Biblioteka Miejska w Łodzi

ZP.26.63.2022

ZAŁĄCZNIK NR 2

Czynności administracyjne związane z utrzymaniem infrastruktury serwerowej

Czynności okresowe

- Archiwizowanie obrazów maszyn wirtualnych i baz danych systemu Patron oraz zarządzania plikami archiwalnymi zgodnie z ustalonym z Zamawiającym planem archiwizacji, przechowywania i retencji kopii archiwalnych
- Okresowa przebudowa indeksów w bazach MS SQL systemu Patron
- Zapewnienie prawidłowych mechanizmów rotacji logów generowanych przez oprogramowanie Patron.

Czynności bieżące

- Bieżące monitorowanie dostępności infrastruktury: serwerów wirtualnych i podstawowych usług funkcjonujących na tych serwerach; monitoring musi być prowadzony z lokalizacji poza serwerownią.
- Bieżąca kontrola wykorzystania zasobów i realokacja zasobów w razie konieczności; informowanie Zamawiającego o wszelkich problemach związanych z zasobami i przekazywanie propozycji zmian w tym zakresie.
- Bieżąca administracja wszystkimi systemami wchodzącymi z skład rozwiązania, w tym w szczególności:
    - Bieżąca administracja firewallem brzegowym - dopuszczanie ruchu sieciowego tylko w zakresie niezbędnym dla funkcjonowania rozwiązania, przekierowanie wszystkich niezbędnych dla funkcjonowania rozwiązania portów.
    - Bieżąca administracja serwerem OpenVPN, w tym zarządzanie kluczami szyfrującymi.

Czynności incydentalne

- Wykonywanie instalacji dodatkowego oprogramowania, jeżeli powstanie taka potrzeba.
- Aktualizacja certyfikatu niezbędnego do szyfrowania ruchu sieciowego katalogu on-line OPAC.
- Wykonywania aktualizacji systemów operacyjnych i innych składników systemu oraz aplikacji użytkowych, w szczególności aktualizowania wszelkich składników oprogramowania Patron: systemów bibliotecznych Patron, usług MolService, usług związanych z funkcjonowaniem katalogu on-line OPAC.
- Współpraca w prowadzeniu niezbędnych działań serwisowych dotyczących wszelkich składników rozwiązania, w szczególności:
    - zapewnianie, na żądanie, dostępu do kopii archiwizacyjnych baz danych systemu Patron,
    - zapewnianie, na żądanie, dostępów do logów generowanych przez system Patron oraz oprogramowania systemowe.
- Niezwłoczne reagowanie na wszelkie zauważone incydenty bezpieczeństwa; informowanie Zamawiającego o incydentach i podjętych w związku z tym działaniach.

Wszelkie czynności administracyjne utrudniające Bibliotece niezakłócone korzystanie z systemów muszą być wykonywane po godzinach pracy Biblioteki.

Procedura odtwarzania środowiska hostingowego

1. W ramach procedury przygotowawczej administrator wykona obrazy maszyn wirtualnych w postaci plików img, utworzonych za pomocą polecenia dd w systemie Linux. Przyjęto zasadę, że każda maszyna posiada jeden lub kilka własnych wolumenów logicznych. Obraz wolumenu jest zatem tożsamy z obrazem maszyny wirtualnej lub jej części. Pliki obrazów to odpowiednio:

Oznaczenie maszyny	Nazwa pliku obrazu	funkcja	Rozmiar
VM1	lin-rt-ldz_root.img	router	6 GB
VM2	sql-serw-ldz_hdd1.img	serwer baz danych systemu Patron	100 GB
	sql-serw-ldz_hdd2.img		100 GB
	sql-serw-ldz_ssd1.img		100 GB
VM3	trm-serw-ldz_hdd1.img	serwer terminali RDS, serwer aplikacji Patron	100 GB
VM4	lin-revp-mol_root.img	reverse proxy katalogu OPAC	6 GB

2. Obrazy zostaną skopiowane na dysk przenośny i zaszyfrowane na czas transportu. Dysk i klucz szyfrowania, zawarty w zapieczętowanej kopercie, zostaną przekazane protokolarnie Bibliotece Miejskiej w Łodzi - administratorowi danych osobowych zawartych na tym nośniku. Użyte zostanie szyfrowanie zdefiniowane przez RFC4880. Do deszyfracji można użyć różnych narzędzi np. Gpg4win, dostępnych na licencji GNU GPL.

