**Katowice, 09.01.2022 r.**

Specyfikacja

Aktualizacja serwerów plikowych (Samba) i serwera backupu (Bacula) z jednoczesnym przeniesieniem funkcjonujących maszyn wirtualnych ze środowiska wirtualnego VMware 6.5 do ProxmoxVE 7.1

Spis treści

[Cel i zakres zadania 3](#_Toc94162700)

[Analiza infrastruktury informatycznej Zamawiającego 4](#_Toc94162701)

[Specyfikacja koniecznych do wykonania prac 5](#_Toc94162702)

[Przygotowanie środowiska ProxmoxVE 7.x 5](#_Toc94162703)

[Maszyna wirtualna BACULA 5](#_Toc94162704)

[Stan obecny 5](#_Toc94162705)

[Stan docelowy 5](#_Toc94162706)

[Maszyna wirtualna DEPOZYT 7](#_Toc94162707)

[Stan obecny: 7](#_Toc94162708)

[Stan docelowy 7](#_Toc94162709)

[Maszyna wirtualna DANE 11](#_Toc94162710)

[Stan obecny: 11](#_Toc94162711)

[Stan docelowy 11](#_Toc94162712)

[Maszyna wirtualna WMS 13](#_Toc94162713)

[Stan obecny: 13](#_Toc94162714)

[Stan docelowy 13](#_Toc94162715)

[Maszyna wirtualna FIREWALL 15](#_Toc94162716)

[Stan obecny 15](#_Toc94162717)

[Stan docelowy 15](#_Toc94162718)

[Szacunkowa zajętość danych przez VM przed i po aktualizacji 18](#_Toc94162719)

[Wsparcie techniczne na zaktualizowane maszyny 18](#_Toc94162720)

[Odbiór Zamówienia 18](#_Toc94162721)

[Termin płatności 18](#_Toc94162722)

# Cel i zakres zadania

Celem zadań jest aktualizacja systemów operacyjnych Debian GNU/Linux,Ubuntu i uruchomionych w ramach nich usług do najnowszych ich wersji, objętych wsparciem dostawcy.

Obecnie zdecydowana większość maszyn wirtualnych (VM) Zamawiającego funkcjonuje w ramach wycofywanego środowiska wirtualnego VMware 6.5, którego eksploatacja zostanie zakończona wraz z przeniesieniem wszystkich VM do nowego środowiska ProxmoxVE 7.1.

W niniejszym zadaniuaktualizacją zostaną objęte 4 VM - serwery plikowe Samba oraz VM z systemem backupu Bacula. Zaktualizowane maszyny wirtualne zostaną uruchomione w nowym, funkcjonującym u Zamawiającego środowisku wirtualnym ProxmoxVE. Będzie to możliwe dzięki odpowiedniej reorganizacji woluminów z danymi serwerów oraz reorganizacji (migracji) dysków w obrębie funkcjonujących Datastore w VMware 6.5.

# Analiza infrastruktury informatycznej Zamawiającego

Systemy informatyczne zamawiającego funkcjonują w ramach dwóch systemów wirtualizacji:

1. VMware 6.5 (2 hosty wirtualizacji)

2. Proxmox VE 7.1 (1 host wirtualizacji)

Miejscem dla składowania danych VM dla systemów wirtualizacji jest macierz dyskowa HP MSA2040A. Na macierzy skonfigurowane są 2 grupy RAID6 (po 11 dysków SAS 600GB). W ramach grup zostały wydzielone LUN na 3 datastore VMWARE 6.5 oraz niewielki datastore o pojemności 120GB na maszyny wirtualne funkcjonujące w ramach nowego środowiska ProxmoxVE (1 VM)

Bieżąca konfiguracja pozwala na zaalokowanie na potrzeby ProxmoxVE około 900GB przestrzeni na grupie RAID6 z wolumenem ProxmoxVE. W ramach drugiej grupy RAID6 dostępne jest 1162GB przestrzeni możliwej do zaalokowania. Wykonawca o ile to możliwe powinien alokować w pierwszej kolejności tylko jedną z grup, ponieważ druga grupa RAID docelowo będzie przeznaczona do likwidacji celem utworzenia grupy dedykowanej dla baz danych (RAID10) oraz innej grupy RAID6.

