Szkolenie techniczne

Kopalnia wiedzy o rozwiązaniach firmy G Data dla biznesu
Spis treści

1. G Data ClientSecurity Enterprise ................................................................................................. 4
   1.1. G Data ClientSecurity Business .................................................................................................. 4
   Kategoryzacja ................................................................................................................................. 5
   Komponenty .................................................................................................................................... 5
   Nowe technologie ........................................................................................................................... 10
   Instalacja - ogólnie ....................................................................................................................... 13
   Instalacja G Data AntiVirus ManagementServer ......................................................................... 15
   Instalacja klienta G Data AntiVirus .............................................................................................. 21
   Instalacja klienta G Data AntiVirus dla komputerów z systemem Linux ....................................... 23
   Instalacja G Data AntiVirus WebAdministrator .......................................................................... 25
   1.2. G Data MailSecurity .................................................................................................................. 26
   Kategoryzacja .................................................................................................................................. 26
   Komponenty .................................................................................................................................. 26
   Instalacja ........................................................................................................................................ 27
   Konfiguracja filtra spamu ............................................................................................................... 28
   1.3. Jak dobrze znasz rozwiązania biznesowe G Data Security? ...................................................... 29

2. G Data ClientSecurity Business – podstawy konfiguracji ................................................................. 30
   2.1. Logowanie .................................................................................................................................. 30
   2.2. Zarządzanie serwerem .............................................................................................................. 32
   2.3. Aktualizacje ............................................................................................................................. 33
   2.4. Definicja grup ............................................................................................................................ 33
   2.5. Wiadomości e-mail .................................................................................................................. 34
   2.6. Lokalny filtr spamu ................................................................................................................... 34
   2.7. Zasoby sieciowe ....................................................................................................................... 36
   2.8. Odinstalowywanie bez jednostki ManagementServer ............................................................ 36
   2.9. Migracja jednostki ManagementServer .................................................................................. 36
   2.10. Porty komunikacyjne ............................................................................................................... 37
   2.11. Jak dobrze znasz rozwiązania biznesowe G Data Security? .................................................. 37

3. G Data MailSecurity - podstawy konfiguracji .................................................................................. 38
   3.1. Instrukcje .................................................................................................................................... 38
   Instrukcje zmiany G Data MailSecurity na AVM KEN 4 ................................................................. 38
   Ustawienia G Data MailSecurity ..................................................................................................... 41
   3.2. Wysyłanie kwerend do kilku serwerów POP3 .......................................................................... 43
   3.3. Jak dobrze znasz rozwiązania biznesowe G Data Security? .................................................... 43

4. Instalacja, startowa płyta CD, narzędzia i „często zadawane pytania” .............................................. 44
   4.1. Instalacja klienta programu G Data AntiVirus dla systemu Win2003/2008 ................................. 44
   Przed instalacją ................................................................................................................................ 44
   Instalacja ....................................................................................................................................... 45
   Konfiguracja ................................................................................................................................. 45
   Opcje monitorowania .................................................................................................................... 46
   Funkcje specjalne ........................................................................................................................... 50
   Opcje specjalne ............................................................................................................................. 50
   4.2. Startowa płyta CD ..................................................................................................................... 52
   4.3. Narzędzia ................................................................................................................................... 53
   AV-Cleaner ...................................................................................................................................... 53
   Monitor - MonActivityCS ............................................................................................................... 54
4.4. Często zadawane pytania........................................................................................................................................56
Komunikat o błędzie: „Baza danych wirusów/pliki programu jest/są uszkodzone.” .............. 56
Problemy z aktualizacjami internetowymi używającymi Administratora G Data AntiVirus56
Sprawdź komunikację między ManagementServer a klientami ........................................... 57
Skrzynka pocztowa poddana kwarantannie .............................................................................. 57
Klient na komputerze z systemem Linux – brak połączenia z jednostką ManagementServer................................................................. 58
1. **G Data ClientSecurity Enterprise**


1.1. **G Data ClientSecurity Business**

**Definicje**

- **C$ i Admin$:** standardowe administracyjne udostępnianie plików w systemach Windows.

- **Skrypt logowania:** skrypt przydzielony użytkownikowi w sieci, który jest uruchamiany podczas logowania konkretnego użytkownika.

- **Format zastrzeżonej bazy danych:** niezależny format bazy danych, który jest zastrzeżony zgodnie z prawami licencyjnymi (oprogramowanie, które nie jest darmowe).

- **Rejestr:** centralna, hierarchiczna baza danych konfiguracji systemu operacyjnego Microsoft Windows, w której zarejestrowane są wszystkie zainstalowane programy.

- **Cicha instalacja:** oznacza „bez żadnej interakcji z użytkownikiem”. Instalacja wykonywana automatycznie, bez wyświetlania przez program zapytań oraz bez interwencji użytkownika.

- **Pojedynczy plik EXE:** odnosi się do jednostkowego pliku Exe. Pliki Exe są wykonywalnymi programami. Instalatory są zwykle dostarczane w formie plików Exe.

- **Oparta na SQL:** baza danych, która używa języka SQL (Strukturalnego języka zapytań) jako języka programowania. SQL jest ustandaryzowanym językiem baz danych o bardzo prostej składni, przeznaczonym dla relacyjnych baz danych. Zaletą SQL jest mniejsza bądź większa niezależność od wykorzystywanego oprogramowania.

- **Symbol zasobnika:** symbole zasobnika można znaleźć na pasku zadań po lewej stronie zegara systemowego.

- **Program planujący:** program zarządzający procesami.

- **VPN:** jest to skrót od wirtualnej sieci prywatnej (virtual private network) składającej się z kilku uczestników i/lub podsieci. Zwykle są one połączone korzystając z internetu. Przesyłanie danych jest tajne, autoryzowane, a dane są wysyłane jako liczby całkowite.
Kategoria

Oparta o pliki ochrona przed wirusami dla stacji roboczych, serwerów oraz mobilnych stacji roboczych z wykrywaniem na żądanie (zadania skanowania) i dostępowe (monitorowanie w tle), a także zapora ogniowa klienta zapewniająca zdalną instalację.

Dodatkowo, posiada także zlokalizowane po stronie klienta sprawdzanie poczty dla programu MS Outlook (wtyczka) oraz dowolnego programu pocztowego opartego o protokoły POP3/IMAP/SMTP (lokalne pośrednictwo), a także filtr HTTP służący do sprawdzania zawartości internetowej.

Komponenty

**G Data AntiVirus ManagementServer**

G Data AntiVirus ManagementServer reprezentuje centralną jednostkę konfiguracyjną i administracyjną architektury ochrony antywirusowej G Data ClientSecurity Business.


Do komunikacji z klientami ManagementServer używa protokołu TCP/IP. Zadania dla niepodłączonych klientów są automatycznie zbierane i synchronizowane podczas kolejnej sesji przyłączenia do sieci. ManagementServer posiada centralny folder kwarantanny, w którym podejrzane pliki mogą opcjonalnie zostać zaszyfrowane i zachowane w formie kopii zapasowej, usuniete, wyleczone lub, jeśli jest to konieczne, przekazane do usługi Ambulans.

ManagementServer jest nadzorowany przez program administrujący i sam w sobie nie oferuje żadnej funkcji ochrony antywirusowej. Zadanie to jest przejmowanie przez klienta G Data AntiVirus. Aby także serwer był chroniony przed infekcją wirusową, na serwerze również powinien, oczywiście, być zainstalowany klient programu antywirusowego.


Komputer powinien mieć przynajmniej 256 MB pamięci RAM. Zalecane jest przynajmniej 512 MB.

Administrator G Data AntiVirus

ManagementServer wykorzystuje graficzny interfejs użytkownika Administratora programu antywirusowego G Data AntiVirus. Podczas instalacji jednostki ManagementServer, na serwerze nadzorującym ManagementServer automatycznie instalowany jest program administracyjny.

Administracja może być lokalna, używająca komputera z ManagementServer, lub zdalna - za pomocą sieci lokalnej (LAN). Możliwa jest też administracja za pomocą tunelu VPN lub zdalnego dostępu, pod warunkiem, że te opcje dostępu są obsługiwane przez chronioną sieć.

Komunikacja między administratorem G Data AntiVirus a jednostką ManagementServer wykorzystuje port TCP numer 7168.

Jeśli na miejscu pojawia się problem, program administrujący można zainstalować w szybki i prosty sposób na każdym kliencie, w ten sposób z jednego z nich istnieje pełny dostęp do jednostki ManagementServer.

Interfejs administratora jest podzielony w sposób następujący:
Znajdujący się po lewej stronie obszar wyboru klienta wyświetla strukturę hierarchiczną monitorowanego komputera. Z prawej strony korzystając z zakładek można przełączyć się do konkretnego zadania.

Zawartość obszaru zadań zwykle odnosi się do komputera podświetlonego w obszarze wyboru klienta lub do zaznaczonej grupy klientów. Nad tymi obszarami znajdują się menu oraz pasek narzędzi dla funkcji globalnych, które można użyć dla wszystkich obszarów zadań.

**G Data AntiVirus WebAdministrator**

WebAdministrator jest oprogramowaniem dla ManagementServer opartym na wykorzystaniu sieci web. Może zostać uruchomione w dowolnej przeglądarce internetowej i dzięki temu może być używane niezależnie od systemu operacyjnego.

Niezależna jednostka serwera sieciowego działa także w sieci lokalnej (LAN) i pozwala np. na zdalną administrację sieciami klienta przez internetowe protokoły HTTP/HTTPS.

Usługa WebAdministrator niekoniecznie musi być zainstalowana na samej jednostce ManagementServer, ale może zostać uruchomiona na dowolnym kliencie.
Klient G Data AntiVirus

To moduł klienta G Data AntiVirus zapewnia właściwą ochronę przed wirusami wszystkich klientów w sieci - stacji roboczych, notebooków lub serwerów.

Ponieważ administracja indywidualnymi parametrami skanera dokonywana jest centralnie z użyciem jednostki ManagementServer, po stronie klienta niepotrzebny jest interfejs graficzny użytkownika. Konkretny użytkownik może sam uruchomić standardowe zadanie np. lokalne zadanie skanowania lub aktualizację sygnowr, korzystając z ikony zasobnika skonfigurowanej w ManagementServer jako część przyznanych mu uprawnień.