3. Pierwszym krokiem służącym odtworzeniu infrastruktury jest zainstalowanie na maszynie fizycznej podstawowego systemu operacyjnego Linux z dowolnej dystrybucji serwerowej. Zalecana jest jedna z poniższych dystrybucji:
    a. Gentoo
    b. Debian
    c. Ubuntu Server LTS
    d. CentOS

   Dopuszczalne są też niewymienione dystrybucje, jeśli posiadają stabilną i aktualną wersję serwerową.
4. Następnie należy utworzyć odpowiednie woluminy logiczne, narzędziem LVM lub kompatybilnym. Wielkości woluminów muszą odpowiadać obrazom maszyn wirtualnych: 2 x 6 GB oraz 4 x 100 GB.

5. Instalacja Hypervisora Xen, zależnie od dystrybucji systemu linux może być uruchomiona jednym z przykładowych poleceń:
    a. emerge xen xen-tools (w dystrybucji Gentoo)
    b. apt-get install xen-system-amd64 (w dystrybucji Debian)
    c. apt-get install xen-hypervisor-amd64 (w dystrybucji Ubuntu)
    d. yum install xen (w dystrybucji CentOS)

6. Po zainstalowaniu Hypervisora Xen należy utworzyć własne definicje maszyn wirtualnych, zależnie od bieżącego środowiska systemowego, opierając się na poniższych definicjach.

VM1 - maszyna wirtualna - router.
Plik konfiguracyjny Xen - lin-rt-ldz

```
kernel = "/var/xen/kernels/vmlinuz-4.9.16-gentoo"
vcpus = 2
cpus = "4-23"
memory = 512
name = "lin-rt-ldz"
disk = ['phy:/dev/vg1_lin-host-ldz/lin-rt-ldz_swap,xvda1,w', 'phy:/dev/vg1_lin-host-ldz/lin-rt-ldz_root,xvda2,w']
root = "/dev/xvda2 ro"
vif = ['mac=00:16:3e:44:ab:4f, bridge=xenbr1', 'mac=00:16:3e:44:5e:31, bridge=xenbr2']
```

VM2 - maszyna wirtualna - serwer baz danych.
Plik konfiguracyjny Xen - sql-serw-ldz

```
builder = "hvm"
vcpus = 6
cpus = "24-47"
memory = 32768
name = "sql-serw-ldz"
disk = ['phy:/dev/vg1_lin-host-ldz/sql-serw-ldz_hdd1,xvda,w', 'phy:/dev/vg1_lin-host-ldz/sql-serw-ldz_hdd2,xvdb,w',
'phy:/dev/vg_ssd_lin-host-ldz/sql-serw-ldz_ssd1,xvdc,w', ',xvdd:cdrom,r']
vif = ['mac=00:16:3e:44:d8:17, bridge=xenbr2']
boot = "cd"
acpi = 1
apic = 1
sdl = 0
vnc = 1
vnclisten = "0.0.0.0"
vncdisplay = 0
vncpasswd = "XXX"
usbdevice = "tablet"
on_poweroff = "destroy"
on_reboot = "restart"
on_crash = "restart"
```

VM3 - maszyna wirtualna - serwer terminali.
Plik konfiguracyjny Xen - trm-serw-ldz

```
builder = "hvm"
vcpus = 8
cpus = "4-23"
memory = 32768
name = "trm-serw-ldz"
disk = ['phy:/dev/vg1_lin-host-ldz/trm-serw-ldz_hdd1,xvda,w', ',xvdc:cdrom,r']
vif = ['mac=00:16:3e:44:35:6a, bridge=xenbr2']
boot = "cd"
acpi = 1
apic = 1
sdl = 0
vnc = 1
vnclisten = "0.0.0.0"
vncdisplay = 1
vncpasswd = "XXX"
usbdevice = "tablet"
on_poweroff = "destroy"
on_reboot = "restart"
on_crash = "restart"
```

