**Załącznik numer 11 do OPZ - System zarządzania infrastrukturą sprzętową**

# Specyfikacja systemów zarządzania infrastrukturą

## Wymagania podstawowe

### Pełna kompatybilność wymaganych funkcjonalności z oferowanymi urządzeniami.

### Zamawiający wymaga dostarczenia jednego systemu zarządzania infrastrukturą, umożliwiającego zarządzanie infrastrukturą z jednego centralnego punktu.

### W przypadku oferowania urządzeń od różnych producentów, lub gdy jeden producent więcej niż jednej grupy produktowej nie oferuje jednego systemu zarządzania obejmującego te grupy produktowe, to Zamawiający za równoważne uzna dostarczenie oddzielnych systemów zarządzania infrastrukturą dla danej grupy produktowej, umożliwiające spójne, centralne zarządzanie wszystkimi urządzeniami z danej grupy produktowej spełniające wymagania podstawowe oraz wymagania danej grupy produktowej.

### Systemem zarządzania należy objąć wszystkie dostarczane macierze, serwery, urządzenia sieciowe.

### Dostarczone licencje oprogramowania do zarządzania urządzeniami muszą być bezterminowe.

### Wymagana jest architektura serwer klient z dostępem do systemu przez przeglądarkę. internetową.

### Wymagana jest obsługa lokalnej bazy administratorów systemu. Nie jest akceptowalne rozwiązanie wymuszające stosowanie systemu scentralizowanych usług katalogowych.

### Logowanie do systemu zarządzania musi być wyposażone w mechanizm czasowego blokowania możliwości logowania użytkownika do systemu uruchamiany po kilkukrotnej nieudanej próbie zalogowania (liczba prób definiowana przez Administratora).

### Możliwość stworzenia kopii zapasowej danych systemu zarządzania i odtworzenia tych danych z kopii.

### W przypadku, gdy system zarządzania korzysta z systemu licencjonowania, to należy dostarczyć wystraczającą ilość licencji dla wszystkich dostarczonych urządzeń danej grupy produktowej, której dotyczy system zarządzania oraz powinna być zapewniona możliwość sprawdzenia licencji oraz łatwej zmiany licencji.

### Wymagany interfejs użytkownika w języku polskim lub angielskim.

### Dokumentacja związana z systemem zarządzania musi być dostępna w języku polskim lub angielskim.

### Możliwość automatycznego alarmowania opartego o zadane progi alarmowe.

### Możliwość określenia listy osób i grup osób powiadamianych przy poszczególnych poziomach alertów.

### Możliwość wykorzystania różnych kanałów powiadamiania dla poszczególnych poziomów alertów (w tym konsola operatora, e-mail).

### Zapisywanie informacji o czynnościach wykonanych przez użytkowników systemu.

### Możliwość przeszukiwania dziennika czynności pod kątem użytkownika, adresu IP, z którego nastąpiło logowanie, czasu i rodzaju czynności.

### Zapisywanie informacji o zdarzeniach systemowych.

### Możliwość przeszukiwania dziennika zdarzeń systemowych pod kątem czasu i rodzaju zdarzenia.

### Podstawowe zarządzanie wszelkimi urządzeniami zgodnymi z protokołem SNMP.

### Możliwość ręcznego dodania urządzenia na przykład poprzez podanie jego adresu IP, parametrów SNMP, SSH lub telnet.

### Automatyczne wyszukiwanie i dodawanie urządzeń w ramach zdefiniowanego zakresu adresów IP.

### Możliwość importowania listy urządzeń z pliku.

### Możliwość podglądu podstawowych informacji o urządzeniu.

### Możliwość wizualizacji panelu czołowego urządzenia.

### Możliwość wyświetlenia listy interfejsów urządzenia i włączenia/wyłączenia poszczególnych interfejsów.

### Wyświetlanie adresu IP urządzenia.

### Możliwość zdefiniowania parametrów SNMP, SSH lub telnet dla danego urządzenia.

### Zbieranie alarmów i zdarzeń w dzienniku zdarzeń.

### Możliwość wyświetlenia informacji o alarmach, nazwy, źródła, poziomu alarmu, czasu wystąpienia.

### Możliwość potwierdzenia alarmu przez użytkownika, możliwość wyłączenia alarmu.

### Możliwość eksportu danych o alarmach do pliku.

### Możliwość wyświetlenia historii alarmów zawierającej nazwę alarmu, jego źródło, poziom, status i czas wygenerowania. Możliwość filtrowania wyświetlanej listy przy pomocy powyżej podanych parametrów.