Stacje posiadają swoje własne sygnowry wirusów i swój własny harmonogram skanowania i aktualizacji, aby ochrona mogła być realizowana również poza siecią z serwerem (np. dla notebooków). Zadania serwera są gromadzone i synchronizowane dla takich stacji po podłączeniu do sieci przedsiębiorstwa.

Komunikacja między klientem G Data AntiVirus a ManagementServer wykorzystuje porty TCP numery 7161 i 7166 (serwer) oraz 7167 i 7169 (klient).

Do wersji 8.0 używane były tylko porty 7166 i 7167.

Klient programu G Data AntiVirus działa w systemach operacyjnych opartych o NT, takich jak Win2000 SP4, a także na dystrybucjach Linux z wersją jądra nowszą niż 2.6.25.

Komputery powinny mieć przynajmniej 256 MB pamięci RAM. Zalecane jest przynajmniej 512 MB.
W ten sposób klient system Linux może zostać (tak jak klienci systemu Windows) podłączony do infrastruktury ManagementServer, zarządzanej centralnie przez program G Data Administrator oraz może zostać wyposażony w aktualizacje sygnatur.

**G Data Firewall**

Administrator G Data AntiVirus nadzoruje opcjonalną zdalną instalację zapory ogniowej G Data Firewall.

Oferuje najprostszą administrację z wykorzystaniem trybu autopilota. Sprawdzane są wszystkie połączenia przychodzące i wychodzące, a wszystkie ataki DoS (odmowy usługi), skanowania portów są blokowane i rejestrowane.

Oprócz autopilotów, zapora ogniowa oferuje cztery poziomy zabezpieczeń lub tryb ekspercki dla indywidualnych zasad inteligentnego dostępu dla klienta, a także ukryty tryb utajony.

**Klient G Data AntiVirus dla systemu Linux**

Produkt umożliwia skorzystanie z ochrony antywirusowej G Data na stacjach roboczych z różnymi dystrybucjami systemu Linux.

W ten sposób klient z systemem Linux może (tak samo, jak klienci z systemem Windows) zostać podłączony do infrastruktury G Data ManagementServer, zarządzanej centralnie przez oprogramowanie Administratora G Data i wyposażoną w aktualizacje sygnatur.

Analogicznie jak dla klientów z systemem Windows, dla klienta z systemem Linux zostanie zainstalowany monitor systemu plików z graficznym interfejsem użytkownika, który pod względem funkcjonalności przystosowuje się do wersji dla systemu Windows.
Dla komputerów z systemem Linux działających jako serwery plików i zapewniają autoryzacje Windows dla różnych klientów (używając protokołu SMB) może do tego celu zostać zainstalowany moduł. Nadzoruje on dostęp do autoryzacji i przeprowadza skanowanie plików dla każdego zdarzenia dostępu tak, by żadne złośliwe oprogramowanie nie mogło przenieść się z serwera Samba na klientów Windows (i na odwrot).

Dla klienta - stacji roboczej wymagana jest wersja jądra przynajmniej 2.6.25 - tak jest w przypadku: Ubuntu 8.10, Debian 5.0, Suse Linux Enterprise Desktop 11 i innych aktualnych dystrybucji. Dla innych dystrybucji, w odosobnionych przypadkach, wymagane jest dostosowanie.

Klient serwera pliku może być użyty ze wszystkimi popularnymi dystrybucjami.

**Nowe technologie**

Dodatkowo, oprócz technologii DoubleScan, w której dwa silniki antywirusów idealnie się uzupełniają osiągając stuprocentowe wykrywanie wirusów, w nowych rozwiązaniami dla biznesu firmy G Data zostały zaimplementowane następujące technologie (dostępne począwszy od wersji 10.0.x):
Identyfikacja odciskami palców (IntelliScan)

Korzystając z identyfikacji odciskami palców nie jest już konieczne wielokrotne poddawanie analizie na żądanie – OnDemand bądź dostępowemu – OnAccess (monitorowanie plików podczas odczytu, zapisu itp.).


W ten sposób oprogramowanie G Data „uczy się”, a sprawdzenie komputera staje się szybsze ze skanowania na skanowanie.

Tak więc dla pliku, który nie zmienia się, a który został przeskanowany wiele razy bez wykrycia wirusa, pojawia się taka sytuacja, w której nie jest on skanowany przez cztery tygodnie.

Aby zachować rozmiar bazy danych najmniejszy, jak to tylko możliwe, używane są skróty (wartości hash) – ich pełną wersję można zawsze znaleźć w głównej pamięci klienta.
Scanserver

Poczynając od wersji 10.x ScanServer jest centralną usługą systemu (GDScan.exe), przez którą wykonywane są wszystkie procesy skanowania.

Zapytania do silników skanowania są przekazywane do tej usługi, wykonywane wewnątrz serwera ScanServer, a wyniki skanowania zwracane są do wystawiającego zapytanie. Dzięki temu można równolegle przesyłać wiele zapytań, przez co takie podejście, porównując je do wcześniejszych wersji, nie prowadzi do ograniczeń prędkości.

W ten sposób ScanServer gromadzi wszystkie wyniki w centralnej usłudze i eliminuje wielokrotne użycie tego silnika w systemie. Stąd też znacznie mniej zasobów jest rezerwowanych w systemie.

Białe listy

Implementując białe listy, jak w wersji 10.x, G Data AntiVirus zapobiega przypadkowemu usunięciu ważnych plików systemu operacyjnego lub pewnych aplikacji przez fałszywe wykrycie wirusa przez ScanEngine lub odmowie dostępu do tych plików powodującej niemożność dalszego korzystania z systemu.

Same pliki białych list są tworzone centralnie przez G Data i rozprowadzane wraz z aktualizacjami sygnał tak, by ManagementServer zawsze posiadał aktualną białą listę, którą roześle klientom.

Biała lista zawiera serię parametrów, które pomagają sprawdzić, czy plik systemowy uległ zmianie. Przy potwierdzeniu zainfekowania plików systemowych przez wirusa parametry te są używane, aby wyeliminować fałszywe alarmy.
Instalacja - ogólnie
Należy zawsze upewnić się, że instalowana jest najnowsza wersja programu. Odpowiedni instalator jest dostępny na żądanie pod naszym adresem (pomoc@gdata.pl) lub bezpośrednio, przy użyciu łącza pobierania znajdującego się na naszej stronie: www.gdata.pl.

Należy się też upewnić, że w danym systemie nie pozostał żaden z zainstalowanych wcześniej programów antywirusowych. Zawsze należy korzystać z narzędzi czyszczących oferowanych przez konkretnych dostawców.

Po naciśnięciu przycisku „Instaluj” na ekranie auto startu pojawia się menu instalacyjne, w którym można wybrać, które z komponentów programu G Data AntiVirus powinny zostać zainstalowane.

G Data ClientSecurity Business
Wybierz składnik, który chcesz zainstalować:

**G Data AntiVirus ManagementServer**
Serwer zarządzający steruje ochroną antywirusową stacji roboczych, komputerów przenośnych i serwerów plików, a także zapewnia je w aktualne bazy wirusów. Wraz z tym składnikiem instalowany jest automatycznie moduł G Data AntiVirus Administrator.

**G Data AntiVirus Administrator**
Administrator to moduł służący do zdalnego zarządzania składnikiem G Data ManagementServer. Można go zainstalować na dowolnym komputerze w sieci.

**G Data AntiVirus Klient**
Klient realizuje ochronę antywirusową na stacjach roboczych i wykonuje zadania Serwera zarządzającego bez udziału użytkownika stacji.

**Kreator płyt startowych**
Aplikacja służąca do tworzenia płyt startowych G Data z aktualnymi bazami wirusów. Płyta startowa umożliwia przeklanianie dysków komputera bez uruchamiania systemu Windows.

**G Data AntiVirus WebAdministrator**
Moduł umożliwiający zdalne administrowanie Serwerem zarządzającym z poziomu przeglądarki internetowej.

**G Data Firewall**
Klieni zapory połączeń sieciowych dla stacji roboczej.
Dla wersji 9.0 i wyższych, aby móc zainstalować ManagementServer lub WebAdministrator konieczny jest Microsoft .NET Framework 3.5.
Jeśli zajdzie taka potrzeba, instalator G Data automatycznie zainstaluje .NET Framework. Spowoduje to tylko wydłużenie czasu instalacji o kilka minut.
Instalacja G Data AntiVirus ManagementServer
Instalacja G Data AntiVirus ManagementServer jest intuicyjna i niewymagająca tłumaczenia. System operacyjny dla serwerów nie jest niezbędny. Instalując ManagementServer, instalowana jest także aplikacja Administrator G Data AntiVirus. Może on także zostać później zainstalowany oddzielnie na innych komputerach w sieci.

Aby zagwarantować optymalną ochronę, komputer powinien być zawsze dostępny (włączony) i powinno być możliwe automatyczne ładowanie sygnatur wirusów przez połączenie internetowe.

Typy serwerów
Dla wersji 9.0 i wyższych można wybrać z pośród następujących typów serwerów:

<table>
<thead>
<tr>
<th>Wybierz rodzaj serwera</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do zainstalowania serwera podzielenia wymagana jest nazwa komputera zainstalowanym serwerem głównym.</td>
</tr>
</tbody>
</table>

**Rodzaj serwera**
- Zainstaluj serwer główny
- Zainstaluj serwer zapasowy
- Zainstaluj serwer podmiotowy

**Nazwa serwera głównego:**

- Włącz obsługę Klienta w wersji 0.0. Zaznacz tę opcję, jeśli chcesz korzystać ze starszych wersji programu G DATA Antivirus Klient.

**Serwer główny (Główny MMS):**
G Data AntiVirus ManagementServer musi być zawsze tworzony jako serwer główny. Główny serwer reprezentuje centralną jednostkę konfiguracyjną i administracyjną opartej na sieci architektury zabezpieczenia przed wirusami.
Serwer pomocniczy (Pomocniczy MMS):
Gdy używana jest baza danych SQL, można uruchomić drugi serwer (pomocniczy MMS), który korzysta z tej samej bazy danych, co serwer główny. Jeśli serwer główny jest niedostępny przynajmniej przez godzinę, klient automatycznie łączy się z pomocniczym MMS i to z niego ładowa aktualizacje sygnatur. Przełączenie z powrotem do serwera głównego nastąpi, gdy tylko będzie on znów osiągalny. Obydwa serwery niezależnie od siebie ładują aktualizacje sygnatur.

