**ARCHITEKTURA REFERENCYJNA**

**ŚRODOWISKA IT CPD MF**

**Załącznik B – Standardy parametrów oprogramowania infrastrukturalnego**

# Standardy parametrów oprogramowania infrastrukturalnego

# Wartości progowe parametrów technicznych, funkcjonalnych i niefunkcjonalnych komponentów

Dokument zawiera zestawienie parametrów technicznych funkcjonalnych i niefunkcjonalnych dla poszczególnych komponentów.

Każdy komponent opatrzono nagłówkiem zawierającym informacje o klasach systemów informatycznych oraz klasach bezpieczeństwa, w których ten komponent może być wykorzystany. Przypisanie komponentu do odpowiedniej klasy bezpieczeństwa nie oznacza w tym przypadku, iż komponent dostarcza mechanizmy właściwe dla tej klasy – oznacza jedynie, że może on być użyty w systemach tej klasy.

Poniższa tabela zawiera indeks wszystkich komponentów, wraz z ich identyfikatorami. Identyfikatory są równoznaczne z pojęciem „kod komponentu”, stosowanym zamiennie.

| Identyfikator | Komponent |
| --- | --- |
| C.CL.HA | Oprogramowanie klastrowe HA |
| [C.CL.HA.1](#C_CL_HA_1) | [Oprogramowanie klastrowe – typ 1](#C_CL_HA_1) |
| [C.CL.HA.5](#C_CL_HA_5) | [Oprogramowanie klastrowe – typ 2](#C_CL_HA_5) |
| [C.CL.HA.7](#C_CL_HA_7) | [Oprogramowanie klastrowe – typ 3](#C_CL_HA_7) |
| [C.CL.HA.8](#C_CL_HA_8) | [Oprogramowanie klastrowe – typ 4](#C_CL_HA_8) |
| [C.CL.HA.9](#C_CL_HA_9) | [Oprogramowanie klastrowe – typ 5](#C_CL_HA_9) |
| [C.CL.HA.11](#C_CL_HA_11) | [Oprogramowanie klastrowe – typ 6](#C_CL_HA_11) |
| [C.CL.HEF.RAC](#C_CL_HEF_RAC) | [Oprogramowanie klastrowe wydajnościowe – typ 1](#C_CL_HEF_RAC) |
| [C.CL.HEF.SYB](#C_CL_HEF_SYB) | [Oprogramowanie klastrowe wydajnościowe – typ 2](#C_CL_HEF_SYB) |
| [C.CL.HEF.DBX](#C_CL_HEF_DBX) | [Oprogramowanie klastrowe wydajnościowe – typ 3](#C_CL_HEF_DBX) |

## Oprogramowanie bazodanowe

|  |  |
| --- | --- |
| [**Identyfikator**](file:///Q%3A/ZUI/Robocze/Architektura%20referencyjna%20HARF/PROJEKT%20NOWEGO%20UK%C5%81ADU%20ARCHITEKTURY%20IT/ARIT-A-Bloki-Architektoniczne-Srodowiska-Teleinformatycznego-1.6.docx#Identyfikator) | S.SW.DB |
| **Nazwa** | Standard oprogramowania dla serwerów baz danych. |
| **Obszar** | Oprogramowania |
| **Strefa** | Serwerów |
| **Warstwa** | Baz danych |
| **Rodzaj** | Oprogramowania |
| **Klasy systemów** | IIIIIIIV |
| **Klasy bezpieczeństwa** | B3B2B1BX |
| **Streszczenie** | Niniejszy dokument opisuje standard oprogramowania baz danych. |
| **Opis** | **Funkcjonalność i technologie**Klasa I:* Rozwiązanie musi być zbudowane w oparciu o specjalizowane oprogramowanie, działające w systemie operacyjnym zdefiniowanym dla platformy x86-64
	+ na maszynie fizycznej, zgodnej z opisem w
		- *Standardzie serwerów kasetowych*;
		- *Standardzie serwerów stelażowych*.
	+ na maszynie wirtualnej, zgodnej z platformą wirtualizującą, zdefiniowaną w:
		- *Standardzie oprogramowania do wirtualizacji platformy x86/64* – dla rozwiązania działającego pod kontrolą systemów operacyjnych typ 1, typ 2 i typ 3;
* musi posiadać cechy skalowalności poziomej, pozwalające na rozbudowywanie środowiska o nowe komponenty oraz powiększanie jego mocy obliczeniowej poprzez dodawanie kolejnych bloków funkcjonalnych.
* Rozwiązanie musi umożliwiać zarządzanie danymi w bazie z użyciem języka SQL.
* Rozwiązanie musi posiadać możliwość partycjonowania danych.

Klasa II:* Rozwiązanie musi być zbudowane w oparciu o specjalizowane oprogramowanie, działające w systemie operacyjnym zdefiniowanym dla platformy x86-64:
	+ na maszynie fizycznej, zgodnej z opisem w
		- *Standardzie serwerów kasetowych*;
		- *Standardzie serwerów stelażowych*.
	+ na maszynie wirtualnej, zgodnej z platformą wirtualizującą, zdefiniowaną w:
		- *Standardzie oprogramowania do wirtualizacji platformy x86/64* – dla rozwiązania działającego pod kontrolą systemów operacyjnych typ 1, typ 2 i typ 3;
* Rozwiązanie musi posiadać cechy skalowalności poziomej, pozwalające na rozbudowywanie środowiska o nowe komponenty oraz powiększanie jego mocy obliczeniowej poprzez dodawanie kolejnych bloków funkcjonalnych.
* Rozwiązanie musi umożliwiać zarządzanie danymi w bazie z użyciem języka SQL.
* Rozwiązanie musi posiadać możliwość partycjonowania danych.

Klasa III:* Rozwiązanie musi być zbudowane w oparciu o specjalizowane oprogramowanie, działające w systemie operacyjnym zdefiniowanym dla platformy x86-64 lub RISC, na maszynie wirtualnej, zgodnej z platformą wirtualizującą, zdefiniowaną w *Standardzie oprogramowania do wirtualizacji platformy x86/64*.
* Rozwiązanie musi posiadać cechy skalowalności poziomej, pozwalające na rozbudowywanie środowiska o nowe komponenty oraz powiększanie jego mocy obliczeniowej poprzez dodawanie kolejnych bloków funkcjonalnych.
* Rozwiązanie musi umożliwiać zarządzanie danymi w bazie z użyciem języka SQL.

Klasa IV:* Rozwiązanie musi być zbudowane w oparciu o specjalizowane oprogramowanie, działające w systemie operacyjnym zdefiniowanym dla platformy x86-64 na maszynie wirtualnej, zgodnej z platformą wirtualizującą, zdefiniowaną w *Standardzie oprogramowania do wirtualizacji platformy x86/64*.
* Rozwiązanie musi umożliwiać zarządzanie danymi w bazie z użyciem języka SQL.

**Wirtualizacja**Klasa I:* Rozwiązanie musi być uruchamiane na maszynach fizycznych lub w środowiskach wirtualnych.

Klasa II:* Rozwiązanie musi być uruchamiane:
	+ na maszynach fizycznych;
	+ lub w środowiskach wirtualizujących.
* Oprogramowanie musi posiadać wsparcie producenta dla rozwiązań uruchamianych w środowiskach wirtualizujących, w których działa.

Klasa III, IV:* Rozwiązanie musi być uruchamiane w środowiskach wirtualizujących.

**Niezawodność i dostępność*** Rozwiązanie musi umożliwiać odbiorcy monitorowanie dostępności świadczonych przez nie usług.

Klasa I:* Rozwiązanie musi działać z użyciem jednej z konfiguracji:
	+ wysokiej dostępności;
	+ ciągłej dostępności.
* Rozwiązanie musi mieć możliwość partycjonowania danych.
* Rozwiązanie musi umożliwiać odbiorcy monitorowanie dostępności usług.