### Możliwość podejrzenia alarmów wygenerowanych na podstawie kilku innych alarmów z tego samego źródła.

### Możliwość zdefiniowania reguł ignorowania alarmów.

### Możliwość generowania powiadomienia o alarmach w postaci email.

### Możliwość zdefiniowania reguł powiadamiania.

### Monitorowanie obciążenia procesora i zajętości pamięci urządzenia, stanu dostępności urządzenia i opóźnienia.

### Możliwość monitorowania informacji o przesyłanym przez urządzenie ruchu.

### Możliwość generowania alarmu w przypadku przekroczenia zdefiniowanych wartości.

### Możliwość przechowywania historycznych danych wydajnościowych z ostatnich 30 dni.

### Możliwość obrazowania danych historycznych na wykresach.

### Możliwość eksportu danych historycznych do pliku.

## System zarządzania macierzami

### Jednolite zarządzanie dostarczanymi macierzami poprzez interfejs graficzny.

### Interfejs graficzny zapewniający intuicyjny widok mapowań między fizycznymi i logicznymi składnikami macierzy dyskowych.

### Ułatwienie lokalizowania usterek i diagnozowania stanu systemów dyskowych.

### System pokazuje logiczny związek pomiędzy:

#### portami frontowymi połączonymi z hostami a kontrolerami,

#### grupami RAID,

#### wolumenami logicznymi i dyskami.

### Analiza stanu działania urządzenia pamięci masowej począwszy od obciążenia, nieprawidłowości działania i sytuacji alarmowych do oceny ogólnego stanu urządzeń. W szczególności możliwość wykrycia z wyprzedzeniem sytuacji typu „wąskie gardło” wydajności systemu.

### Zarządzanie zużyciem pojemności macierzy dyskowych:

#### w obszarze całego systemu pamięci masowej,

#### dysków i wolumenów logicznych.

### System umożliwia wyświetlenia informacji o pojemności powyższych całego systemu pamięci masowej, dysków i wolumenów logicznych.

### Centralna analiza informacji dotyczących pojemności urządzeń i udostępnianie statystyki dotyczące wydajności i pojemności w tym prognozy trendów.

### Możliwość analizy użycia pojemności z okresu jednego tygodnia, dwóch tygodni, trzech tygodni i jednego miesiąca.

### Zarządzanie wydajnością hostów składające się ze:

#### statystyk hostów,

#### podsumowania wydajności i prognozy trendu wydajności.

### Statystyki hostów wyświetlają listę wszystkich dostępnych hostów oraz pokazują aktualne wykorzystanie pojemności i prognozę wykorzystania pojemności w ciągu najbliższych miesięcy.

### Podsumowanie wydajności wskazujące zużytą pojemność i przydzieloną pojemność hostów i systemów plików.

### Prognoza trendu pojemności przewiduje trend wykorzystania pojemności w ciągu najbliższych miesięcy.

### Powinna istnieć możliwość zarządzania wewnętrznymi mechanizmami macierzy dyskowych, w szczególności co najmniej tworzenie wolumenów logicznych (LUN) i mapowanie ich do hostów, w tym dla wielu urządzeń w grupie, zapewniając jednorodną alokację zasobów i zarządzanie większą liczbą macierzy dyskowych.

### System powinien umożliwiać zarządzanie poprzez interfejs graficzny jak również z wykorzystaniem skryptów.

### System powinien dawać możliwość tworzenia zadań administracyjnych i szablonów ułatwiających zarządzanie i powtarzalność procesów konfiguracji oraz zarządzania.

## System zarządzania serwerami

### System umożliwia scentralizowane zarządzanie dużą ilością serwerów (w tym wszystkimi dostarczonymi w ramach przetargu), w tym monitorowanie stanu serwerów i ich alertów, analizę wydajności oraz zadania administracyjne opisane poniżej.

