System i

Poczta elektroniczna

Wersja 6 wydanie 1

System i

Poczta elektroniczna

Wersja 6 wydanie 1

Uwaga

Przed skorzystaniem z tych informacji oraz z produktu, którego dotyczą, należy przeczytać informacje zawarte w sekcji “Uwagi”, na stronie 55.

To wydanie dotyczy systemu operacyjnego IBM i5/OS (numer produktu 5761-SS1) wersja 6, wydanie 1, modyfikacja 0, a także wszystkich kolejnych wydań i modyfikacji, chyba że w nowych wydaniach zostanie określone inaczej. Wersja ta nie działa na wszystkich modelach komputerów z procesorem RISC ani na modelach z procesorem CISC.

Spis treści

Poczta elektroniczna

Poniższe informacje dotyczą planowania korzystania z poczty elektronicznej w systemie, konfigurowania i użytkowania jej, zarządzania nią oraz rozwiązywania problemów z nią związanych.

Informacje te oparte są na założeniu, że użytkownik ma już doświadczenie w pracy z systemem operacyjnym i5/OS i posiada praktyczną znajomość protokołów TCP/IP oraz SMTP, a także pojęć związanych z pocztą elektroniczną.

Co nowego w wersji V6R1

Poniżej omówiono nowe lub znacznie zmienione informacje zawarte w sekcji dotyczącej poczty elektronicznej w wersji V6R1.

Obsługa protokołu SMTP S/MIME

Protokół secure/Multipurpose Internet Mail Extensions (S/MIME) może zostać zastosowany do weryfikacji nadawców poczty elektronicznej w przypadku wielokrotnych transakcji dostarczanych z wykorzystaniem protokołu SMTP. Za pomocą tego protokołu dokumenty poczty elektronicznej mogą być podpisywane lub szyfrowane. Obsługę protokołu S/MIME udostępnia nowa funkcja API QtmsCreateSendEmail.

Informacje na temat definicji protokołu S/MIME i czynności konfiguracji do zastosowania funkcji API w scenariuszu zawierają następujące rozdziały:

- “Koncepcje poczty elektronicznej” na stronie 2
- “Scenariusz: konfigurowanie funkcji API QtmsCreateSendEmail do używania standardu S/MIME” na stronie 7

Uwierzytelnianie SMTP i obsługa SSL/TLS

Obecnie można śledzić nadawcę wiadomości e-mail za pomocą uwierzytelniania SMTP. Serwer SMTP platformy i5/OS obsługuje również sesje chronione przez warstwę Secure Sockets Layer (SSL) lub Transport Layer Security (TLS).

- “Kontrola dostępu do serwera SMTP” na stronie 11
- “Śledzenie nadawcy poczty elektronicznej” na stronie 26

Obsługa SSL/TLS dla serwera POP

Serwer POP platformy i5/OS obsługuje obecnie sesje SSL/TLS. Serwer może szyfrować identyfikatory użytkowników i hasła.

- “Konfigurowanie klientów poczty POP” na stronie 31

Znajdowanie nowych lub zmienionych informacji

Aby ułatwić odnalezienie miejsc, w których wprowadzono zmiany techniczne, użyto następujących symboli:

- symbol » służący do zaznaczania początku nowego lub zmienionego fragmentu;
- symbol « służący do zaznaczania końca nowego lub zmienionego fragmentu.

Nowe i zmienione informacje w plikach PDF mogą być oznaczone symbolem | na lewym marginesie.

Więcej informacji na temat zmian i nowości w bieżącej wersji zawiera Wiadomość dla użytkowników.

Plik PDF z informacjami na temat poczty elektronicznej

Informacje zawarte w tym temacie są także dostępne w postaci pliku PDF, który można wyświetlić i wydrukować.

Aby otworzyć lub pobrać wersję dokumentu w formacie PDF, kliknij odsyłacz Poczta elektroniczna (około 692 KB).

Zapisywanie plików PDF

Aby zapisać plik PDF na stacji roboczej w celu jego wyświetlenia lub wydrukowania, wykonaj następujące czynności:

1. Kliknij prawym przyciskiem myszy odsyłacz do pliku PDF w przeglądarce.
2. Kliknij opcję zapisania pliku PDF lokalnie.
3. Przejdź do katalogu, w którym ma zostać zapisany plik PDF.
4. Kliknij opcję **Zapisz**.

Pobieranie programu Adobe Reader

Do przeglądania i drukowania plików PDF potrzebny jest program Adobe Reader. Bezpłatną kopię tego programu można pobrać z serwisu WWW firmy Adobe (www.adobe.com/products/acrobat/readstep.html) .

Odsyłacze pokrewne

"Informacje pokrewne dotyczące poczty elektronicznej" na stronie 53
Informacje, które wiążą się z kolekcją tematów dotyczących poczty elektronicznej, można znaleźć w podręcznikach produktów, dokumentacji technicznej IBM (Redbooks), serwisach WWW i w innych kolekcjach tematów centrum informacyjnego. Wszystkie pliki PDF można wyświetlić lub wydrukować.

Koncepcje poczty elektronicznej

Poczta elektroniczna (wiadomości e-mail) stała się bardzo ważnym narzędziem w wielu firmach. System operacyjny i5/OS używa protokołów SMTP i POP, aby zapewnić płynną i efektywną obsługę poczty w sieci.

Metody dystrybucji

Poniższe dodatkowe zagadnienia dotyczące poczty elektronicznej omawiają inne metody dystrybucji poczty elektronicznej:

- Standard MIME (Multipurpose Internet Mail Extensions)

  MIME to zestandaryzowana metoda organizowania różnych formatów plików. Wiadomości wysyłane w protokole SMTP muszą być zakodowane w 7-bitowym kodzie ASCII, a długości wierszy tekstu nie mogą przekraczać 1000 znaków. Standard MIME opracowano w celu obsługi bardziej złożonych formatów plików, na przykład tekstu formatowanego, obrazów, plików dźwiękowych i plików wideo. W standardzie tym pliki zawierające dane binarne są kodowane tak, aby wyglądały jak dane tekstowe obsługiwane przez protokół SMTP. Różne pliki wchodzące w skład wiadomości oddzielane są odpowiednimi nagłówkami. Dopiero po takim zakodowaniu wiadomość jest wysyłana za pomocą protokołu SMTP. Klient poczty, który odbiera wiadomość, odpowiednio ją dekoduje, interpretując nagłówki MIME.
- protokół S/MIME

