Zamówienie podstawowe Nr postępowania: ZP248//055/D/21

Załącznik nr 5 do SWZ

Zadaniem systemu monitoringu jest monitoring routerów, przełączników, modemów i innych urządzeń aktywnych w sieci Zamawiającego wraz z zarządzaniem

Minimalne wymagania dla systemu monitoringu i zarządzania siecią:

1. Dostarczone oprogramowanie monitorowania i zarządzania powinno być obsługiwane z jednej platformy systemowej, dostarczonej przez jednego producenta.
2. Celem systemu jest:
    - natychmiastowe powiadamianie obsługi o anomaliach pracy infrastruktury sieci;
    - umożliwienie szybkiej reakcji obsługi w przypadku sytuacji awaryjnych;
    - uzyskanie pełnego i dokładnego wglądu w pracę urządzeń;
    - dokładna diagnostyka problemów;
    - podniesienie jakości obsługi użytkowników;
3. Interfejs graficzny systemu powinien prezentować sieć w postaci mapy z wyszczególnionymi lokalizacjami.
4. Schemat sieci powinien mieć strukturę hierarchiczną: po wybraniu (kliknięciu) lokalizacji powinien otwierać się widok lokalizacji z podsieciami grupami monitorowanych urządzeń, Kolejny wybór grupy urządzeń powinien otwierać widok z urządzeniami i połączeniami między nimi. Postępowanie powinno prowadzić do najgłębszego w hierarchii widoku lokalizacji.
5. System powinien testować dostępność adresów IP i urządzeń tworzących infrastrukturę sieciową w regularnych odstępach czasu.
6. Testowanie powinno odbywać się z częstotliwością co najmniej raz na minutę, przy czym system powinien umożliwiać konfigurowanie różnych częstotliwości testów dla różnych urządzeń. W przypadku niedostępności adresu IP urządzenia przez zadany okres czasu, system powinien powiadamiać użytkownika o tym fakcie.
7. Ze wszystkich urządzeń, które umożliwiają zarządzanie z wykorzystaniem protokołu SNMP, system powinien zbierać dane potrzebne do zarządzania urządzeniami. Użytkownik powinien mieć możliwość określenia częstotliwości i rodzaju zbieranych danych indywidualnie dla poszczególnych urządzeń.
8. System powinien gromadzić te dane w swojej bazie danych przez co najmniej 1 rok. Administrator powinien mieć możliwość przeglądania tych danych (w postaci wykresów lub tabel) z ostatnich 24 godziny, ostatniego tygodnia lub ustalonego innego okres czasu.
9. Wymagane jest zbieranie następujących danych:
    - obciążenie procesorów;
    - zajętość pamięci;
    - zajętość twardych dysków;
    - utylizacja interfejsów w bit/s oraz % pasma;
    - liczba błędów na interfejsach;
    - stany interfejsów (włączony / wyłączony);
    - temperatury.
10. System powinien zbierać również dane specyficzne dla urządzenia, inne niż wymienione w punkcie poprzedzającym, udostępniane z wykorzystaniem protokołu SNMP.
11. W przypadku urządzenia posiadającego własną bazę MIB, przechowującą wyżej wymienione dane, powinna istnieć możliwość wczytania do systemu opisu bazy danych w formie pliku

tekstowego (ułatwienie użytkownikowi wyselekcjonowania informacji, które mają być udostępniane).