Klasa II:* Rozwiązanie musi działać z użyciem konfiguracji o wysokiej dostępności.
* Rozwiązanie może posiadać zaimplementowane mechanizmy ciągłego działania, charakteryzujące się tym, że awaria pojedynczego węzła w klastrze nie powoduje przerwy w dostępie do usług.
* Rozwiązanie musi mieć możliwość partycjonowania danych.
* Rozwiązanie musi umożliwiać odbiorcy monitorowanie dostępności usług.

Klasa III, IV:* Rozwiązanie musi posiadać możliwość integracji z systemem monitorowania usług.

**Bezpieczeństwo*** Rozwiązanie musi posiadać wsparcie ze strony producenta w zakresie ujawniania oraz naprawiania błędów i luk bezpieczeństwa, dostarczane przez dedykowany zespół specjalistów.
* Producent rozwiązania musi udostępniać listę opisującą historię wykrytych w rozwiązaniu błędów i zawierającą stosowne poprawki.
* Rozwiązanie musi posiadać możliwość integracji z automatycznym systemem tworzenia kopii zapasowych w zakresie kopiowania konfiguracji serwera aplikacyjnego i aplikacji, ich plików wykonawczych, bibliotek oraz danych.

Klasa B1:* Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:
	+ podczas uwierzytelniania użytkowników,
	+ podczas przesyłania danych konfiguracyjnych.
* Rozwiązanie musi posiadać możliwość centralnego uwierzytelniania użytkowników.
* Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników.
* Musi posiadać możliwość centralnego autoryzowania dostępu użytkowników.
* Rozwiązanie musi wspierać granularny przydział uprawnień.
* Rozwiązanie musi wspierać mechanizmy jednokrotnego logowania.
* Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa.
* Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.
* Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi mieć możliwość integracji z systemem rejestrowania i monitoringu zdarzeń bezpieczeństwa.
* Rozwiązanie musi umożliwiać audytowanie zmian jego konfiguracji.
* Rozwiązanie musi umożliwiać audytowanie zmian w strukturze obiektów bazodanowych.
* Rozwiązanie musi umożliwiać audytowanie zmian danych na poziomie bazy danych.

Klasa B2:* Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:
	+ podczas uwierzytelniania użytkowników,
	+ podczas przesyłania danych konfiguracyjnych.
* Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników.
* Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników.
* Rozwiązanie musi posiadać możliwość centralnego autoryzowania dostępu użytkowników.
* Rozwiązanie musi wspierać granularny przydział uprawnień.
* Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa.
* Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.
* Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.

Klasa B3:* Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:
	+ podczas uwierzytelniania użytkowników,
	+ podczas przesyłania danych konfiguracyjnych.
* Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników.
* Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników.
* Rozwiązanie musi posiadać możliwość centralnego autoryzowania dostępu użytkowników.
* Rozwiązanie musi wspierać granularny przydział uprawnień.
* Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa.
* Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.

Klasa BX:* Rozwiązanie wykorzystane w klasie BX musi być odseparowane fizycznie od innych systemów resortu finansów.
* Jeśli rozwiązanie korzysta z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:
	+ kontroli dostępu,
	+ monitorowania zdarzeń bezpieczeństwa,
	+ filtrowania ruchu.

Klasa I, II:* Rozwiązanie musi umożliwiać tworzenie kopii danych bez konieczności zatrzymywania usług bazodanowych.
* Rozwiązanie musi posiadać możliwość integracji z automatycznym systemem tworzenia kopii zapasowych w zakresie kopiowania konfiguracji serwera baz danych, jego plików wykonawczych, bibliotek oraz danych.

**Zarządzanie**Klasa I, II, III, IV:* Rozwiązanie musi umożliwiać administrowanie konfiguracją, stanem i zasobami oprogramowania z wykorzystaniem konsoli administracyjnej lub aplikacji webowej.
* Rozwiązanie musi umożliwiać administrowanie konfiguracją, stanem i zasobami oprogramowania w trybie wsadowym, np. z wykorzystaniem skryptów powłoki systemu operacyjnego, w którym działa.
* Musi istnieć możliwość zdalnej aktualizacji oprogramowania.

Klasa I:* Dla rozwiązania musi istnieć możliwość uzyskania wsparcia technicznego producenta w trybie *non-stop* (24 h, 7 dni w tygodniu).
* Musi istnieć możliwość aktualizacji oprogramowania bez zatrzymywania środowiska (ang. *rolling upgrades*).

Klasa II:* Dla rozwiązania musi istnieć możliwość uzyskania wsparcia technicznego producenta w trybie *non-stop* (24 h, 7 dni w tygodniu).
 |
| **Serwer bazy danych – typ 1** |

|  |  |
| --- | --- |
| **[Identyfikator](file:///Q%3A%5C%5CZUI%5C%5CRobocze%5C%5CArchitektura%20referencyjna%20HARF%5C%5CPROJEKT%20NOWEGO%20UK%C5%81ADU%20ARCHITEKTURY%20IT%5C%5CARIT-A-Bloki-Architektoniczne-Srodowiska-Teleinformatycznego-1.6.docx%22%20%5Cl%20%22A_Identyfikator)** | C.DB.ORA |
| **Nazwa** | Serwer baz danych – typ 1 |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |
| **Charakterystyka** | Serwer bazy danych w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie Oracle Database. W przypadku zastosowania oprogramowania innego niż obecnie funkcjonujące, musi o zapewnić co najmniej te same funkcjonalności co oprogramowanie wyżej wymienione. |

 |
| **Serwer bazy danych – typ 2** |

|  |  |
| --- | --- |
| **[Identyfikator](file:///Q%3A%5C%5CZUI%5C%5CRobocze%5C%5CArchitektura%20referencyjna%20HARF%5C%5CPROJEKT%20NOWEGO%20UK%C5%81ADU%20ARCHITEKTURY%20IT%5C%5CARIT-A-Bloki-Architektoniczne-Srodowiska-Teleinformatycznego-1.6.docx%22%20%5Cl%20%22A_Identyfikator)** | C.DB.SQL |
| **Nazwa** | Serwer baz danych – typ 2 |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |
| **Charakterystyka** | Serwer bazy danych w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie Microsoft SQL Server. W przypadku zastosowania oprogramowania innego niż obecnie funkcjonujące, musi o zapewnić co najmniej te same funkcjonalności co oprogramowanie wyżej wymienione. |

 |
| **Serwer bazy danych – typ 3** |

|  |  |
| --- | --- |
| **[Identyfikator](file:///Q%3A%5C%5CZUI%5C%5CRobocze%5C%5CArchitektura%20referencyjna%20HARF%5C%5CPROJEKT%20NOWEGO%20UK%C5%81ADU%20ARCHITEKTURY%20IT%5C%5CARIT-A-Bloki-Architektoniczne-Srodowiska-Teleinformatycznego-1.6.docx%22%20%5Cl%20%22A_Identyfikator)** | C.DB.SYB |
| **Nazwa** | Serwer baz danych – typ 3 |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |
| **Charakterystyka** | Serwer bazy danych w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie Sybase Adaptive Server Enterprise. W przypadku zastosowania oprogramowania innego niż obecnie funkcjonujące, musi o zapewnić co najmniej te same funkcjonalności co oprogramowanie wyżej wymienione. |

 |
| **Serwer bazy danych – typ 4** |

|  |  |
| --- | --- |
| **[Identyfikator](file:///Q%3A%5C%5CZUI%5C%5CRobocze%5C%5CArchitektura%20referencyjna%20HARF%5C%5CPROJEKT%20NOWEGO%20UK%C5%81ADU%20ARCHITEKTURY%20IT%5C%5CARIT-A-Bloki-Architektoniczne-Srodowiska-Teleinformatycznego-1.6.docx%22%20%5Cl%20%22A_Identyfikator)** | C.DB.MYS |
| **Nazwa** | Serwer baz danych – typ 4 |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |
| **Producent****Produkt** | Serwer bazy danych w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie Oracle MySQL. W przypadku zastosowania oprogramowania innego niż obecnie funkcjonujące, musi o zapewnić co najmniej te same funkcjonalności co oprogramowanie wyżej wymienione. |