  Secure/MIME to chroniona wersja protokołu MIME, która umożliwia użytkownikom wysyłanie zaszyfrowanych i podpisanych elektronicznie wiadomości, nawet jeśli użytkownicy używają różnych programów poczty elektronicznej.
- Struktura AnyMail/400

  Cała poczta przychodząca z serwera SMTP dla użytkowników lokalnych (użytkowników mających konta pocztowe w danym systemie) jest przetwarzana przez środowisko AnyMail/400. Struktura serwera poczty jest strukturą dystrybucji poczty umożliwiającą dystrybucję poczty elektronicznej. Struktura serwera poczty wywołuje programy obsługi wyjścia lub programy snap-in do obsługi określonych typów poczty.
- Usługi SNADS (Systems Network Architecture distribution services)

Usługi SNADS to asynchroniczne usługi dystrybucyjne opracowane przez IBM, określające zestaw zasad do odbierania, kierowania i wysyłania poczty elektronicznej w sieci systemów. W tym rozdziale SNADS odnosi się do profilu użytkownika, w którym opcja **Preferowany adres** (Preferred address) ustawiona jest na **ID/adres użytkownika** (User ID/Address). Adres preferowany określa w katalogu dystrybucyjnym systemu pola, które zawierają adres i które zostaną wykorzystane przez strukturę serwera poczty.

Pojęcia pokrewne

"Wysyłanie i pobieranie poczty elektronicznej" na stronie 30
System jest serwerem poczty elektronicznej i ma zarejestrowanych użytkowników poczty elektronicznej (SNADS, POP lub Lotus). Użytkownicy poczty elektronicznej mogą wysyłać, pobierać i odczytywać wiadomości e-mail za pomocą klienta POP lub SNADS.

Zadania pokrewne

"Zatrzymywanie kolejek usług dystrybucyjnych architektury systemów sieciowych (SNADS)" na stronie 13
Istnieje możliwość zatrzymania kolejek dystrybucyjnych SNADS, które są wykorzystywane przez aplikację SMTP do wysyłania poczty. Zapewni to dodatkowe zabezpieczenie w ograniczaniu dystrybucji poczty elektronicznej.

Protokół SMTP w systemie i5/OS

Protokół SMTP umożliwia systemowi operacyjnemu wysyłanie i pobieranie poczty elektronicznej.

Protokół SMTP dostarcza pocztę z jednego serwera pocztowego do innego na całej trasie. Istnieje bezpośrednie połączenie pomiędzy nadawcą SMTP (klientem) a docelowym odbiorcą SMTP (serwerem). Klient SMTP zachowuje pocztę u nadawcy, dopóki nie zostanie ona przekazana i pomyślnie skopiowana do odbiorcy SMTP (serwera).

Protokół SMTP w tym systemie operacyjnym obsługuje dystrybucję informacji, komunikatów i dokumentów tekstowych w formacie ASCII. SMTP potrafi także obsłużyć formaty inne niż zwykły tekst, stosując protokół MIME (Multipurpose Internet Mail Extensions). MIME to standard internetowy do wysyłania poczty z nagłówkami, które opisują zawartość wiadomości pocztowych dla odbiorcy. Wiadomości te mogą zawierać pliki wideo, pliki dźwiękowe lub inne dane binarne.

Dostarczanie poczty przez serwer SMTP

Aby poczta elektroniczna dotarła do celu, serwer SMTP musi ją dostarczyć zarówno do właściwego hosta, jak i do rezydującego na tym hoście użytkownika o właściwym ID. Załóżmy, że wiadomość ma zostać wysłana do użytkownika robertnowak@naszafirma.com.

W tym celu serwer SMTP sprawdza najpierw, czy adresatem poczty (robertnowak) jest lokalny użytkownik systemu. Jeśli nie, serwer SMTP przekazuje pocztę do następnego hosta, który nie musi być hostem docelowym. Serwer SMTP określa nazwę hosta na podstawie informacji o adresie dostarczanych przez protokół SMTP.

Następnie serwer SMTP określa adres hosta, wykorzystując serwer DNS lub tabelę hosta lokalnego. Nazwa hosta jest elementem nazwy konta poczty elektronicznej (naszafirma.com), adres IP jest potrzebny serwerowi SMTP do znalezienia właściwego serwera i wysłania do niego poczty.

1. Adresy IPv6 są ignorowane podczas sprawdzania przez serwer SMTP adresów hostów w tabeli hosta lokalnego.
2. Jeśli dowolny ze skonfigurowanych serwerów DNS posiada adres IPv6, wszystkie skonfigurowane serwery DNS muszą obsługiwać rekurencję, aby móc tłumaczyć domeny poczty elektronicznej, dla których skonfigurowane serwery nie mają uprawnień.

Poniższe zagadnienia dotyczą współpracy DNS z protokołem SMTP:

- konfiguracja domeny DNS,
- poczta i rekordy wymiany poczty (MX).

Dla poczty przychodzącej serwer SMTP najpierw tłumaczy nazwę hosta docelowego na adres IP. Z uwagi na funkcję aliasowania serwer może mieć kilka nazw hosta. Dlatego serwer SMTP wykorzystuje interfejs gniazd do określenia, czy adres IP jest jednym z adresów wykorzystywanych przez interfejsy dla lokalnego hosta.

Pojęcia pokrewne

DNS

rekordy Poczty i Wymiennika poczty

Zadania pokrewne

konfiguracja domeny DNS

“Konfigurowanie poczty elektronicznej” na stronie 14
Aby skonfigurować pocztę elektroniczną w systemie, należy skonfigurować protokół TCP/IP, serwery SMTP i POP oraz uruchomić serwery poczty elektronicznej.

Serwer POP w systemie i5/OS

Serwer POP jest implementacją interfejsu pocztowego POP3 w systemie i5/OS.

Serwer POP udostępnia elektroniczne skrzynki pocztowe w systemie, z których programy klienckie mogą pobierać pocztę. Korzystać z tego serwera mogą wszyscy klienci poczty obsługujący protokół POP3, na przykład Netscape Mail, Outlook Express czy Eudora. Klienci mogą pracować na dowolnej platformie, na przykład Windows, Linux, AIX, lub Macintosh.