VM4 - maszyna wirtualna - reverse proxy katalogu Opac.
Plik konfiguracyjny Xen - lin-revp-mol

```
kernel = "/var/xen/kernels/vmlinuz-4.9.16-gentoo"
vcpus = 2
cpus = "4-23"
memory = 512
name = "lin-revp-mol"
disk = ['phy:/dev/vg1_lin-host-ldz/lin-revp-mol_swap,xvda1,w', 'phy:/dev/vg1_lin-host-ldz/lin-revp-mol_root,xvda2,w']
root = "/dev/xvda2 ro"
vif = ['mac=00:16:3e:44:10:b2, bridge=xenbr2']
```

7. Po utworzeniu odpowiednich woluminów logicznych i definicji maszyn wirtualnych należy skopiować odpowiednie obrazy na woluminy poleceniem dd.

8. Po zakończeniu kopiowania można uruchomić maszyny wirtualne. Te elementy środowiska, które uległy zmianie (np. adresacja IP) muszą zostać zrekonfigurowane. Sam system i jego komponenty nie powinny wymagać rekonfiguracji. Najwygodniej jest zachować adresację sieci wewnętrznej (192.168.10.x). Wtedy jedynym interfejsem do przekonfigurowania będzie eth0 na lin-rt-ldz (VM1).

9. Po wykonaniu powyższych czynności, można przystąpić do sprawdzenia poprawności działania systemu:
    a. Sprawdzić czy uruchomienie systemu Patron przez RDP jest możliwe
    b. Sprawdzić czy zalogowanie w systemie przebiegło prawidłowo (ewentualne komunikaty o błędzie)
    c. Sprawdzić czy widoczne są konta czytelników, zawartość wybranego konta, wyszukiwanie opisu i prezentacja zasobów
    d. Sprawdzić czy jest łączność z katalogiem OPAC
    e. Wykonać przykładowe wyszukiwanie w katalogu OPAC
    f. Wyświetlić pełny opis oraz informację o egzemplarzach

Jeśli podczas wykonywania operacji w podpunktach a do f nie pojawiły się komunikaty o błędach – środowisko hostingowe zostało poprawnie odtworzone.

Schemat systemu – wariant z dwoma serwerami fizycznymi.