 |
| **Serwer bazy danych – typ 5** |

|  |  |
| --- | --- |
| **[Identyfikator](file:///Q%3A%5C%5CZUI%5C%5CRobocze%5C%5CArchitektura%20referencyjna%20HARF%5C%5CPROJEKT%20NOWEGO%20UK%C5%81ADU%20ARCHITEKTURY%20IT%5C%5CARIT-A-Bloki-Architektoniczne-Srodowiska-Teleinformatycznego-1.6.docx%22%20%5Cl%20%22A_Identyfikator)** | C.DB.DBX |
| **Nazwa** | Serwer baz danych – typ 5 |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |
| **Charakterystyka** | Serwer bazy danych w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie IBM DB2. W przypadku zastosowania oprogramowania innego niż obecnie funkcjonujące, musi o zapewnić co najmniej te same funkcjonalności co oprogramowanie wyżej wymienione. |

 |
| **Serwer bazy danych – typ 6** |

|  |  |
| --- | --- |
| [**Identyfikator**](file:///Q%3A/ZUI/Robocze/Architektura%20referencyjna%20HARF/PROJEKT%20NOWEGO%20UK%C5%81ADU%20ARCHITEKTURY%20IT/ARIT-A-Bloki-Architektoniczne-Srodowiska-Teleinformatycznego-1.6.docx#A_Identyfikator) | C.DB.PGS |
| **Nazwa** | Serwer baz danych – typ 6 |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |
| **Charakterystyka** | Serwer bazy danych w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie PostgreSQL. W przypadku zastosowania oprogramowania innego niż obecnie funkcjonujące, musi o zapewnić co najmniej te same funkcjonalności co oprogramowanie wyżej wymienione. |

 |

## Oprogramowanie klastrowe HA

### Oprogramowanie klastrowe – typ 2

|  |  |
| --- | --- |
| [**Identyfikator**](#A_Identyfikator) | C.CL.HA.5 |
| **Nazwa** | Oprogramowanie klastrowe – typ 2 |
| **Charakterystyka** | Oprogramowanie klastrowe w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie klastrowe **Microsoft Windows Server Failover Clustering**.  |

### Oprogramowanie klastrowe – typ 3

|  |  |
| --- | --- |
| [**Identyfikator**](#A_Identyfikator) | C.CL.HA.7 |
| **Nazwa** | Oprogramowanie klastrowe – typ 3 |
| **Charakterystyka** | Oprogramowanie klastrowe w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie klastrowe **Red Hat Cluster Suite**.  |

### Oprogramowanie klastrowe – typ 4

|  |  |
| --- | --- |
| [**Identyfikator**](#A_Identyfikator) | C.CL.HA.8 |
| **Nazwa** | Oprogramowanie klastrowe – typ 4 |
| **Charakterystyka** | Oprogramowanie klastrowe w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie klastrowe **SUSE Linux Enterprise High Availability Extension**.  |

## Oprogramowanie klastrowe HA

### Oprogramowanie wirtualizujące – typ 1

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.VM.X86.VMW |
| **Nazwa** | Oprogramowanie wirtualizujące – typ 1 |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |
| **Charakterystyka** | Dla funkcjonalności ***typ 1*** *oprogramowanie musi spełniać poniższe wymagania:*1 Warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym i nie może być częścią innego systemu operacyjnego.2 Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego.3 Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym. Wymagana jest możliwość przydzielenia maszynie większej ilości wirtualnej pamięci operacyjnej niż jest zainstalowana w serwerze fizycznym oraz większej ilości przestrzeni dyskowej niż jest fizycznie dostępna.4 Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do 4TB pamięci operacyjnej. 5 Oprogramowanie do wirtualizacji musi zapewnić możliwość przydzielenia maszynom wirtualnym do 128 procesorów wirtualnych.6 Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. 7 Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. 8 Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, SLES 11, SLES 10, RHEL 5, RHEL 4,. Solaris wersja 10 dla platformy x86, SCO OpenServer, SCO Unixware, Mac OS X.9 Rozwiązanie musi zapewniać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania trybu XP mode w Windows 7 a także instalacji wszystkich funkcjonalności w tym Hyper-V pakietu Windows Server 2012 na maszynie wirtualnej.10 Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania środowiskiem serwerów wirtualnych. Konsola graficzna musi być dostępna poprzez dedykowanego klienta i za pomocą przeglądarek, minimum IE i Firefox.11 Dostęp przez przeglądarkę do konsoli graficznej musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.12 Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root.13 Rozwiązanie musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej i zdefiniowania alertów informujących o przekroczeniu wartości progowych.14 Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji.15 Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi.16 Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie. 17 Kopie zapasowe muszą być składowane z wykorzystaniem technik de-duplikacji danych.18 Musi istnieć możliwość odtworzenia pojedynczych plików z kopii zapasowej maszyny wirtualnej przez osoby do tego upoważnione bez konieczności nadawania takim osobom bezpośredniego dostępu do głównej konsoli zarządzającej całym środowiskiem.19 Mechanizm zapewniający kopie zapasowe musi być wyposażony w system cyklicznej kontroli integralności danych. Ponadto musi istnieć możliwość przywrócenia stanu repozytorium kopii zapasowych do punktu w czasie, kiedy wszystkie dane były integralne w przypadku jego awarii.20 Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością wskazania konieczności zachowania stanu pamięci pracującej maszyny wirtualnej. 21 Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. 22 Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, Open LDAP. 23 Platforma wirtualizacyjna musi umożliwiać zastosowanie w serwerach fizycznych procesorów o dowolnej ilości rdzeni.24 Rozwiązanie musi umożliwiać tworzenie jednorodnych wolumenów logicznych o wielkości do 62TB.25 Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.26 Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.27 Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi. 28 Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania.29 Rozwiązanie musi gwarantować współczynnik RPO na poziomie minimum 15 minut30 Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. 31 Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.32 Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.33 System musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE.34 Rozwiązanie musi umożliwiać utworzenie jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie serwery fizyczne platformy wirtualizacyjnej. Przełącznik taki musi zapewniać możliwość konfiguracji parametrów sieciowych maszyny wirtualnej z granulacją na poziomie portu tego przełącznika. Pojedyncza maszyna wirtualna musi mieć możliwość wykorzystania jednego lub wielu portów przełącznika z niezależną od siebie konfiguracją. 35 Konsola zarządzania platformą wirtualizacji musi umożliwiać centralną konfigurację przełącznika rozproszonego a mechanizmy wewnętrzne muszą zapewniać propagację tej konfiguracji do wszystkich serwerów fizycznych tworzących wzajemnie ten przełącznik.36 Platforma wirtualizacji powinna w ramach przełącznika sieciowego musi zapewniać możliwość integracji z produktami (przełącznikami wirtualnymi) firm trzecich, tak aby umożliwić granularną delegację zadań w zakresie zarządzania konfiguracją sieci do zespołów sieciowych.37 Przełącznik rozproszony musi współpracować z protokołem NetFlow.38 Przełącznik rozproszony musi umożliwiać funkcjonalność duplikowania ruchu sieciowego dowolnego jego portu wirtualnego na inny port.39 Przełącznik musi mieć wbudowane mechanizmy składowania kopii konfiguracji, przywracania tej kopii a także mechanizmy automatycznie zapobiegające niewłaściwej konfiguracji sieciowej, które w całości lub w części mogą eliminować błędy ludzkie i utratę łączności sieciowej.40 System musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych.41 Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, pamięciami masowymi niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi rodzajami virtualnych przełączników sieciowych, pomiędzy Centrami Przetwarzania Danych oraz pomiędzy Centralnymi Konsolami Zarządzającymi platformami wirtualnymi.42 Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury.43 Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury. 44 Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania. 45 Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa jak i zmianę jej wersji.46 Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej lub partycjonowania sieci.47 Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu po jakim taka decyzja jest wykonywana.48 Rozwiązanie musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie czterech procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych. 49 Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia usług pomiędzy serwerami fizycznymi, wolumenami dyskowymi, klastrami, centrami przetwarzania danych bez przerywania pracy usług. 50 Rozwiązanie musi umożliwiać automatyczne równoważenie obciążenia serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej.51 System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu sieciowego oraz ustalania priorytetów w zależności od jego rodzaju.52 System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn.53 System musi mieć możliwość grupowania pamięci masowych o podobnych parametrach w grupy i przydzielania ich do wirtualnych maszyn zgodnie z ustaloną przez administratora polityką.54 System musi mieć możliwość równoważenia obciążenia i zajętości pamięci masowych wraz z pełną automatyką i przenoszeniem plików wirtualnych maszyn z bardziej zajętych na mniej zajęte przestrzenie dyskowe lub/i z przestrzeni dyskowych bardziej obciążonych operacjami I/O na mniej obciążone.55 Rozwiązanie musi gromadzić i umożliwiać zunifikowaną, graficzną prezentację informacji o wszystkich aspektach infrastruktury serwerów wirtualnych z uwzględnieniem danych szczegółowych takich jak poziom obciążenia sieci czy ilość IOPS w komunikacji z pamięcią masową.56 Zgromadzone dane muszą zapewniać ocenę kondycji, wydajności i pojemności dowolnego elementu infrastruktury, wliczając centrum danych, klastry, serwery fizyczne, podsystemy dyskowe i grupy maszyn wirtualnych. Ocena ta powinna być wartością jednowymiarową wyliczoną na podstawie agregacji zgromadzonych danych szczegółowych.57 Dostęp do warstwy prezentacji wyników analiz wydajnościowo pojemnościowych musi być możliwy przez dedykowanego klienta oraz przez przeglądarkę internetową.58 Uprawnienia do warstwy prezentacji wyników muszą dopuszczać rozłączność z uprawnieniami do infrastruktury.59 Rozwiązanie musi precyzyjnie określać na podstawie aktualnej i historycznej dynamiki rozwoju infrastruktury pozostałą pojemność i czas pozostały do przewidywanego wysycenia zasobów.60 Progi alertowe muszą być generowane dynamicznie na podstawie zebranych danych z infrastruktury i trybie ciągłym korygowane na podstawie aktualnego obciążenia i pozostałej pojemności infrastruktury. 61 Musi istnieć możliwość zdefiniowania progów alertowych dla wydzielonej części infrastruktury, w tym poprzez zadanie warunków brzegowych, które w danym momencie poszczególny komponent spełnia.62 Rozwiązanie musi zapewniać mechanizmy szybkiej identyfikacji incydentów oraz rekomendacje i mechanizmy do ich rozwiązania. W szczególności rozwiązanie musi umożliwiać analizę korelacji wystąpień incydentów wydajnościowych ze zmianami infrastrukturalnymi o których wiedzę w danym momencie posiada system zarządzający platformą serwerów wirtualnych.63 Rozwiązanie musi posiadać możliwość generowania alertów i raportów wydajnościowo-pojemnościowych dla statycznie i dynamicznie zdefiniowanych grup maszyn wirtualnych.64 System analizy kondycji, wydajności i pojemność środowiska musi być wolny od wszelkich ograniczeń, technicznych i licencyjnych w zakresie jego instalacji na maszynach wirtualnych i przenoszenia tych maszyn pomiędzy serwerami fizycznymi.65 Rozwiązanie musi posiadać zaawansowany mechanizm umożliwiający prognozowanie zmian pojemności platformy wirtualnej (w szczególności: zmiana liczby maszyn wirtualnych, zmiana liczby hostów fizycznych, zmiana liczby i rodzaju przestrzeni dyskowej) z możliwością planowania umieszczania tych zmian w konkretnym momencie czasu.Atrybuty:* + *Poziom funkcjonalności:*