Serwer POP służy jako miejsce tymczasowego przechowywania poczty, dopóki nie zostanie ona pobrana przez klienta poczty. Gdy klient poczty łączy się z serwerem, zadaje zapytanie o zawartość skrzynki pocztowej, aby sprawdzić, czy są jakieś wiadomości do pobrania. Jeśli są, pobiera kolejno po jednej wiadomości. Po otrzymaniu wiadomości klient zaznacza na serwerze wiadomość, która ma zostać usunięta po zakończeniu sesji klienta. Klient pobiera wszystkie wiadomości ze skrzynki pocztowej, po czym uruchamia komendę, która nakazuje serwerowi usunięcie wszystkich oznaczonych wiadomości i zakończenie połączenia z klientem.

Klient poczty POP korzysta z *rozkazów* w komunikacji z serwerem POP. Rozkazy obsługiwane przez serwer POP dla tego systemu operacyjnego opisane są w rozdziale na temat serwera POP.

Zadania pokrewne

“Dostęp do serwerów poczty elektronicznej za pomocą programu System i Navigator” na stronie 14
Można wykorzystać program System i Navigator do konfigurowania serwerów poczty elektronicznej SMTP i POP i zarządzania nimi.

“Konfigurowanie serwerów SMTP i POP na potrzeby poczty elektronicznej” na stronie 15
Aby móc używać poczty elektronicznej, należy skonfigurować w systemie serwery SMTP i POP.

Odsyłacze pokrewne

“Protokół POP (Post Office Protocol)” na stronie 49
Interfejs poczty elektronicznej Post Office Protocol (POP) Version 3 zdefiniowany jest w Request for Comments (RFC) 1939 (POP3), RFC 2449 (POP3 Extension Mechanism), i RFC 2595 (Using TLS with IMAP, POP3, and ACAP). RFC jest mechanizmem służącym do definiowania ciągle rozwijających się standardów w sieci Internet.

Informacje pokrewne

indeks RFC

Scenariusze: poczta elektroniczna

Scenariusze te ilustrują sposób, w jaki poczta elektroniczna jest przetwarzana pomiędzy użytkownikami lokalnymi i w jaki można skonfigurować funkcję API QtmsCreateSendEmail do wykorzystania S/MIME.

Scenariusz: wysyłanie i odbieranie poczty elektronicznej lokalnie

Scenariusz ten demonstruje sposób, w jaki poczta elektroniczna jest przetwarzana pomiędzy użytkownikami lokalnymi.

Sytuacja

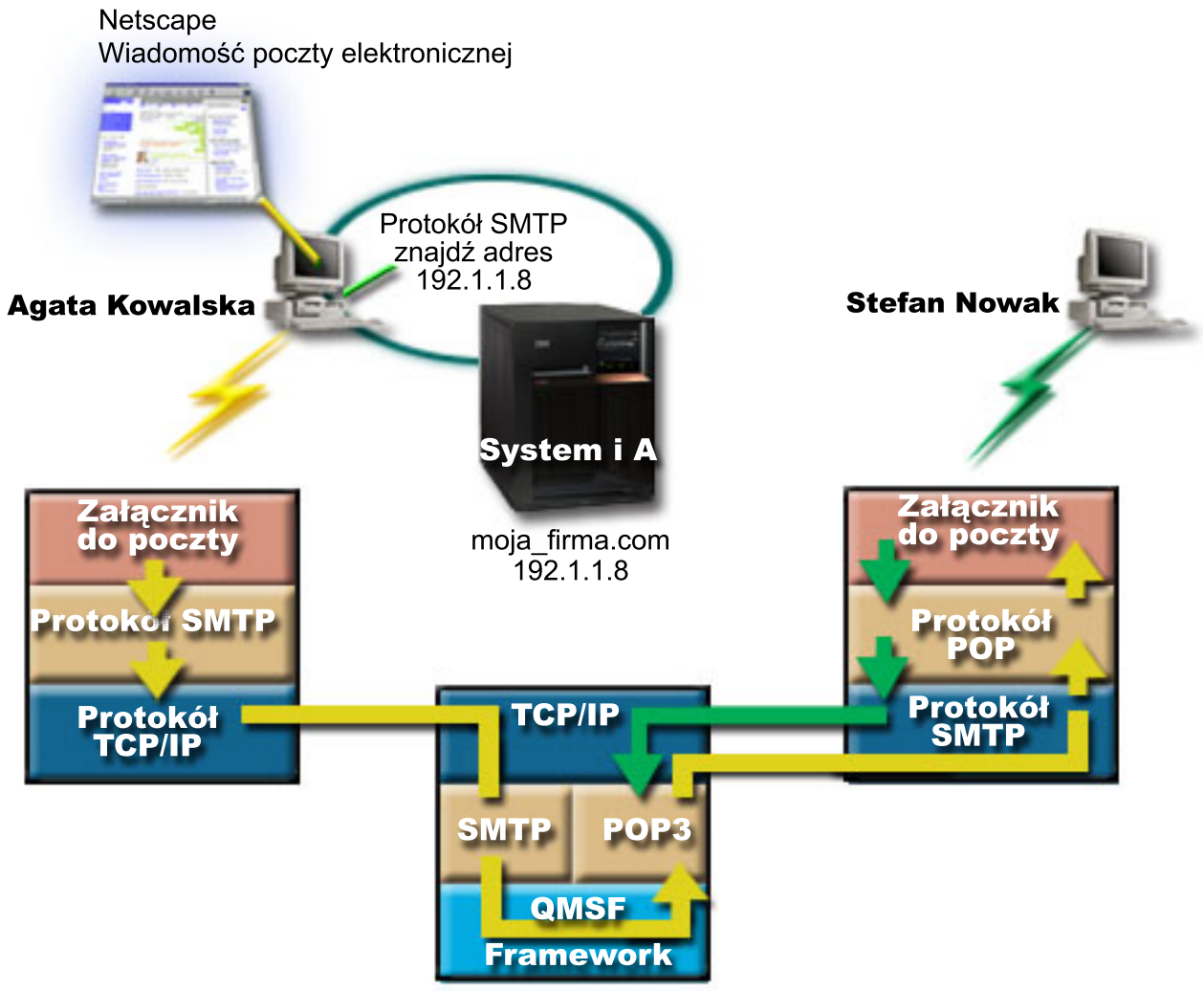
Agata Kowalska, dyrektor działu kadr, chce wysłać wiadomość do Stefana Nowaka, pracującego w dziale prawnym. Oboje pracują w centrali ″Nasza firma″. Proces ten pokazuje sposób, w jaki poczta elektroniczna jest przetwarzana w systemie.

