MADE IN GERMANY

G DATA TechPaper

Network Monitoring

Copyright © 2019 G DATA Software AG

Spis treści

Copyright © 2019 G DATA Software AG

Wprowadzenie

Wzajemne połączenia komponentów IT, takie jak stacje robocze, serwery, urządzenia mobilne, drukarki i wiele innych urządzeń peryferyjnych gwałtownie wzrosło w ostatniej dekadzie. Dostępność dużej liczby urządzeń sieciowych prowadzi do coraz bardziej skomplikowanych wdrożeń sieciowych dla przedsiębiorstw oraz strategii zarządzania. To sprawia, że trudno jest śledzić wszystkie zasoby i utrzymanie wymaganego poziomu know-how. Monitorowanie sieci pomaga personelowi IT zapewnić ciągłość biznesową, śledzenie stanu szerokiej gamy zasobów sieciowych, w tym sprzętu, jak i oprogramowania. Wspomagany przez regularne raporty i konfigurowalne alarmy, personel może zapewnić utrzymanie i wsparcie, a także aktywnie zmniejszyć liczbę awarii. Monitorowanie sieci sprawia, że zarządzanie zasobami, optymalizacja, konserwacja, planowanie i rozbudowa infrastruktury wykonuje się bardziej wydajnie i opłacalnie dla każdej firmy od małego do globalnego przedsiębiorstwa.

1. Korzyści monitorowania sieci

1.1. Dostępność

Rosnąca liczba urządzeń sieciowych utrudnia administratorom identyfikację ryzyka dostępności. Monitorowanie sieci pomaga przeciwdziałać tej tendencji. Ciągłe monitorowanie umożliwia administratorom rozpoznanie problemu z wydajnością, jeżeli występuje ale również pozwala im śledzić trendy i przewidywać problemy z dostępnością. Korzystając z danych historycznych trendów, słabe punkty w sieci można optymalizować przed zmniejszeniem wydajności lub obciążenia, które powoduje przestój. Dzienniki błędów są bardzo przydatne, gdy użytkownicy zgłaszają problemy z bazą danych, systemu CRM lub sklepu internetowego, który nie jest dostępny.

1.2. Migracja i rozwój

Monitorowanie sieci może wspierać rozwój infrastruktury, elementy takie jak migrację sieci i ekspansję. Na przykład, za pomocą wykresów topologii sieci, administratorzy mogą identyfikować elementy infrastruktury wymagające poprawy, a także upewnienie się, że sieć wymaga jakiekolwiek wdrażania - specyficzne warunki wstępne.

W wyniku śledzenia wydajności przez pewien okres czasu, administratorzy mogą zyskać pogląd poziomu wydajności. Punkty pomiarowe mogą zawierać wniosek i czas reakcji infrastruktury, wykorzystanie, przepustowość i pojemność. Mogą one następnie służyć jako wskaźniki bazowe przy planowaniu nowej infrastruktury dla scenariuszy migracji i ekspansji, aby podejmować świadome decyzje odnośnie skalowalności i dostępności. Pomaga odnaleźć równowagę w planowaniu przepustowości, upewniając się, że szczytowe obciążenia są przetwarzane odpowiednio.

1.3. Zgodność

Monitorowania sieci można skonfigurować tak, aby zbierać szeroki zakres danych. Bardzo dobrze nadaje się do kontroli zgodności i audytu. Nie tylko śledzi zużycie danych przez urządzenia w infrastrukturze sieciowej, może również monitorować i rejestrować domyślne konfiguracje oraz zmiany konfiguracji. Pozwala to firmom przygotować ich infrastruktury do certyfikacji i upewnić się, że nie jest znoszona ze zgodności tak jak infrastruktura rozszerzana w miarę upływu czasu.