*-* ***typ 1***  |

### Oprogramowanie wirtualizujące – typ 2

|  |  |
| --- | --- |
| [**Identyfikator**](#A_Identyfikator) | C.VM.X86.HPV |
| **Nazwa** | Oprogramowanie wirtualizujące – typ 2 |
|  |  |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |
| **Charakterystyka** | Oprogramowanie wirtualizujące w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie wirtualizacyjne Microsoft Hyper-V. W przypadku zastosowania oprogramowania innego niż obecnie funkcjonujące, musi ono spełnić wymagania opisane poniżej.**Funkcje wirtualizatora**1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
	1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
	2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
	3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
	4. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
8. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
9. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
	1. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
	2. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
10. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
	1. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
	2. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
	3. Obsługi 4-KB sektorów dysków
	4. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
	5. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
	6. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)
11. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
12. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
13. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

**Funkcje systemu zarządzania wirtualizatorem**System zarządzania środowiskami wirtualnymi musi posiadać następujące cechy:1. Architektura
2. System zarządzania środowiskiem wirtualnym powinien składać się z:
* serwera zarządzającego,
* relacyjnej bazy danych przechowującej informacje o zarządzanych elementach,
* konsoli, instalowanej na komputerach operatorów,
* portalu self-service (konsoli webowej) dla operatorów „departamentowych”,
* biblioteki, przechowującej komponenty niezbędne do budowy maszyn wirtualnych,
* agenta instalowanego na zarządzanych hostach wirtualizacyjnych,
* „konektora” do systemu monitorującego pracę hostów i maszyn wirtualnych.
1. System musi mieć możliwość tworzenia konfiguracji wysokiej dostępności (klaster typu fail-over).
2. System musi pozwalać na zarządzanie platformami wirtualizacyjnymi co najmniej trzech różnych dostawców.
3. Interfejs użytkownika
4. Konsola musi umożliwiać grupowanie hostów i nadawanie uprawnień poszczególnym operatorom do grup hostów.
5. Widoki hostów i maszyn wirtualnych powinny mieć możliwość zakładania filtrów, pokazując tylko odfiltrowane elementy, np. maszyny wyłączone, maszyny z systemem operacyjnym X, itp...
6. Widok szczegółowy elementu w przypadku maszyny wirtualnej musi pokazywać stan, ilość alokowanej pamięci i dysku twardego, system operacyjny, platformę wirtualizacyjną, stan ostatniego zadania, oraz wykres utylizacji procesora i podgląd na pulpit.
7. Konsola musi posiadać odrębny widok z historią wszystkich zadań oraz statusem zakończenia poszczególnych etapów i całych zadań.
8. Scenariusze i zadania
9. Tworzenie maszyn wirtualnych – system musi umożliwiać stworzenie maszyny wirtualnej w co najmniej dwóch trybach:
10. Ad hoc – gdzie wszystkie elementy są wybierane przez operatora podczas tworzenia maszyny,
11. Nadzorowany – gdzie operator tworzy maszynę korzystając z gotowego wzorca (template), a wzorzec składa się z przynajmniej 3-ech elementów składowych:
12. profilu sprzętowego
13. profilu systemu operacyjnego,
14. przygotowanych dysków twardych,
15. Predefiniowane elementy muszą być przechowywane w bibliotece systemu zarządzania.
16. System musi umożliwiać przenoszenie maszyny wirtualnej pomiędzy zarządzanymi hostami:
* w trybie migracji „on-line” – bez przerywania pracy,
* w trybie migracji „off-line – z zapisem stanu maszyny
1. System musi umożliwiać automatyczne, równomierne rozłożenie obciążenia pomiędzy zarządzanymi hostami.
2. System musi umożliwiać wyłączenie hosta, gdy jego zasoby nie są konieczne do pracy, w celu oszczędności energii. System powinien również umożliwiać ponowne włączenie takiego hosta.
3. System musi umożliwiać przełączenie wybranego hosta w tryb „maintenance” w przypadku wystąpienia awarii lub w celu przeprowadzenia planowanych prac serwisowych. Uruchomienie tego trybu musi skutkować migracją maszyn na inne hosty lub zapisaniem ich stanu.
4. System musi posiadać możliwość konwersji maszyny fizycznej do wirtualnej.
5. System musi posiadać (bez potrzeby instalowania dodatkowego oprogramowania) - możliwość wykrycia maszyny fizycznej w sieci i instalacje na niej systemu operacyjnego wraz z platformą do wirtualizacji.
6. Wymagania dodatkowe
7. System musi informować operatora o potrzebie migracji maszyn, jeśli wystąpią nieprawidłowe zdarzenia na hoście lub w innych maszynach wirtualnych mające wpływ na ich pracę, np. awarie sprzętu, nadmierna utylizacja współdzielonych zasobów przez jedną maszynę.
8. System musi dawać operatorowi możliwość implementacji w/w migracji w sposób automatyczne bez potrzeby każdorazowego potwierdzania.
9. System musi kreować raporty z działania zarządzanego środowiska, w tym:
* utylizacja poszczególnych hostów,
* trend w utylizacji hostów,
* alokacja zasobów na centra kosztów,
* utylizacja poszczególnych maszyn wirtualnych,
* komputery-kandydaci do wirtualizacji
1. System musi umożliwiać skorzystanie z szablonów:
* wirtualnych maszyn
* usług