Serwer podrzędny
W przypadku dużych sieci rozsądne rozwiązaniem jest również uruchomienie serwerów podrzędnych. Serwery podsieci pomagają zmniejszyć obciążenie ruchu w sieci między klientami a głównym MMS. Mogą być one używane w podsieciach, gdzie ich zadaniem jest zarządzanie przydzielonymi im klientami. Informacje o klientach, np. raporty związane z wynikami wykrywania wirusów lub datą sygnatur, są przede wszystkim zbierane centralnie od serwera podsieci, a następnie po 5 minutach są one przekazywane do serwera głównego MMS. Serwery podsieci pozostają w pełni funkcjonalne, nawet jeśli niedostępny jest główny lub pomocniczy MMS.

Poniżej przedstawiono schematyczną strukturę typów serwerów w dużej sieci: serwery podsieci gromadzą indywidualnych klientów lub grupy klientów i przekazują ich serwerowi głównemu. Główny serwer jest wspierany przez serwer pomocniczy, który działa jako kopia zapasowa na wypadek awarii serwera głównego.
Wybór bazy danych

Do wersji 5.x, do przechowywania ustawień, centralnego raportowania itp. wykorzystywana była jedynie baza zintegrowana.

Począwszy od wersji 6.0 podczas instalacji można wybrać, czy baza danych ma być stworzona we wcześniejszym, własnym formacie bazy danych czy ma być oparta o SQL (istniejący serwer SQL w wersji minimum 2005, lub instalowana na żądanie baza SQL Express). Baza nie musi znajdować się na tym samym komputerze, co serwer zarządzający.

Wybór jednej z dwóch opcji SQL jest szczególnie zalecany dla dużych sieci, gdzie liczba klientów przekracza 30, ponieważ ten format bazy danych oferuje zalety, jeśli chodzi o wydajność przy dostępie do indywidualnych rekordów danych.

Decyzja, czy chcesz przydzielić inną bazę danych do istniejącego serwera SQL w swojej sieci należy do Ciebie. Jeśli istniejący serwer SQL jest już mocno obciążony, ManagementServer powinien być obsługiwany przez lokalną bazę danych SQL Express, aby nie dociągać głównego serwera baz.

Wybrana baza danych nie ma wpływu na działanie serwera ManagementServer. Jedyną różnicą jest czas dostępu do bazy.
Konfiguracja typu bazy danych

Ten krok instalacji pojawia się tylko podczas ponownej instalacji ManagementServer lub jeśli baza danych SQL jest już zainstalowana na danym komputerze. Zwykle jedyne, co trzeba zrobić, to zamknięcie tego okienka informacyjnego przez kliknięcie przycisku Zamknij.
Rejestracja online

Rejestracja online powinna zostać przeprowadzona po ukończeniu instalacji. Bez rejestracji online nie można przeprowadzić żadnej internetowej aktualizacji baz danych wirusów. Możliwa jest także późniejsza rejestracja. Do tego celu uruchamiana jest aplikacja „Internet Update”, znajdująca się w „Start > Programy > G Data AntiVirus ManagementServer”. W oknie aplikacji należy kliknąć przycisk Rejestracja online.

Natychmiast po rejestracji online, Twoja nazwa użytkownika i hasło zostaną pokazane w okienku informacyjnym.
Administrator programu G Data AntiVirus automatycznie przesyła tę informację do internetowego formularza aktualizacji.

**Ostrzeżenie!!!**

Nazwa użytkownika i hasło powinny zostać zanotowane i, oczywiście, przechowywane w bezpiecznym miejscu tak, by dane aktualizacji były dostępne nawet po możliwym wprowadzeniu nowej konfiguracji.

**Kreator instalacji**

Gdy Administrator G Data jest następnie uruchamiany pierwszy raz na serwerze, uruchamia się kreator instalacji, który przeprowadzi użytkownika krok po kroku przez konfigurację bazową.

W dowolnym momencie można przerwać działanie kreatora instalacji, aby ręcznie przeprowadzić konfigurację.

Po uruchomieniu początkowym kreator może też zostać w dowolnym momencie uruchomiony poprzez polecenie „Kreator instalacji” znajdujące się w menu pliku administratora G Data.
Instalacja klienta G Data AntiVirus

Każdy komputer w sieci, który ma być zabezpieczany przed wirusami musi być wyposażony w moduł klienta aplikacji G Data AntiVirus. Instalację można przeprowadzić na kilka sposobów:

**Instalacja lokalna**

W przypadku tej opcji klient program G Data AntiVirus kopiowany jest na każdy komputer bezpośrednio z nośnika instalacyjnego. Jest to szczególnie zalecane dla małych sieci.

Podczas instalacji pojawi się pytanie o nazwę / adres IP serwera, na którym zainstalowany jest główny MMS.

Lokalna instalacja zapory ogniowej może wtedy odbyć dopiero po tym, jak zainstalowany zostanie klient G Data Antivrus.

**Bezpośrednia instalacja sieciowa**

G Data AntiVirus ManagementServer może bezpośrednio przez sieć wyposażyć komputer w zabezpieczenie modułem klienta.

W tym przypadku komputery, na których ma zostać zainstalowany klient programu antywirusowego, są włączone w administratorze G Data AntiVirus, a następnie wykonywana jest dla nich instalacja klienta z wykorzystaniem odpowiedniej funkcji.

Wymaga to dostępu z poziomu jednostki ManagementServer do uprawnień administracyjnych C$ oraz Admin$, a także do rejestrów stacji roboczej. Do tego celu po stronie klienta musi zostać uruchomiona usługa „Dostęp zdalny”.


Przed ukończeniem instalacji użytkownik ma także opcję instalacji w tym samym czasie zapory ogniowej.
Instalacja w sieci przez pakiet cichej instalacji

W przypadku dużych sieci do instalacji może zostać użyty pakiet instalacyjny. Do tego celu w jednostce ManagementServer tworzony jest pakiet instalacyjny w postaci pojedynczego pliku EXE, zawierającego pakiet cichej instalacji. Może on zostać rozprowadzany wśród indywidualnych komputerów przy wykorzystywaniu mechanizmów domenowych (np. GPO, skrypty logowania). W tym przypadku użytkownik nie otrzymuje żadnej informacji na temat postępu instalacji.

Po ukończeniu instalacji użytkownik musi wylogować się i zalogować się ponownie tak, by wyświetlna była także ikona paska zasobników klienta, ponieważ działa ona w kontekście użytkownika.
**Instalacja klienta G Data AntiVirus dla komputerów z systemem Linux**

Aby zainstalować oprogramowanie klienta dla systemu Linux, należy wykonać następujące kroki:

**Zdalna instalacja oprogramowania klienta przez sieć**

W obszarze zadań „Klienci” menu „Ustawienia klienta” wybierz polecenie **Zainstaluj klienta G Data AntiVirus dla systemu Linux**. Pojawi się okno dialogowe, za pośrednictwem którego można zdefiniować klienta, do którego ma zostać przekopiowane oprogramowanie klienta. Do tego celu komputer musi być rozpoznawany przez sieć.

Wybierz nazwę komputera, jeśli na komputerze klienta zainstalowana jest usługa Samba lub jeśli komputer jest zarejestrowany w sieciowym serwerze nazw. Jeśli nazwa komputera nie zostanie rozpoznana, użyj adresu IP komputera.

![Zainstaluj program G Data Linux Client](image.png)

- **Rodzaj klienta**: Program Client dla stacji roboczych
- **Dane dostępu**: Nazwa komputera lub Adres IP
- **Adres IP**: 192.163.1.50
- **Hasło root**: ************
- **Status**: Pokaż raport...
Teraz wprowadź hasło administratora (root) dla tego komputera. Hasło administratora musi być przydzielone dla instalacji zdalnej. Domyślnie w pewnych dystrybucjach tak się nie dzieje, na przykład w Ubuntu.

Następnie kliknij przycisk Instaluj. W obszarze stanu możesz sprawdzić, czy instalacja oprogramowania klienta powiodła się.

**Ręczna instalacja oprogramowania klienta**

W specjalnym katalogu płyty CD programu można znaleźć następujące pliki:

- `installermsmb.bin` - instalator dla serwera plików Samba,
- `installerws.bin` - instalator dla stacji roboczej.

Możesz przekopiować te pliki na komputer klienta i uruchomić odpowiedni plik, instalując tym samym oprogramowanie klienta.

Dodatkowo znajdziesz tam również plik z sygnaturami wirusów. Instalacja tego pliku jest opcjonalna, ponieważ po instalacji program automatycznie otrzymuje z serwera najnowsze sygnatury wirusów.

- `signatures.tar` = archiwum z sygnaturami wirusów.
Instalacja G Data AntiVirus WebAdministrator

Przed zainstalowaniem jednostki WebAdministrator musisz włączyć funkcję systemu Windows „Kompatybilność z konfiguracjami IIS Metabasis oraz IIS 6". Jeśli funkcja ta nie jest dostępna, instalacja elementu WebAdministrator zostanie anulowana.

Ustawienie to można znaleźć, na przykład w systemie Windows Vista, w: „Start > Panel sterowania > programy > Programy i funkcje > Włącz lub wyłącz funkcje Windows”.

Możesz włączyć lub wyłączyć ustawienie w: „Internetowe usługi informacyjne > Narzędzia administracji sieci > Zarządzanie kompatybilnością z IIS 6 > Kompatybilność z konfiguracją IIS Metabasis oraz IIS 6”.

Dodatkowo, włączone muszą być także usługi www, o ile do tej pory były wyłączone. Ustaw znak zaznaczenia dla “Internetowe usługi informacyjne >usługi www”.

![Włącz lub Wyłącz funkcje systemu Windows](image.png)
1.2. G Data MailSecurity

**Definicje**

**e-mail routing:** odnosi się do przekazywania poczty, ogólnie za pomocą protokołu SMTP (Protokół prostego przekazywania poczty), tj. bezpośrednio z wysyłającego do otrzymującego komputera, z wykorzystaniem nazw domen zgodnych z serwerem DNS.