Cele przykładu:

- pokazanie sposobu komunikacji między klientem i serwerem poczty oraz przetwarzania wiadomości,
- prezentacja sposobu wykorzystania serwera SMTP do wysłania wiadomości,
- prezentacja sposobu dostarczenia wiadomości do użytkownika za pomocą protokołu POP;

Informacje szczegółowe

Agata używa klienta poczty Netscape. Po napisaniu listu wysyła go na adres StefanNowak@naszafirma.com. Poniższy rysunek ilustruje ścieżkę przesyłania wiadomości pocztowej w systemie.



Rysunek 1. Przykładowa konfiguracja sieci

Poniżej opisano każdą fazę ścieżki przesyłania wiadomości pocztowej w systemie.

Faza 1: klient SMTP do serwera SMTP

Klient SMTP znajdujący się na komputerze PC Agaty odczytuje dane konfiguracyjne związane z serwerem poczty wychodzącej i adresem nadawcy. Adres nadawcy jest wpisywany w polu **Od**. Serwer poczty wychodzącej to host, z którym komunikuje się klient SMTP znajdujący się na komputerze PC. Ponieważ adres został wprowadzony jako domena, klient SMTP żąda od serwera DNS (Domain Name System - system nazw domen) podania adresu IP serwera SMTP, i otrzymuje informację, że jest to 192.1.1.8.

Klient SMTP kontaktuje się z serwerem SMTP na porcie SMTP (Port 25 dla adresu 192.1.1.8). Dialog między klientem i serwerem przebiega według protokołu SMTP. Serwer SMTP akceptuje żądanie dostarczenia wiadomości, po czym wiadomość jest przesyłana od klienta do serwera z wykorzystaniem protokołu TCP/IP.

Faza 2: serwer SMTP dostarcza wiadomość do serwera POP

Serwer SMTP sprawdza, czy domena w adresie odbiorcy jest domeną lokalną. Ponieważ jest to domena lokalna, poczta jest zapisywana do pliku IFS, a funkcja API Utwórz wiadomość (Create Message) struktury QMSF przekazuje informację o wiadomości do kolejki QMSF. Struktura QMSF umożliwia rozsyłanie wiadomości e-mail i wywoływanie programów obsługi wyjścia lub programów snap-in do obsługi określonych typów wiadomości. Dane określają, że adres Stefana ma format SMTP, więc w strukturze QMSF zostanie wywołany program obsługi wyjścia SMTP Address Resolution. W programie tym następuje ponowne sprawdzenie, czy adres jest lokalny. Ponieważ adres jest adresem lokalnym, do znalezienia adresu odbiorcy SMTP zostaje użyty katalog dystrybucyjny systemu (dane wprowadzone za pomocą komendy WRKDIRE). W pozycji katalogu odpowiadającej odbiorcy zapisany jest jego ad res i poziom obsługi poczty, który ma wartość ″systemowa pamięć komunikatu″. Dlatego konto Stefana jest rozpoznawane jako konto POP. Program SMTP Address Resolution dodaje do wiadomości dane profilu. Oznacza je jako dostarczane lokalnie za pomocą protokołu POP. Struktura QMSF wywołuje następnie program obsługi wyjścia lokalnego dostarczania POP, który odczytuje informacje o profilu oraz nazwę pliku zintegrowanego systemu plików i dostarcza pocztę do skrzynki pocztowej Stefana.

Faza 3: klient POP odbiera wiadomość dla Stefana Nowaka z serwera POP

Po pewnym czasie Stefan sprawdza swoją skrzynkę pocztową za pomocą klienta pocztowego Netscape. Klient POP znajdujący się na jego komputerze PC sprawdza konto na serwerze POP naszafirma.com z nazwą użytkownika StefanNowak i hasłem (******). Nazwa domenowa zostaje ponownie zamieniona na adres IP (za pomocą serwera DNS). Klient POP komunikuje się z serwerem POP korzystając z portu POP i protokołu POP3. Serwer POP w systemie operacyjnym sprawdza, czy nazwa użytkownika skrzynki pocztowej i hasło odpowiadają nazwie użytkownika i hasłu użytkownika systemu i5/OS. Po zatwierdzeniu powyższych danych, do znalezienia skrzynki pocztowej Stefana użyta zostaje nazwa profilu. Klient POP pobiera wiadomość i wysyła zgłoszenie do serwera POP w celu usunięcia wiadomości ze skrzynki pocztowej POP. Wiadomość zostaje wyświetlona w oknie programu Netscape i Stefan może ją przeczytać.

Pojęcia pokrewne

“Planowanie korzystania z poczty elektronicznej” na stronie 10
Przed skonfigurowaniem poczty elektronicznej należy przygotować podstawowy plan korzystania z niej w systemie.

Odsyłacze pokrewne

“Protokół SMTP (Simple Mail Transfer Protocol)” na stronie 47
Protokół SMTP (Simple Mail Transfer Protocol) jest protokołem TCP/IP używanym przy wysyłaniu i odbieraniu poczty elektronicznej. Jest on zazwyczaj używany razem z protokołem POP3 lub protokołem IMAP (Internet Message Access Protocol) w celu zapisania wiadomości w skrzynce pocztowej serwera i okresowym pobieraniu ich z serwera przez użytkownika.

“Protokół POP (Post Office Protocol)” na stronie 49
Interfejs poczty elektronicznej Post Office Protocol (POP) Version 3 zdefiniowany jest w Request for Comments (RFC) 1939 (POP3), RFC 2449 (POP3 Extension Mechanism), i RFC 2595 (Using TLS with IMAP, POP3, and ACAP). RFC jest mechanizmem służącym do definiowania ciągle rozwijających się standardów w sieci Internet.

Scenariusz: konfigurowanie funkcji API QtmsCreateSendEmail do używania standardu S/MIME

Scenariusz ten demonstruje sposób, w jaki można skonfigurować funkcję API QtmsCreateSendEmail do używania standardu secure/MIME (S/MIME).

Sytuacja

Użytkownik Jan Kowalski, którego identyfikator użytkownika to jkowalski, chce skonfigurować funkcję API QtmsCreateSendEmail do używania standardu S/MIME. Standard S/MIME to metoda programowego wysyłania poczty elektronicznej, która jest bezpieczniejsza niż użycie funkcji API QtmmSendMail.

Informacje szczegółowe

Aby móc wysyłać podpisane i szyfrowane wiadomości e-mail, Jan musi mieć na systemie działającym pod kontrolą systemu operacyjnego i5/OS V6R1 zainstalowane następujące opcje:

- i5/OS PASE (5761-SS1 opcja 33),
- Digital Certificate Manager (5761-SS1 opcja 34),
- OpenSSL (5733-SC1 opcja 1).

