stanami czujników w szafie rack i informuje w czasie rzeczywistym o stanie szafy rack.

Te czujniki kontrolują:

- Czy drzwi są otwarte.
- Temperaturę wewnątrz szafy rack.
- Czujnik napięcia w szafie rack, zarówno z zasilania liniowego, jak i z zasilacza awaryjnego.
- Stan działania wentylatorów powietrza.

Poniżej przestawione są czujniki i schematy elektryczne wchodzące w skład systemu.

1.2.3.1 Wspólny czujnik magnetyczny otwartych drzwi:

Tego rodzaju czujnik sprawia o wiele mniej kłopotów niż konwencjonalne czujniki mechaniczne lub wyłączniki krańcowe oraz doskonale wpasowuje się w konstrukcję. W drzwiach szafy rack wygląda czysto i profesjonalnie; dostępny jest w kolorze szafy rack.

1.2.3.2 Czujnik temperatury w szafie rack.

Regulator temperatury TS 141

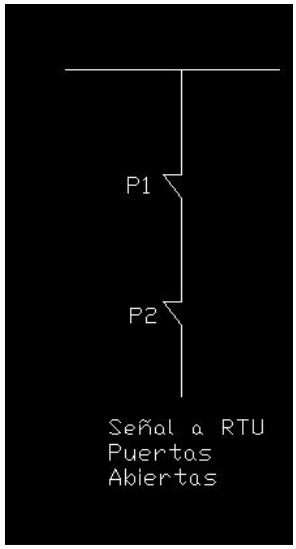
Regulator temperatury marki Himel. Ten regulator zazwyczaj jest włączony, w celu kontrolowania działania wentylatora, gdy temperatura przekroczy wyświetlaną, wcześniej ustaloną wartość. Urządzenie to pozwala regulować temperaturę wewnątrz szafy, uruchamiając wentylator tylko wtedy, gdy należy wprowadzić zimne powietrze. Pozwala to na wydłużenie okresu przydatności silnika wentylatora oraz mniejsze zużycie filtrów.

1.2.3.3 Czujniki utraty napięcia i wentylatorów.

Te czujniki są kontrolowane bezpośrednio na wyjściu przekaźnika do RTU. W ten sposób otrzymamy bezpośredni sygnał zarządzany za pomocą kontroli centralnej.

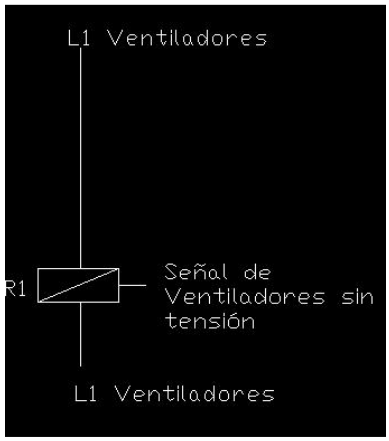
Schematy elektryczne.

Czujnik drzwi



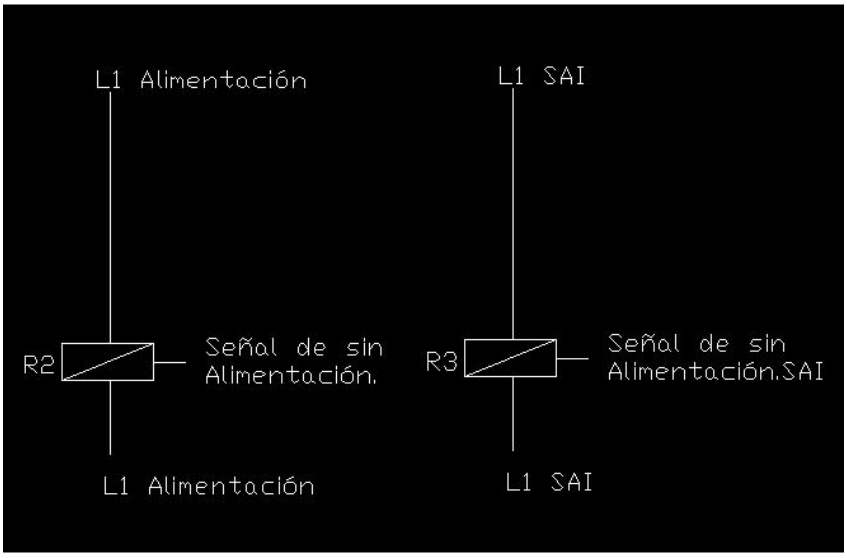
W przypadku czujnika drzwi posiadamy połączenie seryjne, które daje tylko jeden alarm “otwarte drzwi w szafie rack XX”.

Czujnik napięcia w wentylatorach.



W przypadku czujnika utraty napięcia w wentylatorach, do przeprowadzania monitoringu użyjemy przekaźnika.

Czujnik braku napięcia w zasilaniu i zasilaczu awaryjnym.



W tym przypadku za pomocą dwóch niezależnych przekaźników analizujemy utratę napięcia w każdej linii zasilania, z sygnałem w RTU. W przypadku większej ilości linii napięcia, takich jak linie redundantne lub źródła zewnętrzne, zastosuje się tę samą procedurę.

1.3.- Serwery

Właściwościami, które wzięto pod uwagę podczas wyboru serwerów, były głównie ich wysoka wydajność, dyspozycyjność i niezawodność. Uwzględniono także ich optymalizację dla Vmware vsphere Essentials Kits plus. System ten składać się będzie z trzech urządzeń serwerowych, w których zainstalowane zostaną używane w tym projekcie poszczególne serwery/ usługi wirtualne.

1.3.1 Wymiary

Właściwości fizyczne:

Wysokość: 86.7 mm
Szerokość: 445.2 mm
Głębokość: 664.6 mm

1.3.2 Części składowe

Wszystkie trzy serwery zostaną zbudowane z wykorzystaniem następujących części:

- 1x Procesor Intel Xeon X5660 (2,80GHz, 6N, pamięć podręczna 12M, QPI 6,40 GT/s, TDP 95W,Turbo, HT), DDR3-1333MHz
- 1x 24GB pamięci (3x8GB RDIMM LV w podwójnym bloku) 1333MHz
- 3x 2TB Near-Line SAS 6Gbps 7.2k 3.5" HD Hot Plug
- 1x PERC H700 zintegrowany sterownik RAID, pamięć podręczna 512MB, obudowa 12 HDD
- 1x Redundantne źródło zasilania (2 PSU) 750W, do obudowy dysków twardych łączonych na gorąco
- 2x Szafa rack jednostka rozprowadzania napięcia kable napięcia
- 1x Intel Gigabit ET czteroportowa serwerowa karta sieciowa, Cu, PCIe x4
- 1x iDRAC6 Express
- 1x Ruchome prowadnice dla szafy rack

- 2x C45 12 twardych dysków wymiennych „na gorąco-w czasie pracy” - R5 dla PERC H700, min. 3 max. 12 jednostek SAS/SATA/SSD łączonych „na gorąco-w czasie pracy”

1.4.- Przechowywanie

W celu zwiększenia pojemności magazynowania danych, do serwerów zostaną dodane dwie kasety dyskowe iSCSI 14.4 TB SAS podzielone na 6 macierzy po 4 dyski 600GB w Raid 5. Każda macierz zapewni 1,8TB magazynowania.

1.4.1 Konfiguracja

Jednostka przechowująca zostanie podzielone na 6 macierzy:

- Macierz główna (SAS) 1, 8 Tb
- Macierz główna Redundantna (SAS) 1, 8 Tb
- Macierz dodatkowa (SATA / SAS) 1,8 Tb.
- Macierz dodatkowa Redundantna (SATA / SAS) 1,8 Tb.
- Macierz Backup’u (SATA/SAS) minimum 1,8 Tb
- Macierz Backup’u Redundantna (SATA/SAS) minimum 1,8 Tb.

1.4.1.1 Macierz Główna i Dodatkowa

W tych dwóch macierzach będą magazynowały się dane z

- DANE KONFIGURACJI SYSTEMU ITS
- DANE HISTORYCZNE + DANE Z PODSYSTEMÓW

1.4.1.1.1 DANE KONFIGURACJI SYSTEMU ITS

Rozmiar jaki zajmują te dane będzie poniżej 1Gb.

1.4.1.1.2 Wielkość DANYCH HISTORYCZNYCH + PODSYSTEMÓW

1.4.1.1.2.1 Podsystem Wideonadzoru i Urządzenia Wizualizacyjne i Zapisu Obrazu.

Podsystem generuje dwa rodzaje danych:

- Dane rejestru działań wykonanych przez operatora w systemie, ze zmianami stanu urządzeń.
- Nagrania z kamer monitoringu wizyjnego.

Przy założeniu że każdego dnia zostanie zarejestrowanych 1000 zdarzeń, wymagane jest 55,7 MB miejsca potrzebnego do archiwizacji danych w ciągu 4 lat.

W celu obliczenia wymaganego miejsca na dysku, zostały przyjęte następujące założenia:

- 20 kamer monitoringu wizyjnego
- Wideo 1 klatka na sekundę
- Rozdzielczość klatki zgodna z rozdzielczością kamery
- Widmo koloru zgodne z kamerą
- 30 dni nagrywania

1.4.1.1.2.2 Podsystem Obliczania Czasów Przejazdu

Dane wygenerowane przez system składają się z:

- Danych historycznych wyliczonych czasów przejazdów jak i zdarzeń wynikających ze zmian stanu ruchu oraz z alert kamer ARTR.
- Obrazów zidentyfikowanych pojazdów.
- Stałego nagrywania ruchu pojazdów za pomocą wideo

Aby zarchiwizować tego rodzaju dane w okresie 4 lat potrzeba 2,25 GB wolnego miejsca.

Pojazdy zidentyfikowane to pojazdy, których numery rejestracyjne zostały zidentyfikowane przez jedną z kamer wideo ARTR..

W celu oszacowania średniej ilości zdjęć wygenerowanych w ciągu dnia wykonano badanie wykorzystujące dane z innych urządzeń SUR, za pomocą których obliczono średnie wartości przejazdu pojazdów przez miejsca w których umieszczone są detektory miejskie.

Podczas dni roboczych wyliczono, że średnio 4500 pojazdów mija punkt lokalizacji detektora, natomiast w weekendy na jeden detektor przypada średnio 3500 pojazdów.

Jako przeciętną średnią wartość dla jednego detektora oszacowano 4500 pojazdów.

Miejsce niezbędne do archiwizacji w ciągu trzech miesięcy wynosi **959,42 GB.**

1.4.1.1.2.3 Podsystem Sterowania Sygnalizacją

Dane wygenerowane przez system to:

- Stany alert y urządzeń tworzących system.
- System organizacji ruchu pojazdów zastosowany w sterowniku.
- Zadania wykonane w systemie.
- Zebranie danych dotyczących ruchu pojazdów.

Została przeprowadzona analiza wydawanych poleceń dotyczących archiwizowania danych w innych urządzeniach SUR. W oparciu o liczbę urządzeń kontrolujących ruch oraz na bazie innych cech systemu, wyliczono że miejsce potrzebne do archiwizacji danych w ciągu 4 lat powinno wynosić 47 GB.

1.4.1.1.2.4 Podsystem Priorytetów dla Transportu Publicznego i Lokalizacja Pojazdów Uprzywilejowanych

Podsystem generuje następujące dane:
- Dane ze zgłoszeń priorytetów dla pojazdów.
- Dane związane z lokalizacją pojazdów uprzywilejowanych.
- Stany i alerty wykorzystywanych urządzeń.
- Działania wykonywane przez operatora w systemie.

Ilość pojazdów uprzywilejowanych będzie miała bezpośredni wpływ na wymaganą ilość miejsca na dysku. Magazynowanie danych w okresie 4 lat wymaga miejsca archiwizowania o wielkości 6,853 GB.

1.4.1.1.2.5 Podsystem Informowania poprzez Panele Informacyjne o Zmiennej Treści.

Dane przechowywane w tym podsystemie będą obejmowały:
- Wiadomości wysyłane przez operatorów na do paneli
- Zmiany wiadomości na panelach (uporządkowane przez operatora albo wyświetlane automatycznie).
- Stany i alerty urządzeń podsystemu.

Po zestawieniu wymagań dotyczących archiwizacji danych w innych urządzeniach SUR oraz ilości tablic zmiennej treści można oszacować że potrzebne będzie 15,8 GB miejsca na przechowywanie danych w okresie 4 lat.

1.4.1.1.2.6 Podsystem Wykrywania i Zarządzania Zdarzeniami

Podczas szacowania miejsca potrzebnego do przechowywanie danych wzięto pod uwagę ilość urządzeń służących do detekcji zdarzeń kryzysowych w ciągu dnia, wraz ze zmianą stanu urządzeń. Wymagane jest 120 MB miejsca dla potrzeb rejestracji danych generowanych przez podsystem w okresie 4 lat.

1.4.1.1.3 Streszczenie obliczonych danych

Prezentuje się ilość potrzebnego miejsca dla wszystkich podsystemów:

Podsystem Wideo Nadzoru	Dane Historyczne	0,0544	GB
Podsystem Obliczania Czasów Przejazdu	Dane Historyczne	2,25	GB
	Obrazy ARTR	959,42	GB
Podsystem Sterowania Sygnalizacją	Dane Historyczne	46,7578	GB
Podsystem Priorytetów dla Transportu Publicznego i Lokalizacja Pojazdów Uprzywilejowanych	Dane Historyczne	6,853	GB
Podsystem Informowania poprzez Panele Informacyjne o Zmiennej Treści	Dane Historyczne	14,6851	GB
Podsystem Wykrywania i Zarządzania Zdarzeniami	Dane Historyczne	0,1172	GB

ŁĄCZNIE: Dane konfiguracji: 1 Gb.
Dane historyczne (4 lata): 70 Gb.
Zdjęcia ARTR 1 Tb

1.4.1.2 Matryca Backup'u

W matrycy backup'u przechowuje się kopie bezpieczeństwa Podsystemów, danych systemu, danych z serwerów.

1.4.2 iSCSI

iSCSI (skrót od Internet SCSI) jest standardem pozwalającym na stosowanie protokołu SCSI w sieciach TCP/IP. iSCSI jest protokołem warstwy transportowej opisanym w specyfikacjach SCSI-3.
Zastosowanie iSCSI w korporacyjnych otoczeniach produkcyjnych zostało niedawno przyspieszone dzięki zwiększeniu Gigabit Ethernet.

1.4.2.1 Działanie iSCSI

Protokół iSCSI do przesyłu danych używa TCP/IP. W przeciwieństwie do innych protokołów sieciowych zaprojektowanych do magazynowania, jak na przykład Fibre Channel (który jest podstawą większości sieci w obszarze magazynowania), do swego działania jedynie wymaga prostego interfejsu Ethernet (lub jakiejkolwiek innej kompatybilnej sieci TCP/IP). Pozwala to na scentralizowane rozwiązanie magazynowe, o niskim koszcie, nie wymagające kosztownych inwestycji ani nie narażające na częsty brak kompatybilności związany z rozwiązaniami typu Fibre Channel dla sieci w obszarach magazynowania.

1.4.3 Wymiary

Właściwości fizyczne:
Obudowa:

Wysokość	86,8 mm
Szerokość	446,3 mm
Głębokość	508,0 mm

1.4.4 Komponenty

Na macierz dyskową składają się:

- 2x Obudowa
- 24x 600GB SAS nearline 6Gb/s 7200 2,5" dysk twardy łączony „na gorąco-w czasie pracy"
- 2x Redundantne źródło zasilania (2 PSU) 600W
- 4x Zapasowy kabel zasilania 2F
- 2x Prowadnica do szafy rack

1.5.- Biblioteka taśmowa

Biblioteka taśmowa oferuje elastyczną i przystępną automatyczną obsługę taśm dla firm napotykających konieczność obsługi szybko wzrastającej ilości danych. Jest to rozwiązane wybierane przez małe, średnie i duże firmy, które potrzebują niedrogiego, prostego w obsłudze, zautomatyzowanego urządzenia do tworzenia kopii zapasowych na taśmach.
Dzięki rozwiązaniu 4U może być zamontowane w szafie rack. Można też w łatwy sposób zdalnie zarządzać wszystkimi funkcjami biblioteki taśmowej, takimi jak stan systemu, dzienniki, diagnostyka, konfiguracja i aktualizacja.
Z pomocą biblioteki taśmowej wykonuje się kopie bezpieczeństwa zainstalowanych serwerów.

1.5.1 Właściwości

Właściwości fizyczne:

Obudowa
4U form factor

Wysokość: Rack Mount 185.2 mm
Szerokość: Rack Mount 447.5 mm
Głębokość: Rack Mount 810 mm

1.5.2 Komponenty

Do biblioteki taśmowej dołączone są następujące składniki:

- 1x LTO Tape Cleaning Cartridge - Includes Barcode
- 10x LTO5 taśma pakiet 5 taśm
- 1x LTO5 etykieta na nośniki 61-120
- 1x Redundantne źródło zasilania
- 2x 2M SAS kabel 6Gbps do zewnętrznej taśmy

1.6.- Komputery / PC

Wybrane komputery zostały zaprojektowane specjalnie do otoczeń sieciowych. Są wydajne z punktu widzenia energii oraz łatwe w utrzymaniu.
Zostały zaprojektowane dla firm potrzebujących długoterminowej wydajności i niezawodnej sieci. Można je rozbudować w łatwy i niezawodny sposób.

1.6.1 Części składowe

Stacje operacyjne zbudowane są z części o następujących parametrach:

- Procesor: Intel® 2nd Generation Core i3
- Chipset: Intel® Q65 Express Chipset
- Pamięć RAM: 4GB Non-ECC dual-channel 1333MHz DDR3 SDRAM
- Karta graficzna: 512MB AMD RADEON HD 6350
- Integrated Ethernet LAN 10/100/1000
- Dysk twardy: 250GB SATA III
- Napęd optyczny: DVD+/-RW; DVD-ROM
- Wymiary korpusu: wysokość 36.0 cm x szerokość 10.2 cm x głębokość 41.0 cm.
- Źródło zasilania: Standard 250W PSU or optional 250W up to 90% Efficient PSU; Energy Star 5.0 compliant, Active PFC
- Monitor LCD – 26''
- Klawiatura USB
- Mysz optyczna USB

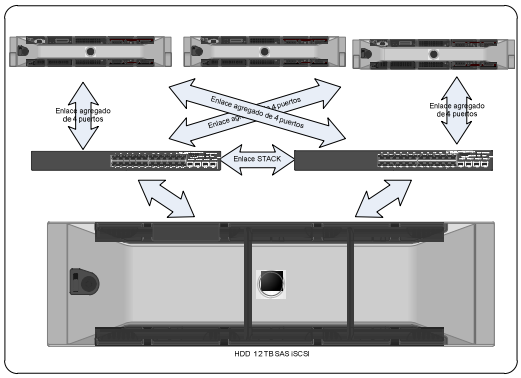
1.7.- Architektura

1.7.1 Proponowana architektura

Zaproponowana architektura jest w pełni redundantna w swej drodze, urządzeniach i łączności, tak że nie istnieje żaden SPoF (Single Point of Failure). Uwzględniamy redundancję N+1 w serwerach oraz redundancję 1+1 w pozostałych urządzeniach.

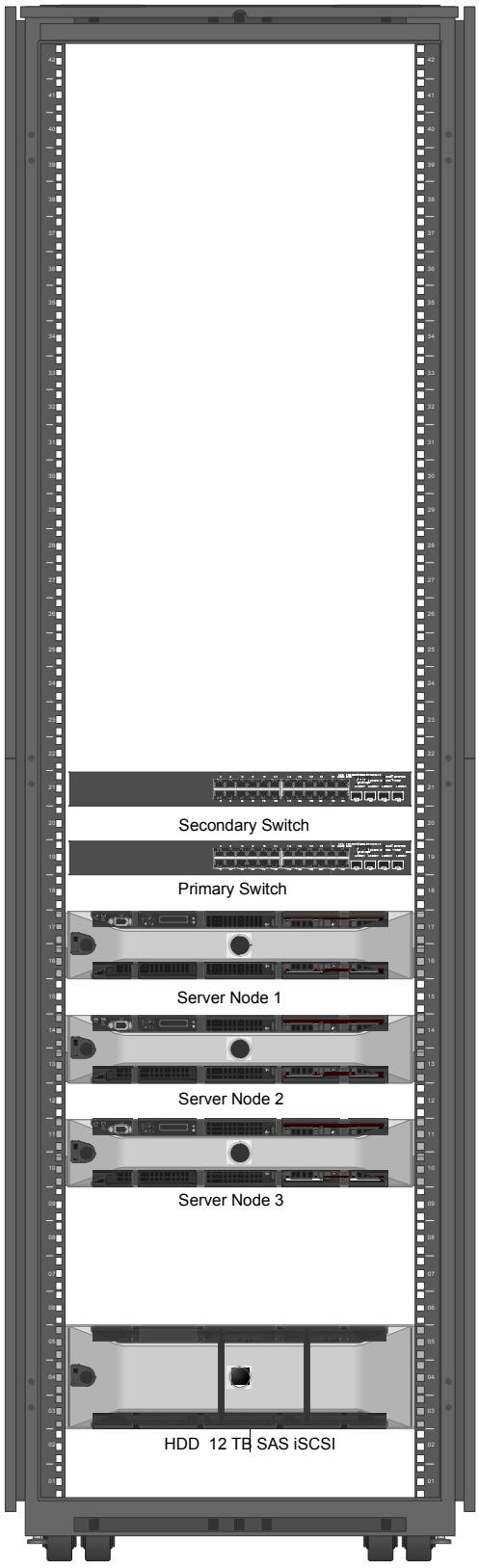
Połączenia również posiadają redundancję N+1, tak że każde urządzenie posiada przynajmniej dwa połączenia z każdym urządzeniem.

Schemat poniżej:



1.7.2 Schemat ramy

Poniżej pokazany jest typowy schemat ramy:


Secondary Switch
Primary Switch
Server Node 1
Server Node 2
Server Node 3
HDD 12 TB SAS iSCSI

2.- Software

2.1.- Otwartość systemu - cele

W niniejszym dokumencie zostanie przedstawiona propozycja oprogramowania bazowego, która ma być zainstalowana w poszczególnych urządzeniach TI systemu kontroli ruchu w Lublinie.

Jako norma ogólna są stosowane zasady European Interoperability Framework (EIF 2004) dotyczące następujących zagadnień:

- Dostępność: Stosowane są ogólnie przyjęte zasady projektowania dla interfejsów w celu zapewnienia dostępu osobom niepełnosprawnych oraz zapewnienia pomocy technicznej w języku zrozumiałym dla użytkownika.
- Wielojęzyczność: leżące u podstaw systemu architektury informatyczne muszą być językowo neutralne, aby wielojęzyczność nie była problemem utrudniającym świadczenie usług administracji elektronicznej.
- Bezpieczeństwo: W odniesieniu do użytkownika funkcje związane z bezpieczeństwem (identyfikacja, uwierzytelnianie, brak odrzucania, poufność) muszą mieć najwyższy poziom przejrzystości, zakładać minimalny wysiłek ze strony użytkownika i jednocześnie zapewniać zakładany poziom bezpieczeństwa.
- Polityka prywatności: Należy zapewniać pełną zgodność z istniejącym prawodawstwem danych na poziomie krajowym i europejskim (w szczególności z dyrektywą 2002/58/WE). W szczególności prace dotyczące interoperacyjności muszą być koordynowane z zastosowaniem mechanizmów już ustanowionych w Dyrektywie 95/46/WE (w szczególności artykuł 29). Należy stosować technologie zgodne z ochroną prywatności i jej wzmacnianiem, o ile są dostępne.
- Stosowanie otwartych standardów: orientacja musi opierać się na otwartych standardach. Słowo „otwarte” rozumie się w kontekście spełniania następujących wymogów:
    - koszty przy użytkowaniu standardów są niskie i nie są przeszkodą w dostępie do norm,
    - standard jest opublikowany,
    - standard jest przyjmowany w ramach otwartego procesu podejmowania decyzji (konsensus lub większość głosów itp.),
    - prawa własności intelektualnej standardu należą do organizacji non profit stosujących politykę w pełni swobodnego dostępu,
    - nie ma żadnych ograniczeń dotyczących reutylizacji standardu. Ocena korzyści płynących z oprogramowania z otwartym kodem.

2.2.- Interfejs - cele

Protokoły w oparciu o które zbudowany będzie interfejs nie będą powodować konieczności wnoszenia opłat na rzecz Dostawcy systemu ITS (bezpłatna rozbudowa), a korzystanie z interfejsu i obsługiwanych przez niego danych w zakresie określonym umową nie spowoduje utraty gwarancji i wsparcia na SZR.

Zawsze tam, gdzie będzie to możliwe, ACISA będzie dążyć do tego, aby wszystkie interfejsy udostępniane w SZR i podlegające ocenie spełniały brzegowe warunki technologiczne:
W zakresie protokołów komunikacji modelem odniesienia jest model OSI (ang. Open System Interconnection), lub Model ISO-OSI (pełna nazwa ISO OSI RM, ang. ISO OSI Reference Model – model odniesienia łączenia systemów otwartych) – standard zdefiniowany przez ISO oraz ITU-T opisujący strukturę komunikacji sieciowej.

Wymagane protokoły :
Warstwy Aplikacji - XML lub HTML - dla struktury przesyłanych danych
Warstwy Prezentacji - kodowanie ASCII lub Unicode – dla danych znakowych RTF lub PDF – dla danych blokowych JPEG lub BMP – dla obrazów MPEG2 lub MPEG4 lub SEQ – dla materiału wideo MP3 – dla materiałów audio (lub innego zgodnego z zaleceniem UE)
Warstwy Sesji - JMS lub kompatybilny z JMS (lub innego zgodnego z zaleceniem UE)
Warstwy Transportowe - TCP lub UDP (lub innego zgodnego z zaleceniem UE)
Warstwa Sieciowa - IP (lub innego zgodnego z zaleceniem UE)
Warstwa Łącza Danych - IEEE 802.3z 1000Base-LX lub RS-232 lub RS-485 (lub innego zgodnego z zaleceniem UE)
Warstwa Fizyczna - technologie dostępne nie będące w sprzeczności z wymaganiami dla warstw wyższych

Składowanie i dostępu do danych dla interfejsów zewnętrznych winno:
a) wykorzystywać bazy relacyjne,
b) zapewniać dostęp do danych za pośrednictwem protokołów JDBC lub ODBC (lub innego zgodnego z zaleceniem UE),
c) zapewniać możliwość tworzenia zapytań i dostępu do danych z wykorzystaniem języka SQL (lub innego zgodnego z zaleceniem UE),
d) zapewniać aby modele logiczne i fizyczne danych udokumentowane były w języku polskim,
e) Zamawiający powinien mieć prawo do zapisywania i odczytywania danych zgodnie ze specyfikacją udostępnionego interfejsu bez utraty gwarancji na System.

