Dodatek nr 2

SPECYFIKACJA SPRZĘTU INFORMATYCZNEGO

Niniejszy dodatek przedstawia minimalne wymagania Zamawiającego dotyczące parametrów i ukompletowania następujących urządzeń informatycznych:
- serwer wraz z oprogramowaniem do wirtualizacji - 2 kpl.;
- macierz dyskowa z oprogramowaniem do tworzenia kopii zapasowych – 1 kpl.

Nazwę i typ urządzeń Wykonawca poda w formularzu ofertowym.

Serwer wraz z oprogramowaniem do wirtualizacji – 2 kpl.

SERWER:

Element	Minimalne wymagania
Obudowa	Typu Rack o wysokości max 2U z możliwością instalacji 8 i więcej dysków 3.5" lub 2,5" HotPlug. Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Organizator do kabli. Wyposażona w przedni panel zamykany na klucz, zabezpieczający dyski twarde przed nieuprawnionym wyjęciem z serwera.
Płyta główna	Z możliwością zainstalowania minimum dwóch procesorów ośmio, dziesięcio lub dwunasto. Musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach minimum dwuprocesorowych
Procesor	Dwa procesory minimum ośmiordzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 600 punktów w teście SPECint_rate_base2006 lub min. 72,6 punktów w teście SPECint_rate_base2017, dostępnych na stronie www.spec.org w konfiguracji dla 2 dwóch procesorów dla oferowanego rozwiązania.
Pamięć RAM	Minimum 128 GB pamięci RAM typu ECC o częstotliwości pracy minimum 2133 MHz (w konfiguracji 2x64GB). Możliwość rozbudowy pamięci do minimum 512 GB pamięci RAM. Płyta główna wyposażona w minimum 12 gniazd przeznaczonych dla pamięci RAM. Wymagane zabezpieczenia pamięci: Advanced ECC, Memory Rank Sparing, Memory Mirror.
Gniazda PCI Express	Minimum 2 wolne gniazda x16 generacji 3. Minimum 2 wolne gniazda x8 generacji 2.
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1280x1024
Wbudowane porty	2 porty USB 2.0 oraz 2 porty USB 3.0 2 porty RJ45 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym) 1 port RS232
Interfejsy sieciowe	8 portów min. Gigabit Ethernet RJ45
Kontroler dysków	Sprzętowy kontroler dyskowy, umożliwiający obsługę dysków z prędkościami transferu 3, 6, 12 Gbit/s; umożliwiający skonfigurowanie na wewnętrznej pamięci dyskowej zabezpieczeń RAID: 0, 1, 5, 6, 10, 50, 60. Wyposażony w min. 1GB pamięci cache.

Wewnętrzna pamięć masowa	Możliwość instalacji wewnętrznej pamięci masowej typu SATA, NearLine SAS, SAS, SSD. Zainstalowane trzy dyski twarde o pojemności min. 300 GB, 15K RPM. Dyski skonfigurowane w RAID5.
System diagnostyczny	Panel LCD lub LED umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o: stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Zasilacze	Dwa redundantne zasilacze o mocy maksymalnej 750W każdy, posiadające certyfikat efektywności energetycznej 80%+ Platinum.
Wentylatory	4 redundantne wentylatory
Bezpieczeństwo	Zintegrowany z płytą główną moduł TPM. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
Karta zarządzająca	Niezależna od zainstalowanego systemu operacyjnego. Zintegrowana z płytą główną lub jako dodatkowa karta rozszerzeń (dodatkowa karta nie może spowodować zmniejszenia minimalnej ilości wymaganych wolnych gniazd). Wymagana minimalną funkcjonalność: – komunikacja poprzez interfejs RJ45 – podstawowe zarzadzanie serwerem poprzez protokół IPMI 2.0, DCMI 1.5, SNMP, VLAN tagging – wbudowana diagnostyka – wbudowane narzędzia do instalacji systemów operacyjnych – dostęp poprzez interfejs graficzny Web karty oraz z linii poleceń – monitorowanie temperatury oraz zużycia energii przez serwer w czasie rzeczywistym – lokalna oraz zdalna konfiguracja serwera – wsparcie dla IPv4 i IPv6
System operacyjny	System MS Windows Server 2016 Standard lub równoważny spełniający wymagania serwera. W przypadku dostawy systemu operacyjnego wymagającego dodatkowo licencji dostępowych, wymagane jest dostarczenia razem z systemem tych licencji zapewniających jednoczesny dostęp do systemu dla min. 100 użytkowników.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklarację CE. W przypadku dostarczenia systemu operacyjnego firmy Microsoft oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016.
Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub jeżeli dokumentacja nie występuje w języku polskim w języku angielskim.