12. Rozwiązanie musi być bezagentowe (brak dodatkowego oprogramowania agenta na urządzeniach) oraz rozwiązanie dostarczone z licencją umożlwiającą monitorowania dowolnej ilości interfejsów i urządzeń
13. Zbierane dane powinny być udostępniane w postaci wykresów, tabel, wskaźników, paneli alarmowych itp., umożliwiających ich czytelną prezentację w osobnych oknach na oddzielnych monitorach.
14. System powinien umożliwiać łatwe tworzenie list urządzeń, dla których zbierane dane przyjmują największe wartości, np. najbardziej zutylizowane interfejsy, najbardziej obciążone procesory itp.
15. System powinien umożliwiać łatwe tworzenie grup urządzeń i monitorowanych obiektów oraz umożliwiać przypisywanie uprawnień administratorom lub grupom administratorów to pogrupowanych urządzeń i monitorowanych obiektów.
16. System powinien umożliwiać konfigurowanie hierarchii zależności typu rodzic dziecko ang. parent child dla grup i monitorowanych obiektów.
17. System powinien umożliwiać konfigurowanie alarmów z uwzględnieniem logicznych zależności hierarchii rodzic dziecko i np. dla niedostępności obiektu rodzic zgłaszać tylko jeden alarm dla obiektu rodzic z wyłączeniem niedostępności obiektów zależnych typu dziecko.
18. Interfejs graficzny systemu powinien umożliwiać tworzenie osobnych widoków prezentujących stany pracy urządzeń w postaci:
    - wykresów;
    - tabel ze szczegółowymi wartościami danych dostarczanych przez urządzenia;
    - symboli: stan normalny / stan ostrzegawczy / stan alarmowy;
    - graficznych wskaźników danych analogowych (np. CPU) dostarczanych przez sensory.
    - własnego menu,
19. System powinien umożliwiać zdefiniowanie wartości progowych , z którymi zbierane dane będą porównywane na bieżąco, w tym co najmniej dwóch wartości progowych odpowiadających np. stanowi ostrzegawczemu i stanowi alarmowemu. Po przekroczeniu przez daną zadanego progu system powinien automatycznie informować o tym fakcie użytkownika.
20. System powinien umożliwiać tworzenie raportów z gromadzonych danych. Raporty powinny obejmować przynajmniej następujące dane:
    - utylizację procesora;
    - zajętość pamięci;
    - utylizację interfejsów w bit/s i % pasma;
    - Błędy na interfejsach;
    - listę urządzeń wraz z informacją o producencie, numerze seryjnym, wersją oprogramowania, wielkością pamięci RAM, zainstalowanymi modułami;
    - listę urządzeń i interfejsów wraz z ich statusem, adresami IP i MAC, pasmem i dupleksem;
    - listę połączeń wraz z nazwami urządzeń i interfejsów po obu stronach łącza;
    - listę powtarzających się adresów IP wraz z nazwą urządzeń i interfejsów.
21. Administrator powinien mieć możliwość definiowania własnych raportów zawierających dane gromadzone przez system.
22. System powinien powiadamiać użytkownika o następujących zdarzeniach:
    - przekroczeniu wartości progowych danych pobieranych przez system z urządzeń w regularnych odstępach czasu;
    - pojawieniu się błędów transmisyjnych na interfejsach urządzeń sieciowych;

- nieudanych próbach zalogowania się do urządzeń sieciowych (routery, przełączniki, serwery Windows / serwery Linux);
- awariach interfejsów urządzeń sieciowych, w tym włączeniach interfejsu;
- restarcie urządzeń;
- zmianie w zasilaniu urządzenia, np. praca na jednym zasilaczu;
- braku komunikacji z urządzeniem z wykorzystaniem protokołu IP;
- braku kontaktu z urządzeniem z wykorzystaniem protokole SNMP.