2.3.- DATEX II

DATEX II jest protokołem wymiany danych oraz informacji o ruchu drogowym pomiędzy różnymi organizacjami rządowymi na poziomie międzynarodowym. Jeśli chodzi o transport drogowy określa również różne standardy usług dla użytkowników dróg publicznych, np. usługi związana z powiadamieniem o zdarzeniach drogowych lub powiadamienie kierowców o stanie i warunkach ruchu drogowego.

DATEX II to również zbiór specyfikacji standaryzujących przesyłanie informacji o ruchu i podróży w Europie. W Polsce w chwili obecnej protokół DATEX II nie jest przyjęty i stosowany. ACISA projektując System Zarządzania Ruchem dla Lublina stosować się będzie do wymogów opisanych w Programie Funkcjonalno-Użytkowym.

2.4.- Systemy operacyjne

W dalszej części niniejszego rozdziału zostaną skrótowo przedstawione systemy operacyjne, które będą instalowane na komputerach TI oraz ich charakterystyki.

2.4.1 Definicja

System operacyjny (OS) jest programem lub zestawem programów, który w systemie informatycznym zarządza zasobami sprzętowymi i zapewnia usługi programom aplikacyjnym, pracując w trybie uprzywilejowanym w stosunku do innych programów.

2.4.2 Serwery

2.4.2.1 Windows Server 2008

Windows Server 2008 jest nazwą systemu operacyjnego firmy Microsoft zaprojektowanych dla serwerów.
Nowy Windows Server 2008 R2 jest produktywną i ekonomiczną platformą serwerową, zapewniającą ponadto wirtualizację z niskimi kosztami, możliwości oszczędności energii oraz dobre doświadczenia dla użytkowników końcowych.

Umożliwia profesjonalistom TI większą kontrolą nad infrastrukturą serwerową i sieciową i udostępnia organizacjom korporacyjną platformę dla skutecznej realizacji zadań biznesowych dzięki zoptymalizowanemu zarządzaniu, dłuższemu czasowi działanie i zwiększeniu wydajności pracowników w biurach zdalnych, zwiększeniu wydajności wirtualizacji i zarządzania zużyciem energii.

2.4.2.1.1 Charakterystyki

Istnieją pewnie różnice (mniej lub bardziej znaczące) dotyczące architektury nowego serwera Windows Server 2008, które mogą drastycznie zmienić sposób używania tego systemu operacyjnego. Te zmiany dotyczą sposobu, w jaki jest zarządzany system, by można było kontrolować sprzęt w sposób forma bardziej efektywny, można go lepiej kontrolować zdalnie i zmieniać radykalnie politykę bezpieczeństwa. Do wprowadzonych usprawnień należą:

- Nowy proces naprawy systemów plików NTFS: działający w tle proces naprawiający uszkodzone pliki.
- Umożliwia zbudowanie klastra.
- Równoległe tworzenie sesji użytkownika: skraca czas oczekiwania dla usług terminalowych i czas masowego tworzenia sesji użytkownika.
- Czyste zatrzymywanie usług.
- System plików SMB2: 30 do 40 razy szybszy dostęp do serwerów multimediów.
- Address Space Load Randomization (ASLR): ochrona przed złośliwym oprogramowaniem (malware) zapewniana przez kontrolery pamięci.
- Windows Hardware Error Architecture (WHEA): usprawniony i ustandaryzowany protokół raportowania błędów.
- Wirtualizacja Windows Server: zwiększenie wydajności wirtualizacji.
- PowerShell: włączanie ulepszonej konsola z obsługą GUI dla administracji.
- Server Core: jądro systemu zostało odświeżone, zastosowano wiele nowych usprawnień. W niektórych wersjach zostało całkowicie usunięte środowisko graficzne systemu operacyjnego, obsługa .NET Framework, w tym aplikacji ASP.NET oraz obsługa Windows PowerShell.
- Wprowadzenie dwóch nowych funkcji wirtualizacji, RemoteFX i Dynamic Memory.
    - Dynamic Memory jest funkcją Hyper-V wspomagającą wykorzystanie pamięci fizycznej w sposób bardziej skuteczny, poprzez traktowanie jej jako zasobu współdzielonego, który może być przydzielany w locie uruchomionym maszynom wirtualnym. Dopasowuje ona ilość pamięci dostępnej dla maszyny wirtualnej w oparciu o zmiany zapotrzebowania i zdefiniowane wartości. W ten sposób umożliwia

ona zwiększenie gęstości maszyn wirtualnych bez szkody dla wydajności i skalowalności.

- Remote FX jest technologią wprowadzającą ulepszenia w doświadczeniach użytkownika końcowego, dodane do protokołu pulpitu zdalnego (RDP). Umożliwia on między innymi wirtualizowanie GPU (procesor karty graficznej) na serwerze, dodawanie multimediów i doświadczeń 3D dla VDI (infrastruktura pulpitu wirtualnego)

2.4.2.1.2 Licencja

2 x Windows Server 2008 R2 Enterprise Edition
2 x CAL Windows 2008 R2
N x CAL Client Access License

2.4.2.2 Red Hat Cluster Suite

Systemy klastrowe zapewniają niezawodność, skalowalność i dostępność dla krytycznych usług produkcyjnych. Dzięki Red Hat Cluster Suite, można tworzyć klaster spełniający wymagania dotyczące wydajności, wysokiej dostępności, równoważenia obciążenia, skalowalności, współdzielenia plików i oszczędności. Niniejszy rozdział przedstawia podsumowanie komponentów i funkcji sieciowych Red Hat Cluster Suite, zawiera on następujące punkty:

- Podstawowe informacje o klastrze
- Red Hat Cluster Suite Introduction
- Infrastruktura klastra
- Administracja usługami o wysokiej dostępności
- Red Hat GFS
- Menedżer wolumenów logicznych klastra
- Globalne sieciowe urządzenie blokowe (GNBD)
- Serwer wirtualny Linux
- Narzędzia administracyjne klastra
- Interfejs graficzny do administrowania serwerem wirtualnym Linux

2.4.2.2.1 Podstawowe informacje o klastrze

Klaster składa się z dwóch lub więcej komputerów (nazywanych węzłami lub członkami), które, działając razem, wykonują jedno zadanie. Istnieją cztery klasy klastrów, zapewniające różne funkcje:

Pamięć masowa
Wysoka dostępność
Równoważenie obciążenia
Wysoka wydajność
Klastry obsługujące pamięć masową obsługują obraz systemu plików, który jest spójny dla serwerów w klastrze, umożliwiający serwerom jednoczesny zapis i odczyt we współdzielonym systemie plików. Klaster obsługujący pamięć masową upraszcza administrację pamięcią masową poprzez ograniczenie instalowania aplikacji do jednego systemu plików. I tak, w przypadku systemu plików współdzielonego w klastrze, klaster obsługujący pamięć masowa eliminuje konieczność kopiowania większej ilości danych aplikacji i upraszcza tworzenie kopii bezpieczeństwa i odtwarzanie danych. Red Hat Cluster Suite zapewnia pamięć masową dla klastra dzięki technologii Red Hat GFS.

Klastry wysokiej dostępności zapewniają stałą dostępność usług poprzez wyeliminowanie przestojów w wyniku awarii jednego elementu i poprzez proces odtwarzanie funkcjonalności po awarii przez przeniesienie usługi z uszkodzonego węzła klastra do innego, w pełni sprawnego węzła. Zwykle usługi w klastrach o wysokiej dostępności odczytują i zapisują dane poprzez odczyt i zapis w zamontowanym systemie plików. W ten sposób klaster o wysokiej dostępności mysi utrzymywać integralność danych, gdy węzeł uzyskuje przejmuje nad usługą od innego węzła. Węzły uszkodzone nie są widoczne przez klientów spoza klastra. Klastry wysokiej dostępności są określane również jako klastry odzyskujące funkcjonalność po awarii. Red Hat Cluster Suite zapewnia klaster o wysokiej dostępności za pomocą komponentu administracji usługami o wysokiej dostępności.

Klastry obsługujące równoważenie obciążenia odpowiadają na żądania usług sieciowych, korzystając z różnych węzłów w celu zrównoważenia obsługi żądań przez węzły klastra. Równoważenie obciążenia zapewnia ekonomiczną skalowalność, ponieważ można konfigurować liczbę węzłów zgodnie z wymaganiami równoważenia obciążenia. Jeżeli węzeł w klastrze obsługującym równoważenie obciążenia ulega awarii, oprogramowanie obsługujące równoważenie obciążenia wykrywa awarię i przekierowuje żądania do innych węzłów w klastrze. W klastrze obsługującym równoważenie obciążeń węzły uszkodzone nie są widoczne przez klientów spoza klastra. Red Hat Cluster Suite zapewnia równoważenie obciążeń za pomocą LVS (serwer wirtualny Linux).

Klastry zapewniające wysoką wydajność wykorzystują węzły do współbieżnego wykonywania obliczeń. Klaster o wysokiej wydajności umożliwia aplikacjom jednoczesne wykonywanie, zwiększając w ten sposób ich wydajność. Klastry o wysokiej wydajności są znane jako klastry obliczeniowe lub klastry do przetwarzania sieciowego.

2.4.2.2.2 Omówienie Red Hat Cluster

Red Hat Cluster Suite (RHCS) jest zintegrowanym pakietem komponentów oprogramowania, który może być zaimplementowany w dużej liczbie konfiguracji w celu zapewnienia wydajności, wysokiej dostępności, równoważenia obciążenia, skalowalności, współdzielenia plików i ekonomicznego wykorzystania zasobów.

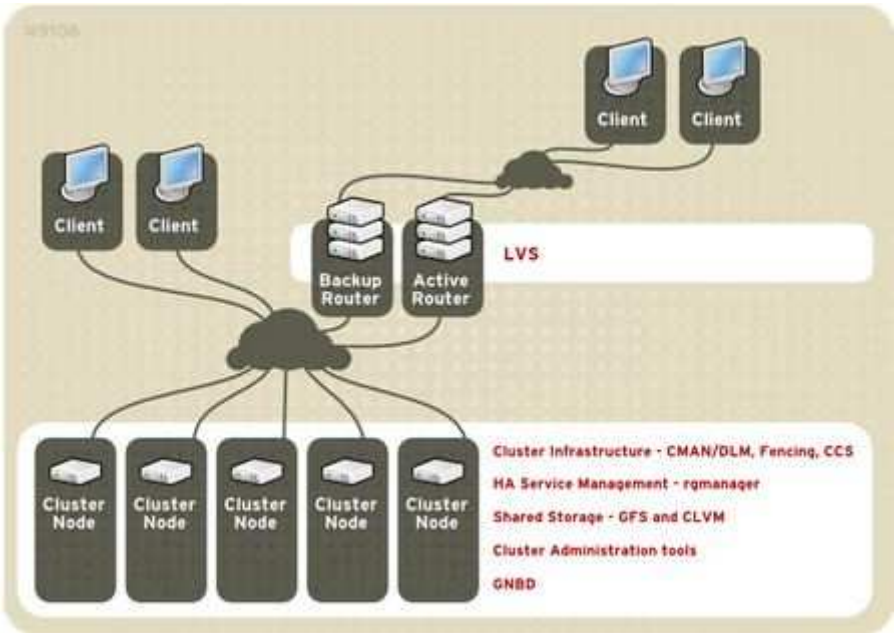
RHCS składa się z następujących głównych komponentów (zob. fig 1.1 „Wstęp do Red Hat Cluster Suite”:
Infrastruktura klastra — zapewnia podstawowe funkcje umożliwiające połączone działanie węzłów w klastrze: administracja plikiem konfiguracyjnym, administracja członkami, administracja wyłączeniami w celu odłączenia i odizolowania.

Administracja usługami o wysokiej dostępności — Zapewnia przenoszenie usług klastra w przypadku awarii węzła.
Narzędzie administracyjne klastra — narzędzia konfiguracyjne i administracyjne do konfigurowania i administrowania klastrami Red Hat. Narzędzia są używane w połączeniu z komponentami infrastruktury klastra, komponentami zapewniającymi wysoką dostępność, komponentami do administrowania usługami i pamięcią masową.

Serwer wirtualny Linux (LVS) — Oprogramowanie obsługując routing zapewniające równoważenie obciążenia adresów IP. LVS jest uruchamiany na parze dedykowanych serwerów rozdzielających żądania klientów do serwerów rzeczywistych znajdujących się za serwerami LVS.

Do Red Hat Cluster Suite można dodać inne komponenty. Te komponenty stanowią część dodatkowego pakietu (nie są one częścią Red Hat Cluster Suite):

Red Hat GFS (globalny system plików) — zapewnia system plików dla klastra, który można stosować dla Red Hat Cluster Suite. GFS umożliwia węzłowe współdzielenie pamięci masowej na poziomie bloków, jakby były podłączone lokalnie w każdym z węzłów.
Administrator wolumenów logicznych klastra (CLVM) — Zapewnia administrowanie wolumenami pamięci masowej klastra.



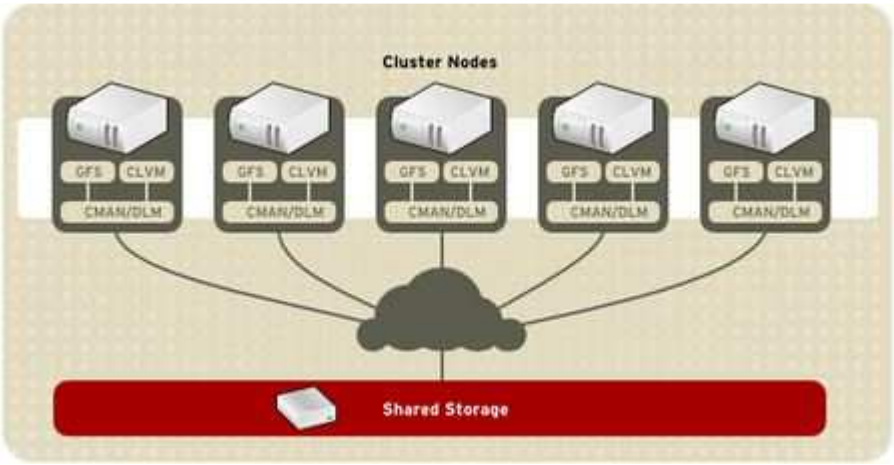
2.4.2.2.3 Infrastruktura klastra

Infrastruktura klastra Red Hat Cluster Suite zapewnia podstawowe funkcje umożliwiające grupie komputerów (nazywanych węzłami lub członkami) wspólną pracę w klastrze. Po utworzeniu klastra z użyciem infrastruktury klastra można używać innych komponentów Red Hat Cluster Suite w celu zapewnienia funkcji wymaganych dla klastra (na przykład, można utworzyć klaster w celu współdzielenia plików w systemie plików GFS lub utworzenia usługi odpornej na awarie). Infrastruktura klastra zapewnia następujące funkcje:

- Administracja klastrem
- Administracja zamykaniem w celu odłączenia
- Fencing
- Administracja konfiguracją klastra

2.4.2.2.3.1 Administracja klastrem

Cluster management zarządza kworum i członkostwem klastra. CMAN (skrót od cluster manager) zapewnia zarządzania klastrami w systemie Red Hat Cluster Suite dla Red Hat Enterprise Linux 5. CMAN jest rozproszonym menadżerem klastra, działającym w każdym węźle klastra, zarządzania klastrami jest rozproszone we wszystkich węzłach w klastrze.

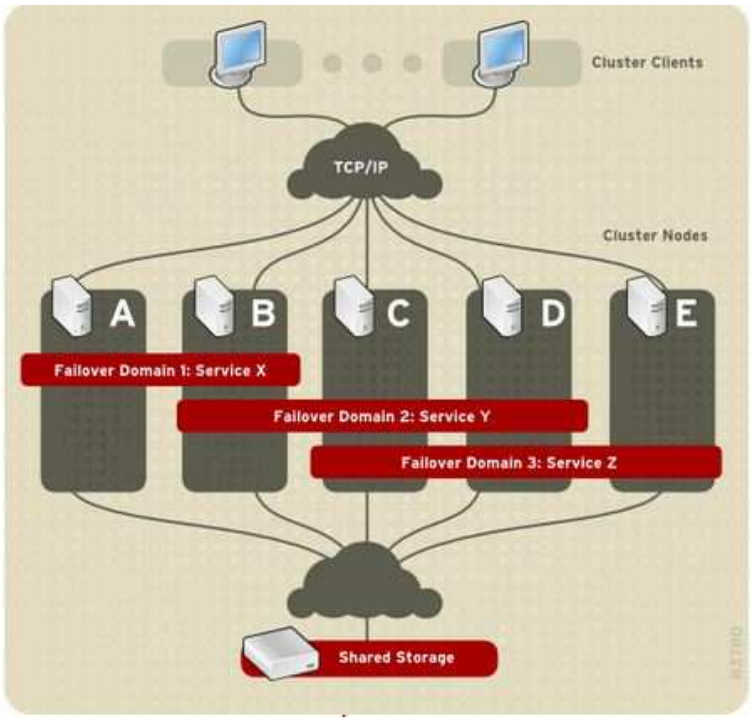


CMAN kontroluje członkostwo, sprawdzając komunikaty innych węzłów klastra. Kiedy członkowie klastra zmieniają się, administrator klastra informuje inne komponenty infrastruktury, aby wykonywały odpowiednie działania. Na przykład kiedy węzeł A dołącza do klastra i montuje system plików GFS, który jest zamontowany przez węzły B i C, jest wymagany nowy dziennik i nowa administracja zamknięciami w celu wyłączenia, aby węzeł A mógł używać tego systemu plików.
Jeżeli węzeł klastra nie przekazuje komunikatu w określonym czasie, administrator klastra usuwa węzeł klastra i informuje inne komponenty infrastruktury klastra, że węzeł nie jest już członkiem klastra.

2.4.2.2.4 Administracja usługami o wysokiej dostępności

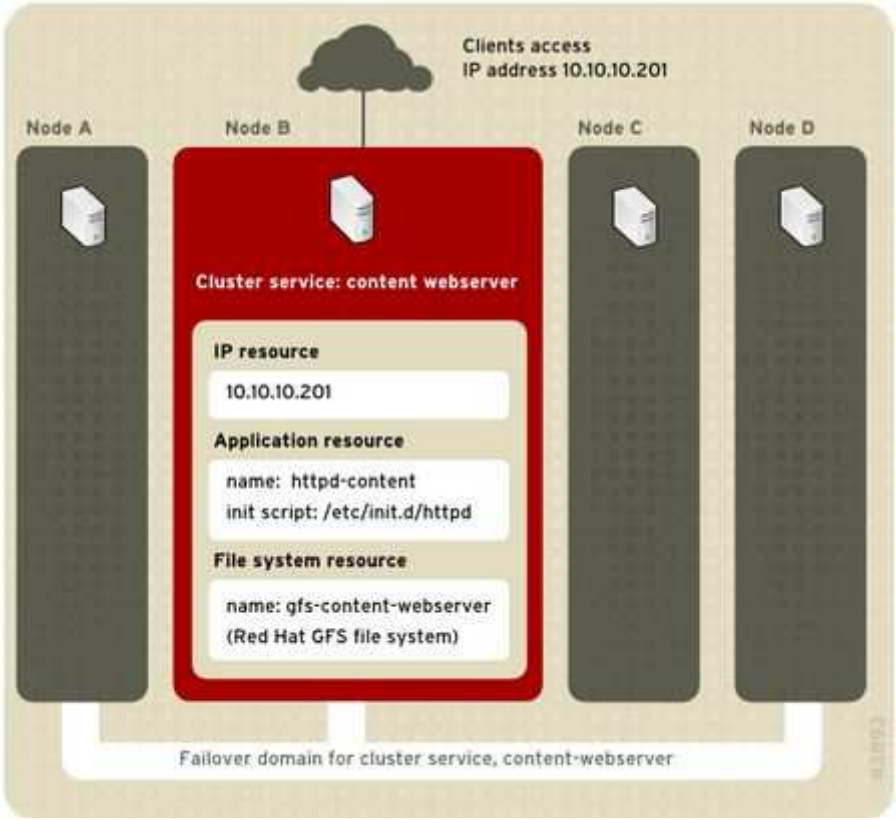
Administracja usługami o wysokiej dostępności zapewnia możliwość tworzenia usług klastra o wysokiej dostępności w klastrze Red Hat i administrowanie nimi. Kluczowym komponentem administracji usługami o wysokiej dostępności w klastrze sieciowy Red Hat jest rgmanager. Ten komponent zapewnia odporność na awarie dla aplikacji. W klastrze Red Hat aplikacja jest skonfigurowana z innymi zasobami klastra w celu utworzenia usługa klastra o wysokiej dostępności. Usługa klastra wysokiej dostępności może być przenoszona między węzłami bez przerwy w działaniu widocznej dla klientów klastra. Odtwarzanie funkcjonalności może następować, gdy jeden z węzłów klastra ulega awarii lub gdy administrator systemu klastrowego przenosi usługę między węzłami (na przykład jeśli jest konieczne przeprowadzenie konserwacji węzła).

Aby utworzyć usługę wysokiej dostępności należy ją konfigurować w pliku konfiguracyjnym klastra. Usługa klastra wykorzystuje zasoby klastra. Zasoby klastra są blokami konstrukcyjnymi, które są tworzone i administrowane w pliku konfiguracyjnym klastra — na przykład adres IP, skrypt inicjalizujący aplikacji lub współdzielona partycja Red Hat GFS.
Można powiązać usługę klastra z domeną failover. Domena awaryjna (failover) jest podzbiorem węzłów klastra, na których może być uruchamiana dana usługa klastrowania.



Domena pracy awaryjnej 1 jest skonfigurowana, aby ograniczyć funkcje pracy awaryjnej do tej domeny, dlatego usługa klastrowania X może tylko przełączana między węzłem A i węzłem B. Jest również skonfigurowana domena pracy awaryjnej 2, aby ograniczyć funkcję procy awaryjnej do tej domeny, dodatkowo, jest skonfigurowany priorytet pracy w sytuacji awaryjnej. Priorytet domeny pracy awaryjnej 3 jest skonfigurowany z węzłem C z priorytetem 1, węzłem B z priorytetem 2 i węzłem D z priorytetem 3. Jeśli węzeł C zawiedzie, usługa klastra

Y zostaje przełączona do następnego węzła B. Jeśli nie może przełączyć się do węzła B, próbuje przełączyć się do węzła D. Domena pracy awaryjnej 3 jest skonfigurowana bez priorytetu i bez ograniczeń. Jeśli węzeł, na którym działa usługa klastrowania Z zawiedzie, usługa klastrowania Z próbuje przełączyć się na jeden z węzłów w domenie pracy awaryjnej 3. Jednakże, jeśli żaden z tych węzłów nie jest dostępny, usługa klastrowania Z może zostać przełączona na dowolny węzeł w klastrze.



Przedstawia przykład usługi klastrowania wysokiej dostępności, którą jest serwer WWW o nazwie „content-serwer”. Działa on w węźle klastra B i należy do domeny failover składającej się z węzłów A, B i D. Ponadto domena pracy awaryjnej jest skonfigurowane z priorytetem pracy awaryjnej tak, by następowało przełączania do węzła D przełączeniem do węzła A oraz ograniczenie pracy awaryjnej wyłącznie do węzłów tej domeny pracy awaryjnej. Usługa klastrowania obejmuje następujące zasoby klastra:

- Zasób adres IP — adres IP 10.10.10.201.
- Zasób aplikacji o nazwie „httpd-content” — skrypt inicjalizacji serwera WWW /etc/init.d/httpd (określający httpd).
- Zasób systemu plików — Red Hat GFS noszący nazwę „gfs-content-webserver”.

Klienci uzyskują dostęp do usługi klastra przez adres IP 10.10.10.201, umożliwiając interakcję z aplikacją serwera WWW (httpd-content). Aplikacja httpd-content korzysta z systemu plików gfs-content-webserver. Jeżeli węzeł B ulega awarii, usługa klastra content-webserver jest przenoszona do węzła D. Jeśli węzeł

D nie jest dostępny lub ulega awarii, usługa jest przenoszona do węzła A. Odtwarzanie funkcjonalności po awarii nie będzie widoczne dla klientów. Uzyskanie dostępu do usługi klastra będzie dostępne z innego węzła klastra z użyciem tego samego adresu IP, który był używany przed awaria.

2.4.2.2.5 Red Hat GFS

Red Hat GFS jest systemem pliku klastra umożliwiającym węzłom klastra jednoczesny dostęp do współdzielonego urządzenia blokowego. GFS jest natywnym systemem plików współdziałającym bezpośrednio z warstwą VFS interfejsu systemu plików jądra Linuksa. GFS korzysta z rozproszonych metadanych i różnych dzienników (journals) w celu zapewnienia optymalnej pracy w klastrze. W celu zachowania integralności systemu plików, GFS stosuje wzajemne blokady w celu kontrolowania operacji I/O. Gdy węzeł zmienia dane w systemie plików GFS, zmiany są natychmiast widoczne dla innych węzłów klastra, które używają tego systemu plików.

