



Poradnik administratora

Korporacyjne rozwiązania G Data

Przejrzyj wybrane zagadnienia dotyczące obsługi aplikacji G Data do ochrony przedsiębiorstw.

Dowiedz się w jaki sposób funkcjonują aplikacje G Data dla przedsiębiorstw.

Sprawdź jak zaplanować i zainstalować oprogramowanie chroniące stacje robocze i serwery.

Poznaj i wypróbuj nietypowe funkcje oraz dodatkowe możliwości ochrony przed zagrożeniami.

Dołącz do najlepszych specjalistów!

Go safe. Go safer. G Data.



Planowanie architektury i instalacja

Właściwe zaplanowanie implementacji systemów zabezpieczających jest równie ważne jak prawidłowe planowanie sieci komputerowej przedsiębiorstwa. Elastyczność rozwiązań korporacyjnych G Data ułatwia dostosowanie zestawu aplikacji zabezpieczających do przygotowanej wcześniej struktury firmy.

Hierarchizacja Serwerów zarządzających ochroną stacji roboczych.

Rozwiązania korporacyjne G Data AntiVirus/ClientSecurity umożliwiają zainstalowanie jednej instancji głównego Serwera zarządzającego ochroną stacji roboczych. W celu zapewnienia nadmiarowości można zainstalować na innym komputerze Serwer zapasowy, pełniący rolę serwera głównego w momencie, kiedy serwer główny jest niedostępny.

Oprócz Serwerów zarządzających pierwszego poziomu, można zastosować dowolną ilość serwerów podrzędnych – w zależności od potrzeb i zastosowanej segmentacji sieci. Serwery podrzędne przechowują i synchronizują zadania serwera głównego minimalizując jego obciążenie, a także ruch sieciowy.

Dostępne z programu G Data Administrator polecenie *Plik > Zarządzanie serwerami...* umożliwia przydzielanie poszczególnych stacji roboczych do wybranych serwerów.

Baza danych przechowująca ustawienia i raporty

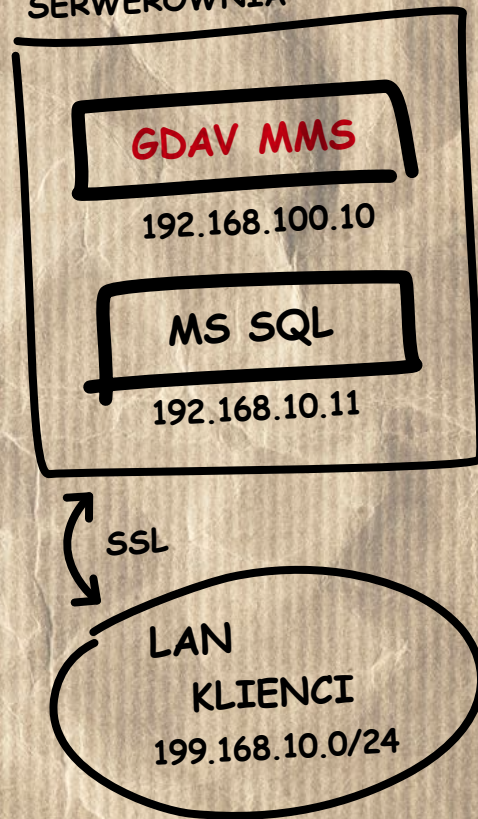
Podczas instalacji głównego Serwera zarządzającego ochroną stacji roboczych program pyta, jaką bazę danych zastosować do przechowywania ustawień i raportów aplikacji zabezpieczających. Do wyboru jest zintegrowana baza w formacie dBASE, baza SQL Express 2005 lub też istniejąca instancja bazy SQL w wersji od 2005 wzwyż.

W przypadku większych sieci, zalecamy stosowanie baz korzystających z języka SQL, które są wydajniejsze niż tradycyjne bazy danych dBASE.