23. Powiadamianie użytkownika o wyżej opisanych zdarzeniach powinno odbywać się dzięki:
    - wyróżnieniu na mapie sieci ikony reprezentującej urządzenie, którego zdarzenie dotyczy;
    - umieszczenie w logu odpowiedniej informacji;
    - zmianę symboli;
    - wysłanie wiadomości pocztą elektroniczną.
24. Wyświetlenie informacji o alarmie dotyczącym interfejsu powinno uwzględniać hierarchiczny schemat sieci:, wyróżnienie np. różnymi kolorami ikon reprezentujących urządzenie, podsieć lub grupę urządzeń na wyższych poziomach hierarchii.
25. Opisy zdarzeń zarejestrowanych w logu powinny mieć przyporządkowaną ważność (informacja, ostrzeżenie, alarm itp.) oraz być wyróżnione osobnymi kolorami. Log powinien umożliwiać filtrowania opisów (według ważności, rodzajów urządzeń itp.). Powinna istnieć możliwość zapisywania zdefiniowanych filtrów tak, by można je było szybko i łatwo aplikować. Log powinien być prezentowany w osobnym oknie z możliwością umieszczenie na osobnym ekranie.
26. System powinien umożliwiać potwierdzanie i opatrywanie komentarzami zdarzeń umieszczanych w logu oraz ukrywanie (bez usuwania) potwierdzonych zdarzeń. Użytkownik powinien mieć możliwość odraczania zdarzeń (zaznaczanie ich do późniejszej obsługi, bez usuwania z logu).
27. Wszystkie zdarzenia i alarmy powinny być gromadzone i przechowywane przez co najmniej 1 rok. Użytkownik powinien mieć możliwość przeglądania historii tych danych.
28. Interfejs graficzny systemu powinien umożliwiać umieszczanie przez użytkownika w hierarchicznej strukturze sieci własnych map zapisanych w jednym z popularnych formatów graficznych.
29. System musi umożliwiać wizualizacje Sieci LAN oraz Sieci WAN poprzez konfigurację map, na których:
    - będą umieszczane urządzenia oraz połączenia
    - kolory będą wyświetlane w zależności od dostępności lub przepustowości połączeń
    - możliwość stosowania własnych grafik/ikon
    - prezentowania statusu urządzeń (min. dostępne, niedostępne, problem)
    - prezentacje sieci w postaci mapy z wyszczególnionymi lokalizacjami.
    - umożliwiać umieszczanie przez użytkownika w hierarchicznej strukturze sieci własnych map zapisanych w jednym z popularnych formatów graficznych.
    - schemat sieci musi mieć strukturę hierarchiczną:
        i. po wybraniu (kliknięciu) lokalizacji musi otwierać się widok lokalizacji
        ii. z podsieciami/grupami monitorowanych urządzeń,
        iii. kolejny wybór grupy urządzeń musi otwierać widok z urządzeniami
        iv. i połączeniami między nimi.
        v. postępowanie powinno prowadzić do najgłębszego w hierarchii widoku lokalizacji.
30. Proces wykrywania urządzeń i topologii sieci powinien być wykonywany cyklicznie z zadaną częstotliwością i o zadanej porze, a także uruchamiany na żądanie użytkownika.