**POP3:** oznacza protokół pocztowy wersja 3 i jest odpowiedzialny za otrzymywanie wiadomości e-mail przez port 110.

**Porty:** porty przyporządkują pakiety danych odpowiednim usługom. Pozwalają na jednoczesne korzystanie z wielu usług, choć zalecane jest zainstalowanie serwera dla każdej usługi indywidualnej. Jeśli jeden serwis przestaje działać, inne usługi ciągle mogą być używane.

**Proxy:** odnosi się do serwera poczty elektronicznej akceptującego i przekazującego wiadomości e-mail.

**SMTP:** skrót ten oznacza protokół prostego przesyłania plików i jest odpowiedzialny za wysyłanie wiadomości e-mail używając portu 25.

**Kategoryzacja**

Uniwersalna, niezależna od serwera poczty, brama SMTP/POP3 z filtracją wirusów i spamu.

**Komponenty**

**G Data MailSecurity (brama poczty)**

Głównym elementem G Data MailSecurity jest komputer-brama, na którym wykonywana jest filtryacja wiadomości przychodzących i wychodzących. Brama może zostać zainstalowana na osobnym komputerze, a także bezpośrednio na serwerze poczty.


System operacyjny może być wersją dla stacji roboczej lub serwera, dla systemu 32- lub 64-bitowego.

**Administrator G Data MailSecurity**


Administracja może być zarówno lokalna – przez komputer-bramę lub zdalna- przez sieć lokalną LAN bądź przez tunel VPN lub dostęp zdalny, gdy dla chronionej sieci istnieją takie opcje dostępu.
**Instalacja**

**Instalacja na osobnym komputerze-bramie**

Jeżeli dla bramy dostępny jest oddzielny komputer, **routing poczty elektronicznej** powinien zostać tak zmodyfikowany, by wiadomości przychodzące z zewnątrz były najpierw kierowane do komputera – bramy.

Po sprawdzeniu otrzymanych wiadomości zostają one przekierowane do właściwego serwera poczty.

W przypadku wiadomości wychodzących serwer poczty jest skonfigurowany w taki sposób, by były one wysyłane do komputera-bramy jako **przekaźnika nadrzędnego**.

**Instalacja na serwerze poczty**

W przypadku instalacji bezpośrednio na serwerze poczty, obowiązują te same względy, jak w przypadku instalacji na osobnym komputerze-bramie. Jednak przydzielając określone porty, należy wziąć pod uwagę wszelkie cechy specjalne, aby uniknąć konfliktu przy przyporządkowaniu portów przez sam serwer pocztowy.
Konfiguracja filtra spamu

Wartość indeksu spamowania

Aby odróżnić wiadomości pożądaną od niepożądanego wykorzystywany jest system punktów.

System punktowy przyznaje różnicę wartość ważoną w zależności od kryteriów sprawdzanych dla każdej wiadomości, ponieważ nie każde kryterium jest tak samo ważne.

Dla każdego kryterium testowego przyznano specjalną skalę. Po sprawdzeniu wiadomości dodawane są indywidualne oceny tworzące wartość indeksu spamowania.

W zależności od wartości tego indeksu sprawdzana wiadomość jest przydzielana do jednej z trzech kategorii spamu (podejrzenie spamu, wysokie prawdopodobieństwo spamu, bardzo wysokie prawdopodobieństwo spamu).

OutbreakShield

Jako dodatkowe kryterium można użyć technologię OutbreakShield.

Podejście przyjmowane przez OutbreakShield jest zupełnie niezależne od sygnatur wirusów, a nawet niezależne od zawartości wiadomości e-mail.

Punktem wyjściowym jest fakt, że masowe złośliwe oprogramowanie w wiadomościach e-mail oraz w spamie ma wiele wspólnych cech. Wzór powstaje z oznak masowego rozprzestrzeniania się oprogramowania w internecie jest bardzo typowy i do wykrycia go można użyć dokładnie tych samych środków, których używa się do wykrywania spamu.
G Data znalazła partnera w firmie Commtouch, który z powodzeniem zabezpiecza ponad 50 milionów skrzynek pocztowych na całym świecie przed spamem i złośliwym oprogramowaniem. W Centrum wykrywania firmy Commtouch opatentowany system *Wykrywania powtarzających się wzorców* (RPD) ciągle analizuje ruch danych w sieci.

Wykorzystując konkretnie właściwości, powtarzające się wzorce pozyskiwane są z ruchu wiadomości e-mail i przechowywane w bazie danych.

Właściwości te zawierają takie informacje, jak adres IP nadawcy, pochodzenie z botnetu, rozmiar pliku, sumy kontrolne informacji zawartych w nagłówku wiadomości itp. Jeśli liczba identycznych wzorców przekracza ustalony próg, zgłaszany jest alarm. Wiadomości e-mail mogą zostać sklasyfikowane i blokowane jako spam i/lub złośliwe oprogramowanie po około pół do 2 minut.

Ponieważ te właściwości nie bazują na zawartości wiadomości ani na analizie pliku z załącznika, klasyfikacja ta jest niezależna od języka i formatu pliku.

W praktyce wygląda to w sposób następujący: produkty G Data AntiVirus sprawdzają przychodzące wiadomości e-mail w poszukiwaniu wirusów, używając technologii złożonej z dwóch niezależnych skanerów wirusów. Jeśli nie wykryto złośliwego oprogramowania, uruchamianie jest OutbreakShield, które wylicza sumę kontrolną porównywaną z wartością przechowywaną w Centrum wykrywania firmy Commtouch (co trwa około 300 milisekund). Jako odpowiedź OutbreakShield otrzymuje następnie klasyfikację, która w wiarygodny sposób kategoryzuje wiadomość e-mail jako spam lub złośliwe oprogramowanie.

Aby nie trzeba było zawsze przesyłać niektórych zapytań przez połączenie w trybie online, można przechowywać na komputerze bieżące informacje z bazy danych Commtouch.

**1.3. Jak dobrze znasz rozwiązania biznesowe G Data Security?**

**Pytania dotyczące aplikacji**:¹

2. Wymień funkcje komponentów indywidualnych.
3. Jakie są wymagania systemowe dla komponentów produktu G Data ClientSecurity Enterprise?

¹ Odpowiedzi znajdują się na ostatniej stronie.

---

-29-
2. G Data ClientSecurity Business – podstawy konfiguracji

Definicje


DB: skrót od: baza danych (ang.: database).

Ustawienia domyślne: odnosi się do ustawień fabrycznych programu.

Zmapowane napędy: napędy sieciowe, którym została przyporządkowana litera.

Tryb hybrydowy: oznacza podwójny lub wieloelementowy. W tym kontekście proces jest najpierw przetwarzany w jeden sposób, a jeśli się to nie powiedzie - w inny.

Usługa proxy: narzędzie przesyłające skutecznie dane między komputerami osobistymi lub programami a sieciami komputerowymi.

TCP: należy do rodziny protokołów internetowych i w ten sposób tworzy podstawy sieci internet. TCP jest powłoką transportową określającą, w jaki sposób między komputerami osobistymi są przekazywane dane.

2.1. Logowanie

Uruchamiając administratora zostaniesz zapytany o dane serwera, uwierzytelnienie, nazwę użytkownika i hasło.

W polu „Serwer” wprowadź nazwę lub adres IP komputera, na którym zainstalowany została jednostka ManagementServer. Następnie wybierz metodę uwierzytelniania.
Uwierzytelnianie Windows
Jeśli wybierzesz tę opcję uwierzytelniania, możesz zalogować się do tego komputera korzystając z nazwy użytkownika i hasła dla dostępu administratora tj. używając konta użytkownika systemu Windows. Natychmiast po instalacji logowanie będzie dostępne jedynie dla członków grupy Administratorów dla komputera MMS.

Uwierzytelnienie zintegrowane.
Używając zintegrowanego uwierzytelnienia, jako administrator systemu, możesz nadawać innym osobom dostęp do Administratora programu G Data AntiVirus. Na przykład możesz stworzyć specjalne konto, które będzie miało tylko prawa odczytu. Użytkownicy logujący się z takiego konta nie mogą dokonywać zmian w bazie danych.

Takie dodatkowe konto można stworzyć i administrować nim wykorzystując funkcję „Zarządzanie użytkownikami”.

![Jendowy ekran z formularzem do utworzenia konta]
2.2. Zarządzanie serwerem

Możesz przydzielać stacje robocze poszczególnym serwerom podsieci, które następnie łączą komunikację tych klientów z serwerem głównym, optymalizując w ten sposób zużycie sieci.

Korzystając z tego menu możesz zainstalować serwery podsieci.

Klikając przycisk „Przydziel stacje robocze”, możesz przydzielić określonym serwerom podsieci istniejących klientów.
Przydzielenie stacji roboczych serwerom podsieci jest niezależne od grupowania komputerów w drzewie. Różne serwery podsieci jednego klienta mogą naturalnie zostać połączone w grupę, by nadzorować wirusy i wykonywać zadania skanowania.

2.3. **Aktualizacje**

**Rozpowszechnianie aktualizacji w sieci**

Wszyscy podłączeni klienci mogą automatycznie otrzymywać z serwera ManagementServer najnowszą sygnaturę i aktualizację programu.

Mожesz określić, czy ma to zostać przeprowadzone indywidualnie dla każdego komputera czy też aktualizacje sygnatur i programu mają zostać przeprowadzone oddzielnie.

Każdy klient kontaktuje się co pięć minut z serwerem ManagementServer i porównuje swoją lokalną sygnaturę oraz stan wersji programu z tymi znajdującymi się na serwerze ManagementServer. Jeśli wersja posiada przez ManagementServer jest nowsza niż przechowywana wersja lokalna, aktualizacja zostanie przeprowadzona automatycznie (o ile tak zostało wybrane). Przedział czasu dla synchronizacji z serwerem można ustawić w Administratorze programu G Data AntiVirus w: „Ustawienia > Ustawienia serwera > Synchronizacja”.

**Bezpośrednia aktualizacja bez ManagementServer**

Jeśli klient nie ma dostępu do jednostki ManagementServer (np. notebook został usunięty z sieci lokalnej LAN przez pracowników terenowych), można zezwolić indywidualnemu klientowi na samodzielną aktualizację z wykorzystaniem dostępnego połączenia internetowego (na przykład w hotelu).

W tym przypadku zalecane jest skorzystanie z trybu hybrydowego, dla którego klient przede wszystkim próbuje uzyskać aktualizacje za pomocą jednostki ManagementServer. Jeśli nie powiedzie się to z uwagi na niedostępność jednostki ManagementServer, aktualizacja jest automatycznie przeprowadzana bezpośrednio od G Data wykorzystując połączenie internetowe użytkownika.