Istnieje możliwość zmiany rodzaju bazy danych po zainstalowaniu programu, co wiąże się jednak z utratą wszystkich ustawień i raportów. W tym celu otwórz folder *C:\Program Files\G Data\G Data AntiVirus Management Server* i uruchom plik o nazwie *GdmmsConfig.exe*.

Narzędzie konfiguracyjne umożliwia przełączenie między bazą zintegrowaną, a bazami SQL, a także podłączenie się do dowolnej bazy SQL w sieci lokalnej. Można również zmienić domyślnie ustawione uwierzytelnianie systemu Windows na uwierzytelnianie SQL. Dodatkowo narzędzie umożliwia wczytanie listy baz z serwera SQL, a także założenie nowej bazy dla aplikacji korporacyjnych G Data.

SERWEROWNIA





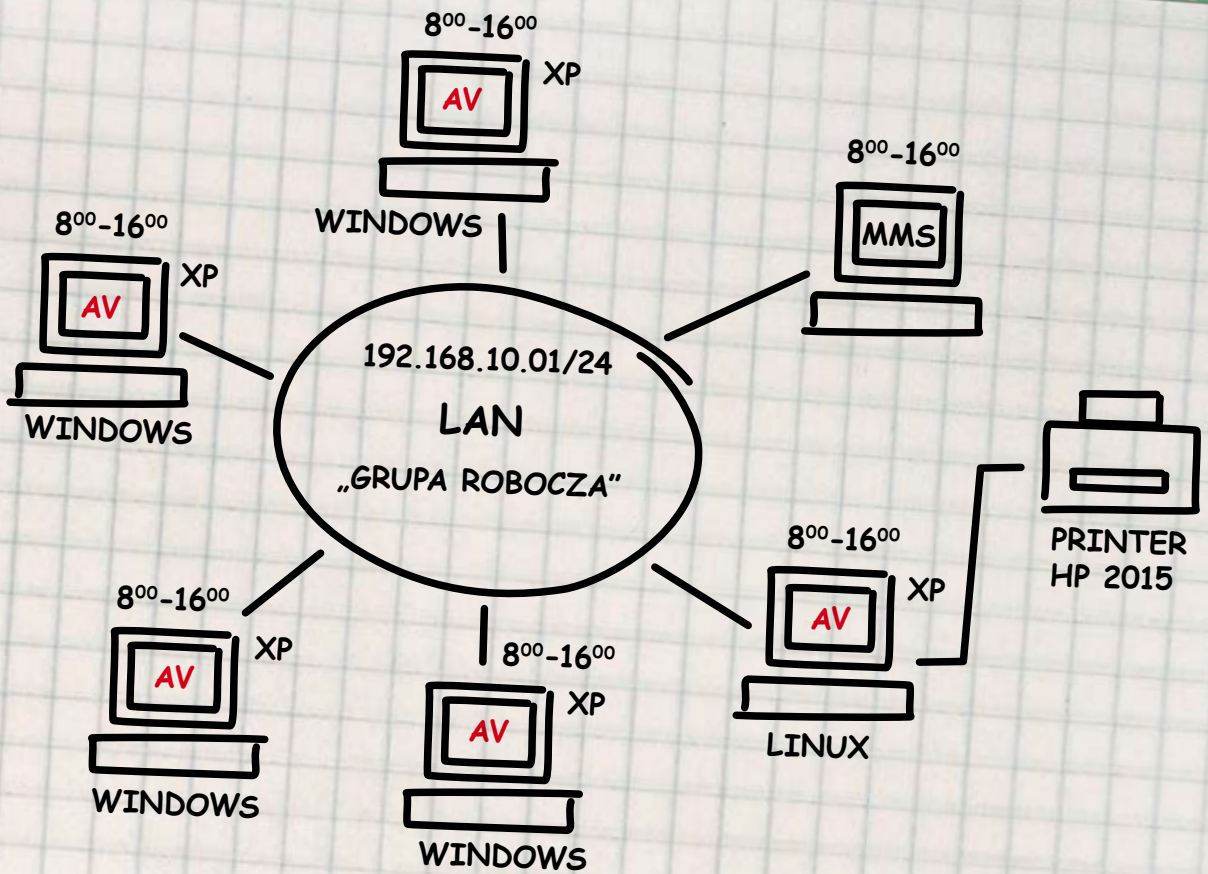
Planowanie architektury i instalacja

Instalacja oprogramowania klienckiego w domenie i grupie roboczej Windows

O ile instalacja zdalna w domenie Windows nie wymaga zaawansowanych umiejętności, instalacja składnika klienckiego na stacjach w grupie roboczej wymaga kilku słów komentarza. Instalacja zdalna wymaga dostępu do zasobów lokalnych i