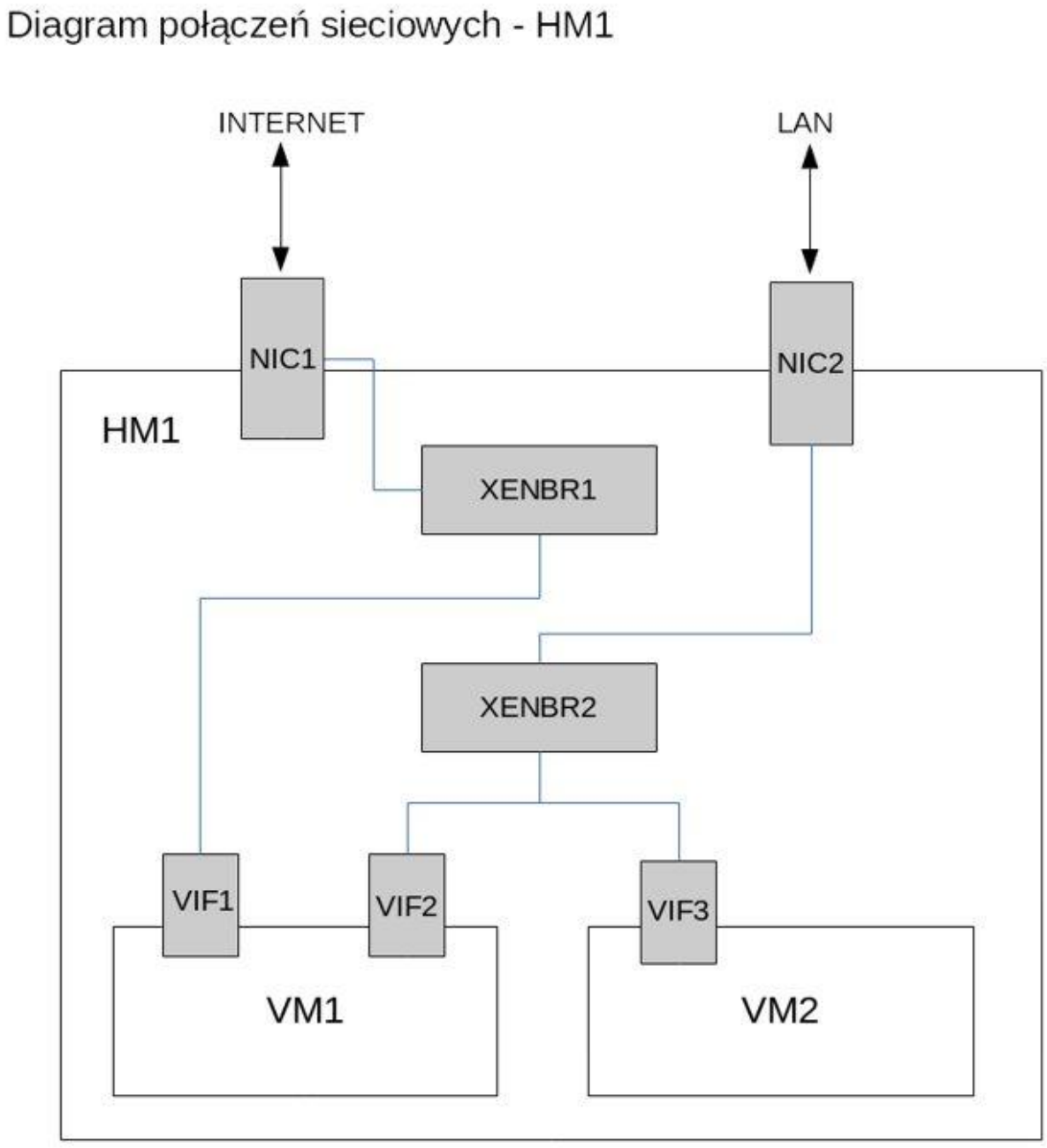
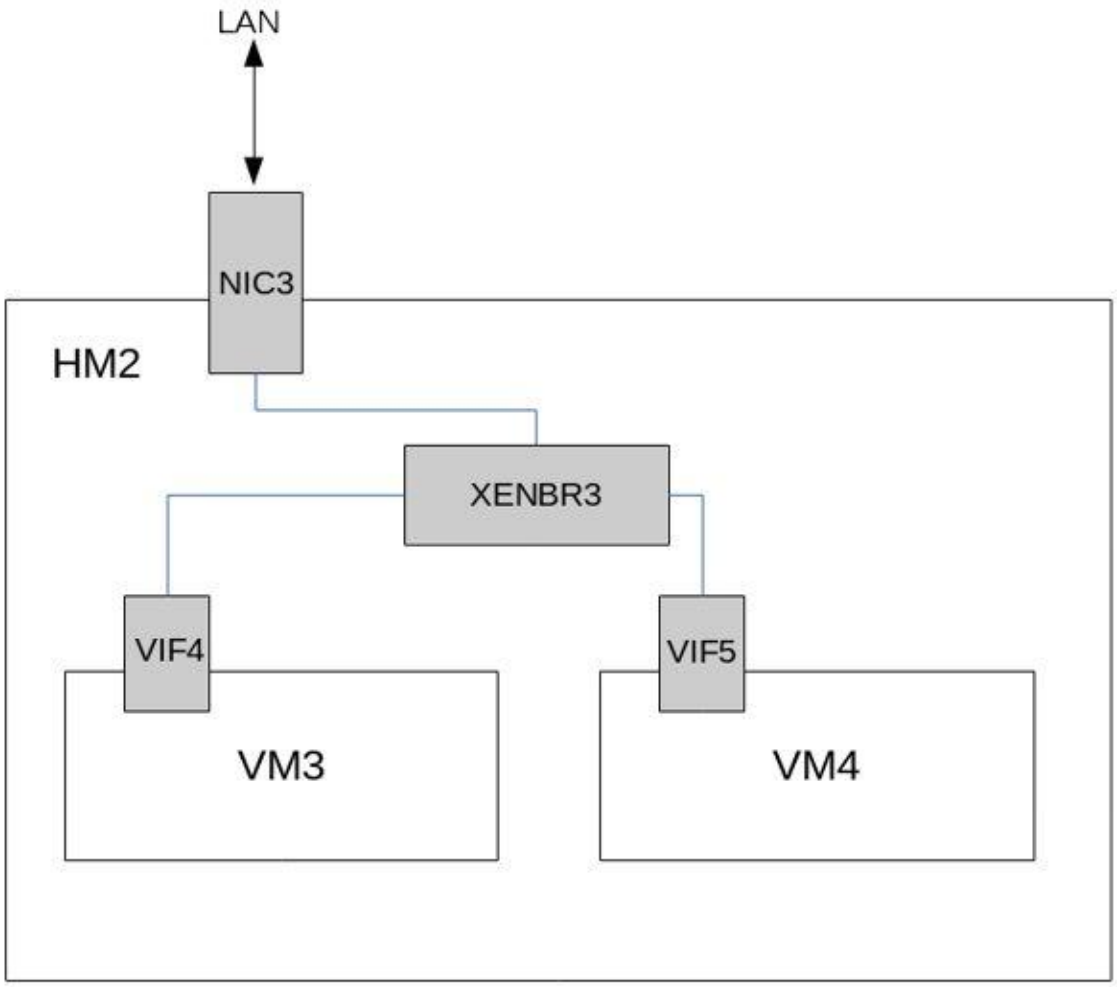