### Wyświetlanie podstawowych informacje o serwerze.

### Podsumowanie udostępniające podstawowe informacje o serwerze i jego stanie.

### Wizualizację serwera oraz listę komponentów z możliwością rozwijania poszczególnych elementów i uzyskania bardziej szczegółowych informacji o poszczególnych podzespołach, ich wizualizację i stan działania

### Monitorowanie alarmów, centralne zarządzanie alarmami wszystkich zarządzanych urządzeń, raportowanie alarmów, kwerendy i przetwarzanie powiadomień.

### Zbieranie wskaźników wydajności serwerów w czasie rzeczywistym i danych historycznych, w tym:

#### wskaźniki zużycia energii,

#### wykorzystanie procesora,

#### wykorzystanie pamięci,

#### utylizacja dysków,

#### temperatura powietrza chłodzącego serwery.

### Automatyczne zarządzanie bazą wersji i aktualizacją firmware serwerów.

### Funkcja zarządzania bazą danych firmware umożliwia konfigurowanie podstawowego pakietu firmware dla serwerów w sposób ręczny lub automatycznie poprzez synchronizację pakietu z bazą dostawcy serwerów.

### Automatyczne sprawdzanie firmware porównuje wersje pakietów w lokalnej paczce bazowej do dostępnych wersji w bazie producenta serwerów.

### Umożliwienie pobrania wybranych najnowszych paczek.

### Pobrane paczki powinny być dystrybuowane do poszczególnych serwerów na zasadzie definiowanych zadań, z możliwością wybrania zakresu instalacji i czasu realizacji zadania.

## System zarządzania przełącznikami

### Wymagania podstawowe

#### Pełna kompatybilność wymaganych funkcjonalności z oferowanymi urządzeniami typu przełączniki typ A i B.

#### Obsługa minimum 100 przełączników.

#### Możliwość rozbudowy systemu do minimum 1000 urządzeń.

### Zarządzanie alertami

#### Możliwość automatycznego alarmowania opartego o zadane progi alarmowe, w tym:

##### Możliwość definiowania dwóch progów – ostrzegawczy i alarmowy,

##### Możliwość automatycznego alarmowania opartego o profil ruchu,

#### Możliwość automatycznego alarmowania o przekroczeniu obciążenia interfejsu z uwzględnieniem dwóch progów - ostrzegawczy i alarmowy,

### Zarządzanie urządzeniami

#### Możliwość wyświetlenia listy interfejsów urządzenia i włączenia/wyłączenia poszczególnych interfejsów.

#### Możliwość przeprowadzenia testów ping i traceroute dla wybranego urządzenia.

#### Zapewnienie skrótu do wyświetlenia list alarmów i konfiguracji urządzenia.

#### Możliwość zdefiniowania skrótów do funkcji dla urządzeń nieznanych producentów.

#### Możliwość zdefiniowania skrótów funkcyjnych skojarzonych z nowym typem urządzenia.

#### Możliwość definiowania nowych typów alarmów nierozpoznawanych domyślnie przez system zarządzania.

#### Możliwość zdefiniowania podstawowych informacji o dowolnym producencie urządzeń w celu ułatwienia definiowania nowych elementów sieciowych nieobsługiwanych domyślnie przez system zarządzania.

#### Możliwość dodawania, kasowania i modyfikacji nowych typów urządzeń.

#### Możliwość określenia ikony reprezentującej urządzenie w systemie.

#### Możliwość definiowania nowych typów liczników danych, ich nazwy, funkcji obliczającej wartość licznika i rodzajów urządzeń, dla których dany licznik może zostać zastosowany.