# Specyfikacja koniecznych do wykonania prac

## Przygotowanie środowiska ProxmoxVE 7.x

W ramach przygotowania do przeniesienia VM Wykonawca powiększy datastore widoczny dla VM w ProxmoxVE, tak by umożliwić tworzenie VM i przenoszenie danych z systemu wirtualizacji VMWare 6.5. Szczegółowe dane dot. bieżącej alokacji przestrzeni przez VM zostały opisane przy wytycznych dla każdej z aktualizowanych maszyn wirtualnych.

## Maszyna wirtualna BACULA

### Stan obecny

|  |  |
| --- | --- |
| **Nazwa domenowa** | bacula.ad.spkatowice.policja.gov.pl |
| **System operacyjny** | Debian GNU/Linux 7 (amd64) |
| **Uruchomione usługi** | bacula-fd 5.2.6  bacula-sd 5.2.6  bacula-dir 5.2.6  PostgreSQL 9.1  Webacula (interfejs WEB GUI bacula) |
| **Zajętość woluminów z danymi / wolna przestrzeń** | 300GB/30GB |
| **System wirtualizacji** | VMWARE 6.5 |

### Stan docelowy

Maszyna wirtualna z systemem backupu Bacula w celu zapewnienia poprawnej realizacji kopii zapasowych na docelowo zaktualizowanych serwerach plikowych Samba, musi zostać zaktualizowana w pierwszej kolejności. Dokumentacja Bacula mówi, że klient (agent) bacula-fd nie może być w nowszej wersji niż serwer bacula-dir i tylko taka konfiguracja jest jedyną supportowaną. Różnice w wersjach w dystrybucji Debian GNU/Linux 11, a Debian GNU/Linux 7 (9.6.7 vs 5.2.6)

1. Wykonawca zainstaluje najnowszą wersję Debian GNU/Linux 11 (bullseye) amd64:

- rozruch z partycji EFI

- grupa wolumenów dla systemu, rootfs umieszczony na LVM

- osobna grupa wolumenów dla danych serwera (PV to osobny dysk w systemie wirtualizacji) i utworzony w ramach niej LVM na potrzeby bazy danych postgreSQL. Rozmiar LVM adekwatny do obecnego zapotrzebowania.

- konfiguracja systemd-timed w oparciu o dostarczone przez Zamawiającego serwery NTP, konfiguracja strefy czasowej, konfiguracja locale pl\_PL.UTF8;

- konfiguracja stub resolver: systemd-resolved, forwarders ustawione w oparciu o dostarczone przez Zamawiającego serwery DNS

- użycie kernela dedykowanego dla maszyn wirtualnych (*linux-image-cloud-amd64)*

- konfiguracja sieci poprzez systemd-networkd. W sekcji Match użyć adres MAC interfejsu.

- wyłączenie niepotrzebnych usług systemowych, odinstalowanie niepotrzebnych i nieużywanych pakietów.

2. Wykonawca skompiluje najnowszą wersję oprogramowania wirtualnej zmieniarki taśm vchanger w najnowszej wersji 1.0.3, przygotuje paczkę dystrubucyjną (deb) i zainstaluje. Oprogramowanie dostępne tutaj: https://sourceforge.net/projects/vchanger/files/vchanger/. Konfiguracja zostanie dostosowana do obecnej wersji serwera Bacula i zmian w obrębie pliku konfiguracyjnego, które nastąpiły od obecnie zainstalowanej wersji.

3. Wykonawca zainstaluje konsolę WEB Bacullum w wersji 9.6.6.3

- komunikacja klientów z serwerem, oraz serwera z API zostanie zabezpieczona (SSL) (zainstalowane certyfikaty wygenerowane podpisane przez wewnętrzne CA Zamawiającego, redirect z HTTP na HTTPS w konfiguracji serwera).