**Aktualizacja programu dla jednostki ManagementServer**

Sam ManagementServer jest aktualizowany z wykorzystaniem elementu menu startowego „Start-> Programy-> G Data AntiVirus ManagementServer -> Aktualizacja internetowa”. W tym miejscu muszą zostać zaktualizowane pliki programu serwera.

2.4. **Definicja grup**

Istnieje opcja zdefiniowania domyślnych ustawień dla każdej grupy. Musi to zostać przeprowadzone przynajmniej raz, w przeciwnym razie dziedziczone będą wartości domyślne dla całej sieci, gdy klienci będą „wciągani” do grupy. Dlatego też najpierw muszą zostać wybrane nowe wartości domyślne.
Kliknij prawym przyciskiem myszy w grupę i wybierz „Ustawienia domyślne”. Jeśli teraz dokonasz zmian w tym miejscu, każdy klient dodany do grupy odziedziczy te ustawienia. Nic nie jest zmieniane w ustawieniach istniejących klientów.

2.5. **Wiadomości e-mail**

Wraz z wprowadzeniem wersji 6.x klienta programu G Data AntiVirus włączona została usługa proxy, przeprowadzająca lokalne skanowanie wiadomości na poziomie protokołów POP3, SMTP oraz IMAP. Może to jednak spowodować problemy, jeśli serwer MailSecurity lub inny z serwerów pocztowych jest włączony równolegle z klientem lub używane porty są już zajęte przez inne programy pocztowe. Z tego powodu sprawdzanie tych trzech portów powinno zostać wyłączone w Administratorze programu G Data AntiVirus w: „E-mail->Nasłuch na portach-> Zmień”.

2.6. **Lokalny filtr spamu**

Lokalny filtr spamu sprawdza przychodzące wiadomości e-mail pod kątem spamu i oznacza je odpowiednio na komputerach służbowych. Oznaczenie tych wiadomości umożliwia szybkie posortowanie ich w kliencie poczty, przez co można zapobiec utratę ważnych wiadomości znajdujących się wśród serii wiadomości ze spamem.

Jeśli do teraz nie zainstalowano żadnego filtra spamu na komputerze służbowym lub jeśli użytkownik nie otrzymuje wiadomości e-mail za pośrednictwem odpowiednio chronionego serwera poczty, praca komputera użytkownika z wiadomościami przychodzącymi jest w ten sposób ułatwiona.

Jeśli użytkownik otrzymuje wszystkie wiadomości e-mail, na przykład za pośrednictwem G Data MailSecurity, to dodatkowe filtrowanie lokalne jest nadmiarowe i powinno zostać wyłączone.


Na stronie „Antispam” zakładki „Ustawienia” administrator może określić, jaki przedrostek powinien być używany dla wiadomości spam lub wiadomości podejrzanych zawierania spamu.
Dodatkowo po stronie klienta można zarządzać dwoma listami domen. Tak zwane białe i czarne listy pozwalają na określenie, czy wiadomość pochodząca z konkretnej domeny nigdy nie będzie oznaczana jako spam (biała lista) lub czy wiadomość pochodząca z konkretnej domeny będzie zawsze oznaczana jako spam (czarna lista).

Aby ustawić to, przejdź do przycisku „Edytuj..” dla odpowiedniej listy i po kolei dodawaj domeny do listy, edytuj domeny lub je usuwaj.
2.7. Zasoby sieciowe

Dla sieciowych stacji roboczych i serwerów opcja monitorowania „Skanuj zasoby sieciowe” powinna być zawsze wyłączona, jeśli wszystkie systemy są chronione przez skaner wirusowy. Opcja ta oznacza, że monitor skanuje nie tylko swoje partycje lokalne, ale także na przykład zmapowane napędy, foldery udostępniane, profile użytkowników itp.

W ten sposób, jeśli wszystkie komputery w sieci są chronione przez G Data AntiVirus, opcja ta powinna także być wyłączona dla każdego z nich, gdyż w przeciwnym wypadku sprawdzenie to będzie wykonywane dwukrotnie lub będzie opóźniane przez sieć. Może to na przykład skutkować opóźnieniami podczas uruchamiania komputera w przypadku, gdy profile użytkownika są ładowane z serwera.

2.8. Odinstalowywanie bez jednostki ManagementServer

Klient programu G Data AntiVirus może zostać zwykle tylko usunięty z wykorzystaniem jednostki ManagementServer, poza przypadkami, gdy użyta została opcja instalacji lokalnej.

Jeśli ManagementServer nie jest już dostępny, można zainicjować odinstalowywanie lokalnie dla każdego klienta wpisując polecenie:

```
unclient/AVKUninst
```

znajdując się w katalogu „C:\Program Files\G Data\AVKCClient”. Upewnij się, że wprowadzasz poprawnie parametr /AVKUninst (ważna wielkość liter).

Następnie uruchom ponownie komputer.

2.9. Migracja jednostki ManagementServer

Czasem konieczne jest stworzenie kopii zapasowej dla całej konfiguracji jednostki ManagementServer i przekopiowanie jej później z powrotem na przykład migrując ManagementServer na inny komputer lub do celów diagnostycznych.

Odinstalowując ManagementServer możesz zdecydować, czy usunąć także istniejącą bazę danych. Zostanie ona wtedy ponownie przyjęta podczas ponownej instalacji.

Przy korzystaniu ze zintegrowanej bazy danych, istniejąca konfiguracja jednostki ManagementServer może zostać przyjęta przez stworzenie kopii zapasowej plików z rozszerzeniem *.dat w katalogu „C:\Program Files\G Data\G Data AntiVirus ManagementServer”.

Aby zaimportować wcześniejszą konfigurację na nowy system, po prostu zakończ usługę „G Data AntiVirus ManagementServer”, a następnie przekopiuj wszystkie pliki *.dat do odpowiedniego katalogu programu. Usługę można teraz ponownie uruchomić i wywołać Administratora programu G Data Antivirus.

Nazwę jednostki ManagementServer można też w łatwy sposób wyzerować u klientów. W Administratorze programu G Data AntiVirus wybierz wszystkie komputery w widoku klienta i kliknij prawym przyciskiem myszy w „Zainstaluj klienta G Data AntiVirus”. Każdy komputer odpowie wtedy, że ochrona klienta jest już zainstalowana, a w tym samym czasie zmodyfikuje odpowiednio wpis do rejestru klienta.
Instalując w systemie ManagementServer, upewnij się, że NIE będzie używana baza danych SQL, a zintegrowana BD (baza danych). W przeciwnym wypadku zachowane ustawienia nie mogą zostać ponownie przesłane z powrotem.

Nie można przekonwertować zintegrowanej bazy danych w BD SQL i na odwrót.

2.10. Porty komunikacyjne

Jeżeli na serwerze aktywna jest zapora ogniowa Windows lub inna zapora ogniowa stacji roboczej, jako wyjątki należy określić porty TCP 7161, 7166, 7167 i 7169! Klient programu G Data AntiVirus i ManagementServer komunikują się używając tych portów.

Port TCP 7168 jest używany do nadzorowania jednostki ManagementServer programu G Data AntiVirus za pomocą Administratora G Data AntiVirus.

Port TCP 7161, 7166: Klient ➔ Serwer
Port TCP 7167, 7169: Klient ← Serwer
Port TCP 7168: Administrator ➔ Serwer

2.11. Jak dobrze znasz rozwiązania biznesowe G Data Security?

Pytania dotyczące aplikacji:2

1. Jakie zadania wykonują monitory klienta G Data AntiVirus oraz G Data AntiVirus?
2. Jakich opcji można pozbyć się wewnątrz ustawień monitora, aby zwiększyć wydajność wolniejszych klientów?
3. Jakie dodatkowe funkcje są włączone, aby zwiększyć wydajność?

2 Odpowiedzi znajdują się na ostatniej stronie.
3. G Data MailSecurity - podstawy konfiguracji

Definicje

Uwierzytelnienie: zawiera sprawdzenie tożsamości. Uwierzytelnienie SMTP zapewnia takie dane uwierzytelniające, jak: nazwa użytkownika i hasło na serwerze pocztowym.

Adresy IP: każdy komputer osobisty i każde inne urządzenie w sieci posiada adres protokołu internetowego (adres IP) składający się z liczb w formie 32 lub 128 cyfrowej liczby binarnej. Internetowe adresy IP są używane na przykład przy adresowaniu serwerów sieciowych.

3.1. Instrukcje

Instrukcje konfiguracji MailSecurity przygotowane na przykładzie serwera poczty AVM KEN.

Instrukcje zmiany G Data MailSecurity na AVM KEN 4

Zmiana portu

Port SMTP i POP3 musi zostać przekierowany z 25 lub 110 przykładowo na port 7025 lub 7110, ponieważ porty 25 i 110 będą teraz używane przez MailSecurity.

Tylko w starszych wersjach KEN konieczne jest ręczne ustawienie w pliku „KEN.cfg” znajdującego się w „C:\Programy\KEN!”.

Fragment pliku file KEN.cfg:
**Odbieranie wiadomości e-mail**

Poniżej zobrazowano zmianę serwera POP3 na adres IP komputera z MailSecurity:

![Zmiana serwera POP3](image)

Nazwa konta i hasło nie zmieniają się!
Wysyłanie wiadomości e-mail

Poniżej przedstawiono zmianę serwera SMTP na adres IP komputera z MailSecurity:

W tym przypadku należy wyłączyć logowanie SMTP w zakładce „Wysyłanie”, ponieważ uwierzytelnianie przejmuje sam MailSecurity!