rejestru stacji roboczej. Ponadto korzysta z portów transportowych protokołu TCP/IP. Do przeprowadzenia instalacji zdalnej w grupie roboczej wymagane jest spełnienie trzech poniższych warunków.

1. Zarówno na komputerze z Serwerem zarządzającym, jak i na stacji roboczej załóż konto z uprawnieniami administratora o tej samej nazwie i z tym samym hasłem
2. W oknie *Panel sterowania > Narzędzia administracyjne > Zasady zabezpieczeń lokalnych > Zasady lokalne > Opcje zabezpieczeń* znajdź ustawienie *Dostęp sieciowy: udostępnianie i model zabezpieczeń dla kont lokalnych*. Zmień ustawienie *Tylko gość* na *Klasyczny*.
3. W ustawieniach Zapory systemu Windows włącz wyjątek dla opcji *Udostępnianie plików i drukarek*.

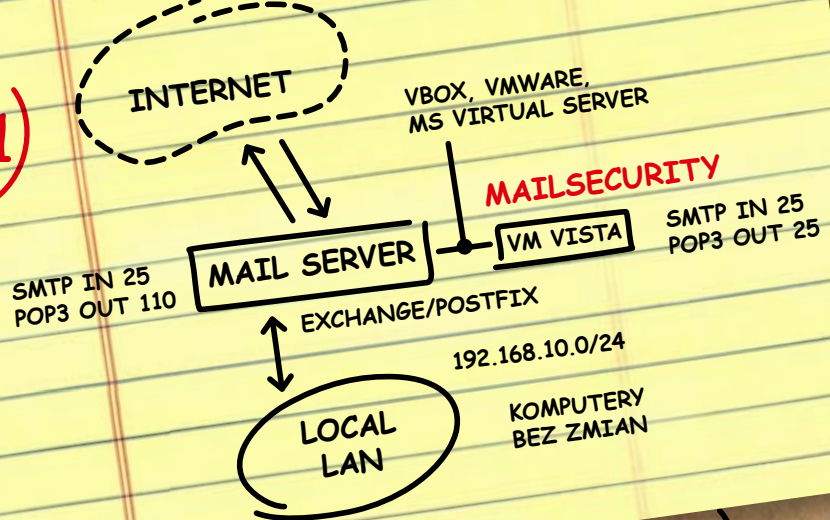
Alternatywą jest zainstalowanie oprogramowania klienckiego na każdej stacji roboczej ręcznie, przy użyciu płyty instalacyjnej, pobranego pliku instalacyjnego lub udostępnionego folderu zawierającego pliki instalacyjne (C:\Program Files\G DATA\G DATA AntiVirus ManagementServer\AvkClientSetup)