Tworzenie bazy certyfikatów użytkownika

Zastosowanie standardu S/MIME wymaga repozytorium certyfikatów użytkownika, nazywanego bazą certyfikatów użytkownika. W systemie operacyjnym dla certyfikatów użytkowników stosuje się konwencję nazewnictwa *userid*.usrcrt. Certyfikaty znajdują się w katalogu /qibm/userdata/icss/cert/download/client.

Jan musi skonfigurować bazę certyfikatów dla swojego profilu użytkownika, na którym wykonywane będą zadania tworzenia i wysyłania wiadomości e-mail. Może zastosować program Digital Certificate Manager (DCM) do zarządzania bazą certyfikatów użytkownika.

Aby utworzyć bazę certyfikatów użytkownika, wykonaj następujące czynności:

1. Utwórz podkatalog zawierający nazwę profilu użytkownika:

   ```
   cd  /qibm/userdata/icss/cert/download/client
   mkdir  jkowalski
   ```

2. Uruchom przeglądarkę WWW, przejdź na stronę Zadania System i (System i Tasks) w swoim systemie pod adresem http://*nazwa_systemu*: 2001.
3. Z listy produktów na stronie Zadania System i wybierz **Digital Certificate Manager**, aby uruchomić interfejs użytkownika programu DCM. W lewym panelu kliknij pozycję **Utwórz nową bazę certyfikatów** (Create New Certificate Store).
4. Na stronie Utwórz nową bazę certyfikatów (Create New Certificate Store), wybierz **Baza certyfikatów innego systemu** (Other System Certificate Store) i kliknij **Kontynuuj** (Continue).
5. Na stronie Utwórz certyfikat w nowej bazie certyfikatów (Create a Certificate in New Certificate Store) wybierz **Nie - nie twórz certyfikatu w bazie certyfikatów** (No - Do not create a certificate in the certificate store).
6. Na stronie Nazwa i hasło bazy certfikatów (Certificate Store Name and Password) wpisz nazwę ścieżki bazy certyfikatów i hasło. Skonfiguruj swoją ścieżkę bazy certyfikatów w taki sposób, aby zawierała Twój identyfikator użytkownika. Na przykład Jan konfiguruje swoją ścieżkę bazy jako /qibm/userdata/icss/cert/download/client/jkowalski/jkowalski.kdb.

Eksportowanie certyfikatu użytkownika nadawcy na platformę System i

Jan używa programu Internet Explorer (IE) 6 jako przeglądarki WWW. Certyfikat użytkownika nadawcy został uzyskany z ośrodka certyfikacji (CA) i następnie został zainstalowany w programie IE 6.

Aby wyeksportować certyfikat użytkownika nadawcy na platformę System i, należy wykonać następujące czynności:

1. W oknie IE wybierz **Narzędzia → Opcje internetowe** (Tools > Internet Options).
2. Na karcie **Zawartość** (Content) kliknij **Certyfikaty**.
3. Na karcie **Osobisty** (Personal) wybierz certyfikat użytkownika i kliknij **Eksportuj...** (Export).
4. Na stronie Kreatorze eksportu certyfikatu - Zapraszamy! (Welcome to the Certificate Export Wizard) kliknij **Dalej** (Next).
5. Na stronie Eksportowanie klucza prywatnego (Export Private Key) wybierz **Tak, eksportuj klucz prywatny** (Yes, export the private key) i kliknij **Dalej** (Next).
6. Na stronie Format pliku eksportu (Export File Format) wybierz **Włącz silną ochronę (wymaga programu IE 5.0, systemu NT 4.0 SP4 lub nowszego)** (Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above) pod pozycją **Wymiana informacji osobistych - PKCS #12 (.PFX)** (Personal Information Exchange - PKCS #12 (.PFX)).
7. W polu Hasło (Password) wpisz hasło dla certyfikatu.
8. Na ekranie Eksport pliku (File to Export) wpisz nazwę pliku, który ma być wyeksportowany, na przykład C:\temp\jkowalskicert.pfx, i kliknij **Dalej** (Next).
9. Na ekranie z podsumowaniem wybranych opcji kliknij **Zakończ** (Finish).
10. Wyślij certyfikat użytkownika nadawcy jkowalskicert.pfx w trybie ASCII za pomocą protokołu FTP na platformę System i. W niniejszym przykładzie zakłada się, że plik jest wysyłany do katalogu /home/jkowalski zintegrowanego systemu plików na platformie System i. Szczegóły na temat sposobu importowania tego certyfikatu można znaleźć w “Importowanie certyfikatu nadawcy na platformę System i”.

Eksportowanie certyfikatu użytkownika odbiorcy na platformę System i

Aby wyeksportować certyfikat użytkownika odbiorcy na platformę System i, należy wykonać następujące czynności:

1. W oknie IE wybierz **Narzędzia → Opcje internetowe** (Tools > Internet Options).
2. W oknie Opcje internetowe (Internet Options) kliknij zakładkę **Zawartość** (Content), a następnie kliknij **Certyfikaty** (Certificates).
3. Na karcie **Osobisty** (Personal) wybierz certyfikat i kliknij **Eksportuj** (Export).

   Jeśli istnieje więcej niż jeden certyfikat, należy powtórzyć czynności od 3 do 7 dla wszystkich certyfikatów.
4. Na stronie Kreatorze eksportu certyfikatu - Zapraszamy! (Welcome to the Certificate Export Wizard) kliknij **Dalej** (Next).
5. W oknie Format pliku eksportu (Export File Format), wybierz **Certyfikat X.509 szyfrowany binarnie algorytmem DER (.CER)** (DER encoded binary X.509 (.CER)).
6. Na ekranie Eksport pliku (File to Export) wpisz nazwę pliku, który ma być wyeksportowany, na przykład C:\temp\receiveruser.cer, i kliknij **Dalej** (Next).
7. Na ekranie z podsumowaniem wybranych opcji kliknij **Zakończ** (Finish).
8. Wyślij certyfikat użytkownika odbiorcy odbiorca.cer w trybie ASCII za pomocą protokołu FTP na platformę System i. W niniejszym przykładzie zakłada się, że plik jest wysyłany do katalogu /home/jkowalski zintegrowanego systemu plików na platformie System i. Szczegóły na temat sposobu importowania tego certyfikatu można znaleźć w “Importowanie certyfikatu odbiorcy na platformę System i” na stronie 9.
9. Powtórz wszystkie opisane powyżej czynności dla każdego odbiorcy obsługiwanego w standardzie S/MIME.