OPROGRAMOWANIE DO WIRTUALIZACJI:

Licencjonowanie:

1. Licencje muszą umożliwiać uruchamianie wirtualizacji na dwóch serwerach fizycznych każdy o łącznej liczbie dwóch procesorów (liczba rdzeni równa liczbie rdzeni dostarczonego serwera) oraz jednej konsoli do zarządzania całym środowiskiem.
2. Zamawiający nie przewiduje rozbudowa infrastruktury ponad tę liczbę.
3. Licencje muszą być bezterminowe.
4. Zamawiający nie dopuszcza licencjonowania na zasadzie abonamentu.

Konsolidacja:

1. Warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym i nie może być częścią innego systemu operacyjnego (hypervisor typu 1).
2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym.
3. Rozwiązanie musi zapewniać współpracę z dostarczoną macierzą dyskową.
4. Wymagana jest możliwość przydzielenia maszynie wirtualnej większej ilości pamięci operacyjnej niż jest zainstalowana w serwerze fizycznym oraz większej ilości przestrzeni dyskowej niż jest fizycznie dostępna.
5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do min. 128 GB pamięci operacyjnej.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość przydzielenia maszynom wirtualnym min. 16 procesorów wirtualnych.
7. Oprogramowanie do wirtualizacji musi zapewnić możliwość przydzielenia min. 4 wirtualnych kart sieciowych dla każdej z maszyn wirtualnych.
8. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
9. Rozwiązanie musi umożliwiać uruchomienie wirtualnych maszyn z następującymi systemami operacyjnymi:
   1) MS Windows 10, MS Windows 8.x, MS Windows 7, MS Windows XP, MS Windows Server 2003 / 2008 / 2008 R2 / 2012 / 2016, Debian 9, Ubuntu 7;
   2) systemy operacyjne dostarczone w ramach niniejszego zamówienia.
10. Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania środowiskiem maszyn wirtualnych. Konsola graficzna powinna być dostępna poprzez dedykowanego klienta i/lub za pomocą przeglądarek, minimum Firefox.
11. 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*.
12. Rozwiązanie musi umożliwiać składowanie logów ze wszystkich serwerów fizycznych i konsoli zarządzającej na serwerze *Syslog*. Serwer *Syslog* w dowolnej implementacji musi stanowić integralną część rozwiązania.
13. Rozwiązanie musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej i zdefiniowania alertów informujących o przekroczeniu wartości progowych.
14. Rozwiązanie powinno umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji.
15. Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie. Kopie zapasowe powinny być składowane z wykorzystaniem dostarczonej macierzy. Rozwiązanie musi zapewniać 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.
16. Mechanizm zapewniający kopie zapasowe powinien być wyposażony w system cyklicznej kontroli integralności danych.
17. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania maszyn wirtualnych wraz z ich pełną konfiguracją i danymi.

18. Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, Open LDAP.
19. Platforma wirtualizacyjna musi umożliwiać wykorzystanie wszystkich dostępnych (dostarczonych) ilości rdzeni procesorów w serwerach fizycznych.
20. Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.
21. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
22. Rozwiązanie musi umożliwiać wykorzystanie technologii 10 GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi.
23. Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej, w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową.
24. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.

<u>Wysoka dostępność</u>

1. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, pamięciami masowymi niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi rodzajami wirtualnych przełączników sieciowych.
2. Należy zapewnić odpowiednią redundancję zasobów tak by w przypadku awarii jednego serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na drugi serwer infrastruktury.
3. Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury.
4. Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to poprawki bezpieczeństwa.
5. 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.
6. Rozwiązanie musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie dwóch procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii jednego z serwerów fizycznych, bez utraty i dostępności danych.

<u>Równoważenie obciążenia i przestoje serwisowe</u>

1. Na czas planowanego przestoju usług, związanego z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy) musi być zapewniona możliwość przenoszenia usług pomiędzy serwerami fizycznymi, wolumenami dyskowymi bez przerywania pracy usług.

Macierz dyskowa wraz z oprogramowaniem do tworzenia kopii zapasowych (backup) – 1 kpl.