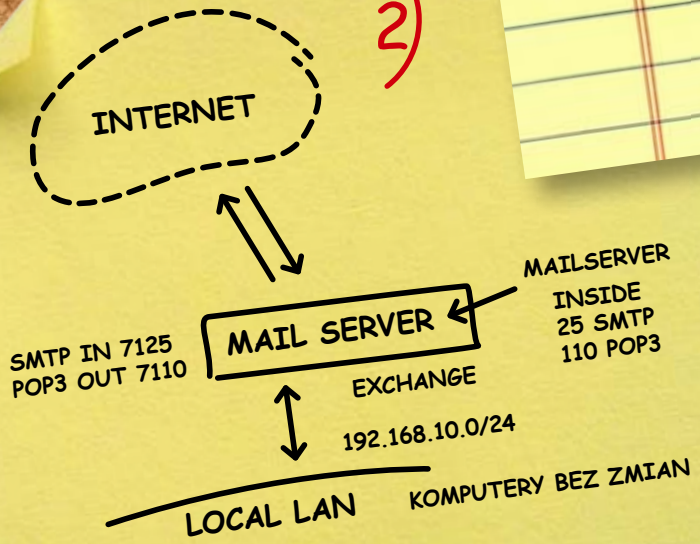


Planowanie architektury i instalacja

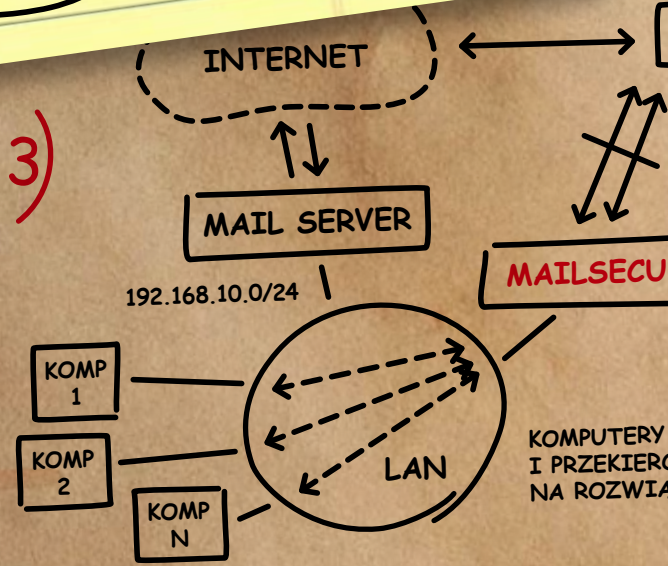
1)



2)



3)



Instalacja antywirusowej i antyspamowej bramy poczty elektronicznej

Aplikacja G Data MailSecurity funkcjonuje w systemie operacyjnym Windows, ale może chronić **dowolny serwer poczty** działający w dowolnym systemie operacyjnym. W zależności od potrzeb możesz zastosować jeden z 3 poniższych wariantów implementacji bramy pocztowej.

1. Instalacja na osobnym systemie (maszyna fizyczna lub wirtualna)

Opcje -> Przychodzące (SMTP) -> Przekazywanie (wprowadź port i adres serwera poczty, na który wiadomości będą przekazywane). To samo analogicznie z pocztą wychodzącą SMTP oraz przychodzącą POP3.

2. Instalacja na komputerze z serwerem Microsoft Exchange

Konfiguracja wygląda podobnie. Wszystko odbywa się na jednej maszynie więc tutaj możemy posłużyć się wysyłką poprzez ustawienia DNS. Należy jednak pamiętać o zmianie portów MS Exchange na wyższe, np.: **7125 (SMTP)** oraz **7110 (POP3)**. MailSecurity będzie nasłuchiwał zawsze na portach 25 oraz 110.

3. Instalacja bez serwera poczty

Jeśli nie posiadasz własnego serwera poczty, możesz również chronić pocztę swoich współpracowników przed spamem i wirusami na poziomie skanowania POP3. W tym celu zainstaluj G Data MailSecurity, następnie *Opcje -> Przychodzące (POP3) -> Edycja poczty przychodzącej POP3 -> Port 110 -> **adres IP serwera zostaw pusty!*** Wszystkich odbierających pocztę przekieruj na MailSecurity zmieniając adres serwera poczty na adres IP bramy pocztowej. W programie pocztowym wprowadź dodatkowo nazwę użytkownika jako: **adres.ip.serwera.poczty.np.wp:nazwa.uzytkownika**.