Importowanie certyfikatu nadawcy na platformę System i

Następnie Jan musi zaimportować swój certyfikat użytkownika i klucz prywatny do bazy certyfikatów użytkownika za pomocą programu DCM. Hasło do importowanego certyfikatu musi być takie samo, jak hasło do magazynu kluczy. Jan musi także zaimportować wszystkie certyfikaty użytkowników, do których chce wysyłać pocztę elektroniczną.

1. Uruchom przeglądarkę WWW, przejdź na stronę Zadania System i (System i Tasks) w swoim systemie pod adresem http://*nazwa_systemu*: 2001.

2. Z listy produktów na stronie Zadania System i wybierz **Digital Certificate Manager**, aby uruchomić interfejs użytkownika programu DCM.
3. Na stronie Wybór bazy certyfikatów (Select a Certificate Store), wybierz **Baza certyfikatów innego systemu** (Other System Certificate Store) i kliknij **Kontynuuj** (Continue).
4. Na stronie Nazwa i hasło bazy certyfikatów (Certificate Store Name and Password) wpisz nazwę ścieżki bazy certyfikatów, nazwę pliku oraz hasło i kliknij **Kontynuuj** (Continue). W przypadku Jana nazwa pliku to /qibm/userdata/icss/cert/download/client/jkowalski/jkowalski.kdb.
5. Rozwiń pozycję **Zarządzanie certyfikatami → Importuj certyfikat** (Manage Certificates > Import Certificate). Wybierz **Serwer lub klient** (Server or client), aby zaimportować certyfikat nadawcy. Kliknij przycisk **Kontynuuj** (Continue).
6. Na stronie Importowanie certyfikatu serwera lub klienta (Import Server or Client Certificate) podaj nazwę katalogu zintegrowanego systemu plików oraz nazwę pliku certyfikatu nadawcy i kliknij **Kontynuuj** (Continue). W scenariuszu "Eksportowanie certyfikatu użytkownika nadawcy na platformę System i" na stronie 7 katalog zintegrowanego systemu plików nazywa się /home/jkowalski a plik - jkowalskicert.pfx.
7. Wpisz etykietę certyfikatu, czyli adres poczty elektronicznej nadawcy, używając małych liter. Kliknij przycisk **Kontynuuj** (Continue).
8. Kliknij przycisk **OK**.

Importowanie certyfikatu odbiorcy na platformę System i

Aby zaimportować certyfikat odbiorcy na platformę System i, wykonaj następujące czynności:

1. Uruchom przeglądarkę WWW, przejdź na stronę Zadania System i (System i Tasks) w swoim systemie pod adresem http://*nazwa_systemu*: 2001.
2. Z listy produktów na stronie Zadania System i wybierz **Digital Certificate Manager**, aby uruchomić interfejs użytkownika programu DCM.
3. Na stronie Wybór bazy certyfikatów (Select a Certificate Store), wybierz **Baza certyfikatów innego systemu** (Other System Certificate Store) i kliknij **Kontynuuj** (Continue).
4. Na stronie Nazwa i hasło bazy certyfikatów (Certificate Store Name and Password) wpisz nazwę ścieżki bazy certyfikatów, nazwę pliku oraz hasło i kliknij **Kontynuuj** (Continue). W przypadku Jana nazwa pliku to /qibm/userdata/icss/cert/download/client/jkowalski/jkowalski.kdb.
5. Rozwiń pozycję **Zarządzanie certyfikatami → Importuj certyfikat** (Manage Certificates > Import Certificate). Wybierz **Ośrodek certyfikacji (CA)** (Certificate Authority (CA)), aby zaimportować certyfikat odbiorcy. Kliknij przycisk **Kontynuuj** (Continue).
6. Na stronie Importowanie certyfikatu ośrodka certyfikacji (Import Certificate Authority (CA) Certificate) podaj nazwę katalogu zintegrowanego systemu plików oraz nazwę pliku certyfikatu odbiorcy i kliknij **Kontynuuj** (Continue). W scenariuszu "Eksportowanie certyfikatu użytkownika odbiorcy na platformę System i" na stronie 8 katalog zintegrowanego systemu plików nazywa się /home/jkowalski a plik dla odbiorcy - odbiorca.cer.
7. Wpisz etykietę certyfikatu, czyli adres poczty elektronicznej odbiorcy, używając małych liter. Kliknij przycisk **Kontynuuj** (Continue).
8. Powtórz wszystkie opisane powyżej czynności dla każdego certyfikatu odbiorcy, którego potrzebuje nadawca.

Pojęcia pokrewne

program Digital Certificate Manager

Odsyłacze pokrewne

tworzenie i wysyłanie poczty w standardzie MIME (Create and Send MIME E-mail - QtmsCreateSendEmail), funkcja API

Planowanie korzystania z poczty elektronicznej

Przed skonfigurowaniem poczty elektronicznej należy przygotować podstawowy plan korzystania z niej w systemie.

Przed przystąpieniem do konfigurowania poczty elektronicznej należy odpowiedzieć na poniższe pytania:

1. Jak będzie wyglądał adres poczty elektronicznej?
2. Jaki jest adres IP serwera DNS?
3. Czy uruchomiony jest firewall? Jeśli tak, jaki jest jego adres IP?
4. Czy uruchomiony jest serwer proxy dla poczty, router poczty lub przekaźnik poczty? Jeśli tak, jaki jest jego adres IP?
5. Czy będzie używana baza danych Domino?
6. Czy do odbierania poczty będzie używany serwer POP systemu i5/OS?

W celu uzyskania podstawowych informacji o działaniu poczty elektronicznej może być potrzebne skorzystanie ze scenariusza poczty elektronicznej.

Jeśli ma być wykorzystywany serwer Domino oraz serwer SMTP systemu i5/OS, sięgnij po informacje zawarte w rozdziale Udostępnianie serwera Domino i serwera SMTP w jednym systemie. Więcej informacji na temat serwera Domino znajduje się w rozdziale Domino lub w serwisie WWW Lotus Domino for i5/OS.

Jeśli nie planuje się wykorzystania serwerów SMTP i POP, należy je wyłączyć, aby bez wiedzy administratora nie mogły ich użyć osoby nieuprawnione.