oraz profili dla:* aplikacji
* serwera SQL
* hosta
* sprzętu
* systemu operacyjnego gościa
1. System musi umożliwiać tworzenie chmur prywatnych na podstawie dostępnych zasobów (hosty, sieci, przestrzeń dyskowa, biblioteki zasobów).
2. System musi posiadać możliwość przygotowania i instalacji zwirtualizowanej aplikacji serwerowej.
3. System musi pozwalać na skalowalność wirtualnego środowiska aplikacji (poprzez automatyczne dodanie wirtualnej maszyny z aplikacją)
 |
|  |  |

## Oprogramowanie antywirusowe dla środowiska wirtualnego

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.VM.X86.VAV |
| **Nazwa** | Oprogramowanie antywirusowe dla środowiska wirtualnego |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |
| **Charakterystyka** | Wszystkie komponenty - na których będzie zainstalowane Oprogramowanie antywirusowe muszą być zainstalowane jako maszyny wirtualne pracujące w środowisku *C.VM.X86.VMW lub C.VM.X86.HPV* Zamawiającego. Wykonawca jest zobowiązany do dostarczenia wszystkich licencji (włącznie z licencjami na systemy operacyjne dla nowych komponentów oraz dodatkowe oprogramowanie), niezbędnych do prawidłowego działania Oprogramowania *.*Licencjonowanie Oprogramowania, ze względu na dynamicznie rozwijającą się infrastrukturę Zamawiającego, musi być oparte na bazie liczby fizycznych procesorów chronionego hosta (licencjonowanie per socket),Wymagania funkcjonalne:I. Wymagania Zamawiającego dotyczące Zarządzania infrastrukturą Systemu AV 1. Pełna administracja konfiguracją oraz monitorowanie środowiska maszyn wirtualnych za pomocą *centralnej* konsoli administracyjnej w pełnej wymaganej przez Zamawiającego funkcjonalności (centralna instalacja, konfiguracja, zarządzanie, raportowanie i administrowanie oprogramowaniem), w szczególności:a) Dostępna funkcjonalność określenia harmonogramu oraz wymuszenia skanowania w danej chwili,b) Określenie reakcji w przypadku wykrycia wirusa,c) Dostępna funkcjonalność określenia obszarów skanowania, typów skanowanych katalogów, plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych obszarów,d) Dostępna funkcjonalność zdefiniowania harmonogramu lub częstotliwości pobierania aktualizacji wirusów od producenta/producentów,e) Dostępna funkcjonalność zarządzania zdarzeniami i raportowanie – natychmiastowe alarmowanie aktywności wirusów w administrowanej sieci,f) Dostępna funkcjonalność prezentacji informacji o poziomie bezpieczeństwa na centralnej konsoli zarządzającej systemami,g) Dostępna funkcjonalność tworzenia kont dla administratorów o różnych stopniach uprawnień dla różnych komputerów lub grup komputerów oraz różnych produktów.II. Wymagania Zamawiającego na Oprogramowanie *Antywirusowe* w zakresie funkcjonalności AntiMalware i Web Reputation (AM / WR):1. Dostarczone Oprogramowanie równoważne musi posiadać następujące funkcjonalności: a) Bezagentowa ochrona maszyn wirtualnych w obrębie serwera hosta bez względu na ich stan (aktywne, uśpione, przywrócone do poprzedniego stanu, sklonowane) realizowana w przypadku wszystkich opisanych poniżej funkcjonalności,b) Zapewnia ochronę nie wspieranych przez ich producentów systemów operacyjnych oraz aplikacji działających na maszynach wirtualnych,c) Oprogramowanie antywirusowe musi zapewniać „bezagentową” ochronę dla serwerów i desktopów wirtualnych~~,~~ *,* d) Oprogramowanie musi pozwalać na określenie obszarów skanowania, typów skanowanych plików oraz na wykluczenie ze skanowania określonych obszarów dla skanowania w czasie rzeczywistym, ręcznego skanowania oraz skanowania określonego w harmonogramie,e) Oprogramowanie musi umożliwiać określenie harmonogramu skanowania (obiekty i grupy), oraz wymuszenia skanowania w danej chwili,f) Oprogramowanie musi opierać się na mechanizmie skanowania nowych bądź zmienionych plików w celu skrócenia czasu skanowania oraz zwiększenia wydajności,g) Oprogramowanie musi posiadać heurystyczną technologię do wykrywania nowych, nieznanych wirusów,h) Oprogramowanie musi posiadać funkcjonalność zdefiniowania harmonogramu lub częstotliwości pobierania aktualizacji bazy wirusów, wszelkich poprawek oprogramowania oraz umożliwiać określenie centralnego punktu dystrybucji uaktualnień i poprawek oprogramowania w infrastrukturze Zamawiającego,i) Oprogramowanie musi pozwalać na określenie reakcji w przypadku wykrycia wirusa (czyszczenie, automatyczne usunięcie, kwarantanna), oraz na natychmiastowe raportowanie o zdarzeniach (e-mail, wiadomości SNMP),j) Oprogramowanie musi realizować funkcję hierarchii i delegacji uprawnień administratorów, zarówno dla grup jak i poszczególnych obiektów,k) Zarządzanie Oprogramowaniem musi odbywać się poprzez standardową przeglądarkę WWW i połączenie https (z wykluczeniem SSL 3.0, 2.0, 1.0), która nie wymaga instalacji żadnych dodatkowych komponentów, umożliwiając dostęp do konsoli na kilku stacjach jednocześnie lub dedykowaną konsolę w technologii Grubego Klienta,l) Oprogramowanie musi posiadać funkcjonalność wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „greyware”, „adware", „keylogger”, „dialer”, „trojan”, „antimalware”,m) Oprogramowanie musi posiadać możliwość blokowania połączeń do adresów URL określonych przez producenta systemu jako niebezpieczne, również w przypadku gdy połączenia są nawiązywane przez procesy działające na chronionych serwerach,n) Oprogramowanie musi mieć możliwość konfiguracji lokalnego serwera reputacji plików, synchronizującego się z chmurą producenta, który umożliwiał będzie weryfikację reputacji plików i adresów URL bez konieczności łączenia się z Internetem,o) Oprogramowanie musi mieć możliwość zdefiniowania statycznych list adresów URL do których połączenia będą zawsze blokowane przez system,p) Oprogramowanie musi mieć możliwość tworzenia logicznych grup serwerów w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa,q) Oprogramowanie musi umożliwiać ochronę maszyn znajdujących się w strefie DMZ,r) Oprogramowanie musi mieć możliwość generowania i wysyłania raportów w wybranym formacie ( minimum pdf),s) Oprogramowanie musi posiadać funkcjonalność przekazywania zdarzeń o zagrożeniach do centralnego serwera lub systemu typu SIEM. W przypadku wysyłanie informacji o zdarzeniach do systemu SIEM administrator musi mieć możliwość zdefiniowania centralnego systemu SIEM lub odrębnych systemów dla każdej z polityk, grup chronionych serwerów lub pojedynczych serwerów,t) Serwer zarządzający oprogramowania musi posiadać w pełni udokumentowane API pozwalające na jego integrację z zewnętrznymi systemami zarządzającymi firm