Diagram połączeń sieciowych - HM2



Serwer fizyczny - HM1.

Dell PowerEdge R430:

- 2 procesory Intel Xeon CPU E5-2650 v4 @ 2.20GHz, 12 fizycznych rdzeni każdy, hyperthreading - łącznie 48 wątków sprzętowych
- RAM: 128 GB
- 2 dyski SSD SATA3 tworzące macierz RAID-1 256GB
- 2 dyski HDD SAS tworzące macierz RAID-1 600GB
- kontroler dysków: Dell PERC H730 Mini
- zasilanie: 2 zasilacze 550W, redundancja zasilania
- system operacyjny: Linux
- role:
  - host wirtualizacji (hypervisor: Xen)
- interfejsy sieciowe:
  - NIC1 – dostęp do internetu
  - NIC2 – sieć wewnętrzna
- IDRAC 8 Enterprise

Serwer fizyczny - HM2.

Dell PowerEdge R430:

- 2 procesory Intel Xeon CPU E5-2650 v4 @ 2.20GHz, 12 fizycznych rdzeni każdy, hyperthreading - łącznie 48 wątków sprzętowych
- RAM: 128 GB
- 2 dyski SSD SATA3 tworzące macierz RAID-1 256GB
- 2 dyski HDD SAS tworzące macierz RAID-1 600GB
- kontroler dysków: Dell PERC H730 Mini
- zasilanie: 2 zasilacze 550W, redundancja zasilania
- system operacyjny: Linux
- role:
  - host wirtualizacji (hypervisor: Xen)
- interfejsy sieciowe:
  - NIC3 – sieć wewnętrzna
- IDRAC 8 Enterprise

Serwer wirtualny - VM1.

- host fizyczny: HM1
- 4 procesory wirtualne (mapowane na wątki sprzętowe hosta)
- RAM: 1GB
- 1 dysk 6GB, realizowany przez LV zlokalizowany na macierzy HDD
- system operacyjny: Linux
- role:
  - router
- interfejsy sieciowe:
  - VIF1 – XENBR1 (bridge programowy)
  - VIF2 – XENBR2 (bridge programowy)

Serwer wirtualny – VM2.

- host fizyczny: HM1
- 32 procesorów wirtualnych (mapowanych na wątki sprzętowe hosta)
- RAM: 64GB
- 1 dysk 100GB, realizowany przez LV zlokalizowany na macierzy HDD
- system operacyjny: Windows 2016 Server Standard x64
- role:
  - serwer terminali RDS
  - serwer aplikacji Patron
- interfejsy sieciowe
  - VIF3 – XENBR2 (bridge programowy)

Serwer wirtualny - VM3.