- opis instalacji: https://www.bacula.org/9.6.x-manuals/en/console/Baculum\_API\_Web\_GUI\_Tools.html

4. Wykonawca przeniesie bazę danych PostgreSQL do obecnej wersji klastra bazodanowego PostgreSQL 13.5. Struktury bazy danych zostaną zupgradowane do najnowszej wersji zgodnie z dokumentacją bacula dostępną pod adresem: https://www.bacula.org/9.6.x-manuals/en.

5. Wykonawca zainstaluje pakiet qemu-guest-agent w celu pełnego wsparcia VM w środowisku ProxmoxVE.

6. Konfiguracja lokalnego firewalla UFW. Konfiguracja wymuszająca jawne odblokowanie portu na firewallu po instalacji dodatkowych usług na serwerze.

a) reguły ruchu przychodzącego:

- odblokowanie tylko niezbędnego ruchu przychodzącego z dowolnych adresów do portów usług;

- zablokowanie innego ruchu przychodzącego;

b) reguły ruchu wychodzącego:

- dozwolony dowolny ruch wychodzący

7. Po wykonanej aktualizacji zostaną przeprowadzone testy funkcjonalne. Zostanie sprawdzone poprawne działanie backupu oraz jego przywracanie.

8. Podsumowanie zmian:

|  |  |
| --- | --- |
| **Nazwa domenowa** | bacula.ad.spkatowice.policja.gov.pl |
| **System operacyjny** | Debian GNU/Linux 11 (amd64) |
| **Uruchomione usługi** | bacula-fd 9.6.7  bacula-sd 9.6.7  bacula-dir 9.6.7  PostgreSQL 13.5  baculum 9.6.6.3 (https://www.bacula.org/9.6.x-manuals/en/console/Baculum\_API\_Web\_GUI\_Tools.html)  vchanger 1.0.3 (https://sourceforge.net/projects/vchanger/files/vchanger/)  qemu-guest-agent  systemd-resolved  openssh-server |
| **Zajętość woluminów z danymi / wolna przestrzeń** | 20GB/6GB |
| **Zasoby zdalne** | Zasób NFS (Magazyn danych - pliki reprezentujące wirtualne taśmy vchanger) |
| **System wirtualizacji** | ProxmoxVE 7.x |

## Maszyna wirtualna DEPOZYT

### Stan obecny:

|  |  |
| --- | --- |
| **Nazwa domenowa** | depozyt.ad.spkatowice.policja.gov.pl |
| **Nazwa NetBIOS** | DEPOZYT |
| **System operacyjny** | Debian GNU/Linux 7 (i486-pc-linux-gnu) |
| **Uruchomione usługi** | samba 3.6.6  bacula-fd 5.2.6  openssh-server  webmin |
| **Zajętość woluminów z danymi / wolna przestrzeń** | 1024GB/ 500GB |
| **System wirtualizacji** | VMWARE 6.5 |

### Stan docelowy

1. Wykonawca zainstaluje najnowszą wersję Debian GNU/Linux 11 (bullseye) amd64:

- rozruch z partycji EFI;

- grupa wolumenów dla systemu, rootfs umieszczony na LVM;

- osobna grupa wolumenów dla danych serwerów SAMBA (PV to osobny dysk w systemie wirtualizacji) i tworzony w ramach niej LVM. Rozmiar LVM adekwatny do obecnego zapotrzebowania

- konfiguracja systemd-timed w oparciu o dostarczone przez Zamawiającego serwery NTP, strefy czasowej

- konfiguracja stub resolver: systemd-resolved, forwarders ustawione w oparciu o dostarczone przez Zamawiającego serwery DNS

- użycie kernela dedykowanego dla maszyn wirtualnych (metapakiet linux-image-cloud-amd64)

- konfiguracja sieci poprzez systemd-networkd;

- wyłączenie niepotrzebnych usług;

2. Przeniesiona zostanie konfiguracja klienta serwera backupu bacula-fd.

3. W zakresie usługi Samba zostaną wykonane następujące prace:

- importu bazy haseł samba oraz wszystkich użytkowników systemowych z obecnej wersji Samba 3.3.6.