#### Możliwość tworzenia kopii zapasowych konfiguracji urządzeń oraz odtwarzania zapisanej konfiguracji.

#### Możliwość definiowania wyglądu panelu urządzenia przy użyciu rysunków urządzenia, modułów i portów.

### Topologia sieci

#### Wyświetlanie topologii sieci z urządzeniami i łączami pomiędzy nimi.

#### Możliwość powiększania i zmniejszania widoku topologii.

#### Obrazowanie statusu dostępności urządzeń i łączy.

#### Możliwość zdefiniowania obrazu tła dla mapy topologii sieci.

#### Możliwość zdefiniowania różnych lokalizacji na mapie sieci.

### Zarządzanie łączami.

#### Automatyczne wyszukiwanie łączy przy wykorzystaniu informacji dostępu z protokołu LLDP oraz z adresacji IP.

### Raportowanie

#### Możliwość generowania raportów na temat urządzeń, modułów, portów i łączy oraz statystyk nt. rodzajów urządzeń.

#### Możliwość generowania raportów wydajnościowych dotyczących urządzeń oraz ich interfejsów.

#### Możliwość tworzenia, wyświetlania, edytowania i kasowania zadań raportowych.

#### Możliwość udostępnienia raportów użytkownikom do podglądu oraz do eksportu do pliku.

#### Możliwość automatycznego generowania raportów w cyklach: dziennym, tygodniowym, miesięcznym, kwartalnym, półrocznym i rocznym.

#### Możliwość generowania raportów w formatach PDF.

#### Możliwość generowania raportów w formatach Excel, Word użytkowanych przez Zamawiającego.

#### Zarządzanie konfiguracjami

#### Możliwość automatycznego wykonywania w określonym czasie kopii zapasowych konfiguracji urządzeń w trybie dziennym, tygodniowym i miesięcznym.

#### Możliwość podglądu i porównania różnych wersji plików konfiguracyjnych, w tym z aktualną konfiguracją urządzenia.

#### Konfigurowanie wielu urządzeń.

#### Możliwość konfiguracji urządzeń, w tym list kontroli dostępu, ustawień QoS, VLAN, poprzez wysłanie szablonów konfiguracyjnych do wielu urządzeń.

#### Możliwość definiowania ww. szablonów konfiguracyjnych.

#### System powinien zostać dostarczony w postaci dedykowanej platformy programowej dla środowiska wirtualnego opisanego w załączniku numer 8 do OPZ wraz z systemem operacyjnym i bazą danych, jeśli taka jest wymagana.

## System zarządzania firewallami

### Architektura systemu

#### System centralnego zarządzania powinien stanowić centralny punkt, w którym definiowana jest polityka bezpieczeństwa dla całej implementowanej infrastruktury bezpieczeństwa obejmującej urządzenia sieciowe.

#### System powinien zostać dostarczony w postaci dedykowanej platformy programowej dla środowiska wirtualnego opisanego w załączniku numer 8 do OPZ wraz z systemem operacyjnym i bazą danych, jeśli taka jest wymagana.

### System operacyjny

#### Dla zapewnienia wysokiej sprawności i skuteczności działania systemu system musi pracować w oparciu o system operacyjny wzmocniony z punktu widzenia bezpieczeństwa zgodnie z zaleceniami producentów i dobrymi praktykami.

#### W przypadku stosowania komercyjnych systemów operacyjnych ogólnego przeznaczenia należy je dostarczyć wraz z bezterminowymi licencjami oraz usługą wsparcia producenta. Ilość licencji musi być zgodna z polityką licencyjną producenta i umożliwiać instalację w dostarczanej infrastrukturze.

### Parametry fizyczne systemu

#### Zarzadzanie co najmniej 150. urządzeniami fizycznymi lub wirtualnymi.

#### Obsługa wirtualnej powierzchni dyskowej o pojemności minimum 1 TB.

#### W zakresie logowania – analizę min 1 GB logów dziennie

#### Interfejs zarządzania poprzez szyfrowane połączenie HTTPS, SSH.

### Funkcjonalności podstawowe i uzupełniające

#### Konfigurację wszystkich funkcji składowych firewalli.

#### Przechowywanie i implementację polityk bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej

#### Wersjonowanie polityk w taki sposób aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości

#### Zarządzanie wersjami firmware’u na urządzeniach oraz zdalne uaktualnienia

#### Zarządzenie wersjami baz sygnatur na urządzeniach oraz zdalne uaktualnienia

#### Monitorowanie w czasie rzeczywistym stanu urządzeń (użycie CPU, RAM)

#### Zapis i zdalne wykonywanie skryptów na urządzeniach

#### Automatyzacię procesu konfiguracji struktur VPN typu hub-and-spoke oraz full-mash

#### Logowanie zdarzeń z systemów bezpieczeństwa

#### System powinien udostępniać zestaw predefiniowanych raportów