trzecich,u) Oprogramowanie musi mieć możliwość tworzenia ról administratorów i przydzielania uprawnień co najmniej w zakresie:a. Serwerów lub grup serwerówb. Polityk lub grup politykc. Poszczególnych funkcjonalności systemu,v) Oprogramowanie musi mieć możliwość tworzenia drzewa polityk zależnych, w którym polityki pochodne dziedziczą ustawienia od polityk na wyższym poziomie. Administratorzy posiadający uprawnienia jedynie do polityk pochodnych nie mogą mieć możliwości wprowadzania zmian do ustawień dziedziczonych.III. Wymagania Zamawiającego na Oprogramowanie Antywirusowe w zakresie funkcjonalności Integrity Monitoring i Log Inspection (IM / LI):1. Dostarczone oprogramowanie równoważne musi posiadać następujące funkcjonalności: a) System musi pozwalać na monitorowanie wskazanych plików, katalogów, serwisów, wpisów w rejestrach oraz procesów i informowanie o wprowadzanych zmianach w oparciu o zdefiniowane kryteria.b) W przypadku serwerów wirtualnych działających pod kontrolą systemu Windows system musi posiadać możliwość realizowania monitorowania wskazanych plików, katalogów oraz wpisów w rejestrach i informowanie o wprowadzanych zmianach w oparciu o zdefiniowane kryteria bez konieczności instalowania dedykowanego agenta na wskazanym, chronionym serwerze.c) Informacja o wprowadzonych zmianach musi zawierać co najmniej nazwę użytkownika lub procesu, który wprowadził zmianę, nazwę pliku lub wpisu w rejestrze, w którym została wprowadzona zmiana, datę i czas wprowadzenia zmiany, nazwę serwera na którym została wprowadzona zmiana, oraz nazwę reguły oraz która została wykorzystanad) System musi posiadać predefiniowany zestaw reguły dostarczonych przez producenta określających wskazane do monitorowania pliki wpisy w rejestrach oraz monitorowane serwisy, w zależności od chronionego systemu lub aplikacji.e) System musi posiadać możliwość ręcznego zdefiniowania przez administratora monitorowanych plików oraz wpisów w rejestrach.g) System musi posiadać możliwość zdefiniowania wykluczeń plików znajdujących się w monitorowanym katalogu.h) System musi posiadać możliwość monitorowania hypervisora i informowania o wprowadzanych w nim zmianach.j) System musi posiadać reguły dostarczone przez producenta określające wskazane do zbierania i analizy logi, w zależności od chronionego systemu o) System musi posiadać możliwość automatycznego uruchamiania odpowiednich reguł niezależnie dla każdego chronionego serwera, w zależności od systemu operacyjnego lub aplikacji.q) System musi posiadać możliwość tworzenia polityk stanowiących zbiór reguł dostarczonych przez producenta oraz zdefiniowanych przez administratorar) System musi posiadać możliwość tworzenia drzew polityk, w których polityki położona na niższych gałęziach dziedziczą ustawienia z polityk położonych na gałęziach wyższychs) System musi posiadać możliwość tworzenia granularnych ról administratorów z możliwością definiowania uprawnień z dokładnością do pojedynczej polityki lub serwera.t) System musi posiadać możliwość automatycznego przypisywania polityk w oparciu o algorytmy zdefiniowane przez administratora co najmniej w przypadku utworzenia nowego serwera wirtualnego, jego przeniesienia u) Algorytmy w oparciu o które system przydziela polityki muszą pozwalać na zdefiniowanie automatycznych działań co najmniej w zależności od nazwy serwera, systemu operacyjnego oraz nazwy wykorzystywanego serwera zarządzającego.v) Wszystkie funkcjonalności systemu muszą być zarządzane z pojedynczej konsoli, tej samej, która jest wykorzystywana do zarządzania funkcjonalnościami AntyMalware i Web Reputation.IV. Wymagania Zamawiającego na Oprogramowanie Antywirusowe w zakresie funkcjonalności Intrusion Detection and Prevention i Firewall (IPS / FW):1. Dostarczone oprogramowanie równoważne musi posiadać następujące funkcjonalności: a) System musi posiadać możliwość kontroli oraz blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną.b) System musi posiadać predefiniowaną bazę najpopularniejszych aplikacji oraz komunikatorów (włączając w to gadu-gadu i skype)c) System musi posiadać możliwość heurystycznego wykrywania transmisji na podstawie częstotliwości jej występowania oraz zdefiniowanego zakresu portów.e) System musi posiadać możliwość przełączania pomiędzy trybem blokowania ruchu i trybem detekcji zdarzeń w sposób globalny dla wszystkich reguł.f) System musi posiadać moduł umożliwiający blokowanie transmisji na podstawie zdefiniowanej charakterystyki ruchu na podstawie sygnatury oraz zdefiniowanego ciągu znaków (patternu). g) System musi pozwalać na sprawdzanie w czasie rzeczywistym poziomu bezpieczeństwa nieznanych aplikacji poprzez zapytania przesyłane poprzez siec do systemu serwerów producenta.h) System musi posiadać możliwość ochrony podatności systemów i aplikacji, bez konieczności instalowania poprawek dostarczanych przez producentów tych systemów oraz aplikacji.j) System musi posiadać dwukierunkowy stanowy firewall (stateful firewall) pozwalający na łatwą izolacje interfejsów i nie wymagający restartów systemuk) System musi pełni wspierać IPv6l) System musi umożliwiać kontrolę połączeń wychodzących i przychodzących w komunikacji sieciowej z możliwością kontroli niestandardowych portów TCP (możliwość zdefiniowania na podstawie numeru protokołu oraz numeru typu ramki). m) System musi posiadać możliwość przełączenia trybu działania reguł firewalla z trybu blokowania ruchu w tryb detekcji zdarzeńn) Wszystkie funkcjonalności powinny być dostarczane bezagentowo.o) System musi posiadać umiejętność pracy ze zdeformowanymi pakietami, brakującymi flagami itp. Anomaliamip) System powinien umożliwiać definiowanie trybu pracy Tap oraz Inline dla każdego chronionego obiektu i polityki bezpieczeństwaq) System powinien umożliwiać inspekcję HTTPS bez potrzeby wykorzystywania dodatkowych rozwiązańr) System musi wykorzystywać mechanizmy pseudo-stanowe (pseudo-stateful) dla protokołów bezstanowych (UDP, ICMP)Atrybuty:* + - Poziom funkcjonalności:

- **AntiMalware i Web Reputation**- **Integrity Monitoring i Log Inspection**- **Intrusion Detection and Prevention i Firewall** |

## Oprogramowanie klastrowe wydajnościowe

### Oprogramowanie klastrowe wydajnościowe – typ 1

|  |  |
| --- | --- |
| [**Identyfikator**](#A_Identyfikator) | C.CL.HEF.RAC |
| **Nazwa** | Oprogramowanie klastrowe wydajnościowe – typ 1 |
| **Charakterystyka** | Oprogramowanie klastrowe wydajnościowe w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie klastrowe wydajnościowe **Oracle Real Application Clusters.**  |