Dzięki Red Hat GFS można uzyskać dłuższy czas działania aplikacji dzięki następującym korzyściom:
Uproszczenie infrastruktury danych
Umożliwienie instalowania aplikacji dla całego klastra.
Uniknięcie konieczności wykonywania niepotrzebnych kopii danych aplikacji (duplikacja)

Umożliwia dostęp dla współbieżnego odczytu i zapisu danych licznych klientów.
Upraszcza tworzenie kopii bezpieczeństwa i odtwarzania danych po awarii (wymagane jest tylko kopiowanie lub odzyskanie tylko jednego systemu plików).
Zwiększa wykorzystanie zasobów pamięci masowych; zmniejsza koszty administracji pamięcią masową.
Administrowanie pamięcią masową jako jedną całością, a nie jako odrębnymi partycjami.
Zmniejszenie ogólnej wielkości pamięci masowych przez wyeliminowanie konieczności duplikowania danych. Skalowania klastra poprzez dodanie serwerów lub pamięci masowej w locie.
Uniknięcie partycjonowania pamięci masowych z użyciem skomplikowanych technik.
Dodawanie serwerów w klaster poprzez montowanie we wspólnym systemie plików.
Węzły, na których jest uruchamiany system GFS mogą być konfigurowane i administrowane za pomocą narzędzi konfiguracyjnych i administracyjnych Red Hat Cluster Suite. Administracja wolumenami jest realizowana za pomocą CLVM (Clúster Logical Volume Manager). Red Hat GFS zapewnia współdzielenie danych między węzłami GFS w klastrze Red Hat. GFS zapewnia spójny, jednolity widok przestrzeni nazw systemu pliku w węzłach GFS w klastrze Red Hat. GFS umożliwia instalowanie i uruchamianie aplikacji bez konieczności posiadania szczegółowej wiedzy o infrastrukturze pamięci masowej. Podobnie GFS zapewnia funkcje, które są typowo wymagane w środowiskach w firmach, takie jak przydziały dyskowe, różnego typu dzienniki i obsługę wielu tras.

GFS zapewnia elastyczną metodę obsługi pamięci masowej w sieci w zależności od wydajności, skalowalności i aspektów ekonomicznych wymaganych dla środowiska pamięci masowej. Ten rozdział przedstawia podstawowe, skrócone informacje umożliwiające czytelnikowi zrozumienie systemu GFS.

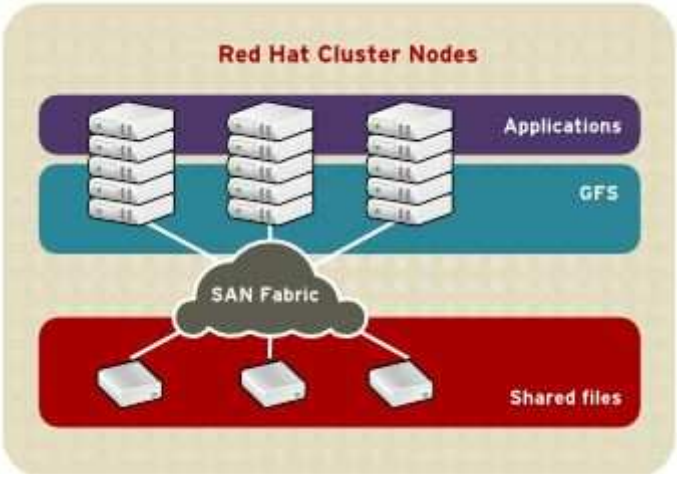
Można implementować GFS w różnych konfiguracjach w zależności od potrzeb dotyczących wydajności, skalowalności i oszczędności. W celu uzyskania najwyższej wydajności i skalowalności można wdrożyć GFS w klastrze podłączony bezpośrednio do sieci SAN. Dla mniej wymagających potrzeb, gdzie możliwe są oszczędności, można wdrożyć GFS w klastrze podłączonym do sieci LAN z serwerami, na których są stosowane rozwiązania GNBD (Global Network Block Device)) lub iSCSI (Internet Small Computer System Interface)

Następne punkty przedstawiają przykłady, w jaki sposób GFS może być zaimplementowany w celu zapewnienia wydajności, skalowalności i oszczędności:

- Wysoka wydajność i skalowalność
- Wydajność, skalowalność i umiarkowana cena
- Oszczędność i wydajność

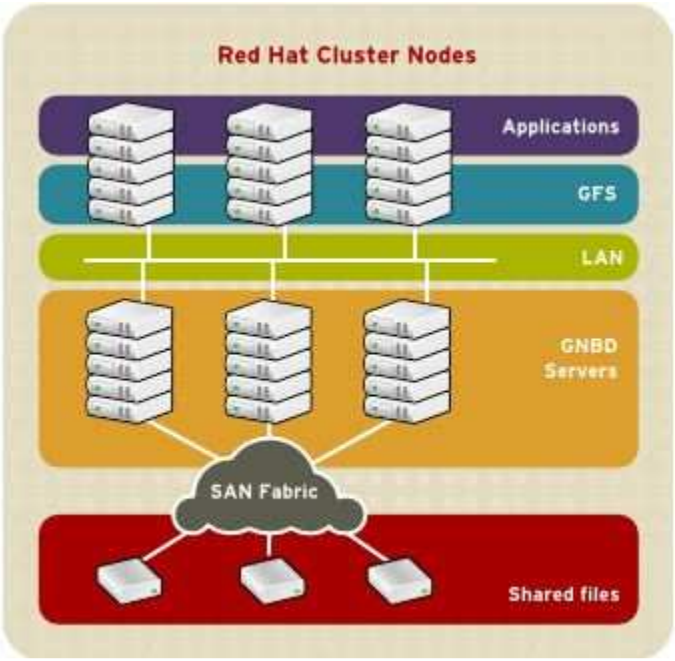
2.4.2.2.5.1 Wysoka wydajność i skalowalność

Najwyższą wydajność dla współdzielonych plików można uzyskać, gdy aplikacje mają bezpośredni dostęp do pamięci masowej. Konfiguracja GFS SAN na ryc. „GFS z SAN” zapewnia wysoką wydajność dla współdzielonych plików i systemów plików. Aplikacje systemu Linux są uruchamiane bezpośrednio na węzłach klastra, w którym jest stosowany GFS. Bez protokołów obsługi plików i serwerów pamięci masowych spowolniających dostęp do danych, wydajność jest podobna do pojedynczych serwerów linuksowych z podłączonymi bezpośrednio pamięciami masowym. Ponadto każdy węzeł aplikacji GFS ma równy dostęp do wszystkich plików danych. GFS obsługuje ponad 300 węzłów GFS.



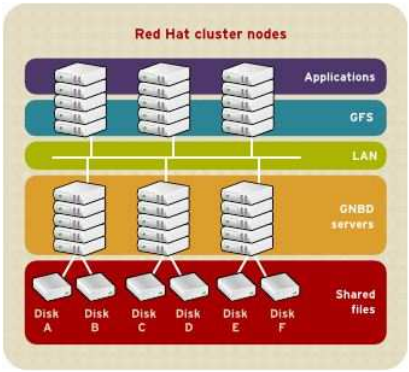
2.4.2.2.5.2 Wydajność, skalowalność i umiarkowana cena

Wiele linuksowych aplikacji klienckich w sieci LAN może współdzielić te same dane w SAN jak przedstawiono na ryc. „GFS, GNBD i sieć SAN”. Blokowa pamięć masowej SAN jest przedstawiane klientom sieciowym przez serwery GNBD jako blokowe urządzenia pamięci masowej. Z punktu widzenia aplikacji klienckiej dostęp do pamięci masowej jest taki sam, jakby byłą przyłączona bezpośrednio do serwera, na którym jest uruchomiona aplikacja. Dane są przechowywane w sieci SAN. Urządzenia pamięci masowej i dane mogą być równie współdzielone przez aplikacje klienckie w sieci. Blokowanie plików i funkcje udostępniania plików są obsługiwane przez GFS dla każdego klienta sieci.



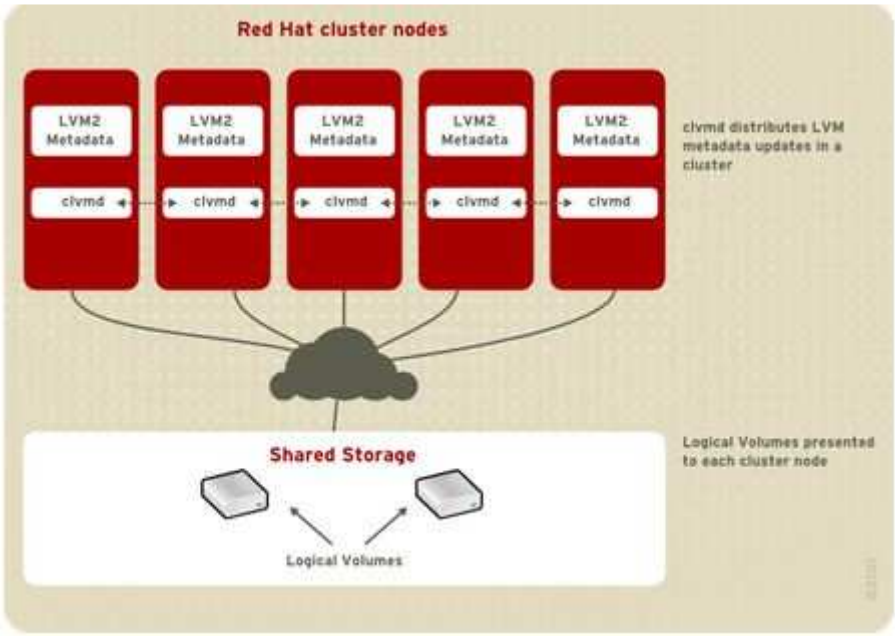
2.4.2.2.5.3 Oszczędność i wydajność

Ryc. „GFS y GNBD z pamięcią masową połączoną bezpośrednio” przedstawia, w jaki sposób jak linuksowe aplikacje klienckie mogą korzystać z istniejącej topologii sieci Ethernet w celu uzyskania współdzielonego dostępu do wszystkich urządzeń blokowych. Pliki danych klienta oraz systemy plików mogą być współdzielone za pomocą GFS na każdym kliencie. Stosowanie pracy awaryjnej można w pełni zautomatyzować za pomocą pakietu Red Hat Cluster Suite.



2.4.2.2.6 Menedżer wolumenów logicznych klastra

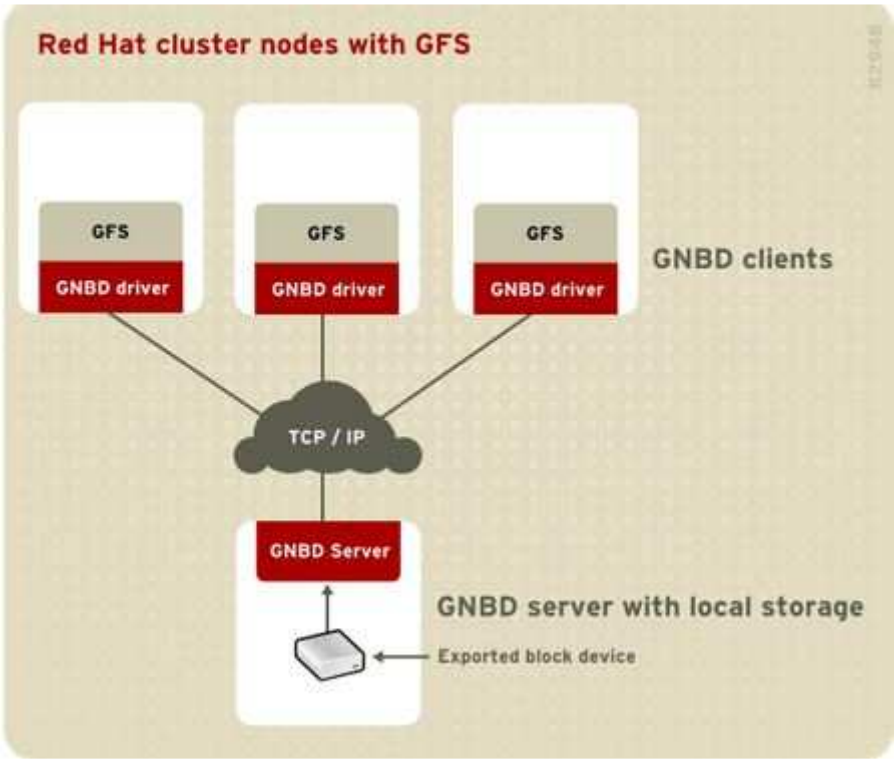
Menedżer wolumenów logicznych klastra (CLVM) zapewnia wersję LVM2 na poziomie klastra. CLVM zapewnia te same funkcje co LVM2 dla pojedynczego węzła, lecz umożliwia dostępność wolumenów dla wszystkich węzłów w klastrze Red Hat. Wolumeny logiczne utworzone za pomocą CLVM sprawiają, że wolumeny logiczne są dostępne dla wszystkich węzłów w klastrze.
Kluczowym elementem w CLVM jest clvmd. clvmd jest demonem zapewniającym rozszerzenie klastrowania dla standardowego zestawu narzędzi LVM2 i umożliwia stosowanie poleceń LVM2 do zarządzania współdzieloną pamięcią masową. clvmd działa w każdym węźle klastra i dystrybuuje aktualizacje metadanych LVM w klastrze, dzięki czemu każdy węzeł klastra widzi w taki sam sposób wolumeny logiczne (zon. ryc. „Przegląd CLVM”). Logiczne wolumeny utworzone za pomocą CLVM we współdzielonych pamięci masowych są widoczne dla wszystkich węzłów, które mają dostęp do wspólnej pamięci masowej. CLVM umożliwia użytkownikowi konfigurowanie wolumenów logicznych we współdzielonej pamięci masowej, blokując dostęp do fizycznej pamięci masowej, gdy jest skonfigurowany wolumen logiczny. CLVM używa usługi zarządzania blokadami udostępnianej przez infrastrukturę klastra.



Można skonfigurować CLVM za pomocą tych samych poleceń co LVM2, korzystając z graficznego interfejsu użytkownika LVM lub też korzystając z funkcji konfiguracji pamięci masowej w graficznym interfejsie użytkownika do konfiguracji klastra Conga.

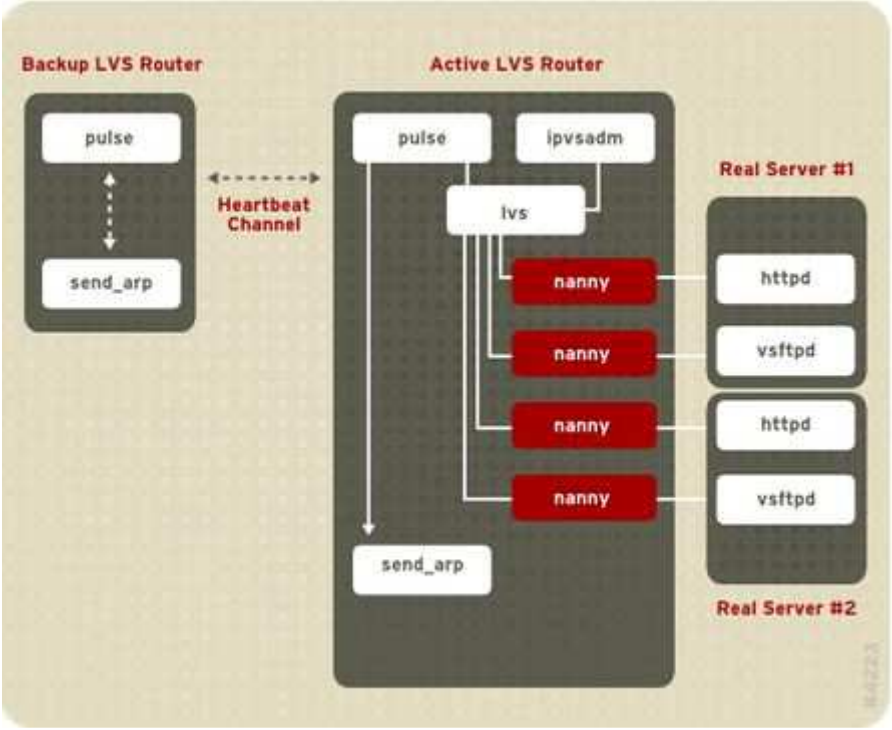
2.4.2.2.7 Globalne sieciowe urządzenie blokowe (GNBD)

Globalne sieciowe urządzenie blokowe globalny (GNDB) zapewnia do urządzenia blokowego dla Red Hat GFS przez TCP/IP. GNBD jest elementem podobnym do NBD, jednak GNBD jest elementem specyficznym dla GFS i został zaprojektowany do użycia specjalnie z GFS. GNBD jest użyteczny, gdy stosowanie bardziej efektywnych technologii— światłowody lub proste inicjatory SCSI — nie są konieczne lub nie jest właściwe z punktu widzenia ekonomii.
GNBD składa się z dwóch głównych komponentów: klienta GNBD i serwera GNBD. klient GNBD działa w węźle z GFS i importuje urządzenie blokowe eksportowane przez serwer GNBD. Serwer GNBD działa w innym węźle i eksportuje pamięć masową na poziomie bloku ze swojej lokalnej pamięci masowej (pamięć masowa podłączona bezpośrednio lub SAN). Zob. ryc. „Schemat ogólny GNBD”. Dostęp do urządzenia eksportowanego przez serwer GNBD może uzyskiwać wielu klientów GNBD, dzięki czemu GNBD nadaje się do użycia przez grupę węzłów korzystających z GFS.



2.4.2.2.8 Serwer wirtualny Linux

Serwer wirtualny Linuks (LVS) jest zintegrowaną grupą komponentów programowych mającą na celu równoważenie obciążenia IP w grupie serwerów rzeczywistych. LVS jest realizowane przez parę komputerów skonfigurowanych w taki sam sposób: jeden z nich działa jako aktywny router LVS, drugi działa jako zapasowy router LVS. Aktywny router LVS ma dwie funkcje:
Równoważenie obciążenia między serwerami rzeczywistymi.
Sprawdzanie integralności usług na każdym serwerze rzeczywistym.
Zapasowy router LVS sprawdza stan aktywnego routera LVS i przejmuje jego funkcje w przypadku awarii.



Demon pulse jest uruchamiana na aktywnym serwerze LVS jak i na serwerze pasywnym. Na zapasowym routerze LVS pulse wysyła sygnał na interfejs publiczny aktywnego routera LVS, aby sprawdzić, czy serwer działa we właściwy sposób. Na aktywnym routerze LVS pulse uruchamia demona lvs i odpowiada na sygnały pochodzące z pasywnego routera LVS.
Po uruchomieniu demon lvs wywołuje program użytkowy ipvsadmin, aby konfigurować i utrzymywać tabela routingu IPVS (IP Virtual Server) w jądrze i uruchamia proces nanny dla każdego serwera wirtualnego skonfigurowanego na każdym serwerze rzeczywistym. Każdy proces nanny sprawdza stan każdego serwera skonfigurowanego na serwerze rzeczywistym i informuje demona lvs, jeżeli usługa na serwerze rzeczywistym nie działa. Jeżeli usługa nie działa, demon lvs zleca ipvsadm usunięcie serwera rzeczywistego z tabeli tras IPVS.
Jeżeli zapasowy router LVS nie otrzymuje odpowiedzi z aktywnego routera LVS, najpierw uruchamia proces przywracania funkcjonalności po awarii, wywołując send_arp, aby przypisać na nowo wszystkie wirtualne adresy IP do adresów sprzętowych NIC (adresy MAC) pomocniczego routera LVS, wysyła polecenie w celu włączenia aktywnego routera LVS za pomocą publicznych i prywatnych interfejsów sieciowych w celu zatrzymania demona lvs na aktywnym routerze LVS i uruchamia demona lvs na zapasowym routerze LVS, aby akceptował żądania skonfigurowanych serwerów wirtualnych.
Dla użytkownika zewnętrznego uzyskującego dostęp do hostowanej usługi (np. witryny WWW lub bazy danych), LVS ma postać jednego serwera. Oczywiście użytkownik ma dostęp do serwera rzeczywistego poprzez routery LVS.
Ponieważ w LVX nie istnieją komponenty wewnętrzne, których funkcją byłoby rozdzielanie danych między serwery rzeczywiste, istnieją dwie opcje podstawowe:

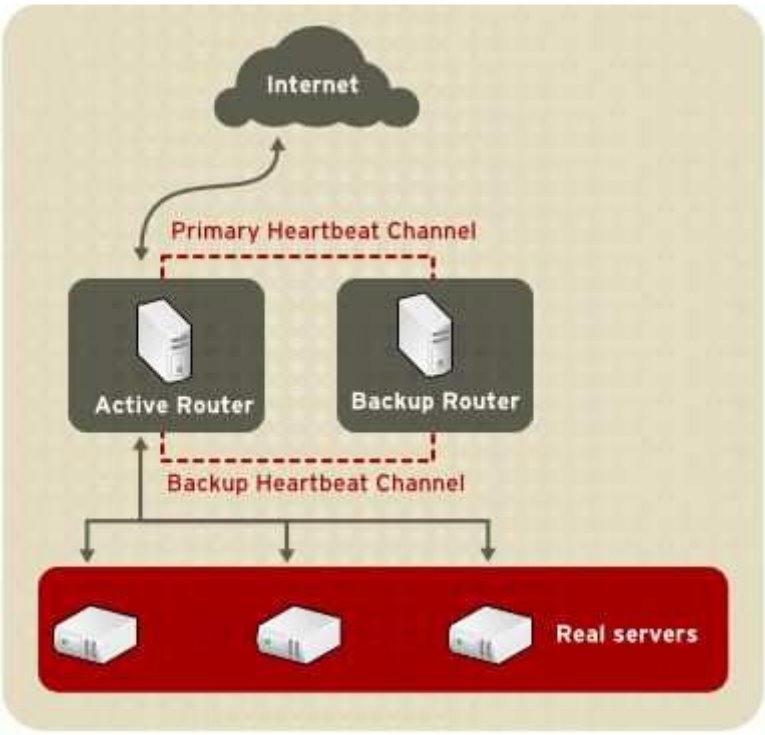
- Synchronizowanie danych między serwerami rzeczywistymi.
- Dodanie trzeciej warstwa do topologii jednoczesnego dostępu do współdzielonych danych

Pierwsza opcja jest preferowana dla serwerów, które nie umożliwiają wielkiej liczbie użytkowników obciążać serwerów rzeczywistych ani zmieniać na nich danych. Jeżeli serwery rzeczywiste umożliwiają modyfikowanie danych przez wielką liczbę użytkowników, na przykład w przypadku witryn WWW obsługujących handel elektroniczny, jest preferowane dodanie nowej warstwy.

Istnieje wiele metod synchronizowania danych między serwerami rzeczywistymi. na przykład może używać skryptu powłoki w celu jednoczesnego publikowania zaktualizowanych stron WWW na serwerach rzeczywistych. Podobnie można używać programów takich jak rsync w celu replikacji co pewien czas zmian danych na wszystkich węzłach. Jednakże w środowiskach, w których użytkownicy ładują pliki lub wykonują transakcje w bazach danych, użycie skryptów lub polecenie rsync dla synchronizacji danych nie działa w sposób optymalny. W związku z tym dla serwerów rzeczywistych z dość dużą ilością obciążeń, transakcjami w bazach danych lub z podobnym ruchem, topologia z trzema warstwami jest najwłaściwszą opcją dla synchronizacji danych.

2.4.2.2.8.1 Dwuwarstwowa topologia LVS

Ryc. „Dwuwarstwowa topologia LVS” przedstawia prostą konfigurację LVS obejmującą dwie warstwy: routery LVS i serwery rzeczywiste. Warstwa routerów LVS składa się z jednego aktywnego routera LVS i jednego zapasowego routera LVS. Warstwa serwerów rzeczywistych składa się z serwerów rzeczywistych podłączonych do sieci prywatnej. Każdy router LVS ma dwa interfejsy sieciowe: jeden z nich jest podłączony do sieci publicznej (Internet), a drugi do sieci prywatnej. Interfejs sieciowy podłączony do każdej z sieci umożliwia routerom LVS regulowanie ruchu między klientami w sieci publicznej i serwerami rzeczywistymi w sieci prywatnej. Na ryc. “Dwupoziomowa topologia LVS”, aktywny router LVS stosuje tłumaczenie adresów sieciowych (NAT) w celu kierowania ruchu z sieci publicznej do serwerów rzeczywistych w sieci prywatnej, które zapewniają żądane usługi. Cały ruch serwerów rzeczywistych przechodzi przez aktywny router LVS. Z punktu widzenia klientów w publicznej sieci router LVS jest widoczny jako jeden element.



Żądania usług kierowane do routera LVS są kierowane na wirtualny adres IP (VIP). Jest to publiczny adres routowalny, który administrator witryny kojarzy z pełni kwalifikowanym adresem IP takim jak www.example.com. Adres ten jest przypisywany jednemu lub wielu serwerom wirtualnym [1]. Należy zauważyć, że adres VIP jest przenoszony z jednego routera LVS na drugi podczas procesu przywracania funkcjonalności po awarii. Sprawia to, że adres IP jest zawsze dostępny (adres IP floating).

Adresy VIP mogą mieć nazwy, które odwołują się do tego samego urządzenie, które łączyć się z routerem LVS w sieci publicznej. Na przykład, jeśli eth0 jest połączony z Internetem, może istnieć wiele serwerów wirtualnych z nazwą eth0:1. Alternatywnie, każdy serwer wirtualny może być skojarzony z oddzielnym urządzeniem dla usługi. Na przykład ruch HTTP może być obsługiwany na interfejsie eth0:1m a ruch FTP na interfejsie eth0:2.
Jednocześnie jest aktywny tylko jeden router LVS. Rolą aktywnego routera LVS jest przekierowywanie żądań usługi z wirtualnego adresu IP do serwera rzeczywistego.
Przekierowywanie jest oparte na jednym z ośmiu algorytmów równoważenia obciążenia:
Programator Round-Robin — dystrybuuje wszystkie żądania sekwencyjnie między serwery rzeczywiste. Przy użyciu tego algorytmu wszystkie serwery rzeczywiste są traktowane w taki sam sposób bez względu na ich wydajność.
Programator Weighted Round-Robin — dystrybuuje wszystkie żądania sekwencyjnie między serwery rzeczywiste, przydzielając więcej zadań serwerom o większych możliwościach . Możliwości są podawane przez użytkownika i są dopasowywane na podstawie informacji o obciążeniach dynamicznych. Jest to preferowana opcja, jeżeli serwery rzeczywiste mają różne wydajności. Oczywiście, jeżeli obciążenie żądaniami zmienia się wyraźnie, serwer o dużej wydajności może odpowiadać na większą liczbę żądań niż powinien.