1.4. Bezpieczeństwo

Nie tylko administratorom monitoring sieci ułatwia zarządzanie infrastrukturą: produkt starannie dopasowuje się do rozwiązań z zakresu bezpieczeństwa. Jako jedna z warstw w koncepcji bezpieczeństwa sieci korporacyjnej, monitorowania sieci może pomóc wykryć oznaki podejrzanych działań, takie jak niezwykle wysokie obciążenie sieci, które może wskazywać na atak Denial of Service (DoS). Zainfekowane urządzenia sieciowe mogą również

Copyright © 2019 G DATA Software AG

wykazywać nietypowe obciążenie procesora, zachowanie usług lub wykorzystanie pamięci, jak również aplikacje działające w kontekście innego programu lub ruch sieciowy spowodowany przez infekcję złośliwym oprogramowaniem. W połączeniu z rozwiązaniem do zarządzania poprawkami na końcówkach monitorowanie sieci szybko i łatwo pozwala administratorom wykryć i ograniczyć luki[1].

1.5. Chmura i wirtualizacja

Do zarządzania infrastrukturą chmurową, serwerami wirtualnymi i innymi scenariuszami korzystania ze wspólnych zasobów przez wielu użytkowników, monitoring sieci jest niezbędny do utrzymania modelu biznesowego. Infrastruktura powinna być zbudowana i obsługiwana w celu organizowania znacznej bazy klientów; monitorowanie sieci pomaga oszacować wymagania i utrzymać wydajność dla wszystkich aplikacji i usług w sieci. Te same metody pomagają w przygotowaniu wirtualizacji serwerów fizycznych na podstawie pomiaru ich dostępu odczytu/zapisu, ruchu sieciowego, wykorzystania procesora i innych statystyk. Ostatecznie, można monitoring sieci wykorzystywać jako narzędzie do monitorowania Service Level Agreement(SLA), jak również warunków użycia – opartych na rozliczeniach.

2. Wybór rozwiązania do monitorowania sieci

Firmy każdej wielkości odkryły wartość dodaną integrowania monitorowania sieci do ich zarządzania przepływem pracy. Rynek rozwiązań do monitorowania sieci rośnie odpowiednio: całkowite dochody za 2012 oszacowano na 2,2$ mld USD i ma wzrosnąć do +4,5$ mld 2017 roku z roczną stopą wzrostu na poziomie 15,2%[2]. Przy tak licznych dostępnych rozwiązaniach, ważne jest, aby dokonać świadomego wyboru kiedy przygotowujemy się do zakupu jednego rozwiązania.

2.1. Funkcje

Patrząc na funkcje rozwiązań do monitorowania sieci, pierwszym punktem do rozważenia jest rodzaj architektury serwera. Monitoring sieci jest dostępny jako rozwiązanie hostowane lokalnie i w chmurze jako usługa. Lokalnie hostowane rozwiązania wymagają znacznej ilości czasu, aby mogły zostać zainwestowane do wdrożonej infrastruktury, zarządzania i utrzymania. Usługi w chmurze z drugiej strony zmniejszają wymaganą ilość czasu i pieniędzy przy wykorzystaniu hostowanej infrastruktury, która również pozwala być rozwiązaniem łatwo skalowanym w przypadku wzrostu zapotrzebowania.

Rozwiązanie powinno być w stanie zbierać dane ze wszystkich najważniejszych urządzeń sieciowych. Kompilacja inwentaryzacji infrastruktury sieciowej pomaga dowiedzieć się, które protokoły monitorowania sieci powinny być wspierane. Wsparcie SNMP jest absolutnym minimum, ale każda dodatkowa obsługa protokołu jest na plus.

Administratorzy powinni również pomyśleć o tym, co mają zamiar zrobić z zebranymi danymi. Przy analizowaniu trendów, na przykład rozwiązanie powinno być w stanie zapisać dane z dłuższego okresu czasu i pokazywać odpowiednie dane do analizy trendów i wykresów. Gdy celem jest stworzenie systemu wczesnego ostrzegania, rozwiązanie musi umożliwiać administratorom ustawianie wartości progowych i konfigurowanie(w czasie rzeczywistym) alarmów, gdy punkty danych zostaną przekroczone lub spadną poniżej wartości progu.