MACIERZ DYSKOWA

1. Macierz musi być wyposażona w zdwojone, redundantne moduły odpowiedzialne za obsługę zarządzanej przestrzeni dyskowej, jej konfigurację, liczenie RAID oraz obsługę protokołów.
2. Moduły obliczeniowe macierzy muszą pracować w trybie aktywny/aktywny. W przypadku awarii jednego z nich drugi musi przejąć jego pracę.
3. Macierz musi być wyposażona w co najmniej 16 GB pamięci podręcznej służącej do buforowania operacji odczytu oraz zapisu dostępne dla każdego wolumenu macierzy.
4. Urządzenie musi być wyposażone w podwójny, redundantny system zasilania.
5. Włączenie lub wyłączenie pamięci cache nie może wymagać operacji usunięcia i utworzenia na nowo wolumenów lub grup dyskowych.
6. Połączenia między dyskami a modułami obliczeniowymi macierzy musi być redundantne (do każdego dysku dwie ścieżki – po jednej z każdego modułu obliczeniowego), w technologii SAS o przepustowości, co najmniej 6 Gbit/s.
7. Macierz musi współpracować równocześnie z dyskami SAS i Near Line SAS.
8. Macierz musi być wyposażona, w co najmniej 6 dysków po 900 GB 15 tyś. RPM każdy.
9. Macierz musi pozwalać na rozbudowę do co najmniej 24 dysków twardych. Dodawanie kolejnych dysków musi odbywać się w trybie on-line.
10. Macierz musi umożliwiać równoczesną obsługę wielu poziomów RAID. Zamawiający wymaga obsługi co najmniej RAID 10, 5 i 6.
11. Macierz musi zapewniać mechanizm thin provisioning.
12. Macierz musi obsługiwać mechanizm migawek / snapshot'ów w trybie do zapisu i odczytu, wykonywanych z poziomu macierzy. Wymagane jest, aby macierz pozwalała na wykonywanie, co najmniej 90 kopii migawkowych, istniejących na niej wolumenów. Mechanizm migawek / snapshot'ów ma umożliwiać przywrócenie zawartości całego wolumenu bazując na jego migawce / snapshot'cie.
13. Przepełnienie przestrzeni dla kopii migawkowych nie może powodować błędów zapisu na przestrzeń produkcyjną.
14. Macierz musi zapewniać możliwość definiowania automatycznej polityki tworzenia kopii migawkowych z wykorzystaniem harmonogramu.
15. W przypadku odtworzenia danych z dowolnej kopii migawkowej, macierz musi pozwalać na poprawne zachowanie wcześniejszych jak i późniejszych migawek, z zachowaniem możliwości kolejnego odtworzenia danych zarówno ze wszystkich istniejących (starszych i nowszych) kopii dostępnych dla danego zasobu.
16. Macierz musi być zarządzalna z poziomu linii komend (CLI) i poprzez interfejs graficzny (GUI).
17. Macierz musi być wyposażona w co najmniej 4 porty do transmisji danych pomiędzy macierzą a serwerami, obsługujące co najmniej protokół iSCSI 1Gbit/s (RJ45) lub inne rozwiązanie umożliwiające współpracę oferowanej macierzy z oferowanymi serwerami z zachowaniem dwóch połączeń pomiędzy macierzą (po jednym na kontroler) a serwerem.
18. Każdy z kontrolerów RAID powinien posiadać dedykowane minimum 2 interfejsy RJ-45 Ethernet obsługujące połączenia z prędkością minimum 1 Gbit/s - dla

zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy.
19. Dla obsługi operacji blokowych I/O w sieci IP SAN kontrolery macierzy muszą wspierać protokoły transmisji: iSCSI 1 Gbit/s, iSCSI 10 Gbit/s.
20. Każdy kontroler macierzy musi pozwalać na konfigurację interfejsów niezbędnych dla współpracy w sieci IP SAN oraz NAS.

OPROGRAMOWANIE DO TWORZENIA KOPII ZAPASOWYCH (BACKUP):