### Oprogramowanie klastrowe wydajnościowe – typ 2

|  |  |
| --- | --- |
| [**Identyfikator**](#A_Identyfikator) | C.CL.HEF.SYB |
| **Nazwa** | Oprogramowanie klastrowe wydajnościowe – typ 2 |
| **Charakterystyka** | Oprogramowanie klastrowe wydajnościowe w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie klastrowe wydajnościowe **Sybase ASE Cluster Edition**.  |

### Oprogramowanie klastrowe wydajnościowe – typ 3

|  |  |
| --- | --- |
| [**Identyfikator**](#A_Identyfikator) | C.CL.HEF.DBX |
| **Nazwa** | Oprogramowanie klastrowe wydajnościowe – typ 3 |
| **Charakterystyka** | Oprogramowanie klastrowe wydajnościowe w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie klastrowe wydajnościowe **IBM DB2 pureScale**.  |

## Systemy operacyjne

### System operacyjny – typ 1

|  |  |
| --- | --- |
| [**Identyfikator**](#A_Identyfikator) | C.OS.X86.LNX.RH |
| **Nazwa** | System operacyjny – typ 1 |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |
| **Charakterystyka** | System operacyjny w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie Red Hat Enterprise Linux.* Obsługa minimum dwóch fizycznych procesorów.
* Szeroki zestaw oprogramowania dołączony wraz z systemem. W wariancie minimalnym oprogramowanie umożliwiające uruchomienie: serwera www, serwera poczty, serwera bazy danych, serwera cache'ującego obiekty w pamięci ulotnej, serwerów sieciowych systemów plików NFSv4 i SMB, wirtualnej maszyny Javy.
* Ochrona obiektów systemu poprzez mechanizm SELinux lub w pełni równoważny. Mechanizm wymusza kontrolę dostępu do obiektów zgodnie z polisą przynajmniej dla takich obiektów jak pliki, katalogi, porty, użytkownicy, procesy, maszyny wirtualne. System operacyjny musi zostać dostarczony wraz z zestawem wspieranych przez producenta i aktualizowanych polis bezpieczeństwa. System powinien zapewniać narzędzia tekstowe i graficzne pozwalające w prosty sposób analizować alarmy bezpieczeństwa.
* Mechanizm izolacji maszyn wirtualnych sVirt bądź w pełni równoważny.
* Certyfikat bezpieczeństwa zgodny z EAL4+.
* Wbudowana w jądro obsługa wirtualizacji oraz narzędzia tekstowe i graficzne służące do zarządzania maszynami wirtualnymi.
* Możliwość uruchomienia nieokreślonej liczby wirtualnych maszyn.
* Posiada wsparcie przynajmniej następujących hypervisorów: KVM, VMware, Hyper-V.
* Ponadto dla wymienionych hypervisorów system operacyjny posiada para-wirtualizowane sterowniki, które zostaną automatyczne załadowane przez jądro systemu przy jego uruchomieniu.
* W przypadku instalacji bezpośrednio na fizycznym sprzęcie musi posiadać oficjalne wsparcie firmy Microsoft dla uruchamiania w maszynach wirtualnych serwerów Windows 2008 lub nowsze.
* Kompatybilność ABI oraz API przez cały okres życia aktualizowanego systemu. Wymaganie dotyczy wersji głównych (ang. major).
* Otwarty kod źródłowy. Wymaganie dotyczy wszystkich elementów systemu operacyjnego włącznie z dostarczonym zestawem oprogramowania.
* Instalator dający możliwość utworzenia szyfrowanych partycji jeszcze przed instalacją systemu operacyjnego.
* Istnienie mechanizmu grup kontrolnych, pozwalającego na dynamiczne klasyfikowanie i grupowanie zadań systemowych oraz wymuszenie zadanego przez administratora sposobu zarządzania zadaniami przez jądro systemy operacyjnego. Grupy kontrolne w szczególności muszą pozwolić na wprowadzenie mechanizmu QoS dla procesów i maszyn wirtualnych. W wariancie minimalnym, dla każdego zadania (ang. task) musi być możliwe:
	+ przyporządkowanie na stałe do określonych przez administratora procesorów
	+ określenie maksymalnych wartości bądź proporcji wykorzystania operacji wejścia/wyjścia (ang. I/O) dla podsystemu sieciowego i dyskowego
	+ określenie udziałów w dostępie do procesorów, np. poprzez utworzenie proporcji czasu dostępu dla różnych zadań
	+ przyporządkowanie do strefy NUMA, zarówno CPU jak i pamięci RAM
* Mechanizm wykonywania kopii migawkowych (ang. snapshots) uprzednio przygotowanych przestrzeni blokowych.
* Wsparcie dla systemów plików EXT3, EXT4, XFS, GFS, GFS2
* Wsparcie dla urządzeń blokowych typu Ceph
* Możliwość wykorzystania jako klient pNFS (ang. parallel NFS) w układzie plikowym (ang. file layout).
* Producent systemu operacyjnego musi:
	+ Dostarczać na bieżąco aktualizowaną listę kompatybilnego i certyfikowanego sprzętu (HCL).
	+ Gwarantować czas życia (utrzymania na rynku wraz z dostarczaniem aktualizacji) przez co najmniej 10 lat od momentu pojawienia się systemu operacyjnego na rynku.

Atrybuty:* *Licencjonowanie:*
* ***2SUV*** *(licencja obejmuje 2 fizyczne procesory i uprawnia do instalacji nieograniczonej liczby bloków wirtualnych o identyfikatorze C.OS.X86.LNX.RH)*
* ***2SLV*** *(licencja obejmuje 2 fizyczne procesory i uprawnia do instalacji bloku C.OS.X86.LNX.RH na 1 fizycznym serwerze lub 2 bloków wirtualnych o identyfikatorze C.OS.X86.LNX.RH)*
 |