Least-Connection — Dystrybuuje więcej żądań do serwerów rzeczywistych mających mniejszą liczbą aktywnych połączeń. Jest to typ algorytmu programowany dynamicznie. Jest on dobrą opcją, jeżeli są istniej duża zmienność poziomu żądań. Jest on idealny dla infrastruktur, w których każdy serwer ma w przybliżeniu tę samą wydajność. Jeżeli serwery rzeczywiste mają różne wydajności, najlepszą opcją jest programowanie weighted least-connection.
Weighted Least-Connections (wstępnie określony) — Dystrybuuje więcej żądań wśród serwerów z mniejszą ilością aktywnych połączeń w porównaniu z ich możliwościami. Możliwości są podawane przez użytkownika i są dopasowywane na podstawie informacji o obciążeniach dynamicznych. Dodanie parametry wydajności sprawia, że ten algorytm byłby idealny, gdyby infrastruktura obejmowała serwery rzeczywiste o różnej wydajności sprzętu.

Locality-Based Least-Connection Scheduling — Dystrybuuje więcej żądań wśród serwerów z mniejszą ilością aktywnych połączeń w odniesieniu do ich docelowego adresu IP. Ten algorytm jest używany w klastrach serwerów cache proxy. Kieruje pakiet do adresu IP do serwera z tym adresem, i ile serwer nie jest przeciążony, w takim przypadku adres IP jest przypisywany serwerowi rzeczywistemu o mniejszym obciążeniu.

Locality-Based Least-Connection Scheduling with Replication Scheduling — Dystrybuuje więcej żądań wśród serwerów z mniejszą ilością aktywnych połączeń na podstawie docelowego adresu IP. Ten algorytm jest używany w serwerach cache proxy. Różni się on od „Locality-Based Least-Connection Scheduling" powiązaniem docelowego adresu IP z grupą serwerów rzeczywistych. Żądania są następnie przesyłane do serwera w grupie z najmniejszą liczbą połączeń. Jeżeli wydajność wszystkich węzłów da docelowego adresu IP jest powyżej wartości granicznej, dodaje nowy serwer rzeczywisty ogólnej do grupy serwerów dla docelowego adresu IP. Węzeł z największym obciążeniem jest przenoszony poza grupę, aby uniknąć nadmiernej ilości replikacji.

Source Hash Scheduling — Dystrybuuje wszystkie żądania na podstawie statycznego słownika adresów IP. Ten algorytm jest stosowany w routerach LVS z wieloma firewallami.
I tak, aktywny router LVS bada dynamicznie stan usług określonych na serwerach rzeczywistych za pomocą skryptu opartego na wysyłaniu żądań i oczekiwaniu. W celu wspomagania wykrywania usług wymagających danych dynamicznych takich jak HTTPS lub SSL, można także wywoływać programy zewnętrzne. Jeżeli usługa na serwerze rzeczywistym nie działa prawidłowo, aktywny router LVS nie wysyła żądań do tego serwera do chwili, gdy zostanie przywrócone jego normalne działanie.

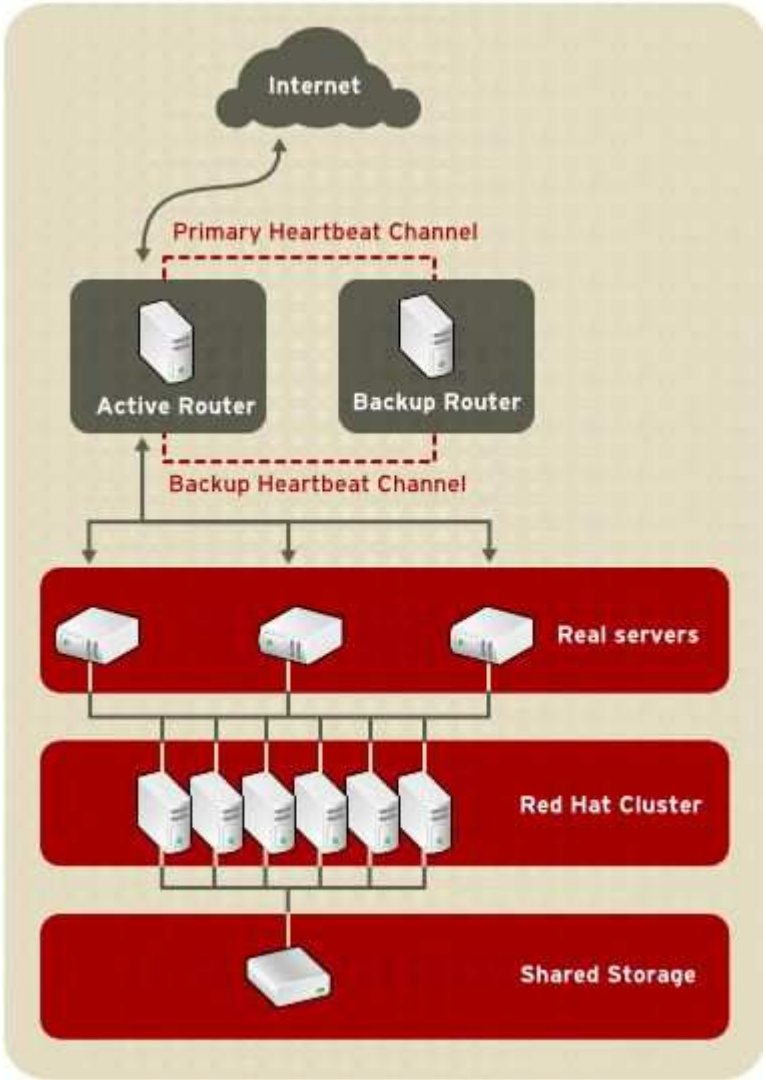
Zapasowy router LVS spełnia rolę pomocniczą w systemie. Okresowo router LVS wymienia komunikaty (heartbeats) przez główny zewnętrzny interfejs publiczny i w przypadku procesów odzyskiwania funkcjonalności po awarii, przez interfejs prywatny. Jeżeli zapasowy router LVS nie odbiera sygnału w określonym czasie, uruchamia proces odtworzenia funkcjonalności po awarii i przejmuje rolę aktywnego routera LVS. Podczas procesu odtwarzania funkcjonalności po awarii zapasowy router LVS przejmuje adres VIP obsługiwany przez router, który uległ awarii, stosując technikę nazywaną przejęciem tożsamości ARP — zapasowy router LVS ogłasza się jako serwer docelowy dla pakietów IP kierowanych do

węzła, który uległ awarii. Kiedy węzeł, który uległ awarii wznawia usługę, zapasowy router LVS przyjmuje ponownie swoją funkcję pomocniczą.

Prosta dwuwarstwowa konfiguracja najlepiej się nadaje dla klastrów obsługujących dane, które nie zmieniają się zbyt często, np. statycznych stron internetowych, ponieważ poszczególne serwery rzeczywiste nie synchronizują automatycznie danych między sobą.

2.4.2.2.8.2 Trójwarstwowa topologia LVS

Ryc. „Trójwarstwowa topologia LVS” przedstawia typową trójwarstwową konfigurację LVS. W tym przykładzie aktywny router LVS kieruje żądania z siei publicznej (Internet) do drugiej warstwy — serwerów rzeczywistych. Każdy serwer rzeczywisty uzyskuje dostęp do udostępnionych źródeł danych klastra Red Hat w trzeciej warstwie w sieci prywatnej.



Ta topologia jest idealna dla stosunkowo aktywnych serwerów FTP, na których dane są przechowywane na centralnym serwerze wysokoiej dostępności i mogą być dostępne z każego serwera rzeczywistego za pomocą udostępnianego katalogu Samba lub NFS. Ta topologia jest również zalecana dla witryn WWW

uzyskujących dostęp do centralnej baza danych wysokiej dostępności w celu realizacji transakcji. Ponadto w przypadku zastosowania konfiguracji aktywny-aktywny w klastrze Red Hat, można konfigurować klaster wysokiej dostępności tak, by obie role były wykonywane jednocześnie.

2.4.2.2.9 Narzędzia administracyjne klastra

Red Hat Cluster Suite zapewnia różne narzędzia do konfigurowania i administrowania klastra Red Hat. Ta sekcja zawiera zestawienie narzędzi administracyjnych dostępnych w Red Hat Cluster Suite.

2.4.2.2.9.1 Conga

Conga jest zintegrowanym pakietem komponentów oprogramowania obsługującego zadania scentralizowanej konfiguracji i administracji dla klastrów i pamięci masowej Red Hat. Conga zapewnia następujące funkcje:

Interfejs WWW do administracji klastrem i pamięcią masową
Zautomatyzowana implementacja danych klastra i pakietów wsparcia
Łatwa integracja z istniejącymi klastrami
Brak konieczności powtórnego uwierzytelniania
Integracja dzienników i stanu klastra
Szczegółowa kontrola nad uprawnieniami użytkowników

Głównymi komponentami Conga są Luci i Ricci, które mogą być instalowane oddzielnie. Luci jest serwerem uruchomionym na komputerze, który komunikuje się z wieloma komputerami klastra za pomocą Ricci. Ricci jest agentem uruchomianym na każdym komputerze administrowanym przez Conga (może on być członkiem klastra lub komputerem niezależnym).
Luci jest dostępny z przeglądarki WWW. Zapewnia on trzy główne funkcje, które są dostępne za pomocą następujących zakładek:

- homebase — Zapewnia narzędzia dla dodawania i usuwania komputerów, dodawania i usuwania użytkowników i konfigurowanie uprawnień użytkowników. Do tej zakładki ma dostęp wyłącznie administrator systemu.

- cluster — Zapewnia narzędzia dla tworzenia i konfigurowania klastrów. każde instancja Luci podaje klastry, które zostały utworzone za pomocą tej instancji Luci. Administrator systemu może administrować wszystkimi klastrami wyświetlanymi na tej karcie. Inni użytkownicy mogą administrować wyłącznie klastrami, dla których mają prawa do administracji (przydzielone przez administratora).

- storage — zapewnia narzędzia dla zdalnego administrowania pamięcią masową. Dzięki narzędziom z tej karty można administrować pamięcią masową w komputerach (bez względu na to, czy należą do klastra czy nie).

W celu administrowania klastrem lub pamięcią masową administrator dodaje (lub rejestruje) klaster lub komputer w serwerze Luci. Kiedy klaster lub komputer zostaje zarejestrowany z Luci, nazwa hosta nazwy w pełni kwalifikowanej domeny lub adres IP każdego komputera się przechowywane w bazie danych Luci.

Można zasilać bazę danych jednej instancji Luci z innej instancji Luci. Ta funkcja zapewnia sposób replikacji dla serwera Luci i zapewnia skuteczną trasę dla testów i aktualizacji. Po zainstalowaniu instancji Luci baza danych jest pusta. Mimo to można zaimportować część lub całą baza danych Luci z istniejącego serwera Luci podczas implementacji nowego serwera Luci.

Każda instancja Luci podczas początkowej instalacji ma jednego użytkownika – administratora. Tylko użytkownik admin może dodawać systemy do serwera Luci. I tak, użytkownik będący administratorem może tworzyć konta dodatkowych użytkowników i określać, którzy użytkownicy mogą mieć dostęp do klastrów i serwerów zarejestrowanych w bazie danych Luci. Podczas jednej operacji w nowym serwerze Luci można zaimportować wielu użytkowników, wiele klastrów i wiele komputerów

Kiedy komputer jest dodawany do serwera Luci w celu umożliwienia administrowania nim, uwierzytelnianie jest wykonywane jednorazowo. Nie ma konieczności wykonywania ponownych uwierzytelnień (o ile stosowany certyfikat nie został odwołany przez CA). Następnie można konfigurować i administrować klastrem i pamięcią masową zdalnie za pomocą interfejsu użytkownika Luci. Komunikacja Luci i Ricci jest zapewniana za pomocą plików XML.

Poniższe ilustracje przedstawiają przykład trzech głównych kart Luci: homebase, clúster i storage.
by uzyskać więcej informacji o Conga, zob. Konfigurowanie i administrowanie klastrem Red Hat i skorzystaj z pomocy dostępnej w serwerze Luci.

2.4.2.2.9.2 Interfejs graficzny do administrowania klastrem

Ta sekcja zawiera przegląd graficznego interfejsu użytkownika (GUI) administracji klastrem system-config-cluster w pakiecie Red Hat Cluster Suite. GUI używa się w połączeniu z komponentami do zarządzania infrastrukturą klastra usługami wysokiej dostępności.
GUI zapewnia dwie główne funkcje: Cluster Configuration Tool i Cluster Status Tool. Narzędzie konfiguracyjne klastra Cluster Configuration Tool umożliwia tworzenie, edytowanie i propagowanie pliku konfiguracyjnego klastra (/etc/cluster/cluster.conf). Narzędzie do monitorowania stanu klastra Cluster Status Tool umożliwia zarządzanie usługami wysokiej dostępności.

2.4.2.2.9.2.1 Cluster Configuration Tool

Narzędzie konfiguracji klastra Cluster Configuration Tool jest dostępne na karcie Cluster Configuration (Konfiguracja klastra) w graficznym interfejsie użytkownika administracji klastrem.

Cluster Configuration Tool przedstawia komponenty konfiguracji klastra w pliku konfiguracyjnym (/itp/klaster/cluster.conf) w hierarchii przedstawionej graficznie

w panelu z lewej strony. Ikona w kształcie trójkąta z lewej strony nazwy komponentu wskazuje, że komponent ma przypisany jeden lub więcej komponentów podrzędnych. Kliknij trójkąt, aby rozwinąć lub zwinąć część drzewa pod komponentem. Komponenty wyświetlane w interfejsie graficznym są następujące:

Węzeł klastra — Wyświetla węzły klastra. Węzły są reprezentowane w zależności od liczby elementów podrzędnych w widoku Węzły klastra. Używając przycisków konfiguracyjnych w dolnej części panelu z prawej strony (pod strefą Właściwości), można dodawać, usuwać, edytować węzły i konfigurować metody izolacji dla każdego węzła.

Urządzenia izolujące — Przegląd urządzeń izolujących. Urządzenia izolujące są przedstawiane jako elementy podrzędne w sekcji Urządzenia izolujące. Używając przycisków konfiguracyjnych w dolnej części panelu z prawej strony (pod strefą Właściwości), można dodawać, usuwać, edytować urządzenia izolujące i edytować właściwości urządzeń izolujących. Urządzenia izolujące muszą być zdefiniowane przed skonfigurowaniem odizolowania (za pomocą przycisku Administracja izolacją dla tego węzła) dla każdego z węzłów.

Administrowane zasoby — Przedstawia domeny dla odtwarzania funkcjonalności po awarii, zasoby i usługi.

- Domena odzyskiwania — Aby skonfigurować jedną lub więcej podgrup węzłów klastra używanych do realizacji usługi wysokiej dostępności w przypadku awarii węzła. Domeny odtwarzania po awarii są przedstawiane jako elementy podrzędne w sekcji Domeny odtwarzania. Używając przycisków konfiguracyjnych w dolnej części panelu z prawej strony (pod strefą Właściwości), można dodawać, usuwać, edytować domeny odtwarzania (gdy opcja Domeny odtwarzania jest wybrana) i edytować właściwości domeny odtwarzania funkcjonalności po awarii (jeżeli domena jest wybrana).

- Zasoby - do konfiguracji współdzielonych zasobów, aby mogły być używane przez usługi wysokiej dostępności. Zasoby współdzielone obejmują systemy plików, adresy IP, współdzielone zasoby NFS i skrypty tworzone przez użytkownika, które są dostępne w dowolnej usłudze wysokiej dostępności w klastrze. Zasoby są reprezentowane jako elementy podrzędne w sekcji Zasoby. Za pomocą przycisków znajdujących się w dolnej części panelu z prawej strony (pod strefą Właściwości) można tworzyć zasoby (Kiedy jest wybrana funkcja Zasoby) lub edytować właściwości zasobu (kiedy zasób jest wybrany).

2.4.2.2.9.3 Cluster Status Tool

Narzędzie Cluster Status Tool jest dostępne na karcie Cluster Management (Zarządzenie klastrem) w graficznym interfejsie użytkownika administracji klastrem.
Węzły i usługi wyświetlane w narzędziu Cluster Status Tool Tool są określane przez plik konfiguracyjny klastra (/itp/klaster/cluster.conf). Narzędzia Cluster Status Tool można używać do włączania, wyłączania, ponownego uruchamiania lub przypisywania usługi wysokiej dostępności.

2.4.3 PC

Komputery PC są skonfigurowane z polską wersją systemu operacyjny Microsoft Windows 7 Professional.

2.4.3.1 Windows 7

2.4.3.1.1 Charakterystyki

Windows 7 ma wiele nowych funkcji, np. ulepszone rozpoznawanie pisma ręcznego, wsparcie wirtualnych dysków twardych, zwiększona wydajność procesorów wielordzeniowych, lepszą wydajność przy uruchamianiu, DirectAccess i usprawnienia w jądrze. W Windows 7 dodano wsparcie dla systemów, w których są stosowane karty graficzne różnych producentów (heterogeneous multi-adapter lub multi-GPU), nową wersję Windows Media Centra i odpowiadający jej gadżet, a także przeprojektowane aplikacje takie jak Paint, Wordpad i Kalkulator. Zostały dodane liczne elementy w Panelu sterowania, m. in. takie jak Kreator kalibracji kolor ekranu, kalibrator tekst ClearType, Rozwiązywanie problemów, Lokalizacja i inne czujniki, Administrator uprawnień, ikony w strefie powiadamiania.17 Centrum zabezpieczeń Windows zmieniło nazwę na Centrum akcji, zastały w nim zintegrowane kategorie bezpieczeństwa i utrzymania komputera.

Pasek zadań został przeprojektowany, stał się szerszy, a przyciski okien nie zawierają tekstu, tylko samą ikonę aplikacji. Te zmiany zostały wprowadzone w celu usprawnienia działania systemów z ekranem dotykowym. Te ikony zostały zintegrowane z paskiem szybkiego uruchamiania stosowanego we wcześniejszych wersjach Windows, a otwarte okna są grupowane w jedną ikonę aplikacji z obramowaniem, oznaczającą, że okna są otwarte. Skróty do aplikacji, które nie są otwarte nie mają obramowania. Został również wprowadzony przycisk wyświetlający, znajdujący się z prawej strony paska zadań, umożliwia on wyświetlanie pulpitu po umieszczeniu na nim kursora myszy.

Zostały dodane „Biblioteki”, które są folderami wirtualnymi łączącymi zawartość wielu folderów, która jest wyświetlana w jednym widoku. Na przykład foldery dodane domyślnie do biblioteki „Wideo” to: „Moje wideo” i „Wideo publiczne”, można też dodać więcej folderów ręcznie. Służą one do klasyfikowania różnych typów plików (dokumentacja, muzyka, wideo, obrazy).

Funkcja „Lump list” przechowuje listę ostatnio otwieranych plików. Po kliknięciu prawym przyciskiem myszy aplikacji na pasku zadań jest wyświetlana lump list, dzięki której można wykonywać proste zadania w zależności od aplikacji. Na przykład, może to być otwieranie ostatnio otwieranych dokumentów MS Office, otwieranie ostatnich kart przeglądarki Internet Explorer, wybieranie list odtwarzania w odtwarzaczu, zmienianie statusu w komunikatorze Windows Live Messenger itp.

2.4.3.1.2 Interfejs

Windows 7 umożliwia obecnie personalizowanie komputera, zapisywanie pełnych kompozycji obejmujących kolor okien, obrazy, zestawy dźwięków, a także wygaszacz ekranu (we wcześniejszych wersjach te funkcje były ograniczone tylko do kolorów okien).

Kalkulator, w którym wcześniej w innych wersjach były dostępne tylko funkcje naukowe i standardowe (od Windows 95 do Windows Vista), zawiera obecnie funkcje związane z programowaniem i statystyką. Ponadto umożliwia on konwertowanie jednostek SI i jednostek imperialnych (angielskich); obliczenia między datami i arkusze obliczeniowe dla hipoteki, najmu samochodów i zużycia paliwa. Podobnie jak w prawdziwych kalkulatorach jest zapisywana sekwencja operacji wykonywanych przez użytkownika.

Pasek boczny Windows, znany bardziej jako Windows Sidebar, został usunięty, jest możliwe rozmieszczanie gadżetów na dowolnym miejscu na pulpicie, z lewej lub prawej strony, u góry lub na dole, bez konieczności używania paska bocznego.

Windows Media Player 12: Jest to nowy odtwarzacz multimedialny, który jest dostarczany standardowo w wersjach Windows 7. W porównaniu z innymi wersjami nie ma już stałego miejsca dla najbardziej podstawowych poleceń takich jak Odtwarzaj, Zatrzymaj, Powtórz, Głośność i pasek wyszukiwania, który jest ukrywany, gdy kursor myszy jest przesuwany poza jego obręb. Obecnie zawiera trzy proste karty do odtwarzania, zapisywania płyt i synchronizowania urządzeń; ponadto obsługuje formaty zewnętrzne, między innymi takie jak MOV, MP4, xvid i DivX. Natomiast jest to pierwsza wersja programu, która nie będzie dostępna dla wcześniejszych wersji Windows i pierwsza, która nie będzie obsługiwać metadanych plików (np. dodawanie tekstów piosenek). Nie będzie on dostarczany w wersjach N systemu operacyjnego, dla których program należy pobrać osobno.

Aero Peek: Podgląd Windows Aero został ulepszony i stał się bardziej interaktywny i użyteczny. Po umieszczeniu kursora myszy na otwartej aplikacji, zostaje wyświetlony podgląd okna, w którym znajduje się nazwa, podgląd i opcja umożliwiająca zamknięcie, ponadto, po umieszczeniu kursora myszy na podglądzie, zostaje wyświetlone pełne okno, po przesunięciu kursora poza pod podgląd, zostaje wyświetlony wcześniejszy widok. Ponadto te same cechy zostały włączone do Windows Flip.

Aero Shake: Jeżeli jest otwartych wiele okien, po kliknięciu i przytrzymaniu paska tytułu oraz potrząśnięciu nim wszystkie pozostałe otwarte okna zostaną zminimalizowane. Po ponownym wykonaniu tej czynności okna zostaną przywrócone.

Flip 3D: Windows Flip 3D jest funkcją Windows Aero usprawniającą funkcję Windows Flip, która pokazuje z efektem 3D aktualnie otwarte okna, umożliwiając wyszukiwanie okien w sposób szybszy i bardziej efektywny. W odróżnieniu od opcji Windows Flip, która jest wywoływana przez kombinację klawiszy Alt+Tab ⇆, ta funkcja jest wywoływana kombinacją klawiszy ⊞ Win+Tab ⇆. Ponadto została udoskonalona funkcja klawiszy Alt+Tab ⇆, która wyświetla w czasie rzeczywistym

miniaturowe okna uruchomionych aplikacji (funkcja zawarta poprzednio w Windows Vista).

Aero Snap: Polega na przesuwaniu okna do bocznych brzegów ekranu, wielkość okna jest automatycznie dopasowywana tak, że zajmuje połowę pulpitu. Po przesunięciu do górnego brzegu ekranu okno jest maksymalizowane, jego wielkość jest przywracana po lekkim przesunięciu w dół. Jest to użyteczne przy jednoczesnym oglądaniu zawartości okien lub ich wyświetlaniu kolejnym, co nie jest zbyt wygodne w przypadku zbyt niskich rozdzielczości ekranu.

Przypinanie: W Windows 7 można przypiąć ulubione programy do paska zadań, aby ułatwić dostęp do nich. Aby to zrobić, istnieją dwa sposoby:
przeciągnąć ikonę programu lub pliku na pasek zadań.
Gdy program jest uruchomiony i jest wyświetlany na pasku zadań, nacisnąć prawy przycisk myszy i wybrać opcję Przypnij. Internet Explorer 9 umożliwia ponadto w taki sam sposób przypinanie ulubionych stron do paska zadań.

2.4.3.1.3 Licencje

Należy zakupić jedną licencję dla każdego dostarczonego komputera.

2.5.- Oprogramowanie biurowe

2.5.1 Apache Open Office

Kompatybilny z większością ważniejszych pakietów biurowych. Apache OpenOffice to darmowy pakiet biurowy, który mogą Państwo pobrać, wykorzystywać i rozpowszechniać bez ograniczeń.

2.5.1.1 Charakterystyki

Główne cechy:
Najważniejsze funkcje:

- MultiOS: Dostępny na Windows, Linux, Mac, Solaris
- Multiversion: kompatybilny ze wszystkimi wersjami OOo
- Multilenguage (wielojęzykowość): język GUI (graphical user interface) może być zmieniony. Pierwsza wersja dysponuje 10 językami.
- Różne sposoby instalacji: można wybierać pomiędzy różnymi instalacjami na jednym serwerze (np.: słowniki mogą być używane przez wszystkich użytkowników) lub instalacja tylko dla jednego wybranego użytkownika.
- Automatyczne aktualizacje: Za każdym razem kiedy program jest używany, DicOOo sprawdza dostępność nowej wersji i pozwala użytkownikowi ją zainstalować.
- Obsługa instalacji off-line za pomocą instalatorów. Instalatory te dostępne są na serwerze projektu Lingucomponent.
- Licencja LGPL, autor: Laurent Godard

2.5.1.2 Pakiety Apache OpenOffice

2.5.1.2.1 WRITER

WRITER, uniwersalny procesor tekstu, mogący służyć do redagowania krótkich tekstów aż po stworzenie kompletnej książki.

2.5.1.2.2 CALC

CALC, zaawansowany arkusz kalkulacyjny zawierający wszystkie niezbędne narzędzia do obliczeń, analiz i prezentacji wyników w formie liczbowej lub bardziej efektywnej graficznej.

2.5.1.2.3 IMPRESS

IMPRESS, szybki i zaawansowany program do tworzenia efektownych prezentacji multimedialnych.

2.5.1.2.4 DRAW

DRAW, program służący do tworzenia i obróbki zaczynając od prostej grafiki i kończąc na dynamicznych ilustracjach 3D.

2.5.1.2.5 BASE

BASE, program pozwalający na kompletną obsługę baz danych. Tworzenie i modyfikowanie tabel, formularzy, zapytań i komunikatów, wszystko to z OpenOffice.

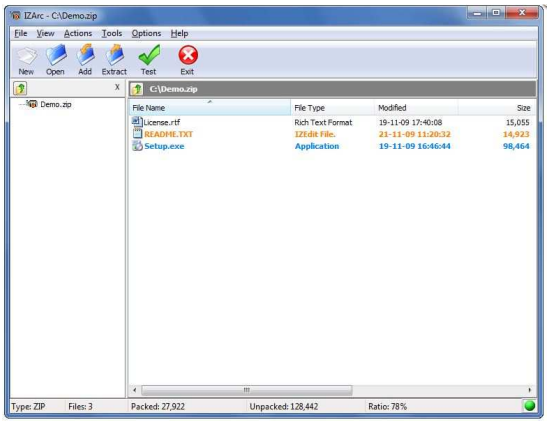
2.5.1.2.6 MATH

MATH, program do tworzenia formuł matematycznych. Oferuje pracę z poziomu interfejsu użytkownika lub poprzez pisanie formuł bezpośrednio w edytorze równań.