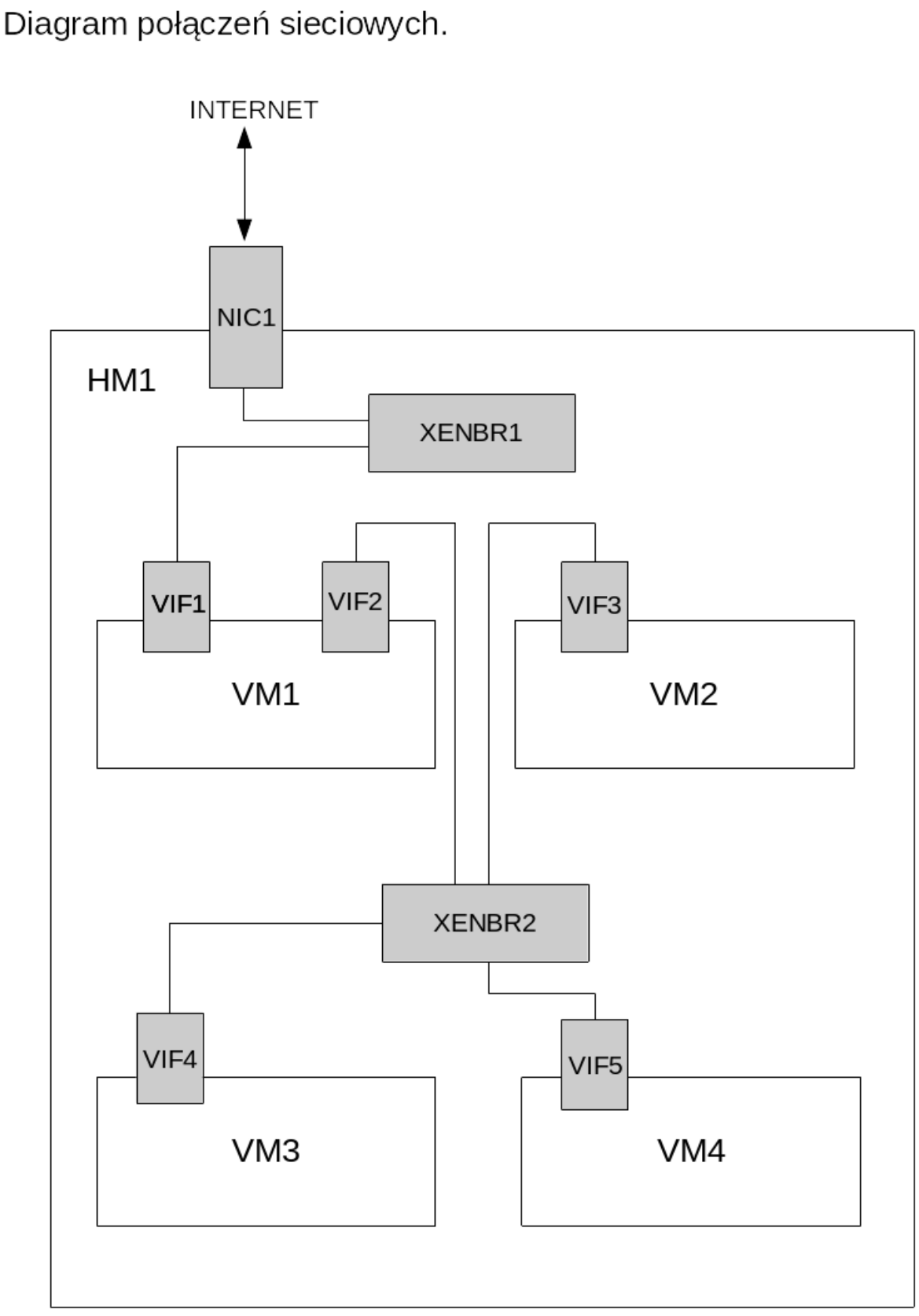
- host fizyczny: HM2
- 6 procesorów wirtualnych (mapowanych na wątki sprzętowe hosta)
- RAM: 64 GB
- dyski:
  - dysk 100GB, realizowany przez LV zlokalizowany na macierzy HDD
  - dysk 100GB, realizowany przez LV zlokalizowany na macierzy HDD
  - dysk 100GB, realizowany przez LV zlokalizowany na macierzy SSD