Finalnie, monitorowanie sieci jest dla ludzi. Każde rozwiązanie powinno być łatwe w obsłudze. Wszystkie funkcje powinny być dostępne w ujednoliconym interfejsie, oferując administratorom przejrzysty pulpit nawigacyjny, pozwalający im szybko sprawdzić wszystkie ważne informacje o statusie.

---

[1] aby uzyskać więcej informacji na temat zarządzania poprawkami, patrz TechPaper #0271 G DATA Patch Management najlepsze praktyki
[2] Frost & Sullivan: Network and Application Performance Management Market (2012).

Copyright © 2019 G DATA Software AG

2.2. Zwrot z inwestycji

Ważnym czynnikiem przy podejmowaniu decyzji jest porównanie funkcji w rozwiązaniach monitorowania sieci w oparciu o wymagane inwestycje. Koszty związane, zarówno ze wstępnym wdrożeniem i utrzymaniem, powinny zostać zaliczone na poczet zysków, które mogą być zrealizowane. Obliczenie zwrotu inwestycji może być następnie wykorzystane do porównania ze sobą różnych rozwiązań.

Najbardziej oczywistym zyskiem jest zapobieganie stratom finansowym ze względu na upływ czasu. Na przykład uruchomiony sklep internetowy. Jego dostępność jest kluczowym elementem w obsłudze klientów i zapewnieniu przychodów. Podobnie, czas przestoju kluczowego serwera bazy danych ma potencjał, aby zakłócić wydajność całego biura, powodując natychmiastowe straty finansowe. Używając monitorowania sieci, liczba przestojów infrastruktury może się zmniejszyć poprzez podjęcie działań naprawczych, zanim sieć zostanie spowolniona lub upadnie całkowicie. A nawet jeśli składnik wymaga pilnej konserwacji, alarmy pomagają w upewnieniu się, że pracownicy są niezwłocznie informowani, zapewniając znaczną redukcję czasu personelu wymaganego do dbania o kwestie infrastrukturalne. Ponadto, alarmy monitorowania sieci i dane dotyczące trendu pomagają skrócić czas naprawy i zwrócić uwagę personelu w stronę odpowiedniego kontekstu. Poprzez skrócenie czasu spędzonego przy awariach, personel IT może pracować przy innych, większych projektach strukturalnych.

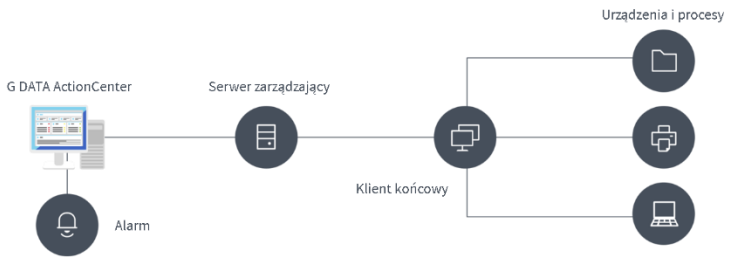
3. G DATA Network Monitoring

G DATA posiada zintegrowane monitorowanie sieci w ramach istniejącej oferty rozwiązań bezpieczeństwa punktów końcowych. Dzięki temu administratorzy mogą skorzystać z synergii między komponentami zarządzania, jak również pomiędzy składnikami klient / agent.

3.1. Wdrożenie

Monitorowanie sieci dostępne jest jako opcjonalny moduł dla wszystkich rozwiązań biznesowych G DATA w wersji 14 i może być łatwo dodawane do nowych i istniejących wdrożeń G DATA. Architektura jest w chmurze przy wsparciu lokalnego G DATA ManagementServer. G Data Security Client funkcjonuje jako agent, który zbiera dane z lokalnych punktów, a także innych zasobów sieciowych. Wartości te są następnie przekazywane do G DATA ManagementServer, co z kolei synchronizowane jest do usługi w chmurze G DATA ActionCenter. Usługa w chmurze przechowuje dane a następnie na podstawie tych danych mogą być: natychmiast przez serwer wysyłane alerty, albo przez administratora, który później analizuje dane.