- rezygnacja z dyrektyw niewspieranych lub deprecated (np. force group, force user itd.)

- uprawnienia do zasobów wynikają bezpośrednio z uprawnień do systemu plików

- wymuszenie min. protokołu SMB210 (level Windows7) oraz uwierzytelnienia min. NTLMv2 (konfiguracja default od Samba >4.12)

- użycie extended ACL oraz wykorzystanie mechanizmów dziedziczenia

- delegowanie uprawnień do zasobów w oparciu o model RBAC. Do zasobów dopisywane są jedynie grupy ACL (rule group)

- nadanie uprawnień zgodnie z wytycznymi Zamawiającego w oparciu o stan bieżący za pośrednictwem tylko i wyłącznie nowo stworzonych grup ACL.

- włączenie audytu operacji wykonywanych na zasobach. Audyt obejmować powinien min. operację połaczenia, rozłączenia, tworzenia pliku/katalogu, usunięcia pliku, zmiany nazwy pliku. Log audytu będzie przechowywany w oddzielnym pliku. Ustawienie rotacji logów wg. retencji żądanej przez Zamawiającego.

- włączenia audytu zdarzeń autentykacji na serwerze. Zdarzenia te zapisywane będą do oddzielnego logo audytu. Ustawienie rotacji logów wg. retencji żądanej przez Zamawiającego.

- przeniesienie danych serwera Samba (katalogów i plików w ramach udostępnionych zasobów) - ~520GB danych

4. Uruchomienie samba-legacy z włączonym wsparciem dla protokołu SMBv1.

Zamawiający posiada w swojej infrastrukturze klientów wspierających jedynie protokół SMBv1 (Windows XP). Dotyczy to 3 udostępnionych zasobów i wąskiej grupy klientów. Dla tych klientów w ramach tej samej maszyny wirtualnej zostanie uruchomiona usługa Samba z włączonym wycofanym już protokołem SMBv1.

5. Instalacja i konfiguracja pakietu Webmin do zdalnego zarządzania serwerem poprzez interfejs webowy. Paczka Debian/Ubuntu dostępna jest pod adresem: *https://prdownloads.sourceforge.net/webadmin/webmin\_1.984\_all.deb*

Konfiguracja obejmuje utworzenie wskazanych przez Zamawiającego użytkowników Administracyjnych. Stworzony użytkownik posiada pełne prawa administracyjne do modułów w Webmin.

6. Konfiguracja lokalnego firewalla UFW:

a) reguły ruchu przychodzącego:

- odblokowanie ruchu z adresów IP stacji Administratorów (Zamawiający dostarczy listę stacji) do portu na którym działa WEBMIN

- odblokowanie ruchu przychodzącego na port 22 z dowolnego hosta (OpenSSH)

- odblokowanie ruchu przychodzącego do portu tcp/445 na którym działa usługa Samba (DEPOZYT)

- odblokowanie ruchu przychodzącego tylko i wyłączenie z adresów IP stacji roboczych, które nie obsługują protokołu SMBv1 i łączą się z usługą Samba (DEPOZYT-LEGACY) na porcie tcp/445

- zablokowanie innego ruchu przychodzącego

b) reguły ruchu wychodzącego:

- dowolny ruch wychodzący dopuszczony

**Podsumowanie konfiguracji:**

|  |  |
| --- | --- |
| **Nazwa DNS** | depozyt.ad.spkatowice.policja.gov.pl / depozyt-legacy.ad.spkatowice.policja.gov.pl |
| **Nazwa Netbios** | DEPOZYT (dla klientów SMBv2), DEPOZYT-LEGACY (dla klientów SMBv1) |
| **System operacyjny** | Debian GNU/Linux 11 (x64) |
| **Uruchomione usługi** | samba (DEPOZYT)  samba (DEPOZYT-LEGACY)  bacula-fd  qemu-guest-agent  systemd-resolved  openssh-server  webmin |
| **Zajętość woluminów z danymi/ wolna przestrzeń** | 534 GB / 10GB |
| **System wirtualizacji** | ProxmoxVE 7.x |