Przykład konta użytkownika:

Serwer POP3: Adres IP komputera z MailSecurity
Port POP3: 7110
Serwer SMTP: Adres IP komputera z MailSecurity
Port SMTP: 7125
Nazwa użytkownika: imie.nazwisko@firma.pl (jak wcześniej)
Hasło: ****** (jak wcześniej)

Następnie uruchom ponownie usługę AVM KEN! W ten sposób ustawienia zostaną ostatecznie zastosowane.
Kopalnia wiedzy o rozwiązaniach biznesowych G Data Security

Ustawienia G Data MailSecurity

Ustawienia w zakładce „Wychodzące (SMTP)”.

| Przychodzące [POP3] | Skanowanie | Parametry skanowania | Kolejka | Inne
|---------------------|------------|----------------------|---------|-----
| Przychodzące (SMTP)| Wychodzące (SMTP)|                      |         |     |

**Odbiór:**
- Edycja poczty wychodzącej
- Port 7025 (IPv4, wszystkie adresy IP)

Adresy IP lub podsieci komputerów wysyłających wiadomości:
- 127.0.0.1
- 192.168.1.2

**Przekazywanie:**
- Użyj serwera DNS do wysyłania wiadomości
- Przekazuj wiadomości na ten serwer SMTP:
  - smtp.provider.com
  - Prgt: 25
  - Uwierzytelnianie...

IP nadawcy: Standardowa karta LAN

OK  Anuluj  Zastosuj  Pomoc
Ustawienia w zakładce „Przychodzące (POP3)”.

<table>
<thead>
<tr>
<th>Przychodzące (POP3)</th>
<th>Wychodzące (SMTP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zapytania</td>
<td></td>
</tr>
<tr>
<td>Edycja poczty przychodzącej POP3</td>
<td></td>
</tr>
<tr>
<td>Port 110 (IPv4, Wszystkie adresy IP)</td>
<td>Konfiguracja...</td>
</tr>
<tr>
<td>Ignoruj limit czasu połączenie w programie pocztowym</td>
<td></td>
</tr>
<tr>
<td>Odbiorze</td>
<td></td>
</tr>
<tr>
<td>Odbierz poczty z tego serwera POP3</td>
<td></td>
</tr>
<tr>
<td>pop3.provider.com</td>
<td>Port: 110</td>
</tr>
<tr>
<td>IP nadawcy</td>
<td>Standardowa karta LAN</td>
</tr>
<tr>
<td>Filtr</td>
<td></td>
</tr>
<tr>
<td>Tekst zastępczy dla odrzuconych wiadomości:</td>
<td></td>
</tr>
</tbody>
</table>

Wyłącz zupełnie „Przychodzące (SMTP)”!
3.2. **Wysyłanie kwerend do kilku serwerów POP3**

Jeżeli kwerendy będą wysyłane do wielu różnych serwerów POP3, w zakładce „Przychodzące (POP3)” dla MailSecurity nie powinny być wpisane żadne serwery POP3. Transmisja serwera korzysta z nazwy użytkownika konta POP3. W tym miejscu przed nazwą użytkownika należy wprowadzić adres serwera POP3 oddzielając nazwę od adresu za pomocą „:”.

**Przykład konta użytkownika:**

Serwer POP3: Adres IP komputera z MailSecurity
Port: 7110
Nazwa użytkownika: pop3.firma.pl:imie.nazwisko
Hasło: ***** (jak wcześniej)

3.3. **Jak dobrze znasz rozwiązania biznesowe G Data Security?**

**Pytania dotyczące aplikacji:**

1. W którym miejscu sieci zaimplementowany jest element MailSecurity?
2. Jakie są konieczne interwencje w systemie głównym dla serwera poczty?

---

³ Odpowiedzi znajdują się na ostatniej stronie.
4. Instalacja, startowa płyta CD, narzędzia i „często zadawane pytania”

Definicje

**Oprogramowanie kopii zapasowych**: oprogramowanie używane do tworzenia kopii zapasowych i odzyskiwania z nich danych.

**Ping**: program używany do sprawdzenia dostępności i czasu odpowiedzi hostów (np. serwerów sieciowych i pocztowych) w sieciach IP.

**Wtyczka**: odnosi się do dodatkowego modułu, będącego częścią oprogramowania.

**Zrestartowanie**: zrestartowanie oznacza ponowne uruchomienie komputera.

**Rootkit**: zbiór narzędzi administratorskich, pozwalających na przejęcie pełnej kontroli nad zaatakowanym systemem.

**Folder Temp**: folder plików tymczasowych. Używany jest do przechowywania plików aktualnie przetwarzanych przez system operacyjny.

4.1. Instalacja klienta programu G Data AntiVirus dla systemu Win2003/2008

Przed instalacją

Przed zainstalowaniem sprawdź, czy:


- w rejestrach i folderach systemowych na dysku nie pozostał żaden program ochrony antywirusowej (jeśli trzeba, użyj odpowiednich narzędzi czyszczących),


Więcej informacji na temat tej aktualizacji można znaleźć na stronie: [http://support.microsoft.com/kb/891861/en-us](http://support.microsoft.com/kb/891861/en-us)

- wszystkie ważne aktualizacje systemu Windows, a zwłaszcza wszystkie dostępne dodatki Service Pack zostały poprawnie zainstalowane (Win2000 - SP4 i aktualizacja Rollup 1, WinXP SP3, WinVISTA SP2, Win2003 SP2),

- została usunięta cała zawartość wszystkich folderów systemowych TEMP.
Instalacja

Zawsze upewnij się, że instalujesz najnowszą wersję klienta programu G Data AntiVirus!

Odpowiedni instalator jest dostępny na żądanie pod adresem: pomoc@gdata.pl.

Proszę zwrócić uwagę: instalując klienta programu G Data AntiVirus, trzeba mieć zawsze najnowszą wersję jednostki ManagementServer.

Konfiguracja

Wiadomości e-mail

Specjalnie dla poczty elektronicznej można w każdym kliencie programu G Data AntiVirus ustawić specjalną ochronę przed wirusami. W tym miejscu sprawdzane są protokoły POP3, IMAP i SMTP na poziomie TCP/IP. Oprócz tego, dla programu Microsoft Outlook używana jest specjalna wtyczka. Wtyczka automatycznie sprawdza wszystkie wiadomości przychodzące pod kątem wirusów i zapobiega wysyłaniu zainfekowanych wiadomości. Sprawdzanie na poziomie TCP/IP może prowadzić do konfliktów, jeżeli MailSecurity lub serwer pocztowy jest aktywny równolegle z klientem programu G Data AntiVirus.

W tym przypadku wyłącz sprawdzanie trzech portów w administratorze programu G Data AntiVirus, korzystając z opcji „Ustawienia-> E-Mail-> Nasłuch na portach->Zmień”!

Tło

Sprawdzenie nie jest konieczne, gdy jako klient poczty używany jest program Outlook, ponieważ MS Outlook jest nadal bezpośrednio chroniony przez wtyczkę antywirusową. Taka pośrednicząca ochrona nie jest ogólnie zapewniana dla serwerów, ale dla np. mobilnych notebooków, które odbierają wiadomości pocztowe bezpośrednio, używając programów Thunderbird lub Outlook Express.

Zadanie skanowania

Opcje monitorowania

Skanery

G Data AntiVirus pracuje z dwoma jednostkami analizującymi wirusy, działającymi niezależnie od siebie. W zasadzie użycie obydwu silników gwarantuje optymalne rezultaty w zapobieganiu infekcji. Z drugiej strony, wykorzystanie tylko jednego silnika ma pewne zalety dotyczące wydajności.

Zalecamy zezwolenie na równoległą pracę obydwu silników dla nowoczesnych komputerów.

Starsze komputery (na przykład te posiadające mniej niż 512 MB pamięci RAM oraz CPU o częstotliwości mniejszej niż 1 GHz) powinny używać ustawienia „Tylko silnik A”, ponieważ w tym trybie monitor jest bardzo szybki i rzadko ma wpływ na wydajność systemu.

Z drugiej strony, można użyć obydwu silników dla zadania cotygodniowego skanowania, aby skorzystać też z ochrony zapewnianej przez technologię DoubleScan.

W przypadku infekcji

W tym miejscu można określić działania, które należy podjąć, gdy wykryty zostanie zainfekowany plik. Istnieje wiele możliwości, które mogą lub nie muszą być skuteczne, w zależności od tego, do czego jest używany konkretny klient. Ustawienie Przenieś plik do kwarantanny powoduje utworzenie przez ManagementServer specjalnego katalogu, w którym szyfrowane są zainfekowane pliki i są w ten sposób przechowywane bez ciągłego szkodliwego skutku. Pliki znajdujące się w kwarantannie mogą zostać zdezynfekowane przez administratora, usunięte przeniesione z powrotem do swojego oryginalnego miejsca przechowywania lub, jeśli jest to konieczne, przesłane do usługi G Data Emergency AntiVirus Service.

Zainfekowane archiwum

Określ w tym miejscu, czy wyszukiwanie wirusów powinno być przeprowadzane osobno dla plików archiwum. W związku z tym, należy wziąć pod uwagę fakt, że wirusy w archiwach będą tylko wtedy szkodliwe, gdy zostaną rozpakowane. Pojedyncze pliki z archiwum nie mogą być usunięte ani zdezynfekowane. Musisz w tym miejscu określić, czy pliki archiwum będą w przypadku infekcji blokowane lub poddawane kwarantannie.

Typy plików

W tym miejscu możesz określić, które typy plików powinny być sprawdzane przez G Data AntiVirus pod kątem wirusów. Wprowadzanie zmian w tej części zwykle nie jest konieczne. Po ustawieniu opcji „Tylko pliki wykonywalne i dokumenty” sprawdzane będą tylko pliki wykonywalne, biblioteki DLL oraz znane zmiany plików.
Sprawdzaj podczas pisania
Oczywiście, w normalnej sytuacji niezawirusowany system nie generuje plików zainfekowanych przez wirusy podczas ich zapisywania. Jednakże, aby zabezpieczyć się na wszelką ewentualność, zwłaszcza w przypadku systemów, dla których nie uruchamiana była żadna podstawowa analiza wirusów, możesz ustawić w tym miejscu procedurę skanowania używaną podczas zapisywania plików. Ogromną zaletą tego jest:

• wykrywanie wirusów, które są kopiowane z innego, prawdopodobnie niechronionego, klienta do katalogu udostępnianego,
• wykrywanie wirusów w plikach pobieranych z internetu podczas procesu pobierania (czyli nie w czasie uruchamiania).

Skanuj zasoby sieciowe
W tym miejscu można określić działanie monitora wobec udostępnionych zasobów. Jeśli cała Twoja sieć jest zazwyczaj monitorowana przez G Data AntiVirus, zaleca się wyłączenie tej funkcji.