Taka konfiguracja oznacza, że administratorzy nie muszą się martwić o zarządzanie i wdrażanie monitorowania infrastruktury serwerowej. Administrowanie i alarmowanie może być przeprowadzane niezależnie od bieżącego obciążenia sieci klienta. Opcja usługi chmurowej jest idealnym rozwiązaniem dla firm, które nie mają budżetu lub czasu na zarządzanie lokalną infrastrukturą monitorowania sieci.



Rysunek 1: Architektura G DATA Network Monitoring

Copyright © 2019 G DATA Software AG

Łącząc różne rodzaje danych, monitorowanie sieci pozwala na kompleksowy przegląd kierunku danych. Typowo obsługuje wiele protokołów, warstwy praktycznie każdego połączenia sieciowego - nie tylko sprzęt, ale także oprogramowanie i usługi. Na przykład obejmuje:

- Sprzęt
    - Punkty końcowe i serwery
    - Dyski twarde
    - CPU
    - RAM
    - NAS
- Infrastruktura sieciowa
    - Punkty końcowe, interfejsy sieciowe i serwerowe
    - Routery
    - Przełączniki
    - Punkty dostępowe
    - Zapory
    - Urządzenia peryferyjne
        - drukarki (sieciowe)
- Oprogramowanie
    - procesy i usługi
    - System operacyjny
    - Aplikacje
- Serwery
    - Web
    - Database
    - Exchange
    - Domain Controller

Lista nie jest wyczerpująca: wiele urządzeń sieciowych może być potencjalnie monitorowane, nawet jeśli metryka nie jest dostępna. Metryki są wdrażane za pośrednictwem usługi chmurowej, zakres dostępnych metryk może być rozszerzony w dowolnym momencie. Jeżeli wymagana jest określona metryka, która jeszcze nie istnieje. Klienci mogą również złożyć prośbę o rozbudowę produktu. Jeśli to możliwe, metryka zostanie zaprojektowana i dostarczana do G DATA ActionCenter.

Monitorowanie sieci opiera się na różnych protokołach w celu zebrania danych z dostępnych środków. Ze względu na swoją wszechstronność, Simple Network Management Protocol (SNMP) stał się popularnym wyborem dla monitorowania i zarządzania wieloma typami urządzeń sieciowych. Charakteryzuje się konstrukcją pytań-i-odpowiedzi: serwer monitorowania sieci może użyć protokołu do żądania informacji od składnika z obsługą SNMP o konkretnej właściwości (np. obciążenia procesora, wykorzystania pasma). Następnie urządzenie reaguje z odpowiednią wartością i serwer zapisuje wynik. Oprócz SNMP istnieją dwa inne ważne źródła pozyskiwania danych takie jak liczniki wydajności oraz Windows Management Instrumentation (WMI) API, oba dostępne są w większości agentów – opartych o Windows. Komponenty niezwiązane z systemem Windows można skomunikować za pomocą polecenia ping lub protokołem HTTP - oparte na komunikacji.

3.2. Konfiguracja

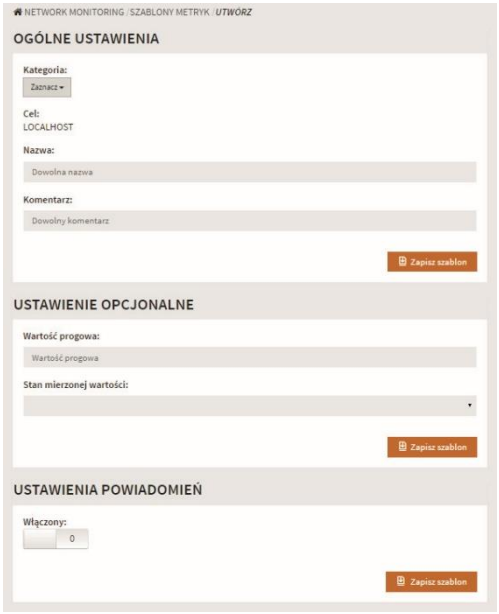
Monitoring sieci jest konfigurowany i zarządzany za pomocą interfejsu webowego G DATA Action Center pod adresem https://ac.gdata.de. Aby zacząć, musi zostać utworzony jeden szablon metryczny lub więcej. Szablon zawiera predefiniowany typ monitoringu i parametry konfiguracyjne. Na przykład obejmuje:

- Monitorowanie procesu specyficznego składnika w systemie Windows
- Monitorowanie dostępności serwera

Copyright © 2019 G DATA Software AG

- Monitorowanie poziomu tonera drukarki

Parametry konfiguracyjne różnią się zależnie od szablonu, ale mogą zawierać wartość progową (generować powiadomienia, jeśli wartość wzrasta powyżej lub spada poniżej progu) i jeden lub więcej adresów e-mail dla alertów. Na przykład, przy pomiarze dostępności serwera może zostać wprowadzona wartość progowa 1000 ms. Administrator otrzyma wiadomość e-mail, gdy wartość osiągnie poziom wyższy niż 1000 ms.



Rysunek 2: Szablon

Po ustaleniu szablonu, metryka jest tworzona poprzez przypisanie szablonu do jednego lub większej liczby klientów. Klient będzie okresowo przeprowadzać konkretne działania monitorowania i raportowania wyników do powiązanego ManagementServer. Serwer będzie synchronizować wyniki do ActionCenter, który z kolei wykona czynności, które zostały zdefiniowane w szablonie (takie jak wysyłanie alertów).

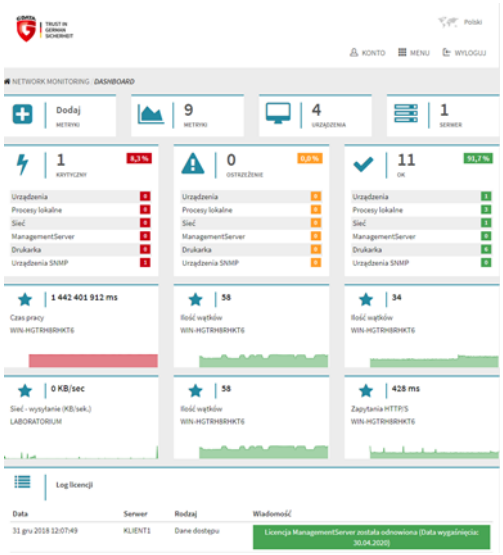
3.3. Analiza

Z jednej lub większej liczby utworzonych metryk administratorzy mogą korzystać z różnych sposobów śledzenia przekazywanie danych, z których każdy pasuje do jednego lub większej liczby typowych zastosowań. W przypadku scenariuszy, które opierają się na bezpośrednich raportach, alarmy są zalecaną metodą powiadamiania. Pozwalają one na szybkie czasy reakcji w przypadku jakiegoś zdarzenia. Alarmy włączane są w szablonie metrycznym i stosowane do wszystkich danych opartych na szablonie. Po włączeniu alarmu, należy zweryfikować czy odpowiednie grupy e-mail zostały również zdefiniowane, aby być pewnym, że zdarzenia krytyczne mogą zostać szybko rozwiązane. Powiadomienia alarmowe mogą zostać wysłane do listy dystrybucyjnej e-mail, takich jak Emergency Response Team w ramach działu IT. Należy upewnić się, że wszyscy odbiorcy alarmów mogą podjąć działania, jeżeli otrzymają alarm. Powinni być w stanie wykonywać czynności niezależnie od administratora oraz otrzymać uprawnienia do korzystania z ActionCenter. Przynajmniej, należy określić przepływ pracy, który gwarantuje, że działanie może być szybko podjęte w przypadku, gdy występuje sytuacja awaryjna.