## 

## Maszyna wirtualna DANE

### Stan obecny:

|  |  |
| --- | --- |
| **Nazwa domenowa** | dane.ad.spkatowice.policja.gov.pl |
| **Nazwa NetBIOS** | DANE |
| **System operacyjny** | Debian GNU/Linux 8 (amd64) |
| **Uruchomione usługi** | samba 4.1.17  bacula-fd 5.2.6 |
| **Zajętość woluminów z danymi / wolna przestrzeń** | 465GB/290GB |
| **System wirtualizacji** | VMWARE 6.5 |

### Stan docelowy

1. Wykonawca zainstaluje najnowszą wersję Debian GNU/Linux 11 (bullseye) amd64:

- rozruch z partycji EFI

- grupa wolumenów dla systemu, rootfs umieszczony na LVM

- osobna grupa wolumenów dla danych serwerów SAMBA (PV to osobny dysk w systemie wirtualizacji) i utworzony w ramach niej LVM. Rozmiar LVM adekwatny do obecnego zapotrzebowania (maksimum. 10GB wolnej przestrzeni dyskowej)

- konfiguracja systemd-timed w oparciu o dostarczone przez Zamawiającego serwery NTP, strefy czasowej.

- konfiguracja stub resolver: systemd-resolved, forwarders ustawione w oparciu o dostarczone przez Zamawiającego serwery DNS

- użycie kernela dedykowanego dla maszyn wirtualnych (linux-image-cloud-amd64)

- konfiguracja sieci poprzez systemd-networkd

- wyłączenie niepotrzebnych usług

2. Przeniesiona zostanie konfiguracja klienta serwera backupu bacula-fd.

3. W zakresie usługi Samba zostaną wykonane następujące prace:

- importu bazy haseł samba oraz wszystkich użytkowników systemowych z obecnej wersji Samba 4.1.17

- rezygnacja z dyrektyw niewspieranych lub deprecated (np. force group, force user itd.), uprawnienia do zasobów wynikają bezpośrednio z uprawnień do systemu plików.

- wymuszenie min. protokołu SMB2.1 (level Windows7) oraz uwierzytelnienia min. NTLMv2 (konfiguracja default od Samba >4.12)

- użycie extended ACL oraz wykorzystanie mechanizmów dziedziczenia

- delegowanie uprawnień do zasobów w oparciu o model RBAC. Do zasobów dopisywane są jedynie grupy ACL (rule group)

- nadanie uprawnień zgodnie z wytycznymi Zamawiającego w oparciu o stan bieżący za pośrednictwem tylko i wyłącznie nowo stworzonych grup ACL.

- włączenie audytu operacji wykonywanych na zasobach. Audyt obejmować powinien min. operację połaczenia, rozłączenia, tworzenia pliku/katalogu, usunięcia pliku, zmiany nazwy pliku. Log audytu będzie przechowywany w oddzielnym pliku. Ustawienie rotacji logów wg. retencji żądanej przez Zamawiającego.

- włączenia audytu zdarzeń autentykacji na serwerze. Zdarzenia te zapisywane będą do oddzielnego logo audytu. Ustawienie rotacji logów wg. retencji żądanej przez Zamawiającego.