2.5.2 IzarC

IZArc jest najlepszym darmowym narzędziem do archiwizacji obsługującym wiele formatów archiwów takich jak: 7-ZIP, A, ACE, ARC, ARJ, B64, BH, BIN, BZ2, BZA, C2D, CAB, CDI, CPIO, DEB, ENC, GCA, GZ, GZA, HA, IMG, ISO, JAR, LHA, LIB, LZH, MDF, MBF, MIM, NRG, PAK, PDI, PK3, RAR, RPM, TAR, TAZ, TBZ, TGZ, TZ, UUE, WAR, XXE, YZ1, Z, ZIP, ZOO.

Dzięki nowoczesnemu, łatwemu w obsłudze interfejs, IZArc obsługuje większość skompresowanych i szyfrowanych plików, zapewnia także dostęp do wielu zaawansowanych funkcji i narzędzi. Umożliwia on przeciąganie i upuszczanie plików między programem i Eksploratorem Windows (w obu kierunkach), tworzenie i wyodrębnianie archiwów bezpośrednio w Eksploratorze Windows tworzenie archiwów wieloczęściowych, tworzenie archiwów samorozpakowujących się, naprawianie uszkodzonych archiwów zip, konwertowanie formatów archiwów, przeglądanie i wpisywanie komentarzy i wiele innych funkcji. IZArc obsługuje również wiele języków.



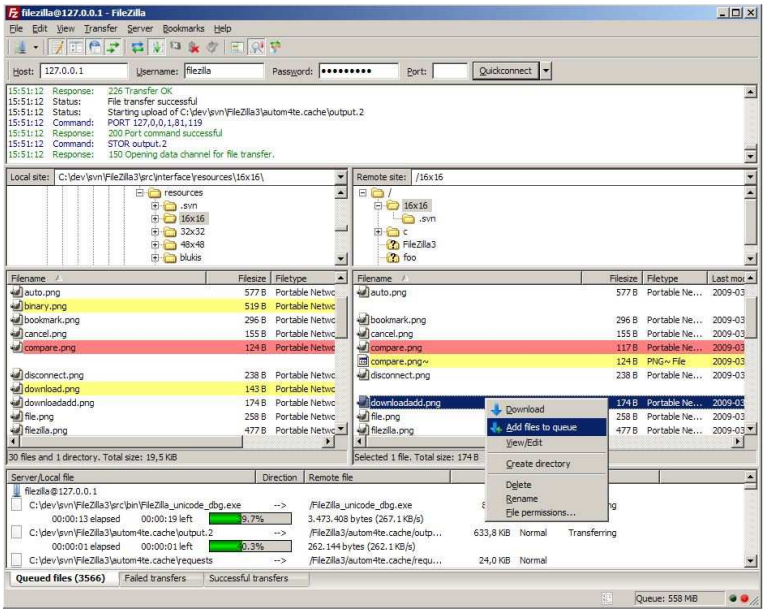
Za pomocą IZArc można otwierać pliki obrazów CD takie jak ISO, BIN, CDI i NRG. Można także konwertować takie pliki na inny format (BIN do ISO, NRG do ISO).

2.5.2.1 Charakterystyki

- IZArc można skonfigurować tak, by podczas otwierania archiwów uruchamiał preferowany skaner antywirusowy.
- IZArc obsługuje 256-bitowe szyfrowanie AES w celu zapewnienia bezpieczeństwa danych.
- IZArc zintegruje się z systemem Windows, dzięki czemu wszystkie operacje archiwizacji można wykonywać, klikając w menu kontekstowe wywoływane prawym przyciskiem myszy w Eksploratorze Windows.
- IZArc może także pomóc łatwo naprawić uszkodzone archiwa.
- Obecnie IZArc jest najbardziej kompletnym narzędzie do archiwizacji.

2.5.3 Filezilla Client

FileZilla jest wieloplatformowym klientem FTP opartym o otwarty kod i ideę wolnego oprogramowania, udzielanym na podstawie Ogólnej Publicznej Licencji GNU. Obsługuje protokoły FTP, SFTP i FTP poprzez SSL/TLS (FTPS).
Początkowy został zaprojektowany dla Microsoft Windows, lecz począwszy od wersji 3.0.0, dzięki zastosowaniu wxWidgets, jest narzędziem wieloplatformowym dostępnym dla innych systemów operacyjnych, między innymi GNU/Linux, FreeBSD i Mac OS X.



2.5.3.1 Charakterystyki

- Menedżer serwerów: umożliwia użytkownikowi utworzenie listy serwerów FTP z danymi połączenia takimi jak numer portu oraz z danymi logowania (normalne lub anonimowe). Dla normalnego logowania jest zapisywana nazwa użytkownika i opcjonalnie hasło.

- Dziennik komunikatów: jest wyświetlany w górnej części okna. Wyświetla w formacie konsoli polecenia wysyłane przez program FileZilla i odpowiedzi serwera zdalnego.

- Widok pliku i folderu: znajduje się w środkowej części okna, zapewnia interfejs graficzny dla FTP. Użytkownicy mogą nawigować po folderach, wyświetlać i zmieniać ich zawartość zarówna na komputerze lokalnym jak i zdalnym, korzystając z interfejsu typu drzewo w eksploratorze. Użytkownicy mogą przeciągać i upuszczać pliki między komputerem lokalnym i zdalnym.

- Kolejka transferów: znajduje się w dolnej części okno, pokazuje w czasie rzeczywistym stan każdego transferu aktywnego lub transferu w kolejce.

- Jest obsługiwanych wiele języków.

2.6.- Narzędzia CAD

2.6.1 AUTOCAD

Zostanie dostarczone oprogramowanie CAD – AUTOCAD, wsparte programami VISIM i VISUM.

Autodesk AutoCAD to program do komputerowego dwuwymiarowego (2D) i trójwymiarowego (3D) komputerowego wspomagania projektowania. Obecnie jest on wytwarzany i sprzedawany przez firmę Autodesk. AutoCAD firmy Autodesk, został zaprezentowany po raz pierwszy w 1982 roku. Oprogramowanie AutoCAD jest oferuje szerokie możliwości wykonywanie planów budynków lub tworzenie obrazów 3D.
AutoCAD jest jednym z najczęściej używanych programów, wybierany przez architektów, inżynierów i projektantów przemysłowych. Auto, odnosi się do własnej firmy, która stworzyła oprogramowanie Autodesk oraz CAD, czyli Computer Aided Projekt (od skrótu w języku angielskim).

2.6.1.1 Charakterystyka

Program jest znany z różnorodności oferowanych funkcji, które z każdym nowym wydaniem stają się coraz bardziej powszechne. Podobnie jak w innych programach komputerowego wspomagania projektowania AutoCAD zarządza bazą danych geometrycznych jednostek (punktów, linii, łuków, itp..), które można obsługiwać poprzez graficzny wyświetlacz, na którym są prezentowane, zwany

edytorem rysunku. Interakcja z użytkownikiem odbywa się z poziomu wiersza poleceń, poprzez polecenia rysowania lub edycji. Nowoczesne wersje programu umożliwiają wprowadzenie poleceń poprzez GUI lub z angielskiego - Graphic User Interface, który automatyzuje cały proces.

Podobnie jak wszystkie programy i CAD, przetwarza obrazy wektorowe. Obsługiwane typy plików to fotograficzne lub bitmap, które dostarczają podstawowe kształty i krzywe (linie, łuki, prostokąty, etc.). Za pomocą palety narzędzi można tworzyć bardziej skomplikowane grafiki. Program pozwala uporządkować obiekty według warstw. Zarządzanie obiektami przy użyciu bloków pozwalają na jednoznaczną identyfikację i modyfikację. Część programu AutoCAD zorientowana jest na stosowanie tradycyjnych zasobów grafiki na rysunku, takich jak kolor, grubość linii i tekstura. AutoCAD od wersji 11 używa pojęcia przestrzeni modelu i przestrzeni papieru, aby rozdzielić fazy projektowania i rysowania w 2D i 3D, od konkretnych planów przygotowanych na papierze do odpowiedniej skali. Rozszerzeniem pliku AutoCAD jest .DWG, ale istenieje możliwość eksportu do innych formatów (najbardziej znanym jest .DXF). Również formaty STEP i IGES zapewniają kompatybilność z innym oprogramowaniem.

Format .DXF umożliwia innym platformom obsługę rysunków CAD, natomiast format .DWG jest zastrzeżony wyłącznie dla programu AutoCAD. Format DXF może być edytowany przy wykorzystaniu edytora tekstu, więc można powiedzieć, że jest formatem otwartym. Natomiast format .DWG może być edytowany tylko programem AutoCAD. Jednak w ostatnim czasie format .DWG został zwolniony i wiele programów CAD, włączyło go do swojej obsługi i umożliwia otwieranie i zapisywanie tego rozszerzenia, przez co .DXF został zredukowany tylko do obsługi konkretnych potrzeb. W wersji 11, pojawia się pojęcie modelowania brył z operacjami obracania i, Boolean union, przecięcia i odejmowanie.

2.7.- GIS

Tak, jak zostało wskazane w PFU zostanie wdrożone i przyjęte rozwiązanie celem umożliwienia przekazywania danych do aplikacji GIS, która obecnie wykorzystywana jest w Urzędzie Miasta.

Oprogramowanie to będzie stosowane przez operatorów, a także do wyświetlania wybranych elementów z sieci drogowej, stanu urządzeń, do przekazywania innych informacji z wykorzystaniem środków komunikacji masowej.

Licencja zapewnia pełne korzystanie z oprogramowania dla 10 użytkowników zasobów informacyjnych (w granicach wskazanych przez administratora). Wśród tych operatorów znajdują się także użytkownicy zdalnych pulpitów.

Ponadto wizualizacja pewnych informacji będzie możliwa dla innych użytkowników, np. poprzez serwer.

Graficzne przedstawienie wszystkich poziomów i form będzie opierało się na rzucie wektorowym będącym tłem dla wizualizacji informacji, który korzysta z jednego z powszechnie stosowanych standardów GIS.

Przedstawienie w rzucie będzie pokazywało:

- sieć ulic miejskich Lublina

- nazwy ulic

- granice administracyjne

- skrzyżowania wyposażone w sygnalizację drogową objętą SZR

- rozmieszczenie sygnalizacji ze zmiennym tekstem

- rozmieszczenie kamer CCTV

- rozmieszczenie CCT

2.8.- Wirtualizacja

2.8.1 Co to jest wirtualizacja

W informatyce wirtualizacja oznacza tworzenie za pomocą oprogramowania wersji wirtualnej jakiegoś zasobu technologicznego, na przykład platformy sprzętowej, systemu operacyjnego, urządzenia pamięci masowej lub innych zasobów sieciowych.

Innymi słowy, odnosi się do abstrakcji zasobów komputera, zapewnianej przez Hypervisor lub VMM (Virtual Machine Monitor), który tworzy warstwę abstrakcji między sprzętem maszyny fizycznej (host) i systemem operacyjnym maszyny wirtualnej (virtual machine, guest), przy czym zasób może być współdzielony przez wiele środowisk.
Ta warstwa oprogramowania (VMM) obsługuje cztery główne zasoby komputera (CPU, pamięć, pamięć masowa i połączenia sieciowe), zarządza nimi i zapewnia dla nich arbitraż i może w ten sposób przydzielać dynamicznie wspomniane zasoby wszystkim maszynom wirtualnym zdefiniowanym w komputerze nadrzędnym. Dzięki temu na jednym komputerze fizycznym może istnieć wiele komputerów wirtualnych.

W celu rozwiązywania problemów związanych z rosnącą liczbą serwerów i nieefektywnym wykorzystaniem zasobów stosowanie wirtualizacji jest coraz częstsze w celu konsolidacji serwerów.

Ze względu na różnice między wymogami infrastruktury i preferencje użytkowania producenci przewidują, że aplikacje wirtualizacyjne stosowane przez działy handlowe i administratorów IT będą się zmieniać w sposób naturalny. Ewentualnie środowiska wirtualne firm będą mieszane.

Elastyczność i prostota, które zapewnia wirtualizacja, są w stanie zmieniać dynamikę systemu. Konsolidacja serwerów z wirtualizacją może znacząco

zmniejszyć liczbę serwerów fizycznych i zminimalizować obciążenie pracami administracyjnymi dzięki scentralizowanemu zarządzaniu. Obecnie na rynku jest dostępna szeroka gama rozwiązań w dziedzinie wirtualizacji i konsolidacji – zarówno dotyczących aplikacji, jak i platform - ułatwiających zmniejszanie kosztów i usprawnianie infrastruktury IT, aby Państwa przedsiębiorstwo mogło szybko się rozwijać, aby mogło sprostać przyszłym wymaganiom.

2.8.2 Zmniejszenie kosztów posiadania (TCO)

Konsolidacja serwerów dzięki wirtualizacji zmniejsza koszty sprzętu, konserwacji, zużycia energii i klimatyzacji. Ponadto, zmniejsza całkowity koszt posiadania (TCO) poprzez zwiększenie efektywności zasobów serwera i zmiany w sposobie działania, a także poprzez charakterystyki specyficzne związane z wirtualizacją. W wyniku zwiększenia wydajności procesorów serwerów, niektóre z nich są używane w wysokim stopniu, lecz większość jest wykorzystywana w zbyt niskim stopniu.
Dzięki wirtualizacja to nieefektywne użycie zasobów CPU jest eliminowane, a zasoby środowiska serwera są optymalizowane. Ponadto, ponieważ serwery z każdego działu przedsiębiorstwa mogą być zarządzane w sposób scentralizowany, koszty zarządzania ulegają istotnemu zmniejszeniu.

2.8.3 Zwiększenie dostępności i ciągłości pracy przedsiębiorstwa

Zaletą serwerów wirtualnych, która nie jest dostępna dla serwerów fizycznych jest migracja w locie. Dzięki migracji w locie serwery wirtualne mogą być migrowane bez konieczności wyłączania na inne serwery fizyczne w celu przeprowadzenie konserwacji. W ten sposób nie ma wpływu na użytkownika końcowego. Inną wielką zaletą technologii wirtualizacji jest fakt, że enkapsulacja i uniezależnienie od sprzętu zwiększa dyspozycyjność i ciągłość działania przedsiębiorstwa.

2.8.4 Charakterystyki

W ofercie są podane wszystkie licencje niezbędne dla zapewnienia wirtualizacji w oparciu o obsługujący wirtualizację produkt VMware® vSphere® Essentials Plus, który zawiera wszystkie pakiety wymienione poniżej:

- VMware ESXi 5 hypervisor, lekki system operacyjny ligero zoptymalizowany do zarządzania maszynami wirtualnymi.

- VMware vCenter Server for Essentials umożliwia scentralizowane zarządzanie i monitorowanie wydajności wszystkich maszyn wirtualnych i urządzeń vSphere, włącznie ze wsparciem dla konwersji maszyn fizycznych do wirtualnych physical-to-virtual (P2V) i szybkim tworzeniem maszyn wirtualnych w oparciu o szablony

- vSphere Virtual Symmetric Multiprocessing (SMP) umożliwia użytkowanie silnych maszyn wirtualnych mających do 4 procesorów wirtualnych

- vSphere vStorage Virtual Machine File System (VMFS) umożliwia maszynom wirtualnym dostęp do wspólnych urządzeń pamięci masowej i stanowi część podstawy dla działania innych pakietów takich jak VMotion.

- vSphere vStorage Thin Provisioning umożliwia dynamiczne rezerwowanie współdzielonej pamięci masowej, umożliwiając ustanowienie strategii dla pamięci masowej umożliwiającej zmniejszenie wielkości pamięci masowej.

- vCenter Update Manager umożliwia zautomatyzowanie aktualizacji wszystkich pakietów i systemów operacyjnych uruchamianych w każdej z maszyn wirtualnych.

- vCenter Converter umożliwia konwertowanie serwerów fizycznych w maszyny wirtualne VMware bez zatrzymywania ich usług.

- vSphere vMotion umożliwia migrowanie w locie maszyn wirtualnych z jednego serwera fizycznego na inny serwer fizyczny bez zatrzymywania lub utraty funkcjonalności usługi, eliminując konieczność uwzględnienia czasu przestoju na serwisowanie.

- vSphere High Availability umożliwia zautomatyzowanie rozwiązanie mające na celu ponowne uruchamianiu usług dla wszystkich aplikacji w przypadku awarii sprzętu lub awarii systemów operacyjnych

- vSphere Data Recovery umożliwia wykonywanie kopii zapasowych i odzyskiwanie maszyn wirtualnych.

2.8.5 Maszyny wirtualne guest

Na ilustracji poniżej są przedstawione maszyny wirtualne, które zostaną zainstalowane na serwerach.

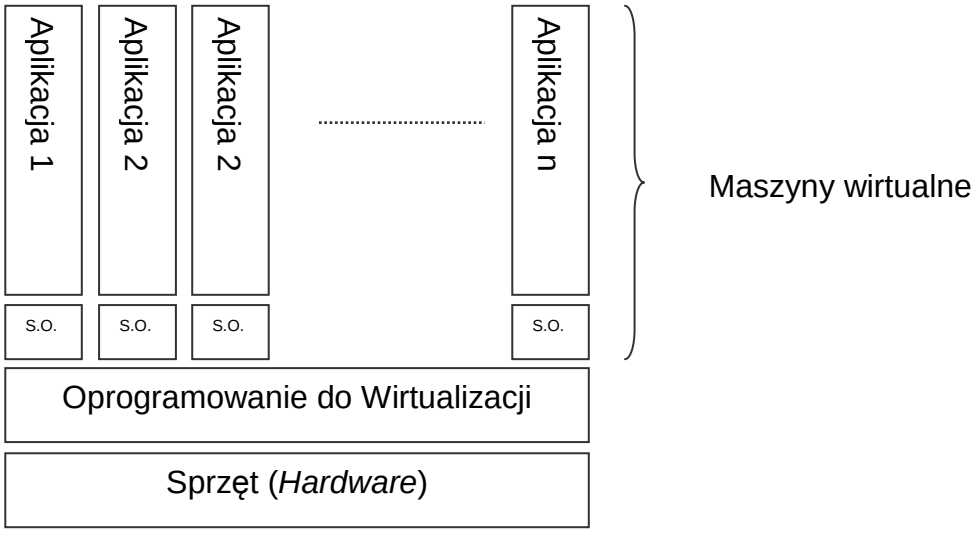
System	Serwer wirtualny	Serwer fizyczny
Podsystem kontroli ruchu i priorytetów	Serwer 6 (front end) Serwer 7 (kontrolery stref)	Serwer 1 / Serwer 2 / Serwer 3 (BACKUP)
Podsystem kontroli PMV	Serwer 5	Serwer 1 / Serwer 3 (BACKUP)
Podsystem lokalizacji pojazdów ratowniczych	Serwer 4	Serwer 1 / Serwer 3 (BACKUP)
Podsystem kontroli wideo i zarządzania ruchem	Serwer 3	Serwer 2 / Serwer 3 (BACKUP)
Podsystem wykrywania incydentów	Serwer 1	Serwer 3 / Serwer 1 (BACKUP)
Podsystem obliczania czasu przejazdu	Serwer 2	Serwer 2 / Serwer 1 (BACKUP)
Baza danych	Serwer 8 i 9 (klaster)	Serwer 2 / Serwer 3 (klaster)

Portal WWW	Serwer 10	Serwer 2 / Serwer 1 i 3 (BACKUP)
Serwer poczty qmail	Serwer 12	Serwer 2 / Serwer 1 i 3 (BACKUP)
Serwer WWW Apache	Serwer 13	Serwer 2 / Serwer 1 i 3 (BACKUP)
Serwer FTP	Serwer 14	Serwer 2 / Serwer 1 i 3 (BACKUP)
Serwer OPENLDAP	Serwer 15	Serwer 2 / Serwer 1 i 3 (BACKUP)
Serwer Radius	Serwer 16	Serwer 2 / Serwer 1 i 3 (BACKUP)
Serwer VPN	Serwer 16	Serwer 2 / Serwer 1 i 3 (BACKUP)

2.8.6 Ogólne przedstawienie rozwiązania

System jest wysoce odporny na ewentualne awarie na dwóch pierwszych poziomach systemu.

Proponowanym rozwiązaniem jest klaster z trzema serwerami z zastosowaniem technik wirtualizacji. Różne aplikacje na maszynach wirtualnych działają z dynamicznym i transparentnym przydziałem wykorzystanych zasobów. Sterowniki obszarowe, centrum sterowania i System zarządzania bazą danych są aplikacjami, które działają na wirtualnych maszynach.



W porównaniu z tradycyjnymi rozwiązaniami (stałe przypisanie aplikacji do urządzenia), głównymi zaletami są:

- Odporność na awarie elementów konfiguracji, ponieważ istnieje automatyczne ponowne przypisanie maszyn wirtualnych do innych elementów sprzętowych.
- Optymalizacja zasobów.
- Ułatwienie skomplikowanego zarządzania

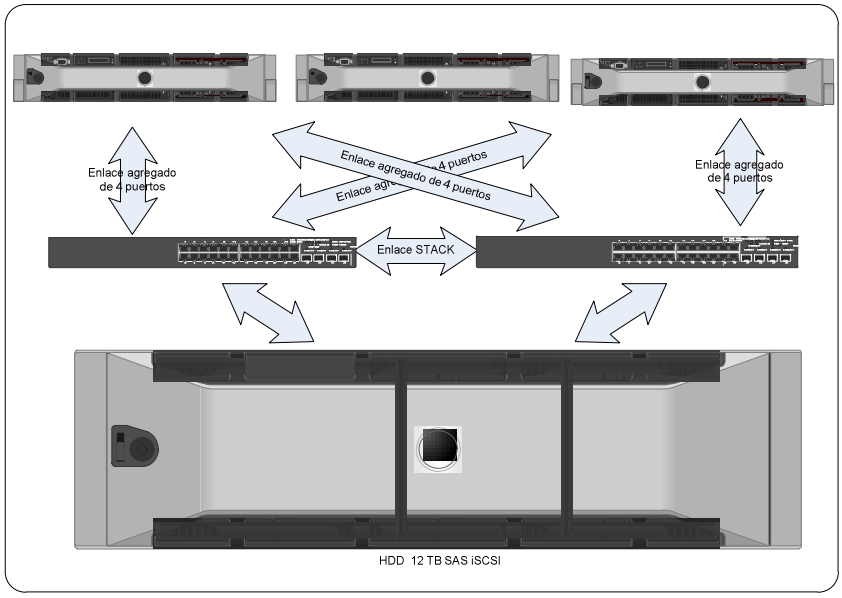
- Zwiększenie elastyczności
- Dostępność i przywrócenie do działania po sytuacjach awaryjnych.
- Naprawa "na gorąco- od razu"

W zaproponowanej konfiguracji wszystkie programy i usługi pracują ponadto na niezależnych systemach operacyjnych, co sprawia, że ogólna konfiguracja jest modularna, niezależna i bezpieczna.

Należy podkreślić, że centrum sterowania wyposażone jest tak, aby zapewnić ciągłość zasilania elektrycznego, dlatego też fizyczna lokalizacja w nim poziomów 1 i 2 stanowi dodatkowe zabezpieczenie.

W przypadku bazy danych, oprócz zabezpieczenia jakie zapewnia system klastra sprzętowego, system zlokalizowany jest dodatkowo na klastrze składającym się z 2 maszyn wirtualnych.

Ponadto, wybrano sprzęt o wysokiej wydajności i dostępności.



Legenda:
„*Enlace agregado de 4 puertos”* oznacza: Dodatkowe połączenie 4 portów,
„EnlaceSTACK” oznacza: Połączenie STACK

2.8.7 Serwery

Przy wyborze serwerów uwzględniono głównie wysoką wydajność, dostępność i niezawodność oraz uwzględniono ich optymalizację dla Vmware Vsphere Essentials Kits plus (oprogramowanie do wirtualizacji). Konfiguracja systemu składać się będzie z trzech fizycznych serwerów, na których zainstalowane zostaną różne serwery/usługi wirtualne, które zostaną użyte w SZR.

2.8.8 Magazynowanie

W celu udostępnienia dodatkowego miejsca do magazynowania, do serwerów dodana zastanie kabina dysków iSCSI 14.4 TB SAS.

Ten system magazynowania, pozwala na projektowanie różnych rozwiązań bezpiecznego magazynowania i ułatwia wykorzystanie systemów klastrowych, ze wszystkimi wiążącymi się z tym zaletami.

2.8.9 Główne zabezpieczenia na wypadek awarii

Serwery, taśmowe magazynowanie tzw. *tape backup* i kabina magazynowania posiadają redundantne źródła zasilania.

Wszystkie urządzenia są redundantne (Serwery, Przełączniki, tzw. *Switches*, itd.)

Zasilanie każdego urządzenia jest redundantne i posiada zasilacz awaryjny, tzw. *UPS*.

Zaproponowana architektura jest całkowicie redundantna na drodze, w urządzeniach i łączności, tak więc nie istnieje żaden pojedynczy punkt systemu, który w przypadku awarii spowodowałby wadliwe działanie całości systemu, tzw. *SPoF (Single Point of Failure)* .

W łączności również uwzględniona jest redundancja N+1, a zatem każde urządzenie posiada przynajmniej 2 połączenia z każdym urządzeniem.

Sprzęt, jako całość, umożliwia posiadanie mocnego systemu, w którym jakikolwiek błąd jednego elementu nie uszkodzi systemu.

Zaletą wirtualnych serwerów, nie dostępną w przypadku fizycznych serwerów, jest migracja na żywo. Z migracją na żywo, wirtualne serwery mogą migrować na inne serwery fizyczne ,dla takich operacji, jak na przykład ich naprawa, bez potrzeby ich wyłączania.

2.8.10 Licencje

1x VMware 5.0, Up to 3 Servers and 6 CPU, NFI, Essentials Plus Ed.