31. Interfejs graficzny systemu powinien umożliwiać powiększanie i tworzenia osobnych widoków dowolnych fragmentów sieci.
32. Powinna istnieć możliwość tworzenia zestawu okien wyświetlanych na osobnych monitorach, zawierających wyżej opisane widoki najważniejszych lokalizacji lub grup urządzeń.
33. Użytkownik systemu powinien mieć możliwość umieszczania wszystkich urządzeń, wykrytych automatycznie lub dodanych ręcznie, w hierarchicznej strukturze.
34. Urządzenia sieciowe, powinny być opatrzone przynajmniej informacjami:
    - nazwa urządzenia;
    - rodzaj urządzenia (router, przełącznik, serwer, itp.). Rodzaj urządzenia powinien być dodatkowo oznaczony odpowiednią ikoną ułatwiającą jego identyfikację;
    - dane interfejsów: adres IP, maska, nazwa, typ (GigabitEthernet, Serial, itp.) status (włączony / wyłączony), tryb pracy (dupleks, półdupleks), wynegocjowana prędkość (100 Mbit/s, 1000 Mbit/s, itp.).
35. System musi umożliwiać prezentację danych historycznych oraz umożliwiać analizowania trendów pojawiających się w infrastrukturze LAN i wykrywanie anomalii w ruchu sieciowym
36. System powinien umożliwiać jednoczesne korzystanie, przez co najmniej trzydziestu użytkowników.
37. System powinien umożliwiać tworzenie kont użytkowników z różnymi uprawnieniami do wykonywania określonych czynności.
38. Autentykacja użytkowników logujących się do systemu powinna być realizowana za pomocą lokalnie zdefiniowanych kont administratorów lub poprzez serwer AD lub RADIUS lub TACACS+.
39. Opcjonalnie system powinien mieć możliwość zbierania z urządzeń komunikatów Syslog.
40. System musi obsługiwać standardowe wartości MIB, własne oraz dostarczanych przez producentów sprzętu sieciowego.
41. System musi mieć możliwość wykonywania poleceń na monitorowanych urządzeniach
42. System musi umożliwiać definiowanie przez użytkownika alarmów wraz z progami.
43. Typy alarmów:
    - status up/down;
    - metryki interfejsu (wydajnościowe;
    - spełnianie SLA.
44. System musi posiadać funkcję zaawansowanego alarmowania polegająca na:
    - wywoływaniu alarmu przy określonych zdarzeniach
    - wywoływaniu alarmu przy długotrwałym stanie
    - wywoływaniu alarmu przy konfigurowalnej kombinacji stanów urządzeń
    - eskalowanie problemu, gdy problem nie jest rozwiązany w określonym czasie
45. System musi monitorować przepustowość sieci bazując co najmniej na protokołach Netflow v5, Netflow v9, J-Flow, IPFIX, sFlow czy NetStream
46. System powinien identyfikować aplikacje, protokoły oraz użytkowników które utylizują pasmo oraz określać ruch ingress oraz egress
47. System musi mieć możliwość wyświetlać konwersację pomiędzy dwoma wybranymi hostami
48. System musi mieć możliwość analizy historycznej komunikacji z gradacją do 1 minuty
49. System powinien być w stanie otrzymywać flowy od urządzeń nie wspierających SNMP
50. System powinien umożliwiać monitorowanie CBQoS wraz z podziałem na polityki
51. System musi wspierać klasyfikację Cisco NBAR2
52. System musi umożliwiać dodawanie kolejnych źródel flowów:
    - W sposób automatyczny, dla urządzeń już monitorowanych
    - W sposób manulany, dla urządzeń niemonitorowanych
53. System musi posiadać funkcjonalność zarządzania przestrzenią IPv4 oraz IPv6, co najmniej przez:

- automatyczne skanowanie pul adresowych na urządzeniach w celu weryfikacji statusu
- Historyczne śledzenie zmian adresacji wykrywanie i monitorowanie konfliktów adresów IP

54. System musi posiadać wbudowane alerty i alarmy zużycia puli adresów IP
55. System powinien wspierać zarządzanie DNS oraz DHCP
56. System musi wspierać serwery DHCP producentów takich jak Windows, Cisco IOS czy ISC
57. System musi mieć możliwość importu puli adresów z przygotowanego wcześniej pliku
58. System nie może być limitowany
59. Rozwiązanie musi posiadać możliwość śledzenia i lokalizowania urządzenia podłączanego do sieci na podstawie adresu IP, adresu MAC oraz nazwy hosta dla przełączników Zamawiającego
60. System może pomóc w odnajdywaniu niechcianych urządzeń w sieci Zamawiającego
61. System potrafi odnaleźć używane oraz nieużywane porty w sieci Zamawiającego.
62. Rozwiązanie może wyzwolić alarm, gdy urządzenie o konkretnej nazwie lub konkretnym adresie MAC pojawi się w sieci.
63. System zapamiętuje lokalizacje urządzeń, dzięki czemu można wyśledzić gdzie dane urządzenie było ostatnio podłączone, nawet gdy nie jest ono aktualnie widoczne w sieci.
64. System może wyświetlać listę switchy, które posiadają wszystkie, lub prawie wszystkie porty zajęte.
65. System powinien monitorować kontrolery pod kątem podpiętych punktów dostępowych.
66. System musi mieć możliwość stworzenia białej listy urządzeń, bazującej na adresach IP, MAC oraz nazwach hostów.
67. System powinien zaciągać dane VRF z urządzeń.
68. Istnieje możliwość zdalnego wyłączenia portów na przełącznikach z poziomu systemu.
69. System ma możliwość spięcia z kontrolerem domeny Active Directory, w celu śledzenia aktywności użytkowników domenowych w sieci.
70. Możliwość śledzenia podpiętych klientów VPN do Cisco ASA.
71. System ma możliwość automatycznego odkrywania portów oraz urządzeń.
72. Opcja odkrywania może być ograniczona, filtrowanie skanowanych urządzeń może bazować na VLANach, zakresie portów, statusie, typie portu, itp.
73. System nie może być ograniczony licencyjnie co do ilości monitorowanych elementów w infrastrukturze Zamawiającego
74. Rozwiązanie powinno mieć możliwość rozbudowy o dodatkowe silniki odpytujące poprzez dodanie dodatkowych serwerów i licencji zwiększających wydajność oprogramowania.
75. System musi mieć możliwość instalacji na systemach Windows Server 2016 lub nowszym.
76. Zamawiający nie dopuszcza instalacji na serwerach typu Linux/Unix.
77. System musi zostać dostarczony jako gotowy produkt ang. out of the box pochodzący od jednego producenta oraz obsługiwany musi być z jednej konsoli GUI. Nie dopuszcza się osadzania systemów innych dostawców.
78. System powinien działać bez ograniczenia co do czasu używania. Nieakceptowalne jest tutaj zaoferowania rozwiązania w modelu subskrypcyjnym.
79. System powinien być dostarczony z modułem oprogramowania do automatycznego wykrywania map sieci które mogą być eksportowane do systemu głównego (licencja na co najmniej trzy stanowiska). Moduł powinien zawierać poniższe funkcjonalności:
    1. Oprogramowanie musi posiadać możliwość wykrywania topologii sieci i tworzenia na ich podstawie diagramów sieci z wykorzystaniem minimum następujących protokołów SNMP v1, SNMP v2, SNMPv3, ICMP, CDP, LLDP, WMI

