



Główny Urząd Statystyczny
Departament Administracyjno-Budżetowy

Warszawa, dnia 18.09.2020 r.

Wyjaśnienia SIWZ

Działając na podstawie art. 38 ust. 1, 1a i 2 ustawy Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843, z późn. zm.), Zamawiający odpowiada na pytania do SIWZ zadane przez wykonawców w postępowaniu o udzielenie zamówienia pn.: „Dostawa i wdrożenie systemu do zarządzania informacją i zdarzeniami bezpieczeństwa klasy SIEM (ang. Security Information and Event Management), gromadzącego i korelującego informacje z systemów, aplikacji oraz urządzeń; numer sprawy: 41/ST/KSZBI/POPC/PN/2020, ogłoszenie o zamówieniu numer 2020/S 162-392310 z dnia 21-08-2020 r.

Pytanie 43:

Zamawiający w dokumencie OPZ pkt II.1.5) a) iv. zawarł wymaganie treści "wymagane jest zastosowanie rozwiązania w trybie pracy klastra niezawodnościowego (HA)" w zakresie pierwszego poziomu zbierania logów - danych źródłowych, stanowiący komponent zbierania i zarządzania logami (log manager) świadczący usługi przechowywania, wyszukiwania i zarządzania zebranymi logami surowymi (danymi źródłowymi) oraz zmodyfikował zapis OPZ w pkt II.1.5) poprzez dokument Modyfikacja i Wyjaśnienia SIWZ z dnia 11.09.2020 dodając ppkt d) "iii. komponent realizujący zadanie zbierania (przechowywania) i zarządzania logami musi być zaprojektowany w architekturze wysokiej dostępności (HA)".

Czy Zamawiający poprzez architekturę wysokiej dostępności na poziomie komponentu w przypadku awarii komponentu z klastra niezawodnościowego rozumie zapewnienie ciągłości funkcjonalności zbierania i zapisywania (przechowywania) logów - danych źródłowych na poziomie aplikacyjnym?

Odpowiedź Zamawiającego:

Tak, Zamawiający wyjaśnia, że poprzez architekturę wysokiej dostępności na poziomie komponentu, w przypadku awarii komponentu z klastra niezawodnościowego, rozumie zapewnienie ciągłości funkcjonalności zbierania i zapisywania (przechowywania) logów - danych źródłowych na poziomie aplikacyjnym.

Pytanie 44:

Zamawiający w dokumencie OPZ pkt II.1.5) a) iv. zawarł wymaganie treści "wymagane jest zastosowanie rozwiązania w trybie pracy klastra niezawodnościowego (HA)" w zakresie pierwszego poziomu zbierania logów - danych źródłowych, stanowiący komponent zbierania i zarządzania logami (log manager) świadczący usługi przechowywania, wyszukiwania i zarządzania zebranymi logami surowymi (danymi źródłowymi) oraz zmodyfikował zapis OPZ w pkt II.1.5) poprzez dokument Modyfikacja i Wyjaśnienia SIWZ z dnia 11.09.2020 dodając ppkt d) "iii. komponent realizujący zadanie zbierania (przechowywania) i zarządzania logami musi być zaprojektowany w architekturze wysokiej dostępności (HA)".

Zamawiający w dokumencie OPZ nie zawarł wymagania osadzenia zdublowanych komponentów klastra wydajnościowego w zakresie pierwszego poziomu zbierania logów w różnych lokalizacjach fizycznych w przypadku proponowania architektury w modelu hardware appliance lub osadzenia maszyn wirtualnych klastra niezawodnościowego na niezależnych platformach wirtualizacyjnych w różnych lokalizacjach fizycznych w zakresie

pierwszego poziomu zbierania logów w przypadku proponowania architektury w modelu wirtualizacji (maszyny wirtualne).

W takim przypadku braku wymagania istnieje możliwość zaproponowania architektury osadzonej w jednej lokalizacji fizycznej co jest zgodne z wymaganiem zapewnienia rozwiązania w trybie pracy klastra niezawodnościowego jednak w szczególnych przypadkach awarii (np. awaria na poziomie platformy wirtualizacyjnej, niedostępność podstawowego DC) będzie miała istotny wpływ na brak dostępności systemu mimo spełnienia warunku OPZ. Czy zamawiając potwierdzenia przyjęte założenia?