MAIL SERVER

ISP (WP, GOOGLE,
ONET ITP.)

RITY

SMTP 25
POP3 110

WYMAGAJĄ ZMIANY
OWANIA
ZANIE G DATA



Planowanie architektury i instalacja

Instalacja oprogramowania klienckiego dla systemów Linux

Instalacja zdalna odbywa się za pomocą protokołu ssh. Konieczne jest wówczas uruchomienie usługi ssh na komputerze przeznaczonym dla instalacji Klienta, a w zaporze sieciowej odblokowanie portu ssh (domyślny: 22). Użytkownik root musi mieć prawo logowania via ssh (**sshd_conf: PermitRootLogin yes**).

1. Na stacji roboczej Linux

Administrator G Data AntiVirus -> Ustawienia Klienci -> Zainstaluj Klienta G Data AntiVirus dla systemu Linux -> Rodzaj Klienta: Klient dla stacji roboczych Linux (Jeśli w sieci funkcjonuje poprawnie skonfigurowany serwer DNS wybieramy opcję „Nazwa komputera”, jeśli nie - „Adres IP”).

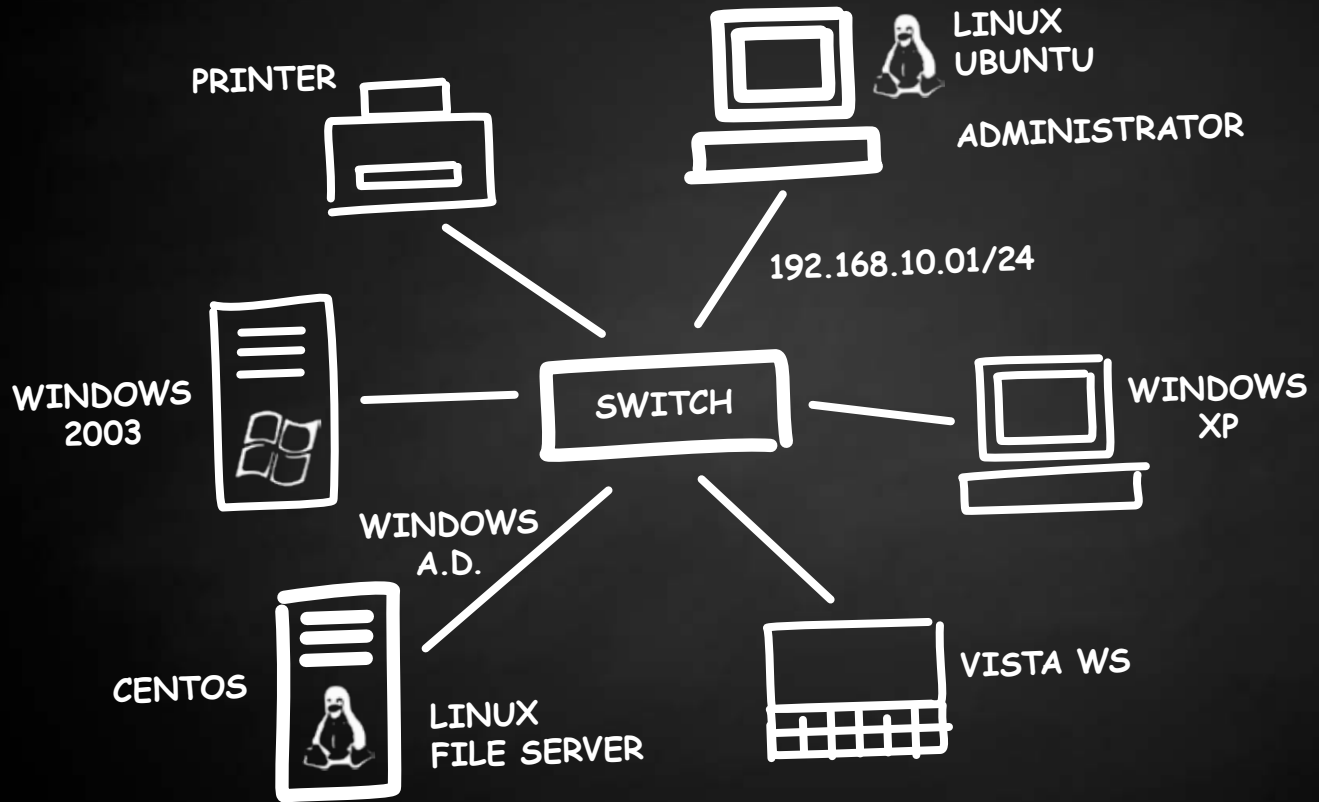
2. Na serwerze Samba

Administrator G Data AntiVirus -> Ustawienia Klienci -> Zainstaluj Klienta G Data AntiVirus dla systemu Linux -> Rodzaj klienta: Klienta dla serwera plików Linux (analogicznie j.w.)

Komendy wykonywane na kliencie:

Stacja robocza: **bash -c sh /tmp/installer.bin WS &> /var/log/gdata_install.log**
(plik logów instalatora)

Serwer plików: **bash -c sh /tmp/installer.bin SMB &> /var/log/gdata_install.log**
(plik logów instalatora)





Praktyczne porady i nietypowe funkcje

Struktura folderów aplikacji korporacyjnych G Data

Folder plików Serwera zarządzającego

C:\Program Files\G Data\G Data AntiVirus ManagementServer

Folder plików oprogramowania klienckiego

C:\Program Files\G Data\AVKClient

Folder repozytorium aktualizacji plików i sygnatur wirusów