2. Możliwość eksportowania map do formatów minimum Microsoft Office Visio, PDF i PNG jak i do systemu głównego monitorowania
3. Oprogramowanie ma możliwość automatycznego wykrywania połączeń na poziomie L2 oraz L3 pomiędzy urządzeniami w sieci zamawiającego
4. Oprogramowanie musi mieć możliwość tworzenia skanowań sieci na żądanie oraz wedle ustalonego harmonogramu
5. Produkt musi mieć możliwość filtracji oraz grupowania urządzeń
6. Oprogramowanie powinno udostępniać widok analizy urządzenia, pokazujący jego porty, połączenia oraz przypisane VLANy
7. Oprogramowanie nie może być ograniczone licencyjnie co do ilości monitorowanych elementów w infrastrukturze Zamawiającego
8. Trzeba dostarczyć to oprogramowanie na 3, niezależne stanowiska administratorskie siecią

Wdrożenie powinno obejmować:

1. Instalację i konfigurację systemu monitoringu.
2. Konfigurację dostarczonych modułów.
3. Automatyzacje tworzenia map sieci z podziałem na VLANy i opcją ich ciągłego monitorowania w głównym systemie.
4. Integrację systemu ze sprzętem Junipera a w szczególności z funkcją stackowania Virtual Chassis wykrywającą poszczególne elementy stosu urządzeń z numerem seryjnym i wersją oprogramowania.
5. Stworzenie automatycznie aktualizowanego raportu zawierającego zestawienie monitorowanego sprzętu w tym nazwy, adresu IP, numeru seryjnego.
6. Integracja rozwiązania z posiadanym LDAP
7. Stworzenie kont użytkowników z ograniczeniami do zarządzania jedynie wydzielonymi urządzeniami jak i przydzieloną podsiecią w systemie IPAM z możliwością rejestracji nowych urządzeń jedynie w tej podsieci.
8. Skonfigurowanie alarmów dla kluczowych portów uplinkowych na wszystkich podłączonych przełącznikach zintegrowanych w systemie.

Wsparcie techniczne.