- system operacyjny: Windows 2016 Server Standard x64
- role:
  - serwer baz danych systemu Patron (MS SQL Server 2016 Standard x64)
  - katalog Opac
  - usługa MOLService
  - serwer SOLR
- interfejsy sieciowe
  - VIF4 – XENBR3 (bridge programowy)

Serwer wirtualny - VM4.

- host fizyczny: HM2
- 4 procesorów wirtualnych (mapowanych na wątki sprzętowe hosta)
- RAM: 1 GB
- 1 dysk 6GB, realizowany przez LV zlokalizowany na macierzy HDD
- system operacyjny: Linux
- role:
  - reverse proxy katalogu Opac (szyfrowanie połączeń)
- interfejsy sieciowe
  - VIF5 – XENBR3 (bridge programowy)

Schemat systemu – wariant z jednym serwerem fizycznym.



Serwer fizyczny - HM1.

Dell PowerEdge R430:

- 2 procesory Intel Xeon CPU E5-2650 v4 @ 2.20GHz, 12 fizycznych rdzeni każdy, hyperthreading - łącznie 48 wątków sprzętowych
- RAM: 128 GB
- 2 dyski SSD SATA3 tworzące macierz RAID-1 min 900GB
- 2 dyski HDD SAS tworzące macierz RAID-1 min 900GB
- kontroler dysków: Dell PERC H730 Mini
- zasilanie: 2 zasilacze 550W, redundancja zasilania
- system operacyjny: Linux
- role:
  - host wirtualizacji (hypervisor: Xen)
- interfejsy sieciowe:
  - NIC1 – dostęp do internetu
- IDRAC 8 Enterprise

Serwer wirtualny - VM1.

- host fizyczny: HM1
- 4 procesory wirtualne (mapowane na wątki sprzętowe hosta)
- RAM: 1GB
- 1 dysk 6GB, realizowany przez LV zlokalizowany na macierzy HDD
- system operacyjny: Linux
- role:
  - router
- interfejsy sieciowe:
  - VIF1 – XENBR1 (bridge programowy)
  - VIF2 – XENBR2 (bridge programowy)

Serwer wirtualny – VM2.

- host fizyczny: HM1
- 32 procesorów wirtualnych (mapowanych na wątki sprzętowe hosta)
- RAM: 48GB
- 1 dysk 100GB, realizowany przez LV zlokalizowany na macierzy HDD
- system operacyjny: Windows 2016 Server Standard x64
- role:
  - serwer terminali RDS
  - serwer aplikacji Patron
- interfejsy sieciowe
  - VIF3 – XENBR2 (bridge programowy)

Serwer wirtualny - VM3.

- host fizyczny: HM1
- 6 procesorów wirtualnych (mapowanych na wątki sprzętowe hosta)
- RAM: 64 GB
- dyski:
  - dysk 100GB, realizowany przez LV zlokalizowany na macierzy HDD
  - dysk 100GB, realizowany przez LV zlokalizowany na macierzy HDD
  - dysk 100GB, realizowany przez LV zlokalizowany na macierzy SSD

- system operacyjny: Windows 2016 Server Standard x64
- role:
  - serwer baz danych systemu Patron (MS SQL Server 2016 Standard x64)
  - katalog Opac
  - usługa MOLService
  - serwer SOLR
- interfejsy sieciowe
  - VIF4 – XENBR2 (bridge programowy)

Serwer wirtualny - VM4.

- host fizyczny: HM1
- 4 procesorów wirtualnych (mapowanych na wątki sprzętowe hosta)
- RAM: 1 GB
- 1 dysk 6GB, realizowany przez LV zlokalizowany na macierzy HDD
- system operacyjny: Linux
- role:
  - reverse proxy katalogu Opac (szyfrowanie połączeń)
- interfejsy sieciowe
  - VIF5 – XENBR2 (bridge programowy)