C:\Documents and Settings\All Users\Dane aplikacji\G Data\AntiVirus ManagementServer\Updates

Folder plików Kwarantanny Serwera zarządzającego

C:\Documents and Settings\All Users\Dane aplikacji\G Data\AntiVirus ManagementServer\Quarantine

Folder plików Kwarantanny oprogramowania klienckiego

C:\Program Files\Common Files\G Data\AVKScanP\QBase

W przypadku wybrania opcji instalacji ręcznej, zastosuj plik instalacyjny z następującej lokalizacji

C:\Program Files\G DATA\G DATA AntiVirus ManagementServer\installer.bin





Komunikacja Serwera z Klientami G Data

Komunikacja między Serwerem zarządzającym, a Klientami na stacjach roboczych jest szyfrowana i odbywa się przy wykorzystaniu protokołu TCP/IP. Serwer nasłuchuje na portach TCP 7161, 7166 Klient zaś na portach TCP 7167, 7168. W środowisku wykorzystującym zaawansowane zapory połączeń (sprzętowe lub programowe) wymagane jest otwarcie wspomnianych portów w celu umożliwienia komunikacji Klientów z Serwerem.

Cofanie wersji sygnatur wirusów

W przypadku stwierdzenia fałszywej detekcji oprogramowania antywirusowego można jednym kliknięciem cofnąć wersję sygnatur wirusów każdego ze skanerów osobno. Domyślnie program przechowuje 5 kolejnych wersji sygnatur wirusów. To ustawienie można zmodyfikować korzystając z polecenia *Narzędzia > Ustawienia serwera...*

Aktualizacje offline

Jeżeli Twoja sieć lub jedna z podsieci z różnych względów nie może mieć połączenia z Internetem, skorzystaj z wygodnej opcji cotygodniowej wysyłki linków do plików instalujących sygnatury wirusów w trybie offline. Wystarczy przenieść plik na komputer z Serwerem zarządzającym i uruchomić go. Instalacja sygnatur wirusów przebiega automatycznie.



DOŁĄCZ DO NAS,
W GRUPIE RAŻNIEJ ;-)