Pojęcia pokrewne

“Scenariusz: wysyłanie i odbieranie poczty elektronicznej lokalnie” na stronie 4
Scenariusz ten demonstruje sposób, w jaki poczta elektroniczna jest przetwarzana pomiędzy użytkownikami lokalnymi.

Domino

Zadania pokrewne

“Konfigurowanie poczty elektronicznej” na stronie 14
Aby skonfigurować pocztę elektroniczną w systemie, należy skonfigurować protokół TCP/IP, serwery SMTP i POP oraz uruchomić serwery poczty elektronicznej.

“Udostępnianie serwera Domino i serwera SMTP w tym samym systemie” na stronie 39
Jeśli w tym samym systemie używane są jednocześnie serwer Domino i serwer SMTP, zaleca się skonfigurowanie każdego z nich w taki sposób, aby przypisane im były konkretne określone adresy IP.

Informacje pokrewne

Lotus Domino for i5/OS

Kontrolowanie dostępu do poczty elektronicznej

Aby ochronić dane przed groźnymi atakami, należy kontrolować, kto uzyskuje dostęp do systemu za pośrednictwem poczty elektronicznej.

Ta sekcja zawiera wskazówki na temat zabezpieczenia serwerów poczty elektronicznej przed zalaniem i spamem.

Pojęcia pokrewne

przykłady niezależnej puli dyskowej

“Wykrywanie problemów z pocztą elektroniczną” na stronie 49
Wykonanie prostych czynności może być pomocne w określeniu przyczyny problemu z pocztą elektroniczną.

Zadania pokrewne

“Ograniczanie przekazywania wiadomości” na stronie 27
Aby zapobiec wykorzystywaniu danego serwera pocztowego do rozsyłania spamu lub masowego rozsyłania poczty

elektronicznej, można zastosować funkcję ograniczania przekazywania i określić, kto może używać danego systemu do przekazywania wiadomości. Jednakże nie można uwierzytelniać poczty elektronicznej po ograniczeniu przekazywania wiadomości.

"Ograniczanie połączeń" na stronie 29
W celu zabezpieczenia systemu należy zablokować połączenia użytkowników, którzy mogliby nieprawidłowo korzystać z serwera poczty.

Informacje pokrewne

AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet

Kontrola dostępu do serwera SMTP

Aby zapobiec zaatakowaniu systemu przez spam, należy kontrolować dostęp do serwera SMTP.

Jeśli chcesz umożliwić klientom SMTP dostęp do systemu, powinieneś chronić system przed atakiem, wykonując następujące czynności:

- Jeśli to możliwe, należy unikać tworzenia pozycji *ANY *ANY w katalogu dystrybucyjnym systemu. Jeśli w systemie nie ma pozycji *ANY *ANY, trudniej jest wykorzystać protokół SMTP do zablokowania systemu lub sieci. Kiedy pamięć dyskowa zostaje wypełniona niepożądaną pocztą, która jest przekierowywana przez dany system do innego systemu, dany system lub sieć zostają zablokowane.
- Aby zapobiec zablokowaniu systemu przez niepożądane obiekty, należy ustawić odpowiednie progi pamięci dla pul ASP. Progi pamięci dla puli ASP można odczytać i ustawić za pomocą narzędzi SSTs (systemowych narzędzi serwisowych) lub narzędzi DST (dedicated service tools).
- Należy dostroić maksymalną liczbę zadań prestartu, jakie mogą zostać utworzone, za pomocą komendy Zmiana pozycji zadania prestartu (Change Prestart Job Entry - CHGPJE). Komenda ta ogranicza liczbę zadań tworzonych podczas ataku polegającego na spowodowaniu odmowy usługi. Wartością domyślną maksymalnej liczby zadań jest 256.
- Należy uniemożliwić osobom nieupoważnionym wysyłającym spam korzystanie z łącza, ograniczając przekazywanie i połączenia.
- W systemach działających pod kontrolą i5/OS V6R1 można zapobiec zalaniu spamem, żądając uwierzytelnienia przed wysłaniem poczty elektronicznej. Jeśli serwer zdalny żąda uwierzytelnienia, można skonfigurować uwierzytelnianie na serwerze lokalnym.

Odsyłacze pokrewne

zmiana atrybutów SMTP (Change SMTP Attributes - CHGSMTPA), komenda

Kontrola dostępu do serwera POP

Aby zapewnić bezpieczeństwo systemu, należy kontrolować dostęp do serwera POP.

Można określić, czy serwer POP ma wykorzystywać szyfrowanie do ochrony strumieni danych POP, w tym identyfikatorów użytkowników i haseł. Szyfrowanie odbywa się za pomocą protokołów SSL (Secure Sockets Layer) lub TLS (Transport Layer Security). Aby wskazać, czy obsługiwane są chronione sesje POP, ustaw parametr ALWSSL komendy CL Zmiana atrybutów serwera POP (Change POP Server Attributes - CHGPOPA).

Aby umożliwić klientom POP dostęp do systemu, należy uwzględnić następujące uwarunkowania:

- Serwer poczty POP stosuje uwierzytelnianie dla klientów starających się uzyskać dostęp do swoich skrzynek pocztowych. Klient wysyła do serwera identyfikator użytkownika oraz hasło.

  Serwer poczty POP weryfikuje zgodność identyfikatora użytkownika oraz hasła z profilem i hasłem użytkownika systemu i5/OS. Ponieważ użytkownik nie ma kontroli nad tym, w jaki sposób identyfikator użytkownika i hasło składowane są na kliencie POP, użytkownik może utworzyć specjalny profil użytkownika z ograniczonymi uprawnieniami systemowymi. Aby uniemożliwić użycie profilu użytkownika w sesji interaktywnej, w profilu użytkownika należy ustawić następujące wartości:
  ustawić menu początkowe (initial menu - INLMNU) na wartość *SIGNOFF,
  ustawić program początkowy (initial program - INLPGM) na wartość *NONE,
  ustawić ograniczenie możliwości (limit capabilities - LMTCPB) na wartość *YES.

- Aby uniemożliwić intruzowi zablokowanie systemu za pomocą niepożądanych obiektów, należy koniecznie ustawić odpowiednie progi dla pul pamięci dyskowej (ASP). Próg ASP pamięci uchroni system przed zablokowaniem z powodu niewystarczającej pamięci dla systemu operacyjnego. Progi pamięci dla puli ASP można odczytać i ustawić za pomocą narzędzi SST (systemowych narzędzi serwisowych) lub narzędzi DST (dedicated service tools).
- Oprócz ustawienia odpowiedniego progu pamięci dla puli ASP, chroniącego system przed zalaniem, należy także zapewnić wystarczającą ilość pamięci dla właściwego przechowywania i dostarczania poczty elektronicznej. Jeśli serwer poczty nie może dostarczyć poczty z powodu niewystarczającej pamięci dla poczty przejściowej, stwarza to użytkownikom problemy z integralnością. Jeśli wykorzystanie systemowej pamięci dyskowej jest zbyt duże, poczta przestaje działać.