- przeniesienie danych serwera Samba (katalogów i plików w ramach udostępnionych zasobów) - ~165GB danych

4. Konfiguracja lokalnego firewalla UFW

Konfiguracja wymuszająca jawne odblokowanie portu na firewall po instalacji dodatkowych usług na serwerze.

a) reguły ruchu przychodzącego:

- odblokowanie tylko niezbędnego ruchu przychodzącego z dowolnych adresów do portów usług;

- zablokowanie innego ruchu przychodzącego;

b) reguły ruchu wychodzącego:

- dozwolony dowolny ruch wychodzący

*5. Podsumowanie konfiguracji:*

|  |  |
| --- | --- |
| **Nazwa DNS** | dane.ad.spkatowice.policja.gov.pl |
| **Nazwa Netbios** | DANE |
| **System operacyjny** | Debian GNU/Linux 11 (x64) |
| **Uruchomione usługi** | samba 4.13.13  bacula-fd 9.6.7  qemu-guest-agent  systemd-resolved |
| **Zajętość woluminów z danymi/ wolna przestrzeń** | 185GB / 10GB |
| **System wirtualizacji** | ProxmoxVE 7.x |

## 

## Maszyna wirtualna WMS

### Stan obecny:

|  |  |
| --- | --- |
| **Nazwa domenowa** | wms.ad.spkatowice.policja.gov.pl |
| **Nazwa NetBIOS** | WMS |
| **System operacyjny** | Debian GNU/Linux 8 (amd64) |
| **Uruchomione usługi** | samba 4.1.17  bacula-fd 5.2.6  openssh-server |
| **Zajętość woluminów z danymi / wolna przestrzeń** | 926GB/ 330GB |
| **System wirtualizacji** | VMWARE 6.5 |

### Stan docelowy

1. Wykonawca zainstaluje najnowszą wersję Debian GNU/Linux 11 (bullseye) amd64:

- rozruch z partycji EFI

- grupa wolumenów dla systemu, rootfs umieszczony na LVM

- osobna grupa wolumenów dla danych serwerów SAMBA (PV to osobny dysk w systemie wirtualizacji) i utworzony w ramach niej LVM. Rozmiar LVM adekwatny do obecnego zapotrzebowania (maksimum. 10GB wolnej przestrzeni dyskowej)

- konfiguracja systemd-timed w oparciu o dostarczone przez Zamawiającego serwery NTP, strefy czasowej.

- konfiguracja stub resolver: systemd-resolved, forwarders ustawione w oparciu o dostarczone przez Zamawiającego serwery DNS

- użycie kernela dedykowanego dla maszyn wirtualnych (linux-image-cloud-amd64)

- konfiguracja sieci poprzez systemd-networkd

- wyłączenie niepotrzebnych usług

2. Przeniesiona zostanie konfiguracja klienta serwera backupu bacula-fd.

3. W zakresie usługi Samba zostaną wykonane następujące prace:

- importu bazy haseł samba oraz wszystkich użytkowników systemowych z obecnej wersji Samba 4.1.17

- rezygnacja z dyrektyw niewspieranych lub deprecated (np. force group, force user itd.), uprawnienia do zasobów wynikają bezpośrednio z uprawnień do systemu plików.

- wymuszenie min. protokołu SMB210 (level Windows7) oraz uwierzytelnienia min. NTLMv2 (konfiguracja default od Samba >4.12)

- użycie extended ACL oraz wykorzystanie mechanizmów dziedziczenia

- delegowanie uprawnień do zasobów w oparciu o model RBAC. Do zasobów dopisywane są jedynie grupy ACL (rule group)

- nadanie uprawnień zgodnie z wytycznymi Zamawiającego w oparciu o stan bieżący za pośrednictwem tylko i wyłącznie nowo stworzonych grup ACL.

- włączenie audytu operacji wykonywanych na zasobach. Audyt obejmować powinien min. operację połaczenia, rozłączenia, tworzenia pliku/katalogu, usunięcia pliku, zmiany nazwy pliku. Log audytu będzie przechowywany w oddzielnym pliku. Ustawienie rotacji logów wg. retencji żądanej przez Zamawiającego.

- włączenia audytu zdarzeń autentykacji na serwerze. Zdarzenia te zapisywane będą do oddzielnego logo audytu. Ustawienie rotacji logów wg. retencji żądanej przez Zamawiającego.