Tło:
Ta opcja powoduje, że monitor skanuje nie tylko partycje lokalne, ale także zmapowane napędy, foldery udostępnione, profile użytkowników itp., pomimo tego, że wszystkie komputery znajdujące się w sieci są i tak chronione przez program G Data AntiVirus. Jeśli opcja ta jest włączona, sprawdzanie będzie wykonywane dwukrotnie i może zakłócać działanie sieci. Może to skutkować także opóźnieniami podczas uruchamiania komputera na przykład w przypadku, gdy profile użytkownika są ładowane z serwera.

Heurystyka
w przypadku analizy heurystycznej wirusy nie tylko są wykrywane z wykorzystaniem ciągle aktualizowanych baz wirusów, ale także wykorzystując pewne cechy charakterystyczne wirusów. Z jednej strony, metoda ta jest dodatkową zaletą związaną z bezpieczeństwem, ale z drugiej strony w rzadkich przypadkach może skutkować zgłoszeniem fałszywych alarmów. Funkcję tę można wyłączyć, aby zwiększyć wydajność starego komputera.

Skanuj archiwa
Sprawdzanie skompresowanych danych w archiwum jest procesem bardzo czasochłonnym i może w większości przypadków zostać pominięte, jeżeli monitor wirusów programu G Data AntiVirus jest w Twoim systemie zawsze włączony. Monitor jest w stanie wykryć podczas rozpakowywania archiwum ukryty wcześniej wirus, a także automatycznie zapobiec jego rozprzestrzenianiu się.

Aby uniknąć pogorszenia się wydajności spowodowanego niepotrzebnymi sprawdzieniami dużych plików archiwn, które są rzadko używane, możesz ustalić graniczny rozmiar (w kilobajtach) plików archiwn, które będą sprawdzane. Jak pokazuje doświadczenie wirusy lub trojany pojawią się w bardzo małych plikach, rozmiar więc można ustawić na poniżej 1 MB bez wystawiania się na większe ryzyko.
Skanuj pliki e-mail

Opcja ta powinna generalnie być wyłączona ponieważ skanowanie archiwów wiadomości zwykle zabiera bardzo dużo czasu, a jeśli znaleziona zostaje zainfekowana wiadomość e-mail, pozostałych wiadomości nie można odczytać.

Ponieważ monitor blokuje uruchamianie załączników wiadomości, wyłączenie tej opcji nie spowoduje pojawienia się dziury w zabezpieczeniach.

Przy korzystaniu z programu Outlook skanowane są także wiadomości przychodzące i wychodzące, z wykorzystaniem zintegrowanej wtyczki.

Skanuj obszary systemowe przy starcie komputera / zmianie nośnika

W ogólnym przypadku obszary systemowe Twojego komputera (np. boot sektory) nie powinny być wyłączone ze sprawdzania wirusów. W tym miejscu możesz określić, czy chcesz sprawdzać je podczas uruchamiania systemu lub zawsze, gdy zmieniane są nośniki (włożona zostanie nowa płyta CD itp.) Ogólnie rzecz biorąc powinno się włączyć przynajmniej jedną z tych funkcji.

Wykrywaj dialery / spyware / adware / riskware

Używając G Data AntiVirus możesz także sprawdzić swój system pod kątem oprogramowania typu dialer i innych złośliwych programów. Są to programy, które ustanawiają na przykład drogia, niechciane połączenia internetowe, a wyrządzone przez nie potencjalne szkody finansowe są wcale nie mniejsze od szkód pochylan przez wirusy. Mogą na przykład zachowywać odwiedzane zwykle przez Ciebie strony internetowe, a nawet rejestrować wszystkie uderzenia klawiszy (łącznie z hasłami), a następnie, przy najbliższej nadarzającej się okazji, przesyłać je do stron trzecich. Jednak dwa silniki, nawet bez tej opcji, są w stanie wykryć standardowe dialery. Ryzykowne oprogramowanie nie jest tylko identyfikowane jako wirus. Jeśli ta opcja w monitorze jest wyłączona, z powodów bezpieczeństwa absolutnie nie powinieneś pozbywać się jej w zadaniach skanowania.
Uwaga: Oczywiście, podział na komputery „szybkie” i „wolne” jest bardzo subiektywny!

Wyjątki

W tym miejscu można także ograniczyć sprawdzanie wirusów do określonych katalogów. W ten sposób można na przykład ominąć foldery zawierające rzadko używane archiwa lub zintegrować je ze specjalnym planem skanowania. Dodatkowo, niektóre pliki i typy plików mogą zostać wyłączone ze sprawowania wirusów. Pliki, katalogi, napędy lub procesy mogą zostać zdefiniowane jako wyjątki.

Znaki wieloznaczności są następujące:

- symbol znaku zapytania (?) reprezentuje pojedyncze znaki,
- symbol gwiazdki (*) reprezentuje całe łańcuchy znaków.

Funkcje specjalne

Wyjatki skanowania
foldery, które nie mają być sprawdzane u klientów podczas wykonywania zadań skanowania muszą zostać oddzielnie zdefiniowane w obszarze roboczym „Ustawienia-> Ogólne”.
Foldery baz danych, kopii zapasowych dysku lub partycji mogą zostać określone jako wyjątki.
Wyjątki mogą zostać zdefiniowane dla całych grup. Modyfikowanie wyjątków dla całej grupy nie wpływa na indywidualne ustawienia stacji. Podobnie działają wyjątki monitora dostępowego.

Opcje specjalne

Serwer Exchange

Serwer terminali
Ustaw element „Symbol na pasku narzędzi” znajdujący się w obszarze roboczym „Ustawienia” konkretnego klienta na: „Wyświetlaj tylko podczas pierwszej sesji”!

Zapora ogniowa
Jeżeli na serwerze aktywna jest zapora ogniowa Windows lub inna zapora ogniowa stacji roboczej, jako wyjątki należy określić porty 7161, 7166, 7167 i 7169 (TCP).
Tlo:
Klient programu G Data AntiVirus i ManagementServer komunikują się między sobą używając tych portów.
Oprogramowanie kopii zapasowych
Generalnie dostępny skaner wirusowy może zakłócić tworzenie kopii zapasowej. Wyłącz go na czas sporządzania kopii zapasowych!

Tło:
Dostępny skaner wirusów sprawdza wszystkie operacje przesyłania danych. Może to spowodować w niektórych okolicznościach problemy np. z zapełnieniem pamięci.

Wskazówka: w przypadku standardowych programów tworzących kopie zapasowe można użyć polecenia, które wyłącza skaner wirusów i włącza go automatycznie ponownie po sporządzeniu kopii. Aby móc tak zrobić, po prostu skontaktuj się ze wsparciem technicznym pod adresem: pomoc@gdata.pl.

Począwszy od wersji 9.0 możliwe jest stworzenie wyjątku dla procesu. Ustawienie jako wyjątku procesu aplikacji tworzącej kopie zapasowe może być rozsądnym krokiem.
4.2. Startowa płyta CD

Złośliwe oprogramowanie ukrywające się przy użyciu technologii rootkitowych może nie zostać wykryte w działających systemach operacyjnych.

Aby dać sobie radę z tym problemem, G Data oferuje startową płyta CD, która umożliwia przeskanowanie systemu z wykorzystaniem specjalnego środowiska startowego opartego na systemie Linux.

Umożliwi to zidentyfikowanie i usunięcie złośliwych rootkitów, które w innym wypadku mogłyby nie zostać wykryte podczas operacji wykorzystującej standardowe środki.

Jeśli używasz routera, który automatycznie przydziela adresy IP (DHCP), program będzie mógł pobrać aktualizacje sygnatur wirusów z Internetu.

---

**G Data AntiVirus BootCD**

**Microsoft Windows**

Płyta startowa G Data
Płyta startowa G Data – Tryb bezpieczny

Wybierz tryb uruchomienia klawiszami strzałek.

22

Wejsnij <Enter>, aby uruchomić system Microsoft Windows.
4.3. Narzędzia

AV-Cleaner

**Funkcja**

Usuwa wszystkie ślady programów znajdujące się nadal w rejestrze pomimo ich odinstalowania. **AV-Cleaner** usuwa wszystkie składniki instalacji wszystkich produktów G Data AntiVirus.

![AV-Cleaner interface](image)

**Działanie:**

Uruchom oczyszczacz używając uprawnień administratora! Zrestartuj komputer i uruchom oczyszczacz raz jeszcze, aby usunąć składniki, które mogły nie zostać natychmiast usunięte przy pierwszym uruchomieniu.
Monitor - MonActivityCS

Narzędzie monitor pozwala na monitorowanie wykonywanych w tle działań monitora AV, aby przeanalizować bardziej szczegółowo problemy z wydajnością.

![Monitor - MonActivityCS](image)

Działanie:
Uruchom narzędzie równolegle, np. pracując „normalnie” na komputerze w trybie czasu rzeczywistego i postaraj się odtworzyć problem. Lub pozwól mu działać przez około 30 minut z funkcją Hitlist, a następnie zaktualizuj wyświetlac. Definicja wyjątków może wtedy poprawić problem, o ile jest on powodowany przez jeden konkretny typ plików.
Quarantine (Kwarantanna)

 Można użyć tego narzędzia do przywracania plików poddanych kwarantannie do dowolnej lokalizacji.

Pliki kwarantanny mają rozszerzenie *.q i można je znaleźć u klienta w katalogu "C:\Program files\Common Files\G Data\AVKScanP\QBase" lub na serwerze w lokalizacji: "C:\Documents and settings\All Users\Dane aplikacji\G DATA\AntiVirus ManagementServer\Quarantine".

Za pomocą tego możesz bez problemu np.: przywrócić zainfekowane bazy danych poczty, takie jak pliki *.pst do wybranej lokalizacji.
4.4. Często zadawane pytania

Komunikat o błędzie: „Baza danych wirusów/pliki programu jest/są uszkodzone.”

Jeśli wiadomość nie będzie pojawiać się codziennie, oznacza to, że problem rozwiązał się samoistnie. ManagementServer wymienił uszkodzony plik.

W przeciwnym wypadku:

1. Problem powinien w zasadzie zostać rozwiązany przez aktualizację jednostki ManagementServer (Start > Programy > G Data AntiVirus ManagementServer > Internet Update) oraz ponowne pobranie sygnatur wirusów (Administrator G Data AntiVirus musi być wtedy zamknięty). Najlepiej wyłączyć na czas operacji opcję Kontrola wersji.