2.9.- System kopii zapasowych

2.9.1 Co to jest kopia zapasowa

Jest to całkowita lub częściowa kopia ważnych informacji z dysku twardego, CD, baz danych i innych pamięci masowych. Ta kopia bezpieczeństwa powinien być zapisywane w innym systemie pamięci masowej, np. dyskach twardych, płytach CD, DVD lub taśmach magnetycznych (DDS, Travan, AIT, SLR, DLT i VXA).

2.9.2 Symantec Backup Exec 2010

Symantec Backup Exec 2010 jest zintegrowanym produktem chroniącym środowiska fizyczne i wirtualne, upraszczającym wykonywanie kopii bezpieczeństwa i odtwarzania po awarii, zapewnia niezrównane możliwości odtwarzania danych. W oparciu o technologię -Ray formy Symantec, Backup Exec 2010 odtwarza całe serwery, aplikacje krytyczne z Microsoft i środowiska wirtualne VMware lub Microsoft Hyper-V w celu znaczącego zminimalizowania czasu przestojów usług w przedsiębiorstwie.

Backup Exec 2010 zapewnie scentralizowane zarządzanie w celu łatwego rozszerzenia infrastruktury kopii zapasowych w rozproszonych zdalnych środowiskach i biurach, aby umożliwić łatwe zarządzanie ochroną serwerów fizycznych lub wirtualnych w miarę rozwoju przedsiębiorstwa. Dzięki pomysłowej i łatwej w użyciu konsoli zarządzania Backup Exec bardziej niż kiedykolwiek ułatwia efektywne zarządzanie operacjami wykonywania kopii zapasowych i ich odtwarzania w infrastrukturze fizycznej i wirtualnej. Backup Exec 2012 skutecznie zapewnia zaawansowane zasoby dla kopii bezpieczeństwa i odtwarzania danych systemów VMware, Hyper-V, Windows®, Linux® i Mac®, dla prostych i skomplikowanych środowisk IT.

2.9.2.1 Główne funkcje

- Proste odtwarzanie maszyn wirtualnych, aplikacji, baz danych, plików lub folderów i obiektów granularnych z kopii bezpieczeństwa w tylko jednym kroku w ciągu sekund za pomocą opatentowanej technologii V-Ray.

- Kopia bezpieczeństwa bez agenta dla maszyn wirtualnych.

- Zintegrowane odzyskiwanie na heterogenicznym sprzęcie i w stanie bare-metal, odtwarzanie maszyn fizycznych w maszynach wirtualnych (P2V).

- Zaawansowane usuwanie zduplikowanych danych w celu optymalizacji dowolnych strategii wykonywania kopii bezpieczeństwa z usuwaniem zduplikowanych danych na urządzeniach, serwerach, nośnikach i klientach.

- Nowoczesna i innowacyjna konsola administracyjna ułatwia bardziej niż kiedykolwiek konfigurowanie kopii bezpieczeństwa, administrowanie politykami kopii bezpieczeństwa, odtwarzanie danych po awarii i konwertowanie kopii bezpieczeństwa dla maszyn wirtualnych w celu umożliwienia ich natychmiastowego odtworzenia po awarii.

- Ochrona szerokiej gamy systemów operacyjnych, platform, aplikacji i baz danych, zarówno w środowiskach fizycznych jaki i wirtualnych, na dyskowych i taśmowych urządzeniach pamięci masowej.

- Kopie bezpieczeństwa i odtwarzanie danych certyfikowane przez Microsoft dla najnowszych środowisk i aplikacji Windows, w tym Windows 2008 R2®, Exchange 2010 SP1, SQL Server i SharePoint.

2.9.2.2 Procedura tworzenia kopii zapasowych

Kopie bezpieczeństwa systemu będą wykonywane w sposób automatyczny, zgodnie z instrukcjami z dokumentu „Program funkcjonalny i eksploatacyjny”

Kopia bezpieczeństwa będzie wykonywana co 3 dni (dane systemu serwerów) w oparciu o urządzenia taśmowe. Będzie to umożliwiać ich odtworzenie do trzech dni po dacie wykonania kopii.
Będzie wykonywana miesięczna kopia zapasowa (Visión i dane systemu + dane systemu serwerów) na dodatkowej macierzy dyskowej, umożliwiającej ich przechowywanie przez 30 dni po dacie wykonania kopii.
Dla każdej wykonanej kopii będzie przeprowadzane automatyczne sprawdzanie ich integralności przez oprogramowanie do wykonywania kopii zapasowych.

2.9.3 Licencja

1x Symantec Backup Exec 2010 R3 Virtual Server Suite z 1 rokiem wsparcia.

2.10.- Bazy danych BBDD

Zgodnie z dokumentacją jest wymagana zgodność ze standardami EIF 2004, w których zaleca się stosowanie oprogramowania FOSS, w związku z tym proponuje się zastosowanie Microsoft SQL 2012. .

2.10.1 Microsoft SQL Server 2012 Enterprise Edition

2.10.1.1 - Microsoft SQL Server Enterprise 2012 Edition

2012 De SQL Server Enterprise Edition to zestaw programów służących do korzystania z bazy danych opartej na modelu relacyjnym, które oferuje narzędzia do przechowywania danych, zarządzania, analizy i raportowania. Znajduje zastosowanie w dużych organizacjach i serwerach zorganizowanych.
Ta wersja programu SQL Server zawiera wszystkie funkcje wersji Standard i Business Intelligence wraz z dodatkowymi funkcjami niezbędnymi dla firm.

2.10.1.2 Charakterystyka

Funkcje znajdujące zastosowanie w dużych organizacjach, zawarte tej wersji mogą być wykorzystane do:

- Służy jako repozytorium danych dla różnych typów danych
- Integracji i zarządzania danymi w wielu systemach baz danych
- Zapewnienia większej wydajności, bardziej efektywne wykorzystanie zasobów sprzętowych i szybszego failover
- Funkcje:
- Najważniejsze cechy
- SQL Server zawiera podstawowe bazy danych, reporting i funkcje business intelligence (BI) analizy.
  System transakcyjne (OLTP) pozwalają na szybki dostęp do dużych ilości danych.
  Przetwarzanie analityczne online (OLAP) wraz z wielowymiarowymi modelami semantycznymi BI (BISM) umożliwiających analizę

wielowymiarowych danych z różnych punktów widzenia i w modelu tabelarycznym.
- xVelocity zwiększa przepustowość prędkości magazynowania danych i funkcji analiz biznesowych.
- Zapewnienie wysokiej, jakości danych w celu poprawienia jakości danych przy użyciu wiedzy organizacyjnej i dostawców danych referencyjnych, porządkowanie i odpowiedniość danych.

2.10.1.3 Licencje

Korzystanie z udostępnionych SAS w celu utworzenia dwóch serwerów SQL Server w konfiguracji Failover wymaga dwóch licencji Windows Enterprise Server, oraz wersji zgodnej z SQL Server Enterprise, w innym przypadku nie będzie można wykonać cluster.

1 x SQL SERVER Enterprise 2012 (w konfiguracji kluster Aktywny/Pasywny)
1 x CAL SQL Server 2012
N x CAL Client Access License

2.11.- Firewall

Jak podano w dokumentacji, zostanie zainstalowany firewall, co zostanie objaśnione w niniejszym rozdziale.

Zapora ogniowa (ang. firewall) jest częścią systemu lub sieci, której zadaniem jest blokowanie lub odmawianie osobom nieuprawnionym dostępu do komputera, umożliwiając jednocześnie połączenia dozwolone.

Chodzi tu o urządzenie lub grupę urządzeń skonfigurowanych w celu umożliwiania, ograniczania, szyfrowania, odszyfrowywania ruchu między poszczególnymi zakresami adresów i portów w oparciu o zestaw norm i innych kryteriów.

Firewalle mogą być implementować sprzętowo lub programowo albo jako kombinacja tych obu podejść. Firewalle są często stosowane aby zapobiec sytuacji, w której nieupoważnieni użytkownicy Internetu nie uzyskali dostępu do sieci prywatnych połączonych z Internet, w szczególności z intranetami. Wszystkie komunikaty wchodzące do intranetu i wychodzące z niego przechodzą przez firewall, który sprawdza każdy komunikat i blokuje komunikaty, które nie spełniają podanych warunków dotyczących kryteriów bezpieczeństwa.

Częste jest również jest podłączanie do firewalla trzeciej sieci, nazywanej strefą zdemilitaryzowaną lub DMZ, w której znajdują się serwery organizacji, które powinny być dostępne z sieci zewnętrznej.
Prawidłowo skonfigurowany firewall zapewnia niezbędną ochronę sieci, lecz w żadnym przypadku nie powinien być traktowany jako ochrona wystarczająca. Zabezpieczenie komputerów obejmuje więcej obszarów, poziomów pracy i ochrony.

2.11.1 Netfilter/iptables

W tym przypadku zdecydowaliśmy się na Netfilter/iptables.

Netfilter to framework dostępny w jądrze Linuksa, umożliwiający przechwytywanie i manipulowanie pakietami sieciowymi. Framework ten umożliwia zapewnienie obsługi pakietów ma różnych poziomach przetwarzania. Netfilter jest również nazwą projektu mającego na celu zapewnienie wolnych narzędzi dla firewalli opartych na Linuksie.

Najbardziej popularnym komponentem zbudowanym w oparciu o Netfilter jest iptables, narzędzie dla firewalli umożliwiające nie tylko filtrowanie pakietów, lecz także realizować tłumaczenia adresów sieciowych (NAT) dla protokołu IPv4 czy obsługę dzienników. Projekt Netfilter zapewnia nie tylko komponenty dostępne jako moduły jądra, lecz także zapewnia narzędzia wykorzystywane w przestrzeni użytkownika i biblioteki.

iptables jest nazwą narzędzia działającego w przestrzeni użytkownika, za pomocą którego administrator może określać polityki filtrowania ruchu przechodzącego przez sieć. Nazwa iptables jest stosowane często nieprawidłowo w odniesieniu do całej infrastruktury zapewnianej przez projekt Netfilter. Projekt oferuje również inne niezależne podsystemy iptables takie jak connection tracking system tj. system śledzenia połączeń, który umożliwia kolejkowanie pakietów w celu ich przetwarzania w przestrzeni użytkownika. iptables jest standardowym elementem praktycznie wszystkich aktualnych dystrybucji Linuksa.

2.11.1.1 iptables

iptables umożliwia administratorowi systemu definiowanie reguł postępowania z pakietami sieciowymi. Reguły są grupowane w łańcuchy: każdy łańcuch jest uporządkowaną listą reguł. Łańcuchy są grupowane w tabele: każda tabela jest skojarzona z innym typem przetwarzania pakietów.

Każde reguła podaje, jakie pakiety są z nią zgodne (match) i co należy robić z pakietem, jeżeli spełnia tę regułę. Każdy pakiet sieciowy docierający do komputera lub wysyłany z komputera przechodzi przez co najmniej jeden łańcuch, do pakiety jest stosowana każda reguła z danego łańcucha. Jeżeli reguła jest zgodna z datagramem, przetwarzanie zostaje wstrzymane i element docelowy reguły określa, co należy zrobić z pakietem. Jeżeli pakiet dochodzi do końca predefiniowanego łańcucha i nie odpowiada jej żadna reguła w łańcuchu, polityka docelowa łańcucha określa, co należy zrobić z pakietem. Jeżeli pakiet dochodzi do końca łańcucha zdefiniowanego przez użytkownika, nie spełniając żadnej reguły z łańcucha lub jeżeli łańcuch zdefiniowany przez użytkownika jest pusty, następuje dalsze przetwarzanie w łańcuchu wywołującym (tzw. implicit target RETURN). Politykę posiadają wyłącznie łańcuchy predefiniowane.

W iptables reguły są grupowane w łańcuchy. Łańcuch jest zestawem reguł dla pakietów IP, które określają, co należy z nimi robić. Każda reguła może odrzucić pakiet z łańcucha (skrót), w wyniku tego inne łańcuchy nie będą uwzględniane. Łańcuch może zawierać odwołanie do innego łańcucha: jeżeli pakiet przechodzi przez cały ten łańcuch lub spełnia jedną z reguł docelowych, będzie dalej przetwarzany w pierwszym łańcuchu. Nie ma ograniczeń co do ilości

zagnieżdżonych łańcuchów. Istnieją trzy podstawowe łańcuchy (INPUT, OUTPUT i FORWARD: WEJŚCIE, WYJŚCIE i PRZEKIEROWANIE), użytkownik może tworzyć dowolną liczbę łańcuchów. Reguła może być tylko odwołaniem do innego łańcucha.

2.11.1.2 Tabele

Istnieją już trzy tabele wbudowane, każde z nich zawiera pewne łańcuchy predefiniowane. Można tworzyć nowa tabele za pomocą modułów rozszerzeń. Administrator może tworzyć i usuwać łańcuchy definiowane przez użytkowników w dowolnych tabelach. Początkowo wszystkie łańcuchy są puste i mają jedna politykę celu, która umożliwia przechodzenie wszystkich pakietów bez blokowania ani modyfikowania.

- filter table (tabela filtrów) — Ta tabela jest odpowiedzialna za filtrowanie (tzn. blokowanie pakietów lub pozwalanie im na kontynuowanie ruchu). Wszystkie pakiety przechodzą przez tabelę filtrów. Zawiera ona następujące łańcuchy predefiniowane i każdy pakiet będzie przechodzić przez jeden z nich:
    - łańcuch INPUT chain (łańcuch WEJŚCIE) — Przez ten łańcuch przechodzą wszystkie pakiety przeznaczone dla tego systemu (z tego względu jest czasem nazywany LOCAL_INPUT)
    - łańcuch OUTPUT chain (łańcuch WYJŚCIA) — Przez ten łańcuch przechodzą wszystkie pakiety tworzone przez ten system (z tego względu jest czasem nazywany LOCAL_OUTPUT)
    - łańcuch FORWARD chain (łańcuch PRZEKIEROWANIA) — W tym łańcuchu będą przetwarzane wszystkie pakiety, które tylko przechodzą przez ten system w drodze do systemu docelowego
- nat table (tabela tłumaczenia adresów sieciowych) — Tabela ta jest odpowiedzialna za konfigurowanie zasad dotyczących przepisywania adresów lub portów dla pakietów. Przez tę tabelę przechodzi pierwszy pakiet z każdego połączenia; wynik określa, w jaki sposób będą przepisywane wszystkie pakiety z tego połączenia. Zawiera ona następujące redefiniowane łańcuchy:
    - łańcuch PREROUTING (łańcuch PREROUTINGU) — Przez ten łańcuch przechodzą pakiety przychodzące przed sprawdzeniem lokalnej tabeli routingu, w szczególności dla DNAT (destination-NAT lub tłumaczenie docelowych adresów sieciowych)
    - łańcuch POSTROUTING (łańcuch POSTROUTINGU) — Przez ten łańcuch przechodzą pakiety wychodzące po podjęciu decyzji o routingu, głównie dla SNAT (source-NAT lub tłumaczenie źródłowych adresów sieciowych)
    - łańcuch OUTPUT chain (łańcuch WYJŚCIA) — Umożliwia wykonanie funkcji DNAT dla pakietów generowanych lokalnie
- mangle table (tabela modyfikacji) — Ta tabela jest odpowiedzialna za dopasowywanie opcji dla pakietów, np. takich jak jakość usługi. Przez tę tabelę przechodzą wszystkie pakiety. Ze względu na to, że została ona zaprojektowana dla zaawansowanych zastosowań, zawiera ona wszystkie możliwe łańcuchy predefiniowane:

- łańcuch PREROUTING (łańcuch PREROUTINGU) — Wszystkie pakiety, którym udało się wejść do systemu, zanim funkcja routingu zdecyduje, że pakiet powinien zostać przekazywany (łańcuch FORWARD), czy też jest dostarczany lokalnie (łańcuch INPUT)

- łańcuch INPUT chain (łańcuch WEJŚCIE) — Przez ten łańcuch przechodzą wszystkie pakiety przeznaczone dla tego systemu

- łańcuch FORWARD chain (łańcuch PRZEKIEROWANIA) — Przez ten łańcuch przechodzą wszystkie pakiety, które przechodzą przez system

- łańcuch OUTPUT chain (łańcuch WYJŚCIA) — Przez ten łańcuch przechodzą wszystkie pakiety utworzone w tym systemie

- łańcuch POSTROUTING (łańcuch POSTROUTINGU) — Przez ten łańcuch przechodzą wszystkie pakiety wychodzące z systemu

Oprócz łańcuchów już wbudowanych, w każdej tabeli można również tworzyć dowolne łańcuchy zdefiniowane przez użytkownika, które umożliwią grupowanie reguł w logiczny sposób.

Każdy łańcuch zawiera listę reguł. Kiedy pakiet jest przesyłany do łańcucha, jest kolejno porównywany z każdą regułą w łańcuchu. Reguła określa, jakie właściwości powinien mieć pakiet, aby regułą miała zastosowanie (no. numer portu lub adres IP). Jeśli reguła nie jest spełniona, przetwarzanie jest kontynuowane od następnej reguły.
Jeśli natomiast reguła jest spełniona dla pakietu, są wykonywane instrukcje dotyczące celu (wszystkie inne przetwarzanie w łańcuchu są zwykle przerywane). Niektóre właściwości pakietów mogą być sprawdzane wyłącznie w pewnych łańcuchach (na przykład wyjściowy interfejs sieciowy nie jest prawidłowy dla łańcucha INPUT). Niektóre cele mogą być używane tylko w niektórych łańcuchach i/lub w niektórych tabelach (np. cel SNAT może być stosowany w łańcuchu POSTROUTING tabeli tłumaczenia adresów sieciowych).

2.11.1.3 Cel reguły

Celem reguły może być nazwa łańcucha zdefiniowanego przez użytkownika lub jeden z celów predefiniowanych ACCEPT, DROP, QUEUE lub RETURN (zaakceptuj, odrzuć, kolejkuj lub powróć). Kiedy cel jest nazwą łańcucha zdefiniowanego przez użytkownika, pakiet jest kierowany do tego łańcucha w celu przetworzenia (podobnie jak wywołanie procedury podrzędnej w języku programowania). Jeśli pakiet przechodzi przez łańcuch określony przez użytkownika i nie zostaje zastosowana żadna regułą z łańcucha, przetwarzanie pakietów jest kontynuowanie od miejsca, w którym zostało przerwane przetwarzanie w bieżącym łańcuchu. Te wywołania między łańcuchami mogą być zagnieżdżanie do dowolnego żądanego poziomu.

Istnieją następujące cele wbudowane:

2.11.1.3.1 ACCEPT (akceptuj)

Ten cel powoduje, że netfilter akceptuje pakiet. Jego znaczenie zależy łańcucha, w którym następuje akceptacja. Dla pakietu akceptowanego w łańcuchu

INPUT zezwala się na jego przyjęcie przez system (host), dla pakietu, który zostanie zaakceptowany w łańcuchu OUTPUT zezwala się na opuszczenie systemu, a dla pakietu akceptowanego w łańcuchu FORWARD zezwala się na jego przekierowanie (routing) przez system.

2.11.1.3.2 DROP (odrzuć)

Ten cel powoduje, że netfilter odrzuca pakiet bez żadnego innego typu przetwarzania. Pakiet po prostu znika bez przekazania żadnego typu do systemu lub aplikacji źródłowej informacji, że pakiet został usunięty w systemie docelowym. Znajduje to odzwierciedlenie w systemie, który często wysyła pakiety, jako communication timeout (przekroczenie maksymalnego czasu oczekiwania w komunikacji) może to powodować zakłócenia, chociaż usuwanie niechcianych pakietów przychodzących jest czasem uważany za dobrą politykę bezpieczeństwa, ponieważ ewentualny intruz nie uzyskuje żadnej wskazówki, czy system docelowy istnieje.

2.11.1.3.3 QUEUE (kolejkuj)

Cel ten oznacza, że pakiet jest przesyłany kolejki w przestrzeni użytkownika. aby zmienić pakiet, aplikacja może użyć biblioteki libipq, która jest także częścią pakietu netfilter/iptables. Jeśli nie ma żadnej aplikacji odczytującej kolejkę, ten cel jest równoznaczny cekowi DROP.

2.11.1.3.4 RETURN (zwróć)

Ten cel sprawia, że dany pakiet przestaje przechodzić przez łańcuch, w którym reguła zrealizowała cel RETURN. Jeśli dany łańcuch jest łańcuchem podrzędnym innego łańcucha, pakiet będzie dalej przetwarzany w łańcuchu nadrzędnym, jak gdyby nic się nie stało. Jeśli natomiast łańcuch jest głównym łańcuchem (na przykład łańcuch INPUT), do pakietu będzie stosowana domyślna politykę danego łańcucha (ACCEPT, DROP itp.).

Istnieje wiele dostępnych celów rozszerzonych. Niektóre z najbardziej typowych celów to:

2.11.1.3.5 REJECT (odrzuć)

Ten cel ma taki sam efekt jak 'DROP', lecz przesyła pakiet z informacją o do błędzie do nadawcy. Jest on stosowany głównie w łańcuchach INPUT i FORWARD w tabeli filtrowania. Typ pakietu można kontrolować za pomocą parametru '--reject-with'. Pakiet odrzucenia może podawać wyraźnie, że połączenie zostało przefiltrowane (pakiet ICMP filtrowany administracyjnie dla połączenia), choć większość użytkowników woli, by pakiet po prostu informował, że komputer nie akceptuje tego typu połączenia (taki pakiet będzie pakietem tcp-reset dla odrzuconych połączeń TCP, icmp-port-unreachable dla odrzuconych sesji UDP lub icmp-protocol-unreachable dla pakietów innych niż TCP i UDP). Jeżeli parametr '--reject-with' nie jest podany, domyślnym pakietem dla odrzucenia jest zawsze icmp-port-unreachable.

2.11.1.3.6 LOG (loguj)

Ten cel powoduje logowanie informacji o pakiecie. Może być stosowany w każdym łańcuchu dowolnej tabeli, jest używany często do debugowania (analiza awarii, np. sprawdzanie, czy pakiety są odrzucane).

2.11.1.3.7 ULOG

Ten cel powoduje tworzenie logu dla pakietów w sposób inny niż w przypadku celu LOG. Cel LOG powoduje wysyłanie informacji do log jądra, natomiast ULOG powoduje rozgłaszanie pakietów zgodnych z tą regułą przez gniazdo netlink, aby programy z przestrzeni użytkownika mogły odebrać ten pakiet łącząc się z gniazdem.

2.11.1.3.8 DNAT

Ten cel sprawia, że adres docelowy (oraz ewentualnie port) pakietu są przepisywane w celu przeprowadzenia tłumaczenia adresów sieciowych. Stosowany cel należy podać pomocą opcji '--to-destination'. Ma on zastosowanie wyłącznie w łańcuchach INPUT i FORWARD w tabeli nat. Ta decyzja ta zapamiętywana dla wszystkich przyszłych pakietów należących do tego samego połączenia, w odpowiedziach będą wpisywane adresy i porty początkowe zmieniane w pakiecie pierwotnym (tj. odwrotnie niż dla tego pakietu).

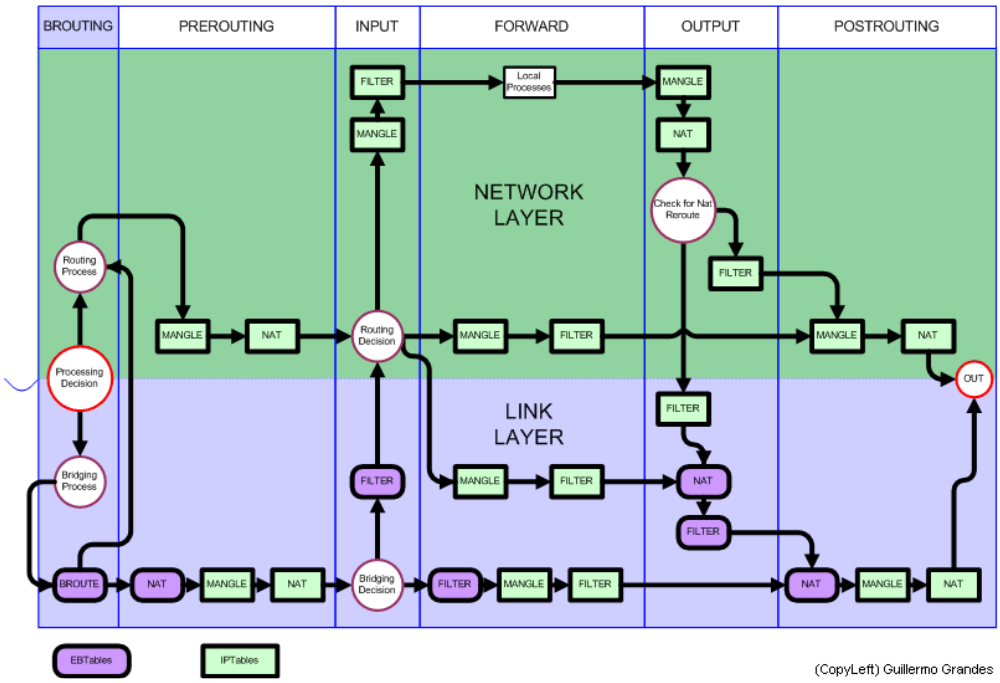
2.11.1.3.9 SNAT

Ten cel sprawia, że adres źródłowy (oraz ewentualnie port) pakietu są przepisywane w celu przeprowadzenia tłumaczenia adresów sieciowych. Stosowane źródło należy podać, korzystając z opcji '--to-source''. Jest on prawidłowy wyłącznie w łańcuchu POSTROUTING w tabeli nat i, podobnie jak DNAT, jest zapamiętywany dla wszystkich pakietów należących do tego samego połączenia.

2.11.1.3.10 MASQUERADE

Jest to specjalna, ograniczona forma SNAT dla dynamicznych adresów IP, takich adresy przydzielane przez większość usługodawców internetowych (ISP) dla modemom i cyfrowym liniom abonenckim (DSL). Zamiast zmieniać reguły SNAT po każdej zmianie adresu IP, jest obliczamy źródłowy adres IP, dla którego ma być prowadzony NAT w oparciu o adres IP na interfejsie wyjściowym, gdy pakiet jest zgodny z tą regułą. Dodatkowo cel zapamiętuje, jakie połączenia korzystają z celu MASQUERADE i czy adres interfejsu zmienia się (na przykład przy ponownym połączeniu się z ISP), wszystkie połączenia z NAT dla starego adresu są zapominane.