Odpowiedź Zamawiającego:

Tak, Zamawiający potwierdza przyjęte założenia.

Pytanie 45:

Zamawiający w dokumencie OPZ pkt II.1.5) a) iv. zawarł wymaganie treści "wymagane jest zastosowanie rozwiązania w trybie pracy klastra niezawodnościowego (HA)" w zakresie pierwszego poziomu zbierania logów - danych źródłowych, stanowiący komponent zbierania i zarządzania logami (log manager) świadczący usługi przechowywania, wyszukiwania i zarządzania zebranymi logami surowymi (danymi źródłowymi) oraz zmodyfikował zapis OPZ w pkt II.1.5) poprzez dokument Modyfikacja i Wyjaśnienia SIWZ z dnia 11.09.2020 dodając ppkt d) "iii. komponent realizujący zadanie zbierania (przechowywania) i zarządzania logami musi być zaprojektowany w architekturze wysokiej dostępności (HA)".

Zgodnie z najlepszymi powszechnymi praktykami wdrożeniowymi systemów klasy SIEM, systemy klasy SIEM nie są traktowane jak krytyczne systemy wpływające na działanie biznesu. Wykorzystanie mechanizmów zapewnienia wysokiej dostępności poprzez klastr niezawodnościowy tylko dla jednej warstwy logicznej systemu nie jest biznesowo wskazana. Zamiast tego rozwiązaniem powszechne jest zapewnienie mechanizmów buforowania przepływu danych na pierwszym poziomie zbierania logów na czas rozwiązania awarii mającej wpływ na funkcjonalność zbierania, korelacji i generowania alertów/incydentów.

Czy Zamawiający akceptuje rozszerzenie zapisu z "komponent realizujący zadanie zbierania (przechowywania) i zarządzania logami musi być zaprojektowany w architekturze wysokiej dostępności (HA)" na zapis o brzemieniu "komponent realizujący zadanie zbierania (przechowywania) i zarządzania logami musi być zaprojektowany w architekturze wysokiej dostępności (HA) lub system musi zapewniać mechanizmy buforowania zdarzeń - logów z systemów źródłowych na czas awarii wpływającej na podstawowe funkcjonalności zbierania, korelacji i generowania alertów/incydentów"?

Odpowiedź Zamawiającego:

Zamawiający nie wyraża zgody na rozszerzenia zapisu "komponent realizujący zadanie zbierania (przechowywania) i zarządzania logami musi być zaprojektowany w architekturze wysokiej dostępności (HA)" na zapis o brzemieniu "komponent realizujący zadanie zbierania (przechowywania) i zarządzania logami musi być zaprojektowany w architekturze wysokiej dostępności (HA) lub system musi zapewniać mechanizmy buforowania zdarzeń - logów z systemów źródłowych na czas awarii wpływającej na podstawowe funkcjonalności zbierania, korelacji i generowania alertów/incydentów". W ocenie Zamawiającego, rozwiązanie w architekturze wysokiej dostępności (HA) jest rozwiązaniem bardziej koherentnym, innowacyjnym oraz zaawansowanym technicznie w porównaniu do systemu, który obsługuje mechanizmy buforowania zdarzeń - logów. Akceptacja rozszerzenia zapisu, o którym mowa powyżej, mogłaby ograniczyć konkurencję przez preferowanie tylko takich Wykonawców, którzy dostarczają rozwiązania oparte o mechanizmy buforowania zdarzeń - logów.

Opis przedmiotu zamówienia opisuje minimalne wymagania ilościowe i funkcjonalne i w żaden sposób nie ogranicza Wykonawcy w zakresie możliwości zaoferowania dodatkowych lub innych komponentów wzbogacających przedmiot zamówienia, w tym np. dostarczenia mechanizmów buforowania zdarzeń - logów.

Przewodnicząca
Komisji Przetargowej
Agnieszka Jagoda

*Konsultant
w Wydziale zamówień Publicznych GUS*