

ZAŁĄCZNIK NR 1 DO ZAPYTANIA OFERTOWEGO

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest:

- a. Przygotowanie i bieżące utrzymanie środowiska serwerowego niezbędnego do prawidłowego funkcjonowania systemu bibliotecznego Patron firmy MOL sp. z o.o. wraz z zapewnieniem łącza internetowego o przepustowości download/upload minimum 160Mb/s
- b. Przeniesienie całości oprogramowania z obecnej infrastruktury do przygotowanego w ramach Zamówienia środowiska serwerowego
- c. Utrzymanie ciągłego działania środowiska serwerowego oraz wszystkich elementów systemu bibliotecznego Patron firmy MOL sp. z o.o.

Umowa zostanie zawarta na okres do końca 2020 r.

A. Specyfikacja techniczna infrastruktury serwerowej i centrum danych.

Centrum danych utrzymujące serwery świadczące usługi bazodanowe/aplikacyjne powinno spełniać poniższe wymagania:

DC1:

- klasa wg Uptime Institute - Tier III
- gwarantowany poziom dostępności - co najmniej 99,98%
- biometryczny system kontroli dostępu
- system sygnalizacji alarmowej włamania i napadu
- monitoring CCTV
- ochrona fizyczna
- dwa niezależne systemy detekcji dymu i ognia
- automatyczny system gaszenia gazem
- zasilanie z dwóch stacji transformatorowych
- dwa w pełni chronione torry zasilania
- zasilanie 2 torowe w układzie 2N+1 (redundancja na poziomie torów zasilania jak i samych UPS)
- zasilanie z dwóch różnych rozdzielni głównych
- dwa niezależne agregaty prądotwórcze w układzie 2N
- system klimatyzacji precyzyjnej
- separacja zimnych i gorących korytarzy
- temperatura w zimnym korytarzu - 20-25 C
- łącze do sieci – co najmniej 40 Gbps, co najmniej dwa niezależne trakty światłowodowe
- pełna protekcja dostępu do wszystkich operatorów telekomunikacyjnych
- TP-IX i KIX – dostęp do największych ogólnopolskich punktów wymiany ruchu
- sieć wykonana w standardzie 10GB zgodnie z zasadą "No Single Point of Failure"
- wsparcie techniczne w lokalizacji - 24h/7/365
- certyfikaty - ISO 9001, PCI DSS, zgodność z ISO 27001

DC1 powinno zapewniać dwa fizyczne serwery o poniższej specyfikacji:

Platforma: DELL PowerEdge R430 (lub równoważna platforma serwerowa)

Procesory: 2 x Intel Xeon E5-2650 v4 lub inny o nie mniejszej wydajności

Pamięć: co najmniej 128 GB DDR4

Dyski: 2 x co najmniej 250 GB SSD + 2 x co najmniej 600 GB SAS

Raid: Hardware H730 (lub równoważny kontroler sprzętowy)
2 PSU, co najmniej 550W każdy
iDRAC 8 Enterprise (lub równoważny kontroler zdalnego zarządzania platformą serwerową)

Dodatkowo: co najmniej 1TB osobnej przestrzeni dyskowej na potrzeby kopii zapasowych danych

Centrum danych zapewniające dodatkową przestarzeń dyskową na potrzeby kopii zapasowych danych powinno spełniać poniższe wymagania:

DC2:

2. gwarantowany poziom dostępności - co najmniej 99,9%
3. ochrona fizyczna
4. monitoring CCTV
5. dwa w pełni chronione tory zasilania
6. zasilacze bezprzerwowe UPS
7. system klimatyzacji precyzyjnej
8. łącze do sieci – co najmniej 10 Gbps, dwa niezależne trakty światłowodowe

DC2 powinno zapewniać 300GB przestrzeni dyskowej na potrzeby kopii zapasowych danych, dostępnej z zewnątrz poprzez protokoły ftp/ftps/sftp.

DC1 powinno dzielić od DC2 co najmniej 100km w linii prostej.

B. 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 zabezpieczonej 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 błędach)
 - 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.

C. Czynności administracyjne związane z utrzymaniem infrastruktury serwerowej

1. Czynności okresowe

- 1.1 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.
- 1.2 Okresowa przebudowa indeksów w bazach MS SQL systemu Patron.
- 1.3 Zapewnienie prawidłowych mechanizmów rotacji logów generowanych przez oprogramowanie Patron.

2. Czynności bieżące

- 2.1. Bieżące monitorowanie dostępności infrastruktury: serwerów wirtualnych i podstawowych usług funkcjonujących na tych serwerach; monitoring musi być prowadzony z lokalizacji poza serwerownią.

- 2.2. 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.
- 2.3. Bieżąca administracja wszystkimi systemami wchodzącymi w 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.

3. Czynności incydentalne

- 3.1. Wykonywanie instalacji dodatkowego oprogramowania, jeżeli powstanie taka potrzeba.
- 3.2. Aktualizacja certyfikatu niezbędnego do szyfrowania ruchu sieciowego katalogu on-line OPAC.
- 3.3. Wykonywanie 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.
- 3.4. 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, dostępu do logów generowanych przez system Patron oraz oprogramowania systemowe.
- 3.5. 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.