2.11.1.4 Diagram Netfilter/Iptables



3.- Facility Management

3.1.- Cele

Zadaniem Facility Management jest ułatwianie zarządzanie centrum kontroli poprzez implementację szeregu usług podstawowych dla jego działania, takich usługa poczty elektronicznej, serwer WWW, FTP, LDAP, RADIUS i VPN.
Całość oprogramowania opisanego w tym dokumencie jest oprogramowaniem open source. z wyjątkiem Open LDAP, który ma swoją własną licencję OpenLDAP Public License (zgodną z licencją GNU GPL) pozostałe rozwiązania są udostępniane na licencji GNU GPL (General Public License).

3.2.- Usługi

3.2.1 Serwer poczty

Został wybrany qmail, ponieważ w przeciwieństwie do szeregu innych starych programów MTA, qmail składa się z około 10 małych programów ściśle powiązanych ze sobą, z których każdy ma niewiele ponad 30 kB kodu. Inne programy takie jak exim czy sendmail zawierają jeden duży plik wykonywalny, który wykonuje wszystkie funkcje. Ta modułowa architektura upraszcza wiele rzeczy, między innymi jego funkcjonalność i konserwację.

Każdy z małych modułów wchodzących w skład qmail wykonuje inną funkcję. Na przykład zadaniem qmail-lspawn jest generowanie wysyłek lokalnych, gdy qmail-clean usuwa z kolejki pliki wiadomości, które zostały już przetworzone w całości.

W przeciwieństwie do innych MTA qmail nie wymaga uprawnień na poziomie root, aby otwierać port 25, nasłuchiwać na nim i obsługiwać dostawy lokalne. W tym przypadku, na przykład, tylko qmail-lspawn jest uruchamiany z uprawnieniami root i obsługuje dostawy lokalne. Nazywa się to zasadą najniższych uprawnień.

Jeśli chodzi o pliki konfiguracyjne, qmail używa wielu małych plików zamiast jednego, ogromnego pliku konfiguracyjnego. Globalnym plikiem konfiguracyjnym jest /var/qmail/control. Poszczególne pliki konfiguracyjne są umieszczane w katalogu home każdego użytkownika.

3.2.1.1 Qmail

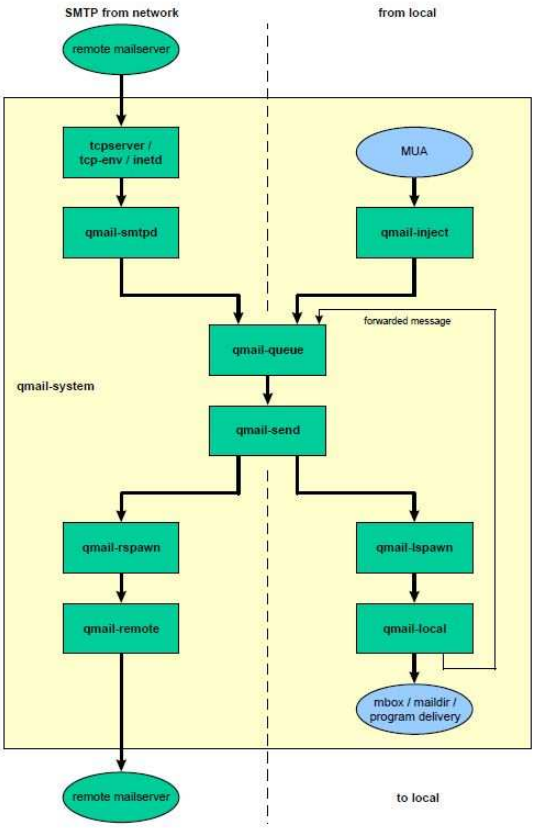
qmail jest agentem transportu wiadomości (MTA, ang. Mail Transport Agent) dla systemów operacyjnych opartych na Uniksie, qmail stosuje protokół Simple Mail Transfer Protocol (SMTP, prosty protokół transferu wiadomości) do wymiany wiadomości z MTA (Mail Transport Agent) innych systemów.

3.2.1.2 Działanie

Program ma konstrukcję modularną, moduły są uruchamiana oddzielnie, w tym celu jest dodawany dodatkowy poziom bezpieczeństwa:

- qmail-smtpd: Obsługuje on przychodzące transakcje SMTP i umieszcza wiadomości w kolejce.
- qmail-queue: zarządza kolejkę, przechowując wiadomości i wywołując qmail-send.
- qmail-send: Uruchamia dostarczanie wiadomości z kolejki do adresatów lokalnych i zdalnych.
- qmail-rspawn / qmail-remote: Wysyłają wiadomości wychodzące do serwerów SMTP odbiorców.
- qmail-lspawn / qmail-local: Dystrybuują wiadomości przychodzące do ich lokalnych odbiorców.

Następnie zostanie przedstawiony schemat, na podstawie którego można zrozumieć architekturę i działanie tego MTA, który jest jednym z najpotężniejszych tego typu systemów.
Zasadniczo zostaną przedstawione wchodzące w skład qmail i sposób, w jaki współpracują.



Wiadomość przychodzi do Qmail albo z programu w systemie lub albo z przychodzącego połączenia SMTP. Niezależne od miejsca, z którego pochodzi program, z którego został wysłany wykonuje program qmail-queue, który kopiuje wiadomość do pliku w katalogu queue, kopiuje dane nadawcy i odbiorcy do drugiego pliku i przekazuje o tym informację do qmail-send.

Jeżeli wiadomość została utworzona lokalnie, qmail-queue zostanie wywołany przez qmail-inject lub newinject, który dopisze brakujące linie w nagłówku wiadomości i skoryguje pola adresów. Jest w pełni dozwolone, by program wysyłający wiadomości bezpośrednio wywoływał qmail-queue. W większości przypadków qmail-inject jest wywoływany bezpośrednio przez sendmail.

Jeżeli wiadomość pochodzi z systemu zdalnego, piąty demon, tcpsever, będzie nasłuchiwać wszystkie połączenia smtp pochodzące z portu 25. Po każdym nadejściu połączenia, uruchamia qmail-smtpd, który otrzymuje komunikat prze smtp i wywołuje qmail-queue, aby umieścić w kolejce nową wiadomość.

Jak przedstawiono powyżej, niezależnie od miejsca, z którego pochodzi komunikat, qmail-queue zapisuje komunikat w pliku tymczasowy w katalogu queue/todo, dodając nową linię „otrzymano” w górnej części i kopiuje kopertę z danymi nadawcy i odbiorcy w drugim pliku. Następnie powiadamia qmail-send, wpisując trigger w pliku socket.

Następnie qmail-send pobiera komunikat stosu queue/todo, analizując możliwych odbiorców i sprawdza czy są oni lokalni, wirtualni czy zdalni.

W przypadku wiadomości lokalnych, informuje qmail-lspawn, by wykonał program qmail-local, aby dostarczył wiadomości lokalnie. Dla każdej z nich qmail-local dopasowuje kontekst użytkownika, który kontroluje adres dostawy (user ID, group ID, katalog home i kilka zmiennych środowiskowych, a następnie wykonuje działania podane w pliku .qmail adresu dostawy. W zależności od zawartości pliku .qmail z katalogu home użytkownika będącego odbiorcą, dostawa lokalna zachować wiadomość w skrzynce pocztowej, podać inny adres dla wysyłania wiadomości, wykonać program obsługujący wiadomość lub wykonać dowolną kombinację tych czynności.

Dla każdego zdalnego adresu z email qmail-send informuje qmail-rspawn, aby wykonał program qmail-remote w celu zrealizowania dostawy zdalnej. Każda z nich jest realizowana za pomocą osobnej sesji SMTP (jest to prawdopodobnie jeden z najbardziej kontrowersyjnych punktów Qmail).

Dla dostaw w domenach wirtualnych, qmail-send przepisuje każdy adres wirtualny, przekształcając go w zmodyfikowany adres lokalny, wykorzystując informacje z plików virtualdomains. Po przekształceniu ma odpowiednie adres lokalny wiadomość zostanie dostarczona podobnie jak każda inna wiadomość lokalna.

Dla każdego tych typów dostaw, lokalnych lub zdalnych, program spawn zwraca raport o statusie do qmail-send. Każda dostawa może być skuteczna, tymczasowa niemożliwa lub trwale niemożliwa. Dostawa, która została określona jako czasowo niemożliwa będzie ponawiana do czas, gdy wiadomość będzie określona jako zbyt stara, domyślnie okres ten trwa tydzień, lecz często jest krótszy. Jeżeli dostawa nie powiodła się przy pierwszej próbie albo po wielu próbach jest tworzony raport o odrzuceniu, który jest wysyłany w wiadomości e-mail do nadawcy wiadomości.

Gdy dla wszystkich adresów wiadomości czynność powiodła się lub nie, qmail-send informuje qmail-clean, by usunął pliki wiadomości z kolejki.

3.2.2 Serwer WWW

3.2.2.1 Wyjaśnienie

Serwer WWW lub serwer HTTP jest programem informatycznym przetwarzającym żądania po stronie serwera realizującego połączenia z klientem dwukierunkowe i/lub jednokierunkowe, synchroniczne lub asynchroniczne poprzez generowanie lub przekazywanie odpowiedzi w dowolnym języku (lub aplikacja po stronie klienta). Kod otrzymany przez klienta jest zwykle kompilowany i wykonywany przez przeglądarkę WWW. Do przekazywania tych danych jest używany pewien protokół.

3.2.2.2 Apache

Skrót od nazwy „a patchy server”. Serwer WWW rozpowszechniany jako wolne oprogramowanie z otwartym kodem jest najbardziej popularnym programem tego

typu na świecie od czerwca 1996 r., obecnie jego udział na rynku serwerów wynosi 50% całkowitej liczby serwerów WWW na świecie (sierpień 2007).

Apache jest rozwijany i utrzymywany przez otwartą społeczność programistów pod patronatem Apache Software Foundation.
Aplikacja może działać na wielu systemach operacyjnych w tym Windows, Novell NetWare, Mac OS X i w systemach opartych na systemie Unix.

3.2.2.3 Charakterystyki

Najważniejsze cechy serwera:

- Obsługa języków PERL, Python, tcl i PHP.
- Moduły uwierzytelniania: mod_access, mod_auth i mod_digest.
- Obsługa SSL i TLS.
- Umożliwia konfigurowanie spersonalizowanych komunikatów o błędach osoba i negocjacji treści.
- Umożliwia uwierzytelnianie baz danych oparte o systemy zarządzania bazami danych.
- Działa na wielu systemach operacyjnych.
- Apache to technologia bezpłatna z otwartym kodem źródłowym.
- Apache jest konfigurowalnym serwerem o konstrukcji modularnej.
- Zapewnia konfigurowalność przy tworzeniu i zarządzaniu dziennikami.
- Apache umożliwia tworzenie plików log w sposób umożliwiający uzyskanie większej kontroli nad tym, co dzieje się na serwerze

3.2.2.4 Działanie

Serwer jest dostarczane z zestawem modułów przetwarzania wielowątkowego, które są odpowiedzialne za połączenia z portami komputera, przyjmowanie żądań i generowanie procesów potomnych, które są odpowiedzialne za ich obsłużenie.

3.2.3 Serwer FTP

Aby ułatwić wymianę plików zostanie zaimplementowana usługa FTP, za pomocą której użytkownicy wewnętrzni i zewnętrzne będą mogli w prosty sposób ładować, pobierać i usuwać pliki po zalogowaniu się do serwera.

W tym przypadku został wybrany serwer FileZilla, który jest jednym z łatwiejszych w użyciu serwerów FTP, umożliwia on ponadto tworzenie certyfikatów, aby serwer FTP był bezpieczny.

3.2.3.1 Wyjaśnienie

FTP (ang. File Transfer Protokół, Protokół Transferu Plików) jest informatycznym protokołem sieciowym stosowanym do transferu plików między systemami połączonymi siecią TCP (Transmission Control Protokół), protokół ten jest oparty na architekturze klient-serwer. z komputera klienckiego można połączyć się z serwerem, aby pobierać z niego pliki lub przesyłać pliki na serwer niezależnie od systemu operacyjnego stosowanego na każdym z komputerów.

3.2.3.2 Opis

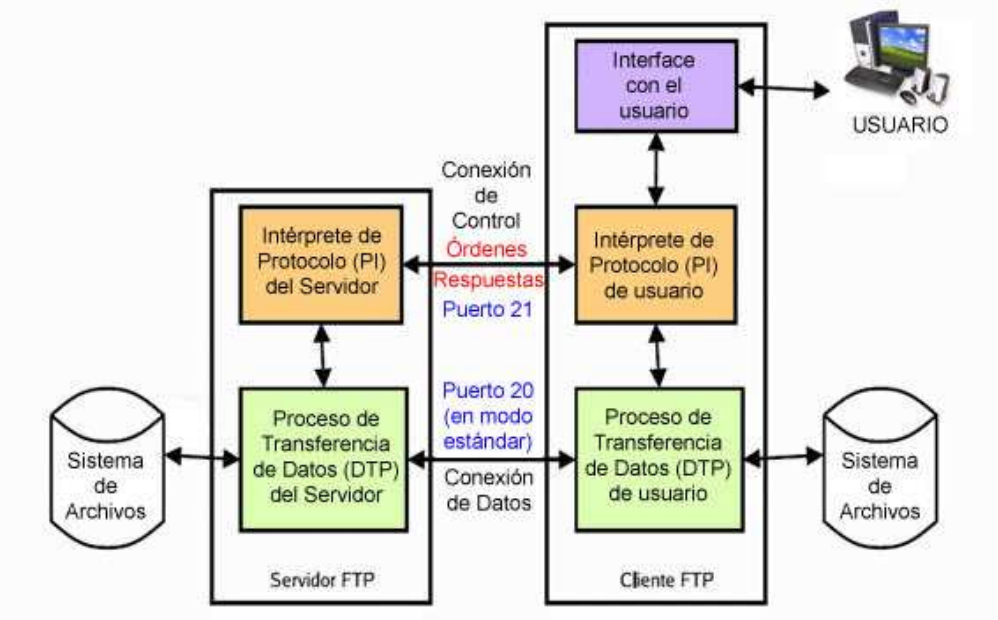
Usługa FTP jest zapewniania w warstwie aplikacji modelu organizacji warstwowej sieci TCP/IP, zazwyczaj są używane porty 20 i 21. Podstawowym problemem protokołu FTP jest to, że został zaprojektowany w celu zapewnienia maksymalnej szybkość połączenia, a nie maksymalnego bezpieczeństwa, ponieważ cała wymiana informacji, począwszy od nazwy i hasło użytkownika na serwerze do przesłania każdego z plików są wykonywane w postaci zwykłego tekstu bez szyfrowania, tak że potencjalny intruz może przechwytywać ruch, uzyskać dostęp do serwera i/lub przejąć przekazywane pliki.

W celu rozwiązania tego problemu są bardzo przydatne aplikacje takie jak SCP i SFTP zawarte w pakiecie SSH, umożliwiają one przesyłanie plików z szyfrowaniem całego ruchu.

3.2.3.3 Działanie

W modelu interpreter protokołu (IP) użytkownika ustanawia połączenie kontrolne na porcie 21. Standardowe polecenia FTP są generowane przez PI użytkownika, są one przesyłane do procesu serwera poprzez połączenie kontrolne. Standardowe odpowiedzi są przesyłane z PI serwera do PI użytkownika za pomocą połączenie kontrolnego w odpowiedzi na polecenia.

Te polecenia FTP podają parametry transmisji danych (port danych, tryb transferu, typ reprezentacji i struktura) oraz charakter operacji w systemie plików (zapis, pobieranie, dodawanie, usuwanie itp.). Proces transferu danych (DTP) użytkownika lub zastępującego go innego procesu musi poczekać, aż serwer ustanowi połączenie z podanym portem danych (port 20 w trybie aktywnym lub standardowym) i przekazywać dane zgodnie z podanymi parametrami.



NA wykresie widać również, że komunikacja między klientem a serwerem jest niezależna od systemu plików używanego na każdym z komputerów, zatem nie jest ważne, ze systemy operacyjne są różne, ponieważ jednostki komunikujące się ze sobą są PI czy DTP, o ile używają tego samego standardowego protokołu: FTP.
Należy również podkreślić, że połączenie dla danych jest dwukierunkowe, tzn. może być używane zarówno do wysyłania i odbierania danych, nie musi ono istnieć przez cały czas trwania połączenia FTP.

3.2.3.4 Filezilla

FileZilla Server jest serwerem obsługującym FTP i FTP z SSL/TLS, zapewniającym bezpieczne, szyfrowane połączenia z serwerem.

Dla zapewnienia ochrony danych FileZilla obsługuje protokół SSL i taki sam poziom szyfrowania jak przeglądarka internetową. Gdy jest stosowany protokół SSL, dane są szyfrowane, aby nie mogły ich odczytać osoby postronne, w ten sposób jest zachowana poufność. Program obsługuje także kompresję danych w locie, co umożliwia przyśpieszenie transferu.

3.2.4 Serwer LDAP

3.2.4.1 Opis LDAP

LDAP (Lightweight Directory Access Protocol, Lekki Protokół Usług katalogowych) jest protokołem typu klient-serwer umożliwiającym dostęp do usługi katalogowej.

Był stosowany początkowo jako front-end lub interfejs końcowy X.500, lecz może być również używany dla pojedynczych serwerów usług katalogowych i innych serwerów usług katalogowych.

Katalog jest bazą danych, lecz zwykle zawiera informacje bardziej opisowe i bardziej oparte na atrybutach.
Informacje zawarte w katalogu są o wiele częściej odczytywane niż zapisywane. W konsekwencji w katalogach zwykle nie są implementowane skomplikowane schematy dla transakcji ani schematy redukcji wykorzystywane w bazach danych w celu przeprowadzania złożonych aktualizacji dużych ilości danych, Aktualizacje w usługach katalogowych są zwykle bardzo proste, i takie podejście jest możliwe.

Usługi katalogowa mają zapewniać szybką reakcję w operacjach wyszukiwania lub przeglądania.
Mogą one być zdolne do replikacji informacji w szerokiej postaci w celu zwiększenia dostępności i niezawodności, przy jednoczesnym zmniejszeniu czasu reakcji. Podczas duplikowania informacji w usłudze katalogowej można zaakceptować tymczasowe niespójności między informacjami przechowywanymi w replikach, pod warunkiem że nastąpi ich synchronizacja.

Istnieje wiele sposobów świadczenia usług katalogowych. Różne metody umożliwiają przechowywanie w katalogu różnych typów informacji, określanie różnych wymogów dla odniesień do informacji, zapytań i aktualizacji, sposobu ochrony usług katalogowych przed niepowołanym dostępem. Niektóre usługi katalogowe są lokalne, zapewniają one usługi w ograniczonym kontekście. Inne usługi są globalne, zapewniać one usługi w dużo szerszym kontekście.

Do przetwarzania żądań (kwerend) i aktualizowania relacyjnej bazy danych jest używany system zarządzania bazami danych (Database Management System lub DBMS) Sybase, Oracle, Informix lub Microsoft. Bazy te mogą otrzymać setki lub tysiące zleceń tworzenia, modyfikacji lub usunięcia na sekundę.

Serwer LDAP jest używany do przetwarzania żądań (kwerend) w usłudze katalogowej LDAP. Jednakże LDAP przetwarza polecenia dotyczące usuwania i aktualizacji w sposób bardzo powolny. Innymi słowy, LDAP jest typem bazy danych, lecz nie jest to relacyjna baza danych. Nie został zaprojektowany do przetwarzania setek czy tysięcy aktualizacji na minutę, jak w systemach relacyjnych, lecz do obsługi odczytu danych prowadzonej w sposób bardzo efektywny. Działanie LDAP Usługa katalogowa

LDAP jest oparty na modelu klient-serwer.

Jeden lub więcej serwerów LDAP zawiera dane tworzące drzewo usługi katalogowej LDAP lub główną bazę danych, klient LDAP łączy się z serwerem LDAP i zadaje pytanie. Serwer udziela właściwej odpowiedzi lub wskazuje, gdzie klient może uzyskać więcej informacji. Bez względu na to, z którym serwerem LDAP klient się łączy, będzie widział zawsze ten sam widok katalogu; nazwa podawana na jednym serwerze LDAP odwołuje się do tego samego wpisu, do którego odwoływałaby się na innym serwerze LDAP.

3.2.4.2 Zalety w stosowania LDAP

Usługa katalogowa LDAP różni się od innych typów baz danych następującymi cechami:

- jest bardzo szybka przy odczycie rekordów
- umożliwia bardzo prostą i ekonomiczną replikację serwera
- wiele aplikacji różnych typów ma interfejsy umożliwiające łączenie się z LDAP i mogą z nim łatwo integrowane
- Posiada globalny model nazw, która gwarantuje, że wszystkie wpisy są unikatowe
- Wykorzystuje hierarchiczny system przechowywania informacji.
- Umożliwia stosowanie wielu niezależnych katalogowych
- Działa z wykorzystaniem protokołów TCP/IP i SSL
- Większość aplikacji obsługuje LDAP
- Większość serwerów LDAP jest łatwa w instalacji, konserwacji i można je łatwo optymalizować.

3.2.5 OpenLDAP

.
Projekt OpenLDAP powstał jako kontynuacja wersji serwera 3.3 LDAP z University of Michigan, gdy zaprzestano jej rozwijania.

OpenLDAP jest serwerem LDAP dystrybuowanym na licencji GNU (OpenSource), umożliwia ona bezpłatne użytkowanie oprogramowania zarówno w celach edukacyjnych jak i profesjonalnych. Ponadto jest dostępny kod źródłowy, aby można było dokonywać samodzielnie modyfikacji w programie.

3.2.6 Serwer Radius

Jak wskazano w dokumencie dotyczącym bezpieczeństwa i jakości usług, zostanie skonfigurowana usługa Radius, aby ograniczyć dostęp niepowołanych urządzeń do sieci.

Poniższy rozdział wyjaśnia skrótowo, co to jest serwer Radius i jaki typ serwera został wybrany.

3.2.6.1 Wyjaśnienie

RADIUS (ang. skrót od Remote Authentication Dial-In User Server). Jest to protokół uwierzytelniania i autoryzacji dla aplikacji obsługujących dostęp do sieci i mobilnych urządzeń IP. Do ustanowienia połączeń jest używany port UDP 1813.

Podczas łączenia się z ISP przez modem, DSL, modem kablowy, Ethernet lub Wi-Fi, są przesyłane informacje, są to zwykle nazwa użytkownika i hasło. Informacja ta jest przekazywana do serwera NAS (serwer dostępu do sieci Network Access Server) za pomocą protokołu PPP, przekierowuje on żądanie do serwera RADIUS, korzystając z protokołu RADIUS.

Serwer RADIUS sprawdza, czy informacje są poprawne, korzystając z protokołów uwierzytelniania takich jak PAP, CHAP lub EAP. Jeśli połączenie zostanie zaakceptowane, serwer zezwoli na dostępu do systemu dostawcy usług internetowych i przydziela zasoby sieciowe takie jak adres IP i inne parametry takie L2TP itp.

3.2.6.2 Free Radius

Został wybrany serwer Free Radius z następujących powodów:

- FreeRADIUS to modularny, wysoko wydajny darmowy pakiet RADIUS opracowany i rozpowszechniany na zasadach GNU General Public Licence, wersja 2, można go pobierać i użytkować za darmo.

- Pakiet FreeRADIUS zawiera serwer RADIUS, bibliotekę kliencką RADIUS na licencji BSD, bibliotekę PAM, moduł Apache oraz liczne dodatkowe programy narzędziowe i biblioteki programistyczne związane z RADIUS.

- W większości przypadków termin „FreeRADIUS” odnosi się do wolnego serwera RADIUS z otwartym kodem źródłowym zawartego w tym pakiecie.

- FreeRADIUS jest najbardziej popularnym serwerem open source RADIUS i najczęściej wdrażanym serwerem RADIUS na świecie.

- Obsługuje on wszystkie popularne protokoły uwierzytelniania, z serwerem jest dostarczane oparte o technologię PHP narzędzie do administrowania użytkownikami za pomocą przeglądarki internetowej noszące nazwę dial-up admin.

Nowa implementacja aplikacji internetowej dla freeradius stworzona w Ekwadorze — SAAAS!. Jest na nim opartych wiele komercyjnych produktów i usług RADIUS takich jak systemy wbudowane, urządzenia RADIUS obsługujące kontrolę dostępu do sieci i WiMAX. Obsługuje on potrzeby AAA wielu firm z listy Fortune-500, firm telekomunikacyjnych i dostawców usług internetowych Tier 1. Jest również szeroko stosowany w środowisku akademickim, w tym w eduroam. Serwer jest szybki, ma wiele funkcji, jest modularny i skalowalny. Jest dostępna stabilna wersja 2.1.11 serwera, w każdej nowej wersji są dodawane kolejne udoskonalenia.

3.2.6.3 Charakterystyki

Jedną z najważniejszych cech protokołu RADIUS jest jego zdolność do zarządzania sesjami, z podawanie informacji, kiedy połączenie zaczyna się i kiedy kończy, więc można zmierzyć wykorzystanie usługi przez użytkownika i je zafakturować, dane mogą być wykorzystywane do celów statystycznych.

3.2.7 Serwer VPN

Virtual Private Network (VPN) to technologia sieciowa, umożliwiająca rozszerzenie sieci lokalnej za pośrednictwem sieci publicznej lub sieci niekontrolowanej.

VPN będzie stosowany, by administrator zdalny mógł administrować w bezpieczny sposób sieciami znajdującymi się poza centralą, z której prowadzona jest kontrola.

W przypadku tej usługi zostało wybrane rozwiązanie oparte na obsługującym SSL oprogramowaniu OpenVPN.

OpenVPN zapewnia połączenia point-to-point z hierarchiczną weryfikacją użytkowników i hostów podłączanych zdalnie, jest to bardzo dobra opcja dla technologii Wi-Fi (sieci bezprzewodowe IEE 802.11), umożliwia konfigurację wielu parametrów, w tym równoważenie obciążenia.
Jest udostępniany na zasadach licencji GPL wolnego oprogramowania.