1. Oprogramowanie backupowe musi umożliwiać tworzenie kopii zapasowych z minimum 1000 backupowanych urządzeń / systemów (serwerów, baz danych, komputerów stacjonarnych, laptopów).
2. System backupowy stworzony w oparciu o dostarczone oprogramowanie backupowe powinien umożliwiać zapis/odczyt danych na/z dostarczaną macierz dyskową - zapis/odczyt danych powinien być realizowany bezpośrednio z zabezpieczanego serwera / komputera na macierz.
3. Oprogramowanie może być zainstalowane na serwerze w postaci maszyny wirtualnej.
4. Oprogramowanie powinno umożliwiać składowanie danych backupowych
5. Oprogramowanie backupowe musi wspierać następujące systemy operacyjne: system dostarczony w ramach dostawy serwerów oraz MS Windows, Linux (Red Hat, SUSE, Debian, CentOS, Ubnutu).
6. Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) backup online następujących baz danych i aplikacji: baza danych dostarczona w ramach dostawy systemów SD i SEOD, MS Exchange, MS SQL, Oracle, MS SharePoint.
7. *[wykreślony]*
8. W przypadku zabezpieczania systemu MS Exchange 2013 musi istnieć możliwość backupu całego obrazu bazy danych i jednocześnie odtworzenia pojedynczego maila bez konieczności odtwarzania całej bazy danych.
9. W przypadku zabezpieczania systemu MS Sharepoint musi istnieć opcjonalna (licencja nie jest wymagana) możliwość odtworzenia pojedynczego elementu systemu MS Sharepoint bez konieczności odtwarzania całego środowiska SharePoint.
10. Oferowane rozwiązanie musi zabezpieczać dane MS Windows Server bez konieczności przywracania danych MS Windows Server do postaci oryginalnej.
11. Zabezpieczane serwery i komputery muszą być backupowane bezpośrednio na medium backupowe (macierz dyskowa) bez pośrednictwa jakichkolwiek innych urządzeń / serwerów. Powyższe wymaganie dotyczy to backupów lokalnych, zdalnych jak również backupu komputerów stacjonarnych i laptopów
12. Oprogramowanie backupowe musi umożliwiać:
    1) backup pojedynczych plików;
    2) backup całych systemów plików;
    3) backup baz danych w trakcie ich normalnej pracy;
    4) backup ustawień systemu operacyjnego MS Windows;
    5) backup całych obrazów maszyn wirtualnych.
13. Rozwiązanie backupowe musi być w pełni konfigurowalne z konsoli centralnej.
14. Backupy komputerów stacjonarnych czy też laptopów muszą być konfigurowalne z poziomu centralnej konsoli bez konieczności logowania się na zabezpieczaną maszynę.

15. Rozwiązanie backupowe musi mieć możliwość odtworzenia plików / baz danych na docelowa maszynę z poziomu centralnej konsoli systemu backupowego. Nie może być wymagane logowanie się na odtwarzaną maszynę celem odtworzenia danych z systemu backupowego.
16. W przypadku wyboru odtwarzania całego systemu plików dla systemów MS Windows / Linux, rozwiązanie backupowe musi automatycznie i samodzielnie porównać pliki znajdujące się w backupie i pliki znajdujące się odtwarzanej maszynie i odtworzyć tylko brakujące pliki. W przypadku wyboru odtwarzania całego dysku / całego systemu plików, rozwiązanie backupowe nie może odczytywać z medium backupowego ani przesyłać do odtwarzanej maszyny plików, które znajdowały się zarówno w backupie jak i na odtwarzanej maszynie. Rozwiązanie backupowe musi samodzielnie ustalić których plików brakuje na odtwarzanym dysku zabezpieczanej maszyny i tylko te pliki odtworzyć.
17. W celu minimalizacji ilości przesyłanych danych, oferowane rozwiązanie musi mieć możliwość przesyłania odtwarzanych danych z medium backupowego do docelowego serwera w postaci skompresowanej, tak aby odtwarzane dane były rozkompresowane na docelowym serwerze przez agenta oferowanego systemu.
18. Oferowane oprogramowanie backupowe musi wykorzystywać technologię bazującą na podziale danych (plików, baz danych, obrazów maszyn wirtualnych) na bloki o zmiennej długości. System musi się dopasowywać do struktury dokumentu zapewniając podział na bloki o różnej długości w ramach pojedynczego dokumentu. Podział na bloki musi następować bezpośrednio na zabezpieczanym serwerze.
19. Każdy backupowany dokument w trakcie pojedynczej sesji powinien być dzielony na bloki o zmiennej długości nie większej niż 256KB.
20. Oprogramowanie backupowe musi backupować (przesyłać do serwera backupu) tylko unikalne bloki nie znajdujące się na docelowym urządzeniu, skracając czas backupu, obciążenie procesora i zmniejszając ruch w sieci LAN.
21. Oprogramowanie backupowe nie może odczytywać tych plików z systemu dyskowego, które się nie zmieniły w stosunku do ostatniego backupu. Raz zbackupowany plik nie może być nigdy więcej odczytany chyba, że zmieni się jego zawartość.
22. Oprogramowanie backupowe musi wykonywać zawsze tylko logicznie pełne backupy systemu plików. Z zabezpieczanego systemu plików muszą być odczytywane i zapisywane tylko nowe lub zmienione pliki, natomiast sam backup musi być logicznie pełnym backupem. W wewnętrznej strukturze musi być przechowywana informacja o każdym backupie i należących do niego danych (blokach). Odtworzenie jakichkolwiek danych plikowych musi być pojedynczym zadaniem identycznym z odtworzeniem danych z pełnego backupu.
23. W konsoli oprogramowania backupowego musi być możliwość definiowania ważności danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy musza być automatycznie usunięte.
24. Oferowanie oprogramowanie backupowe musi mieć możliwość tworzenia z poziomu GUI (konsoli graficznej) polityk typu dziadek – ojciec –syn, to znaczy utworzenia polityki w której zdefiniowano:
    1) czas przechowywania backupów dziennych;
    2) czas przechowywania backupów tygodniowych;
    3) czas przechowywania backupów miesięcznych;
    4) czas przechowywania backupów rocznych.