Administratorzy nie muszą czekać do momentu, aż alarmy zostaną wysłane. Na pulpicie nawigacyjnym G DATA ActionCenter przedstawiane są podstawowe informacje o stanie sieci. Trzy wskaźniki stanu wyświetlają statystyki monitorowania usług według priorytetów (krytyczny, ostrzeżenie i normalny). Dzięki temu administratorzy mogą szybko sprawdzić, czy jakakolwiek część infrastruktury sieciowej musi zostać zbadana. Poszczególne usługi można dodać do ulubionych, aby wyświetlać je bezpośrednio na pulpicie nawigacyjnym, co jest szczególnie przydatne w

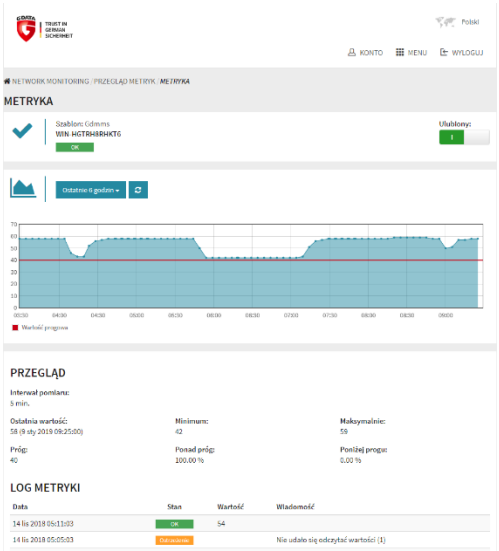
Copyright © 2019 G DATA Software AG

przypadku ważnych i często używanych zasobów. Wyświetlana jest również liczba skojarzonych ManagementServers jak również liczba urządzeń, które pomagają w zachowaniu przeglądu sieci.



Rysunek 3: Pulpit nawigacyjny

Jeśli wymagana jest bardziej szczegółowa analiza poszczególnych stron metrycznych. Każda strona przedstawia schemat, umożliwiając administratorom dostrzec trendy, zanim osiągną poziom krytyczny. Schemat może być skonfigurowany do wyświetlania wartości na określony czas i może być wykorzystany do wskazania kierunków. Gdy zużycie pamięci RAM urządzenia wyświetla tendencję wzrostową, zanim nagle spadnie, na przykład, może to wskazywać na problem zużycia pamięci specyficznych procesów. Administratorzy mogą wykorzystać te informacje do podjęcia natychmiastowych działań, takich jak zdefiniowanie wskaźników dla procesów systemowych lub badać problemy lokalnie na samym urządzeniu.



Rysunek 4: Metryka

Korzystając z dostępnych danych dla poszczególnych usług, administratorzy mogą analizować kierunek danych. Przy użyciu historycznych danych monitorowania, na przykład, jest możliwe określenie czasu maksymalnego i minimalnego dla interfejsu sieciowego. Te punkty danych mogą być wykorzystywane do utworzenia oczekiwanej wartości wyjściowej, a w związku z tym do ustawienia alarmowej wartości progowej. Jest to proces, który powinien zostać zoptymalizowany w pewnym czasie, wartości progowe nie zawsze są łatwe do ustawienia. Niektóre usługi

Copyright © 2019 G DATA Software AG

mogą nadal pracować pod obciążeniem, co prowadzi do niepotrzebnych alertów, jeśli progi są zbyt niskie. Inne mogą przestać razem funkcjonować, gdy wzrasta obciążenie, w niektórych przypadkach ostrzeżenia powinny zostać wysłane gdy wskaźnik faktycznie osiągnie poziom krytyczny. Jaki poziom jest uważany za krytyczny można zaobserwować poprzez śledzenie statystyk wydajności w dłuższym czasie i skorelowanie go z danymi na temat dostępności usług i pogorszenia jakości. Administratorzy mogą także aktywnie skonfigurować testy wydajności, które pomagają znaleźć punkt krytyczny dla ich infrastruktury. Te same testy mogą być uruchamiane po incydencie wydajności, upewniając się, że wszelkie poprawki, które zostały wdrożone dają oczekiwany efekt.

Copyright © 2019 G DATA Software AG