3.2.7.1 OpenVPN

OpenVPN łączy bezpieczeństwo z łatwością obsługi. Lekka architektura OpenVPN sprawia, że nie istnieją w nim liczne skomplikowane problemy właściwe dla innych implementacji VPN. Model zabezpieczeń OpenVPN jest oparty na SSL, który jest standardem przemysłowym w dziedzinie bezpiecznej komunikacji przez Internet. OpenVPN stosuje rozszerzenia warstw 2 lub 3 modelu OSI za pomocą protokołów SSL/TLS, obsługuje elastyczne metody uwierzytelniania klientów oparte na certyfikatach, kartach inteligentnych i dwuskładnikowym uwierzytelnianiu, i umożliwia stosowanie polityk kontroli dostępu dla użytkowników lub grup, w szczególności poprzez stosowanie reguł zapory sieciowej dla interfejsu wirtualnego VPN. OpenVPN nie jest serwerem proxy aplikacji internetowych, nie działa za pośrednictwem przeglądarki internetowej.

3.2.7.2 Opis

OpenVPN to oprogramowanie do tworzenia wirtualnych sieci prywatnych (VPN) opartych na SSL, umożliwia ono bezpieczne łączenie się ze zdalnymi biurami, można również umożliwić użytkownikom mobilnym zdalny dostęp do usług w prywatnej sieci LAN. W oparciu o otwarte standardy SSL/TLS i wolne oprogramowanie OpenVPN zapewnia następujące funkcje:

- Rozwiązanie VPN klasy korporacyjnej oparte o wolne oprogramowania i GNU/Linux

- Tworzenie tuneli VPN dla połączeń point-to-point, site-to-site i użytkowników mobilnych

- Stosowanie jako środka komunikacji protokołów TCP lub UDP

- Umożliwia wiele połączeń z tą samą instancją z użyciem jednego portu TCP lub UDP

- Tunele VPN działają, korzystając z połączeń NAT (Network Address Translation) i dynamicznych adresów IP

- Rozwiązanie jest oparte na standardach przemysłowych SSL/TLS zapewniających bezpieczną komunikację i uwierzytelnianie, korzysta ze wszystkich funkcji OpenSSL w celu szyfrowania, uwierzytelniania i certyfikacji do ochrony ruchu w sieci prywatnej podczas tunelowania przez Internet

- Rozwiązanie może stosować dowolne szyfrowanie, rozmiar klucza, HMAC digest (do sprawdzania integralności datagramów) obsługiwane przez bibliotekę OpenSSL.

- Elastyczne szyfrowanie umożliwia wybór następujących opcji:

  - Tradycyjne szyfrowanie oparte na statycznych kluczach wstępnie współdzielonych

  - Szyfrowanie asymetryczne przy użyciu kluczy publicznych opartych na certyfikatach x509

- Umożliwia stosowanie do wymiany kluczy statycznych kluczy wstępnie współdzielonych (preshared) i kluczy dynamicznych opartych na TLS

- Umożliwia stosowanie kompresji w czasie rzeczywistym i kształtowania ruchu w celu zarządzania wykorzystaniem pasma

- Umożliwia korzystanie z dodatków (wtyczek) w celu rozszerzenia mechanizmów uwierzytelniania, obecnie zawiera dodatki dla PAM i LDAP

- Serwer DHCP zintegrowany z OpenVPN może dostarczać klientom VPN następujących informacji o sieci:

  - Statyczny lub dynamiczny wirtualny adres IP
  - Adres serwerów DNS
  - Sufiks DNS
  - Adres domyślnej bramy
  - Serwer WINS

- Integracja z zaporą sieciową (netfilter/iptables) w celu filtrowania ruchu VPN->LAN

- Natywne wsparcie dla następujących klienckich systemów operacyjnych:
  - GNU/Linux
  - Solaris
  - OpenBSD
  - NetBSD
  - FreeBSD
  - MS Windows XP, Vista i 7
  - Mac OSX

3.2.7.3 Uwierzytelnianie OpenVPN

OpenVPN obsługuje różne metody uwierzytelniania, począwszy od tradycyjnych tajnych kluczy szyfrujących wstępnie współdzielonych (Static Key mode) po metody uwierzytelniania oparte na kluczy publicznych (SSL/TLS mode) przy użyciu certyfikatów X.509 dla serwera i klientów VPN.

3.2.7.4 Uwierzytelnianie oparte na statycznych kluczach wstępnie współdzielonych

OpenVPN obsługuje szyfrowanie przy użyciu tradycyjnych tajnych kluczy wstępnie współdzielonych (Sratic Key), klucze statyczne są stosowane zarówno do uwierzytelniania jak i autoryzacji.

Używanie kluczy statycznych do uwierzytelniania ma swoje wady i zalety, są one wymienione poniżej:

3.2.7.4.1 Zalety

- Łatwa konfiguracja obu punktów VPN

- Brak certyfikatów, urzędów certyfikacji ani skomplikowanych bezpiecznych protokołów i negocjowania. Jedynym wymogiem jest możliwość utworzenia bezpiecznego kanału ustanowionego wcześniej w celu wymiany kluczy statycznych pomiędzy dwoma punktami sieci VPN, może to być scp lub wiadomość e-mail z PGP

3.2.7.4.2 Wady

- Można utworzyć tylko jeden tunel point-to-point przy użyciu kluczy statycznych

- Jeżeli użytkownik chce utworzyć więcej tuneli, musi uruchomić nową instancję OpenVPN z innym plikiem konfiguracyjny i użyć do nasłuchiwania innego, niezależnego portu (opcja port).

- Musi istnieć ustanowiony uprzednio bezpieczny kanał wymiany klucza, nie jest to problemem z PKI, ponieważ użytkownik może wygenerować swój własny klucz prywatny i wygenerować żądanie certyfikatu lub CSR (Certificate Signing Request) i tajny klucz prywatnego nie będzie nigdy przesyłany przez sieć (będzie przesyłany tylko CSR).

- Klucz statyczny nie może zostać zmieniony, o ile nie zostanie wygenerowany nowy klucz, co oznacza. że musi on zostać dostarczony na drugi koniec kanału VPN.

- Jeżeli intruz zdoła przechwycić klucz, wszystkie dane szyfrowane z użyciem klucza będą zagrożone.

W zależności od trybu tunelu VPN jest stosowana metoda uwierzytelniania, zwykle dla połączeń point-to-point lub host-to-host są stosowane klucze uprzednio współdzielone.

3.2.7.5 Uwierzytelnianie oparte na certyfikatach X.509

Przy uwierzytelnianiu opartym na certyfikatach SSL, OpenVPN

Certyfikat główny służy do sprawdzania autentyczności certyfikatu serwera OpenVPN i klientów sieci VPN, tj. jest przeprowadzane wzajemne uwierzytelnianie, klient potwierdza autentyczność certyfikatu, który identyfikuje serwer, a serwer potwierdza autentyczność certyfikatu, który identyfikuje klienta.

Klient OpenVPN używa certyfikatu do uwierzytelniania na serwerze OpenVPN oraz do szyfrowanie pakietów przechodzących przez tunel VPN.

4.- Zużycie Energii

4.1.- Zasilacz bezprzerwowy (UPS) i Generator

Podstawową funkcją bezprzerwowego systemu lub układu zasilania jest zapewnienie stałego zabezpieczenia przed całkowitą lub częściową awarią dostaw prądu dostarczanego przez komercyjną sieć zasilającą zapobiegając jakimkolwiek przerwom zasilania. Ponadto, system ten funkcjonuje również jako kondycjoner linii.

Komputery, serwery, ściany graficzne i urządzenia peryferyjne z pomieszczeń kontrolnych będą zasilane prądem o napięciu 220 VAC i będą podłączone do zasilacza UPS

Aby zapewnić całodobową dostępność, Centrum kontrolne będzie wyposażone w zasilacz bezprzerwowy. Dodatkowy generator będzie zapewniony dla budynku przez Radę i jest poza zakresem tego dokumentu.

UPS umożliwia funkcjonowanie niezbędnego sprzętu w przypadku odcięcia głównego zasilania sieciowego.

Umożliwi to zapewnienie rezerwy energii roboczej na okres minimum 4 godzin bez ładowania i uzupełniania paliwa.

Generator musi zapewnić oświetlenie pomieszczenia kontrolnego oraz utrzymanie pozostałych funkcji na normalnym poziomie, oraz zapewnić oświetlenie awaryjne innych pomieszczeń i korytarzy.

Urządzenia klimatyzacyjne w pomieszczeniu kontrolnym będzie działać nieustannie w warunkach zasilania z UPS lub Generatora.

System zasilania i zabezpieczenia elektryczne dla sprzętu są skonstruowane w następujący sposób.

Główna skrzynka rozdzielcza będzie zasilana z ogólnego gniazda. Skrzynka ta będzie podzielona na dwie sekcje, sprzęt zasilany przez UPS oraz sprzęt zasilany z ogólnego źródła.

Przewód z pierwszej sekcji (sekcja UPS oraz Generatora) jest podłączona do terminalu wejściowego UPS, a przewód wyjściowy z UPS jest podłączony z powrotem do skrzynki. Z tej linii zasilany jest ważniejszy sprzęt.

Skrzynka rozdzielcza zawiera ogólną ochronę elektryczną sprzętu.

Głównymi urządzeniami zasilanymi z UPS są:

- Serwery
- Niektóre stacje robocze
- Switche Ethernet
- Routery
- System alarmów przeciwpożarowych
- System klimatyzacji Serwerowni
- System telefonu IP

Inne urządzenia, jak ściana wizyjna, drukarki, oświetlenie, itd. będą zasilane z rozdzielnicy głównej, a nie z zasilacza UPS.

Pobór mocy Centrum sterowania jest następujący:

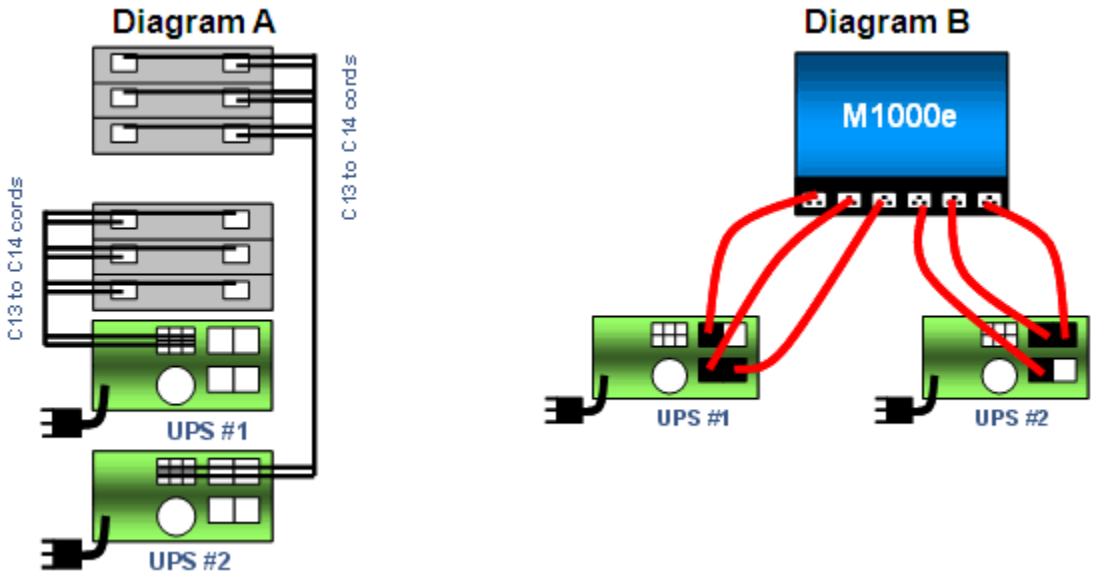
ID	Opis	Ilość	Moc Jednostki	Moc całkowita
1	Serwer	1	2733,78	2734
2	19" Rack	2	250	500
3	Stacja robocza	7	580	4.060
4	Routery	2	50	100
5	Ethernet switch 10/100/1000	1	75	75
6	Video NVR	1	345	345
7	IPBX	1	240	240
8	Telefony IP	7	15	105
9	Klimatyzacja pomieszczenia CPD	1	2600	2600
10	Oświetlenie Awaryjne	12	40	480
11	Ściana wizyjna	1	1256	1256
12	Monitory CCTV	8	100	800
Całkowita ilość Watów				**13300**

Wydajność wynosi 0,8. Tak więc pobór mocy wynosi **13.300/0,8** = 16737 VA

Obliczenia poboru mocy zostały zaprojektowane przy 100% zużyciu energii elektrycznej każdego z urządzeń.

UPS powinien posiadać moc co najmniej 17 KVA. Ze względu na ten aspekt obowiązkowe jest dzielenie urządzeń na kilka UPS, każde urządzenie z podwójnym zasilaniem będzie zasilane różnymi UPS.

Dla tego projektu będą zapewnione 3 UPS o łącznej mocy 5600 W. Urządzenia będą połączone zgodnie z tym schematem:



Główne cechy:

- Interaktywny online
- Tryb oszczędzania energii 50 W, 100 W ... (wyłącza się po 5 minutach, jeśli UPS jest zasilany z akumulatora i moc wejściowa jest poniżej wybranego poziomu)
- System jednofazowy
- Rail kit (4 podpory) w komplecie
- Technologia ABM®
- Segmenty ładowania
- Wielojęzyczny i graficzny wyświetlacz LCD z podświetleniem
- Akumulatory wymieniane przez użytkownika
- Akumulatory wymieniane na ciepło
- Możliwość uruchamiania na zimno
- Idealny do ładowania skorygowanego o współczynnik zasilania (na podstawie Wat)
- Automatyczny bypass
- Automatyczne wykrywanie napięcia i częstotliwości wejściowej
- Port REPO
- Zdalnie włączany/wyłączany
- Aktualizowanie oprogramowania
- Wejście prawdziwej fali sinusoidalnej
- Gniazdko interfejsu bez blokowania od 220 do 240 VAC i 32 A IEC 309 (P + N + T) 332P6 (klasyfikacja IP44)
- Programowanie konfiguracji do odczytu/zapisu/kopiowania
- Kompatybilność z rozbudowanym modułem akumulatora (EBM)
- Rail Kit w komplecie
- Łączność w szeregu
- Złącze USB
- Zgodny z SNMP/Web
- Kontrola temperatury, wilgotności i styków
- Software zarządzania do UPS (CD)

UPS będzie w stanie zapewnić zasilanie do podstawowych usług przez co najmniej 15 minut, co powinno wystarczyć na uruchomienie i ustabilizowanie pracy Generatora.

Pomieszczenie akumulatorów UPS zostanie wyposażone w czujniki określonych gazów oraz automatyczne systemy wentylacji mechanicznej. Monitorowanie powietrza i obieg wentylacji tego pomieszczenia będzie niezależny od innych w centrum sterowania.

Opis i Uruchamianie

a) Filtr Stabilizacyjny: Wykonuje filtrowanie (eliminując zakłócenia statyczne) oraz posiada funkcję stabilizacji napięcia.

b) Inwerter: Umieszczony przy wyjściu z filtra stabilizacyjnego. Gdy zasilanie sieciowe działa prawidłowo, inwerter działa jako prostownik, ładując akumulator.

W przypadku zaniku zasilania sieciowego inwerter pobiera prąd z akumulatora i przekształca go na prąd przemienny, rekompensując brak zasilania. Przejście z jednego trybu pracy na drugi będzie następować bez konieczności przełączania.

c) Akumulatory. Uszczelnione. Nie wymagają utrzymania mieszania gazów. Baterie pełnią funkcję przechowywania energii do zasilania inwertera w przypadku awarii sieci.

d) By-pass (przełącznik statyczny): Utrzymując inwerter stale włączonym, musi on działać przy wyłączonym zasilaniu sieciowym, gdy pojawiają się w nim nieprawidłowości.

W przypadku awarii inwertera, system włącza automatycznie filtr stabilizujący, zapewniając by-pass zasilania sieciowego ze stabilizacją i filtrowaniem.

Główne parametry techniczne zasilacza są następujące:

Ogólne

Moc znamionowa kVA:	30Kva
Moc znamionowa kW:	24kW
Współczynnik mocy wyjściowej	0,8
Typowa Autonomia:	15 min.

Wejście

Zakres napięć:	300V - 480V
Zdolność Pełnego Ładowania:	330V - 480V
Zakres Częstotliwości:	50/60Hz +-20%
Współczynnik mocy:	0,95

Wyjście

Napięcie:	220, 230, 240V (wyjście 1-fazowe) / 380, 400, 415V (wyjście 3-fazowe)
Stabilność napięcia:	Statyczne obciążenie zrównoważone 1% Dynamiczne (100% stopień obciążenia) 5%
Zniekształcenia Napięcia (THD):	<3% (obciążenie liniowe) <5% (3:1 współczynnik szczytu)
Częstotliwość:	Nominalna 50 / 60Hz Zakres synchronizacji 1 do 4% regulowany Stabilność przy normalnej pracy 0.005%
Współczynnik szczytu obciążenia:	3:1 przy pełnym obciążeniu, bez zmiany parametrów
Przeciążenie:	125% przez 10 minut, 150% przez 10 sekund

Fizyczne

Wymiary (Szer. x Głęb. x Wys.):	Wymiary (Szer. x Głęb. x Wys.) 530 x 950 x 1220 mm
Łączność:	Karta SNMP i Web - Serial - Styk
Temperatura Robocza:	0° - 40° C (20° C dla opcjonalnej żywotności akumulatora)
Słyszalny hałas w odległości 1 m:	<52 dBA

Standardy i Normy

Bezpieczeństwo:	EN50091-1-1
EMC:	EN50091-2 Class A

Klimatyzacja dla pomieszczenia CPD i Serwerowni jest obliczana na podstawie tej tabeli:

Wybrane napięcie: **230 V**
Temperatura otoczenia : **10℃ - 25℃ / 50℉ - 77℉**

Nazwa	Obciążenie	Obciążenie prądu stałego	Moc Aktywna	Moc Pozorna	Natężenie	Emisja Ciepła		Przepływ powietrza	
	[%]	[W]	[W]	[VA]	[A]	[kj/h]	[BTU]	[m3/h]	[CFM]
Rack 42U									
Monitor 17" TFT 1U	100	20,00	25,00	25,25	0,11	90,00	85,32	0,00	0,00
Serwer 1	100	397,20	426,46	428,17	1,86	1535,24	1455,48	68,00	40,02
Serwer 2	100	397,20	426,46	428,17	1,86	1535,24	1455,48	68,00	40,02
Serwer 3	100	452,50	497,57	499,57	2,17	1791,27	1698,21	100,00	58,86
Biblioteka taśm			85,00	105,00	0,46	306,00	290,10	0,00	0,00
Kontroler biblioteki taśm	100	325,10	373,49	383,07	1,67	1344,56	1274,71	0,00	0,00
Kontroler pamięci masowej 1	100	386,00	440,51	451,81	1,96	1585,85	1503,46	0,00	0,00
Kontroler pamięci masowej 2	100	366,40	419,29	430,05	1,87	1509,46	1431,04	0,00	0,00
Zmiana konsoli KVM			40,00	80,00	0,35	144,00	136,52	0,00	0,00
			2733,78	**2831,09**	**12,31**	**9841,62**	**9330,32**	**236,00**	**138,90**

5.- Lokalizacja Elementów

5.1.- Ogólnie

Rozdział zawiera opis wyposażenia Centrum Sterowania Ruchem.

System ITS jest rozpoznawanym na świecie Systemem Strategicznym i Systemem Bezpieczeństwa dzięki zadaniom jakie spełnia, oraz dzięki wpływowi na przebieg ruchu miejskiego (np. wypadki samochodowe wywołane nieprzepisową jazdą, wpływem zatorów drogowych na ruch miejski…).

Centrum Sterowania Ruchem jest zaprojektowane do pracy 7 dni w tygodniu, 24 godziny na dobę, przy jednoczesnym spełnieniu najwyższych standardów jakości zarządzania ITS, z możliwością pracy w samodzielnym systemie, bez urządzeń zewnętrznych.

Centrum Sterowania Ruchem będzie nową, specjalnie utworzoną jednostką organizacyjną, której istnienie nie będzie jednakże wymagało nowelizacji szeregu ustaw i rozporządzeń, posługującą się zestawem środków technicznych (np. ściana wizyjna, serwery, oprogramowanie, środki łączności) ulokowanych w wyznaczonych pomieszczeniach.

Uważamy, i tak jak zostało to uwzględnione w naszej ofercie, że elementy techniczne będące własnością CSR powinny być zainstalowane w tym samym miejscu, gdzie zlokalizowane jest CSR. Według punktu 2.5.7 Programu Funkcjonalno-Użytkowego pierwotną lokalizacją była ul. Wieniawska 14, IV piętro, która z powodów Zamawiającego została zmieniona na ul. Lipową 27 dokumentem z dnia 23/04/2012r.

Za normę uznaje się instalację wszystkich elementów w Centrum Sterowania Ruchem, co w tym przypadku rekomendujemy, ale co nie wyklucza możliwości tworzenia kopii zapasowych danych w zewnętrznym CPD.

W tym dokumencie przedstawiono schemat organizacji CSR, który posłuży do realizacji wstępnego projektu centrum. Podczas realizacji umowy, w końcowej fazie projektu systemu, zostanie sporządzony ostateczny schemat oddany do weryfikacji i późniejszej aprobaty.

Z uwagi na lokalizację wejścia, należy zwrócić uwagę że urządzenia przeznaczone do instalacji w centrum kontroli powinny być instalowane na miejscu, z uwagi na to, że istnieje jedynie możliwość korzystania z klatki schodowej budynku.

ACISA zapewnia, że dostawa sprzętu nie zniszczy infrastruktury Centrum Sterowania oraz że miejsce jest wystarczająco wytrzymałe, aby zlokalizować w nim sprzęt.

ACISA dostarczy swoim inżynierom informacji dotyczącej wagi najcięższego sprzętu, wraz z Ostatecznym Projektem Systemu, oraz wykona niezbędne kontrole konstrukcji budynku, których celem będzie zapewnienie, że nie zostanie ona uszkodzona przez instalowany sprzęt.

5.2.- Rysunki & Wizualizacja

Poniższy rozdział zawiera przewidywane rozmieszczenie Sali Centrum Sterowania.

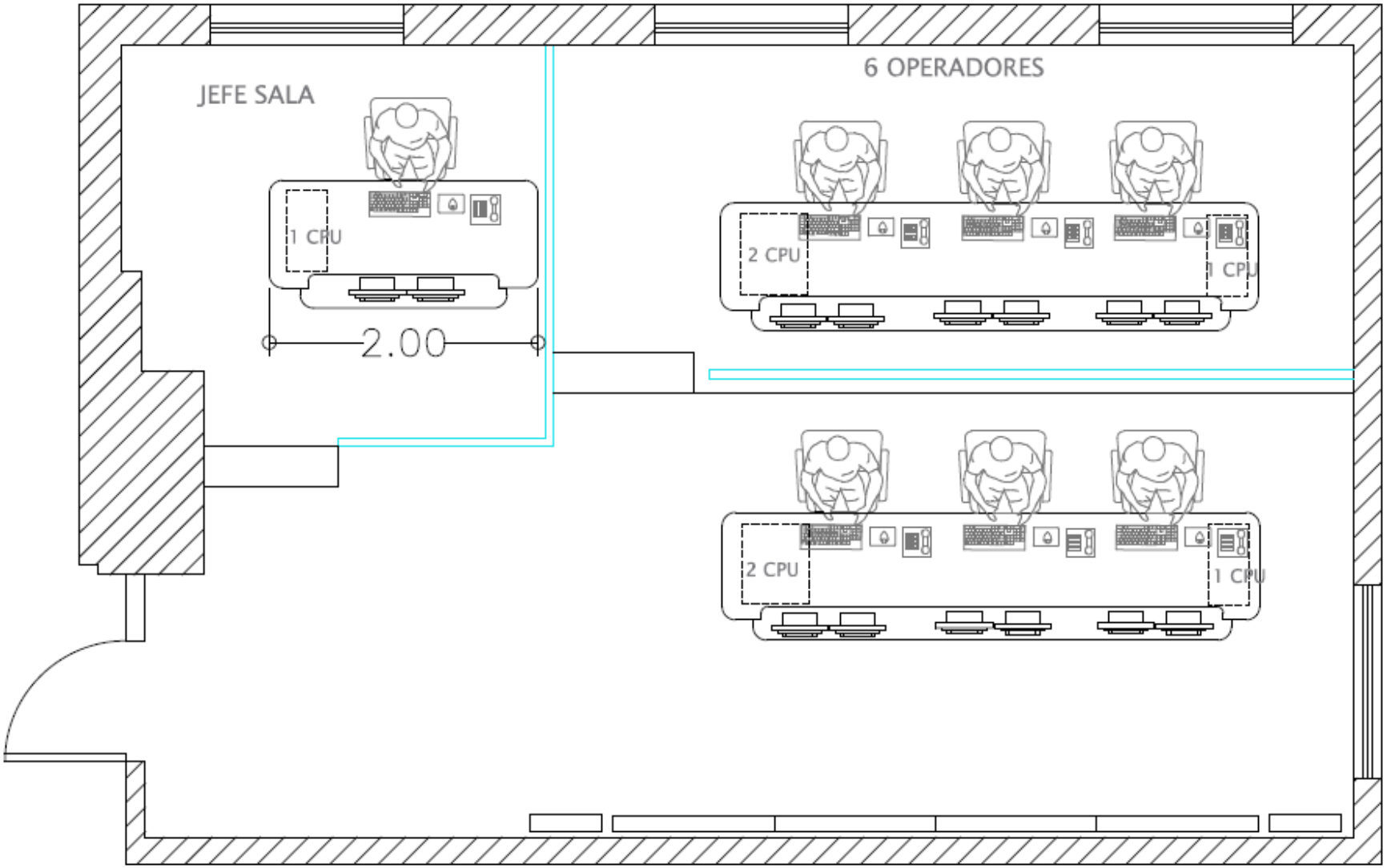

Where Does Your Electricity Come From?
acisa
AERONAVAL DE CONSTRUCCIONES E INSTALACIONES, S.A.


acisa
AERONAVAL DE CONSTRUCCIONES E INSTALACIONES, S.A.


acisa
AERONAVAL DE CONSTRUCCIONES E INSTALACIONES, S.A.


acisa
AERONAVAL DE CONSTRUCCIONES E INSTALACIONES, S.A.


acisa
AERONAVAL DE CONSTRUCCIONES E INSTALACIONES, S.A.


JEFE SALA
6 OPERADORES
1 CPU
2.00
2 CPU
1 CPU
2 CPU
1 CPU