- przeniesienie danych serwera Samba (katalogów i plików w ramach udostępnionych zasobów) - ~600GB danych

4. Konfiguracja lokalnego firewalla UFW

Konfiguracja wymuszająca jawne odblokowanie portu na firewall po instalacji dodatkowych usług na serwerze.

a) reguły ruchu przychodzącego:

- odblokowanie tylko niezbędnego ruchu przychodzącego z dowolnych adresów do portów usług;

- zablokowanie innego ruchu przychodzącego;

b) reguły ruchu wychodzącego:

- dozwolony dowolny ruch wychodzący

**Podsumowanie konfiguracji:**

|  |  |
| --- | --- |
| **Nazwa DNS** | wms.ad.spkatowice.policja.gov.pl |
| **Nazwa Netbios** | WMS |
| **System operacyjny** | Debian GNU/Linux 11 (x64) |
| **Uruchomione usługi** | samba 4.13.13  bacula-fd 9.6.7  qemu-guest-agent  systemd-resolved  openssh-server |
| **Zajętość woluminów z danymi/ wolna przestrzeń** | 650GB / 50GB |
| **System wirtualizacji** | ProxmoxVE 7.x |

## Maszyna wirtualna FIREWALL

### Stan obecny

|  |  |
| --- | --- |
| **Nazwa domenowa** | firewall.ad.spkatowice.policja.gov.pl |
| **Nazwa NetBIOS** | FIREWALL |
| **System operacyjny** | Debian GNU/Linux 8 (amd64) |
| **Uruchomione usługi** | samba 4.1.17  bacula-fd 5.2.6  openssh-server |
| **Zajętość woluminów z danymi / wolna przestrzeń** | 400GB / 180GB |
| **System wirtualizacji** | VMWARE 6.5 |

### Stan docelowy

1. Wykonawca zainstaluje najnowszą wersję Debian GNU/Linux 11 (bullseye) amd64:

- rozruch z partycji EFI

- grupa wolumenów dla systemu, rootfs umieszczony na LVM

- osobna grupa wolumenów dla danych serwerów SAMBA (PV to osobny dysk w systemie wirtualizacji) i utworzony w ramach niej LVM. Rozmiar LVM adekwatny do obecnego zapotrzebowania (maksimum. 10GB wolnej przestrzeni dyskowej)

- konfiguracja systemd-timed w oparciu o dostarczone przez Zamawiającego serwery NTP, strefy czasowej.

- konfiguracja stub resolver: systemd-resolved, forwarders ustawione w oparciu o dostarczone przez Zamawiającego serwery DNS

- użycie kernela dedykowanego dla maszyn wirtualnych (linux-image-cloud-amd64)

- konfiguracja sieci poprzez systemd-networkd

- wyłączenie niepotrzebnych usług

2. Przeniesiona zostanie konfiguracja klienta serwera backupu bacula-fd.

3. W zakresie usługi Samba zostaną wykonane następujące prace:

- importu bazy haseł samba oraz wszystkich użytkowników systemowych z obecnej wersji Samba 4.1.17

- rezygnacja z dyrektyw niewspieranych lub deprecated (np. force group, force user itd.), uprawnienia do zasobów wynikają bezpośrednio z uprawnień do systemu plików.

- wymuszenie min. protokołu SMB210 (level Windows7) oraz uwierzytelnienia min. NTLMv2 (konfiguracja default od Samba >4.12)

- użycie extended ACL oraz wykorzystanie mechanizmów dziedziczenia

- delegowanie uprawnień do zasobów w oparciu o model RBAC. Do zasobów dopisywane są jedynie grupy ACL (rule group)

- nadanie uprawnień zgodnie z wytycznymi Zamawiającego w oparciu o stan bieżący za pośrednictwem tylko i wyłącznie nowo stworzonych grup ACL.

- włączenie audytu operacji wykonywanych na zasobach. Audyt obejmować powinien min. operację połaczenia, rozłączenia, tworzenia pliku/katalogu, usunięcia pliku, zmiany nazwy pliku. Log audytu będzie przechowywany w oddzielnym pliku. Ustawienie rotacji logów wg. retencji żądanej przez Zamawiającego.