### System operacyjny – typ 2

|  |  |
| --- | --- |
| [**Identyfikator**](#A_Identyfikator) | C.OS.X86.LNX.SU |
| **Nazwa** | System operacyjny – typ 2 |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |
| **Charakterystyka** | System operacyjny w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie Novell SUSE Linux Enterprise Server. * Jądro systemu w wersji co najmniej 3.0.x, biblioteka systemowa glibc w wersji co najmniej 2.11.x, środowisko graficzne Xorg-x11 w wersji co najmniej 7.4, środowisko IBM Java JRE w dwóch wersjach:
* seria 1.4, w wersji co najmniej 1.4.x
* seria 1.6, w wersji co najmniej 1.6.x,
* System musi być zgodny ze standardem określonym specyfikacją Linux Standards Base Version w wersji co najmniej 3.1 (www.linuxbase.org)
* System musi obsługiwać serwery z procesorami 32 i 64 bit Intel lub AMD
* System musi posiadać wbudowane mechanizmy wirtualizacji XEN i KVM, oraz posiadać oficjalne wsparcie dla uruchamiania w wirtualnym środowisku:
* XEN – serwerów MS Windows 2003 SP2+, MS Windows 2008 SP2 oraz MS Windows R2+
* KVM – serwerów MS Windows 2003 SP2+, MS Windows 2008 SP2 oraz MS Windows R2+ w ramach programu Server Virtualization Validation Program (SVVP)
* System musi posiadać wsparcie dla nieograniczonej liczby wirtualnych instancji tego systemu uruchomionych na platformie XEN, lub KVM, dostarczonych z tym systemem.
* System powinien posiadać graficzną, zintegrowaną centralną konsolę do zarządzania systemem dostępną w języku polskim (YAST lub inną) obsługującą co najmniej następujące elementy dostępne w trybie graficznym dla użytkownika root:
* konfiguracja sekwencji bootowania (bootloadera),
* konfiguracja urządzeń (kart graficznych, dźwiękowych, sieciowych i innych),
* konfiguracja serwera X (rozdzielczości pulpitu, częstotliwości odświeżania monitora),
* konfiguracja klawiatury i myszy,
* zarządzanie dyskami twardymi i stacjami dysków (tworzenie, usuwanie, formatowanie partycji, ustawianie lokalnych punków montowania w systemie),
* zarządzanie instalacją oprogramowania, uruchamianie i zatrzymywanie usług systemowych (z opcją umożliwiającą wybranie automatycznego startu usługi (demona) przy starcie systemu),
* instalacja i konfiguracja ustawień daty i czasu systemowego,
* konfiguracja klienta DNS w systemie,
* konfiguracja usług sieciowych: DNS, DHCP, serwer Proxy, serwer NFS, serwer pocztowy, serwer www, serwer SLP, serwer Samba, serwer TFTP, serwer NIS
* konfiguracja ustawień sieciowych (adresy IP interfejsów sieciowych, bramka, maska, DNS, serwery pośredniczące Proxy),
* zarządzanie bezpieczeństwem systemu w zakresie praw dostępu oraz dodawania użytkowników,
* konfiguracja zapory ogniowej (firewall),
* backup i odtwarzanie pełnego systemu operacyjnego,
* konfiguracja maszyn wirtualnej XEN, KVM
* konfiguracja polityki bezpieczeństwa
* konfiguracja ustawień zarządzania energią
* zarządzanie użytkownikami i grupami
* zarządzanie poprawkami i aktualizacjami systemu
* zdalny dostęp do konsoli graficznej za pomocą protokołu RDP
* System musi posiadać wsparcie dla protokołu Open Fibre Channel over Ethernet
* System musi umożliwiać skonfigurowanie serwera iSCSI
* System powinien umożliwiać łatwe przygotowanie obrazów płyt instalacyjnych z systemem z zadaną konfiguracją – AutoYAST lub równoważne.
* System musi wspierać serwer aplikacyjny Tomcat 6 dla następujących platform: Intel/AMD x86 (32bit), AMD64/Intel64,
* Producent systemu musi oferować wsparcie dla następujących systemów plików dostepnych w systemie:
* Ext3
* XFS
* ReiserFS
* BtrFS
* OCFS2
* System powinien obsługiwać następujące systemy plików:
* Ext2 i Ext3
* ReiserFS
* XFS
* BtrFS
* OCFS2
* ISO9660 (CD-ROM)
* UDF (DVD/packet mode CDRW)
* EFS (non-ISO9660 CD-ROM, IRIX < 5.3 XFS)
* CRAMFS (compressed RAM file system)
* ROMFS (small ROM file system)
* TMPFS (RAM disk file system)
* BFS (UnixWare boot file system)
* SYSV (SCO/Xenix/Coherent)
* UFS (BSD i pochodne)
* FAT/VFAT (Microsoft DOS i Windows 9x)
* HFS (Macintosh)
* HPFS (OS/2)
* QNX4
* Minix
* System powinien posiadać interfejsy graficzne KDE i Gnome w wersjach co najmniej: KDE 4.3.x i Gnome 2.28.x,
* System powinien umożliwiać zarządzania backupem (tworzenie/odtwarzanie) całego systemu z uwzględnieniem zależności pakietów RPM za pomocą polskojęzycznej graficznej konsoli (Yast lub równoważna).
* System musi posiadać narzędzie umożliwiające centralne pobieranie poprawek przez jeden serwer, który ma dostęp do sieci Internet oraz dystrybucji tych poprawek do pozostałych serwerów, dla których jest zakupiona subskrypcja. Pozostałe serwery muszą mieć możliwość pobierania w automatyczny sposób poprawek z wydzielonego serwera bez konieczności bezpośredniej komunikacji poprzez łącza internet.
* Narzędzie zarządzania maszynami wirtualnymi umożliwiające instalowanie systemów z rodziny Windows Server 2008 SP2+ i Windows Serwer 2008R2.
* System powinien zawierać oprogramowanie mono, środowisko uruchomieniowe, w wersji co najmniej 2.6.x
* System powinien posiadać wbudowane narzędzie zabezpieczające system operacyjny przed nieautoryzowanym dostępem do systemu plików przez chronione aplikacje. Narzędzie powinno wykorzystywać profile oparte o ścieżki do wywoływanych programów
* System powinien posiadać wbudowane narzędzie Orarun służące do przygotowania i wstępnego skonfigurowania oferowanego systemu operacyjnego (ustawienia odpowiednich zmiennych systemowych oraz wymaganych kont systemowych) do instalacji bazy danych Oracle
* System powinien umożliwiać rozbudowanie go o dodatek umożliwiający budowę klastrów ze wsparciem dla 32 węzłów w ramach jednego klastra
* System powinien umożliwiać rozbudowanie go o dodatek umożliwiający budowę klastrów dla maszyn wirtualnych działających na hyperwizorze XEN lub KVM
* System powinien umożliwiać rozbudowanie go o dodatek umożliwiający budowę klastrów działających z systemem plików OCFS2 lub równoważnym
* System powinien umożliwiać rozbudowanie go o dodatek umożliwiający blokową replikację danych (Distributed Replicated Block Devices).
* System powinien umożliwiać rozbudowanie go o dodatek umożliwiający budowę usług klastrowych w oparciu o OpenAIS oraz Corosync cluster engine

Atrybuty:* *Licencjonowanie:*

*-* ***2SUV*** *(licencja obejmuje 2 fizyczne procesory i uprawnia do instalacji nieograniczonej liczby bloków wirtualnych o identyfikatorze C.OS.X86.LNX.SU)**-* ***2SLV*** *(licencja obejmuje 2 fizyczne procesory i uprawnia do instalacji bloku C.OS.X86.LNX.SU na 1 fizycznym serwerze lub 2 bloków wirtualnych o identyfikatorze C.OS.X86.LNX.SU)* |

### System operacyjny – typ 3

|  |  |
| --- | --- |
| [**Identyfikator**](#A_Identyfikator) | C.OS.X86.WIN |
| **Nazwa** | System operacyjny – typ 3 |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |
| **Charakterystyka** | System operacyjny w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie Microsoft Windows Server.*Licencja na oprogramowanie musi być przypisana:**- do każdego zainstalowanego fizycznego procesora na serwerze. Licencja musi obsłużyć, co najmniej 2 fizyczne procesory.**lub**- do każdego fizycznego rdzenia zainstalowanych procesorów na serwerze. Licencja musi obsłużyć, co najmniej 2 fizyczne rdzenie.*Serwerowy system operacyjny (SSO) typ I musi posiadać następujące, wbudowane cechy: 1. Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: a. pozwalają na zmianę rozmiaru w czasie pracy systemu, b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Graficzny interfejs użytkownika. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 20. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 21. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management). 22. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: i. Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. c. Zdalna dystrybucja oprogramowania na stacje robocze. d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiające: i. Dystrybucję certyfikatów poprzez http ii. Konsolidację CA dla wielu lasów domeny, iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. f. Szyfrowanie plików i folderów. g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i. Serwis udostępniania stron WWW. j. Wsparcie dla protokołu IP w wersji 6 (IPv6), k. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, l. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych. ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii. Obsługi 4-KB sektorów dysków. iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra. v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model) 23. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 24. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). 25. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 26. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 27. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 28. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim. Atrybuty:* + - *Licencjonowanie:*

*-* ***Server Standard*** *(uprawniające do uruchamiania serwerowego systemu operacyjnego (SSO) o identyfikatorze C.OS.X86.WIN w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego o identyfikatorze C.OS.X86.WIN za pomocą wbudowanych mechanizmów wirtualizacji);**-* ***Server Datacenter*** *(uprawniające do uruchamiania serwerowego systemu operacyjnego (SSO) o identyfikatorze C.OS.X86.WIN w środowisku fizycznym i nieograniczonej liczby wirtualnych środowisk serwerowego systemu operacyjnego o identyfikatorze C.OS.X86.WIN za pomocą wbudowanych mechanizmów wirtualizacji).* |