Dostarczony system ma być objęty wsparciem technicznym producenta przez okres 12 miesięcy obejmującym:

1. Dostęp do poprawek oraz nowych wersji oprogramowania.
2. Dostęp do pomocy technicznej w trybie 24/7 poprzez portal kliencki oraz telefon
3. Dostęp do materiałów szkoleniowych oraz szkoleń produktowych online
4. Dostęp do bazy wiedzy, dokumentacji, przewodników konfiguracyjnych
5. Dostęp do publicznego forum z możliwością zakładania wniosków o nowe funkcjonalności

Zamówienie objęte prawem opcji:

Moduł zarządzania konfiiguracją urządzeń

1. System musi posiadać funkcjonalność tworzenia kopii zapasowych konfiguracji poszczególnych elementów sieciowych, tj. przełączniki, routery spełniającą poniższe wymagania:
    - rozwiązanie dostarczone z licencją na obsługę minimum 1000 urządzeń
    - automatyczny backup konfiguracji
    - archiwizowanie starszych konfiguracji
    - informowanie o zmianach w konfiguracji
    - automatyczne wykonywanie zaplanowanych zadań
    - możliwość konfiguracji wielu urządzeń jednocześnie z poziomu aplikacji (tzw. bulk configuration)
    - możliwość konfiguracji wykonywania kopi zapasowych zgodnie z określonym interwałem czasowym dla urządzeń różnych producentów dla pojedynczego urządzenia lub grup urządzeń
    - możliwość automatycznego wykrywanie zmian w konfiguracji
    - możliwość wersjonowania konfiguracji danego urządzenia wraz z wyróżnionymi zmianami
    - możliwość przywracania wcześniej konfiguracji
    - wsparcie dla sprzętu różnych producentów
    - wykrywanie przez oprogramowanie możliwych niebezpieczeństw w konfiguracji
    - oprogramowanie powinno posiadać wbudowane, predefiniowane raporty
    - możliwość generowania raportów o urządzeniach w systemie
2. Tworzenie kopii zapasowej konfiguracji musi wspierać wiele protokołów takich jak:
    - SNMP
    - Telnet
    - SSH
    - TFTP
3. Dla monitorowanych urządzeń system musi mieć informację o wygasającym wsparciu producenta, tj. End of Support

Moduł zarządzania środowiskiem wirtualnym

1. System musi mieć możliwość monitorowania oraz zarządzania systemami wirtualizującymi, co najmniej VMware vSphere oraz Microsoft Hyper-V.
2. Rozwiązanie musi zarządzać maszynami wirtualnymi Zamawiającego, co najmniej dla 64 socketów.
3. System musi monitorować wydajność środowisk wirtualnych bazujących na VMware, takich jak VMware ESX, vSphere, EXSi, vCenter server.
4. System powinien zbierać statystki wydajności z VMware vSAN.
5. System musi zbierać statystki wydajności z klastrów, hostów i maszyn wirtualnych hostowanych na zasobach Hyper-V.
6. System dzięki monitorowaniu wydajności, musi pokazać problemy związane z dyskami, tj. duże obciążenie operacji I/O.
7. System musi wykrywać i ostrzegać administratora, gdy pojawią się oznaki wąskiego gardła na dowolnym elemencie wirtualizacji.

8. System pozwala na planowanie zasobów, dzięki czemu Zamawiający będzie w stanie oszacować potrzeby związane z zakupem dodatkowego sprzętu.
9. System pozwala na wyszukanie problematycznych maszyn wirtualnych: tych które nie były dawno włączane, przeskalowanych maszyn, maszyn nie będących pod obciążeniem, itp.
10. System musi śledzić konfiguracje maszyn wirtualnych oraz konfiguracje hostów, umożliwiając historyczny wgląd w ich parametry.
11. System powinien dokładnie określić kiedy nastąpiła zmiana parametrów maszyny, oraz porównać nową i starą konfigurację.
12. System pozwala symulować zmiany i warianty ułożenia maszyn. Przewidywana wydajność systemów może bazować na wydajności wyciągniętej z historycznych danych.
13. Rozwiązanie wyświetla rekomendacje dotyczące rozbudowy CPU, pamięci oraz przestrzeni dyskowej bazując na trendach. System może wygenerować szczegółowy raport bazując na przewidywaniach.
14. System ma możliwość uruchomienia reguł remediacyjnych na żądanie lub wedle harmonogramu.
15. System ma możliwość automatycznego wykrywania i monitorowania nowych instancji wirtualnych.