2. Jeśli to nie rozwiąże problemu, należy przeprowadzić w następujący sposób „aktualizację naprawczą”:
   • Usuń wszystkie podfoldery (Avast, BD, Client, Server) i, o ile to możliwe, foldery tymczasowe znajdujące się w folderze: „C:\Users\All Users\G DATA\AntiVirus ManagementServer\Aktualizacje”.
   • Zamknij administrator G Data AntiVirus.
   • W „Start > Programy > G Data AntiVirus ManagementServer” uruchom moduł „Internet Update” (Zaktualizuj w pliki programów (zarówno dla serwera, jak i klienta) razem z bazą danych wirusów, ale BEZ sprawdzania wersji (!).
   • Następnie zaktualizuj bazę danych wirusów na komputerze klienta korzystając z Administratora.

Problemy z aktualizacjami internetowymi używającymi Administratora G Data AntiVirus

Aby rozwiązać problemy z aktualizacjami, należy:

1. Sprawdzić, czy dane dostepowe zostały wprowadzone poprawnie!
2. Wprowadzić konto użytkownika! Możesz wprowadzić dane dostępu do serwera Proxy korzystając z aplikacji „Internet Update > Ustawienia internetowe”.
3. Sprawdzić, czy poprawne są ustawienia serwera pośredniczącego!
4. Upewnij się, czy dostęp nie jest blokowany przez opcję Zapory ogniowej! (Port 80 (http) musi być otwarty).
Sprawdź komunikację między ManagementServer a klientami

Kolumna „Ostatni dostęp” w obszarze zadania „Klienci” przedstawia datę ostatniego raportowania klienta do jednostki ManagementServer. Zwykle klient raportuje jednostce ManagementServer co pięć minut (o ile nie ma aktualnie żadnych działających zadań skanowania).

Przyczynami nieudanego połączenia może być:

1. Klient jest wyłączony lub odluzony od sieci.

4. Zamiennie, ManagementServer może także odpowiedzieć bezpośrednio przez adres IP. Poniżej przedstawiono ścieżkę dostępu w rejestrach, które należy zmienić na komputerze klienta:
   "HKEY_LOCAL_MACHINE\SOFTWARE\G DATA\AVKClient" w "Serwer" wpisz adres IP jednostki ManagementServer.


Skrzynka pocztowa poddana kwarantannie

Tak się zwykle dzieje, gdy skrzynka pocztowa przed zainstalowaniem programu G Data AntiVirus zawierała już zainfekowaną wiadomość e-mail.

Proszę postępować w następujący sposób, aby wyczyścić np. plik pst z programu MS Outlook:

1. Zamknij program Outlook.
2. W ustawieniach Strażnika wyłącz sprawdzanie plików e-mail.
3. Uruchom narzędzie kwarantannie. Dla podanych plików, który mają rozszerzenie *.q i można je znaleźć na stacjach w folderze „C:\Programy Files\Common Files\G DATA\AVKScanP\QBase” lub na serwerze w następującej lokalizacji: „C:\Users\All Users\Dane aplikacji\G DATA\AntiVirus ManagementServer\Quarantine”).
4. Wybierz plik pst i przywróć go do nowego (!) folderu.
5. Uruchom program Outlook i otwórz to archiwum.
6. Usuń zainfekowaną wiadomość e-mail (o ile jest widoczna).
7. Opróżnij folder „Elementy usunięte”.
8. Skompaktuj foldery poczty! (wewnętrzna funkcja programu Outlook: Kliknij prawym klawiszem myszy w Skrzynkę odbiorczą > Właściwości > Zaawansowane > Kompaktuj teraz)

Dopiero w tym momencie wszystkie usunięte elementy zostają fizycznie usunięte z pocztowej bazy danych, a plik pst jest znów wolny od wirusów.
Klient na komputerze z systemem Linux – brak połączenia z jednostką ManagementServer

1. Sprawdź, czy działają procesy klienta G Data AntiVirus.

   W linii poleceń systemu Linux wpisz: `~# ps ax grep avk`.

   Powinieneś zobaczyć:

   \- `/usr/sbin/avkserver --demon (ScanServer)`

   \- `/usr/sbin/avguard --demon` (tylko dla stacji roboczych, nie dla serwera plików z systemem Samba)

   \- `/usr/sbin/avclient --demon` (m.i. ustanawia połączenie z MMS, przeprowadza aktualizacje).

   Niezależnie od używanej dystrybucji możesz uruchamiać lub zatrzymywać procesy za pomocą polecenia:`/etc/init.d/<nazwa usługi> start|stop`.

   Aby to zrobić, musisz być załogowany jako administrator („root”) na komputerze z systemem Linux.

2. Sprawdź pliki logów.

   Pliki logów `gdav.log`, `avclient.log` i `avguard.log` można znaleźć w katalogu: `/var/log/gdata`.

   Sprawdź te pliki i poszukaj jakichkolwiek komunikatów o błędach. Jeśli chcesz zobaczyć więcej komunikatów, należy zwiększyć ilość wpisów dla `LogLevel` w plikach konfiguracyjnych.

   Pliki konfiguracyjne: `gdav.ini`, `avclient.cfg` i `avguard.cfg` można znaleźć w katalogu: `/etc/gdata`.

   Poziom logowania we wszystkich plikach jest ustawiony na „3”, co oznacza, że rejestrowane są tylko błędy.

   Wyższe wartości powodują generowanie większej ilości wyników:

   - 3: błędy,
   - 4: ostrzeżenia,
   - 5: uwagi,
   - 6: informacje,
   - 7: analiza kodu,
   - 8: śledzenie.

   **Uwaga:** Wysokie wartości dla `LogLevel` generują mnóstwo komunikatów, co sprawia, że pliki logów szybko zwiększają rozmiar. Dla normalnych warunków działania ustawiaj zawsze `LogLevel` na 3!

3. Sprawdź skaner.

   Użyj narzędzia z linii poleceń `avkclient`, aby sprawdzić działanie serwera skanowania `avkserver`. Można wykonać następujące polecenia:

   ```
   linux:~$ avkclient avkversion       - zwraca wersję i datę aktualizacji sygnatur wirusów
   linux:~$ avkclient version         - zwraca wersję w krótkiej formie
   linux:~$ avkclientscan:<plik>    - skanuje plik `<plik>` i zwraca wynik.
   ```

4. Sprawdź plik konfiguracyjny.
Plik etc/gdata/avclient.cfg jest plikiem konfiguracyjnym dla zdalnego klienta avclient. Sprawdź, czy adres głównego serwera zarządzania (Główny MMS) został wprowadzony poprawnie. Jeśli nie, usuń niepoprawny wpis i zarejestruj się ponownie w kliencie Linux za pomocą Administratpra programu G Data AntiVirus lub bezpośrednio wprowadź adres G Data AntiVirus ManagementServer.

5. Sprawdź swoje uprawnienia.

Ochrona antywirusowa dla autoryzacji systemu Samba jest włączana przez: vfs objects = gdfs
w pliku konfiguracyjnym systemu Samba /etc/samba/smb.conf.

Jeżeli wpis znajduje się w sekcji [global], ochrona jest włączona dla wszystkich uwierzytelnień. Wpis ten znajduje się w innej sekcji, ochrona istnieje tylko dla danego uwierzytelnienia. Możesz, do celów testowych, zamienić ten wpis w komentarz (wstawiając symbol „#” na początku linii), aby sprawdzić, czy dostęp działa bez ochrony antywirusowej. Jeśli nie, proszę najpierw poszukać błędów w swojej konfiguracji systemu Samba.


Sprawdź, czy działa proces monitora avguard: ps ax|grep avguard

Monitor wymaga modułów jądra: redirfs i avflt. Za pomocą polecenia lsmod możesz sprawdzić, czy załadowane są moduły: lsmod|grep redirfs i lsmod|grep avflt...

Rozwiązania

Strona 29

1. Wymień składniki produktu G Data ClientSecurity Enterprise!
   G Data ClientSecurity Business (ManagementServer, (Web) Admin, (Samba) Client, Firewall), G Data MailSecurity

2. Wymień funkcje komponentów indywidualnych!
   ManagementServer: centralna jednostka administracyjna, brak aktywnej ochrony antywirusowej
   Administrator (sieciowy): Graficzny interfejs użytkownika dla jednostki ManagementServer
   Klient: Lokalna aktywna ochrona antywirusowa na poziomie plików. Składa się ze skanera (na żądanie – OnDemand) i modułu monitora (dostępowy – OnAccess), a także zaporę ogniową klienta
   G Data MailSecurity: Centralny filtr poczty na poziomie POP3 i SMTP

3. Jakie są wymagania systemowe dla komponentów produktu G Data ClientSecurity Enterprise?
   Klient G Data AntiVirus: jak Win2000 SP4 UR1
   G Data AntiVirus ManagementServer: WinXP lub nowszy, Microsoft .NET Framework 3.5, brak koniecznego systemu operacyjnego dla serwera
   G Data MailSecurity: jak Win2000 SP4, brak obowiązkowego systemu operacyjnego dla serwera

Strona 37

1. Jakie zadania wykonują monitory klienta G Data AntiVirus oraz G Data AntiVirus?
   Klient G Data AntiVirus: skanowanie na żądanie (OnDemand) / koordynacja okresowych i jednokrotnych skanów dysku, opcjonalny nadzór nad różnymi funkcjami klienta
   Monitor G Data AntiVirus: dostępowe (OnAccess) praz ochrona antywirusowa na żywo z dostępem do plików

2. Jakich opcji można pozbyć się wewnątrz ustawień monitora, aby zwiększyć wydajność wolniejszych klientów?
   Zaznacz dostęp do sieci, heurystykę, jeśli konieczne, wyłącz jeden silnik (dostępowe – OnAccess)

3. Jakie dodatkowe funkcje są włączone, aby zwiększyć wydajność?
   Definicja pewnych wyjątków monitora (np. folder instalacyjny często używanych aplikacji, wyłączenie konkretnych typów plików).

Strona 43

1. W którym miejscu sieci zaimplementowany jest MailSecurity?
   Lokalna implementacja znajduje się między serwerem poczty a siecią Internet. Fizyczna implementacja może być różna.

2. Jakie są konieczne interwencje w systemie głównym dla serwera poczty?
   Upewnij się ponad wszelką wątpliwość, że ZRESTARTUJESZ potem usługi.