- włączenia audytu zdarzeń autentykacji na serwerze. Zdarzenia te zapisywane będą do oddzielnego logo audytu. Ustawienie rotacji logów wg. retencji żądanej przez Zamawiającego.

- przeniesienie danych serwera Samba (katalogów i plików w ramach udostępnionych zasobów) - ~220GB danych

4. Konfiguracja lokalnego firewalla UFW

Konfiguracja wymuszająca jawne odblokowanie portu na firewall po instalacji dodatkowych usług na serwerze.

a) reguły ruchu przychodzącego:

- odblokowanie tylko niezbędnego ruchu przychodzącego z dowolnych adresów do portów usług;

- zablokowanie innego ruchu przychodzącego;

b) reguły ruchu wychodzącego:

- dozwolony dowolny ruch wychodzący

Podsumowanie konfiguracji:

|  |  |
| --- | --- |
| **Nazwa DNS** | firewall.ad.spkatowice.policja.gov.pl |
| **Nazwa Netbios** | FIREWALL |
| **System operacyjny** | Debian GNU/Linux 11 (x64) |
| **Uruchomione usługi** | samba 4.13.13  bacula-fd 9.6.7  qemu-guest-agent  systemd-resolved  openssh-server |
| **Zajętość woluminów z danymi/ wolna przestrzeń** | 230GB / 10GB |
| **System wirtualizacji** | ProxmoxVE 7.x |

## Szacunkowa zajętość danych przez VM przed i po aktualizacji

|  |  |  |  |
| --- | --- | --- | --- |
| **Nazwa** | **A - przed aktualizacją [GB]** | **B - po aktualizacji [GB]** | **C = A -B [GB]** |
| bacula | 20 | 20 | 0 |
| depozyt | 1024 | 544 | 480 |
| dane | 465 | 195 | 270 |
| wms | 926 | 660 | 266 |
| firewall | 400 | 240 | 160 |
| **RAZEM** | **2835** | **1659** | **1176** |

## Wsparcie techniczne na zaktualizowane maszyny

Wykonawca zapewni **6-miesięczną** **opiekę techniczną** na zaktualizowane maszyny wirtualne. W ramach opieki technicznej będzie przeprowadzany przegląd serwerów pod kątem dostępnych aktualizacji systemów, weryfikacja zajętości przestrzeni dyskowej, monitoring logów systemowych oraz reakcja na zgłoszone przez Zamawiającego problemy z funkcjonowaniem zaktualizowanych usług. Wykonawca będzie również świadczyć wsparcie merytoryczne dla administratorów systemów. Przegląd i aktualizacja systemów będzie wykonywana nie rzadziej niż 1 raz w miesiącu.

## Odbiór Zamówienia

Podstawą odbioru zamówienia i wystawienia faktury, będzie pozytywnie podpisany protokół odbiorczy. W ramach odbioru zostaną przeprowadzone testy funkcjonalne maszyn po ich aktualizacji, a w szczególności:

- poprawność wykonania backupu i jego odtworzenia przez serwer Bacula, zweryfikowana zarówno dla nowych klientów bacula-fd 9.6.7 oraz bacula-fd 5.2.6;

- weryfikacja poprawności nadanych uprawnień do zasobów SAMBA (możliwość zapisu) dla wybranych zasobów i użytkowników;

- poprawność funkcjonowania serwera DEPOZYT-LEGACY dla klientów SMBv1. Weryfikacja poprawnego wykonania kopii zapasowej systemu magazynowego stołówki, poprawność działania udostępnionej bazy danych Access;

- sprawdzenie funkcjonowania pakietu WEBMIN zainstalowanego na serwerze depozyt i weryfikacja lokalnej polityki firewall;

## Termin płatności

Wykonawca akceptuje **30-dniowy** termin płatności za realizację zlecenia liczony od daty pozytywnie podpisanego protokołu odbioru.