25. Oferowane rozwiązanie musi umożliwiać tworzenie wykluczeń, czyli elementów nie podlegających backupowi w ramach zadania backupowego. Musi istnieć możliwość tworzenia wykluczeń dla dowolnej kombinacji następujących elementów:
    1) wybranych typów plików, np. dla plików z rozszerzeniem pdf;
    2) dla całych katalogów (np.: c:\windows);
    3) dla pojedynczych plików.
26. Oferowane rozwiązanie musi mieć możliwość zdefiniowania aby ostatni backup dowolnego zbioru danych nigdy się nie przeterminował. Oznacza to, że jeśli dany zasób nie jest backupowany to automatycznie ostatnie ważny backup tego zasobu jest trzymany bezterminowo. Jedynie administrator może zdecydować o jego usunięciu.
27. Konsola zarządzająca systemem backupowym musi integrować się z Active Directory. Musi być możliwość przydzielania użytkownikom i grupom Active Directory dostępnych ról (min. administrator, monitoring, tylko wykonywanie odtworzeń) w systemie backupowym.
28. Konsola musi udostępniać raporty dotyczące zajętości przestrzeni przeznaczonej na backupy.
29. Bloki przesyłane z zabezpieczanych serwerów do macierzy muszą być kompresowane i szyfrowane algorytmem z kluczem minimum 256-bitowym.
30. Musi istnieć możliwość szyfrowania danych na medium dyskowym przechowującym backupy. Ewentualna licencja szyfrowania musi być dostarczona w ramach postępowania.
31. Wymagana jest autentykacja komunikacji między klientem a serwerem backupu oparta na certyfikatach.
32. Oprogramowanie backupowe musi pozwalać na odtwarzanie danych poprzez:
    1) wybór odtwarzanych danych;
    2) odtworzenie danych w jednym kroku.
33. Oprogramowanie backupowe musi mieć możliwość limitowania wielkości zadania backupowego. Jeśli zadanie backupowe przekroczy zdefiniowaną wielkość wówczas nie może być zapisane w systemie backupowym.
34. Oprogramowanie backupowe musi umożliwiać ograniczenie mocy procesora używanej do wykonywania zdania backupu, tak by odpowiednią moc procesora zostawić dla innych zadań.
35. Rozwiązanie backupowe musi wspierać backup i odtwarzanie maszyn wirtualnych. Oprogramowanie backupowe musi umożliwiać dla dostarczonego środowiska wirtualizacji następujące typy backupu:
    1) backup całych maszyn wirtualnych;
    2) backup pojedynczych, wybranych dysków maszyny wirtualnej (musi istnieć możliwość zastosowania wyrażeń regularnych do określenia które wirtualne dyski mają być backupowane);
    3) w trakcie backupu odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn.
36. Oferowany system musi pozwalać na szybkie odtworzenie:
    1) całych obrazów maszyn wirtualnych;
    2) pojedynczych dysków maszyny wirtualnej z backupu całej maszyny wirtualnej.
37. Rozwiązanie backupowe musi umożliwiać odtworzenie obrazów maszyn wirtualnych dostarczając następujące funkcjonalności:

1) przy odtwarzaniu całych maszyn wirtualnych odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu;
2) przy odtwarzaniu pojedynczych dysków maszyn wirtualnych odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu;
3) odtwarzanie pojedynczych plików z backupu obrazu maszyny wirtualnej nie wymaga konieczności odtworzenia całej maszyny wirtualnej (funkcjonalność musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym MS Windows oraz Linux);
4) możliwość zamontowania na dowolnym serwerze (fizycznym lub wirtualnym) zbackupowanych obrazów maszyn wirtualnych MS Windows (wirtualnych dysków maszyny wirtualnej MS Windows). Powyższa metoda nie może fizycznie odtwarzać backupów a jedynie pozwalać na przeglądanie zawartości wirtualnych dysków twardych w backupie z poziomu Eksploratora Plików MS Windows na dowolnej maszynie. Powyższe metody odtworzenia muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend.

38. Oprogramowanie backupowe musi mieć możliwość prezentacji (bez konieczności odtworzenia) zbackupowanych obrazów maszyn wirtualnych jako katalogów na maszynie fizycznej w celu ich przeszukiwania (wymagane przeszukiwanie po nazwach plików jak również zawartości plików) z poziomu systemu operacyjnego maszyny fizycznej.
39. Oprogramowanie backupowe musi mieć możliwość automatycznego sprawdzania (weryfikacji) zbackupowanych maszyn wirtualnych. Musi istnieć możliwość ustawienia kalendarza weryfikacji maszyn wirtualnych. Weryfikacja maszyn wirtualnych musi zapewniać minimum:
    1) odtworzenie maszyny wirtualnej;
    2) weryfikacja podstawowych procesów;
    3) możliwość dołączenia własnego skryptu weryfikującego wybrane elementy maszyny wirtualnej;
    4) informacja w konsoli systemu backupu o poprawnej / niepoprawnej weryfikacji maszyny wirtualnej.
40. Właściciel (administrator) danej maszyny wirtualnej musi mieć możliwość samodzielnego (bez konieczności kontaktu z administratorem backupu czy też administratorem) odtworzenia pojedynczych plików z dowolnego backupu obrazu jego maszyny wirtualnej.
41. Oprogramowanie backupowe musi zawsze przechowywać pełne backupy obrazów maszyn wirtualnych dla każdej wykonanej w przeszłości kopii zapasowej. Każdy backup obrazu maszyny wirtualnej musi być backupem pełnym.
42. Backup oraz odtworzenie maszyn wirtualnych musi być możliwy z poziomu graficznego interfejsu oraz linii komend.
43. Dla odtwarzania danych z interfejsu końcowego użytkownika muszą być dostarczone następujące funkcjonalności:
    1) wyszukiwanie pliku do odtwarzania po nazwie / części nazwy pliku;
    2) wybór wersji odtwarzanego pliku / katalogu.
44. W przypadku odtwarzania istniejącego systemu plików (systemu plików, który utracił część zasobów) oprogramowanie backupowe musi samo, automatycznie sprawdzać, których plików znajdujących się w backupie brakuje na odtwarzanej

maszynie, a następnie odczytywać z backupu i przesyłać tylko te pliki, które znajdują się w backupie, a których brakuje na odtwarzanej maszynie.

45. System musi umożliwiać backup serwerów NAS z następującymi funkcjonalnościami:
    1) w trakcie backupu z systemu NAS muszą być wysyłane do medium backupowego tylko zmienione pliki od ostatniego backupu;
    2) w przypadku odtwarzania, uprawnienia użytkowników również są odtwarzane;
    3) *[wykreślony]*
46. System backupu musi mieć możliwość instalacji agentów. Musi istnieć możliwość automatyzacji instalacji agentów poprzez uruchomienie skryptu instalującego agenta na zabezpieczanej maszynie.

46a. System backupu musi umożliwiać przyporządkowanie zabezpieczanej maszyny do określonej polityki backupowej z serwera zarządzania w sposób automatyczny (poprzez uruchomienie odpowiedniego skryptu) lub ręczny (poprzez przypisanie komputera do określonej grupy w konsoli zarządzającej).

47. System backupu musi umożliwiać aktualizację oprogramowania poprzez pobieranie i instalowanie nowych wersji od producenta w sposób automatyczny lub ręczny z konsoli centralnej systemu (po powiadomieniu i zatwierdzeniu aktualizacji przez operatora systemu).
48. System backupu musi umożliwiać aktualizację oprogramowania agentów, wykonywaną bezpośrednio z serwera backupu w sposób automatyczny lub ręczny z konsoli centralnej systemu (po powiadomieniu i zatwierdzeniu aktualizacji przez operatora systemu).