  Zazwyczaj przestrzeń pamięci nie stanowi znaczącego problemu. Po otrzymaniu poczty przez klienta, serwer poczty elektronicznej usuwa ją z systemu.

  Pojęcia pokrewne

  "Wykrywanie problemów z pocztą elektroniczną" na stronie 49
  Wykonanie prostych czynności może być pomocne w określeniu przyczyny problemu z pocztą elektroniczną.

Blokowanie dostępu do poczty elektronicznej

W zależności od sposobu użytkowania systemu, może zajść potrzeba blokowania użytkownikom dostępu do poczty elektronicznej przez serwery SMTP i POP. Dostęp do poczty elektronicznej można całkiem zablokować lub zezwalać na dostęp w pewnych przypadkach.

Blokowanie dostępu za pomocą protokołu SMTP

Aby nikt nie uzyskać dostępu do systemu użytkownika za pomocą protokołu SMTP, należy uniemożliwić uruchamianie serwera SMTP.

Serwer SMTP jest skonfigurowany domyślnie w ten sposób, że uruchamia się automatycznie po uaktywnieniu protokołu TCP/IP. Jeśli nie zamierzasz używać serwera SMTP, nie konfiguruj go w systemie (i nie pozwalaj na to innym użytkownikom).

Blokowanie uruchomienia serwera SMTP wraz z uruchomieniem protokołu TCP/IP:

Może zaistnieć potrzeba okazjonalnego wykorzystania protokołu SMTP, przy jednoczesnym ograniczeniu dostępu innych użytkowników do serwera SMTP.

Aby zablokować automatyczne uruchamianie zadań serwera SMTP po uaktywnieniu protokołu TCP/IP, wykonaj następujące czynności:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** **→ Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Prawym przyciskiem myszy kliknij pozycję **SMTP** i wybierz opcję **Właściwości**.
3. Wyczyść pole **Uruchom wraz z TCP/IP**.

Blokowanie dostępu do portów SMTP:

Aby ochronić serwer SMTP przed nieznanymi aplikacjami, można zablokować dostęp do portów SMTP.

Aby zablokować dostęp do SMTP oraz uniemożliwić innym użytkownikom przypisanie aplikacji użytkownika, na przykład aplikacji gniazd, do portu używanego zwykle przez system na potrzeby protokołu SMTP, wykonaj następujące czynności:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** **→ Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Prawym przyciskiem myszy kliknij pozycję **Konfiguracja TCP/IP** i wybierz opcję **Właściwości**.
3. W oknie Konfiguracja TCP/IP kliknij zakładkę **Ograniczenia dla portów**.
4. Na stronie Ograniczenia dla portów kliknij **Dodaj**.
5. Na stronie Dodaj ograniczenie portu podaj następujące dane:

- **Nazwa użytkownika**: podaj nazwę profilu użytkownika, który jest chroniony w systemie (Chroniony profil użytkownika to taki profil, który nie ma praw właściciela do programów adoptujących uprawnienia, a jego hasło nie jest znane innym użytkownikom). Jeśli port jest ograniczony dla określonego użytkownika, wszyscy pozostali są automatycznie wykluczani.
- **Port startowy**: 25
- **Port końcowy**: 25
- **Protokół**: TCP

6. Kliknij przycisk **OK**, aby dodać ograniczenie.
7. Na stronie **Ograniczenia dla portów** kliknij **Dodaj** i powtórz czynności dla protokołu UDP.
8. Kliknij przycisk **OK**, aby zapisać ograniczenia dla portów i zamknąć okno **Właściwości TCP/IP**. Ograniczenia dla portów zadziałają przy następnym uruchomieniu protokołu TCP/IP. Jeśli podczas ustawiania ograniczeń dla portów protokół TCP/IP był aktywny, należy zakończyć jego działanie, a następnie uruchomić go ponownie.

Zatrzymywanie kolejek usług dystrybucyjnych architektury systemów sieciowych (SNADS):

Istnieje możliwość zatrzymania kolejek dystrybucyjnych SNADS, które są wykorzystywane przez aplikację SMTP do wysyłania poczty. Zapewni to dodatkowe zabezpieczenie w ograniczaniu dystrybucji poczty elektronicznej.

Aby wstrzymać kolejki dystrybucyjne, należy w interfejsie znakowym wpisać następujące komendy:

```
HLDDSTQ  DSTQ(QSMTPQ)PTY(*NORMAL)
HLDDSTQ  DSTQ(QSMTPQ)PTY(*HIGH)
```

Pojęcia pokrewne

“Koncepcje poczty elektronicznej” na stronie 2
Poczta elektroniczna (wiadomości e-mail) stała się bardzo ważnym narzędziem w wielu firmach. System operacyjny i5/OS używa protokołów SMTP i POP, aby zapewnić płynną i efektywną obsługę poczty w sieci.

Blokowanie dostępu za pomocą protokołu POP

Aby nikt nie mógł uzyskać dostępu do systemu użytkownika za pomocą protokołu POP, należy uniemożliwić uruchamianie serwera POP.

Jeśli nie zamierzasz używać serwera POP, nie konfiguruj go w systemie (i nie pozwalaj na to innym użytkownikom).

Blokowanie uruchomienia serwera POP wraz z uruchomieniem protokołu TCP/IP:

Może zaistnieć potrzeba okazjonalnego wykorzystania protokołu POP, przy jednoczesnym ograniczeniu dostępu innych użytkowników do serwera POP.

Serwer POP jest domyślnie skonfigurowany tak, by uruchamiać się wraz z uruchomieniem protokołu TCP/IP. Aby zablokować automatyczne uruchamianie zadań serwera POP po uruchomieniu protokołu TCP/IP, wykonaj następujące czynności:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** **→ Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Prawym przyciskiem myszy kliknij **POP** i wybierz opcję **Właściwości**.
3. Wyczyść pole **Uruchom wraz z TCP/IP**.

Blokowanie dostępu do portów POP (Post Office Protocol):

Aby ochronić serwer POP przed nieznanymi aplikacjami, można zablokować dostęp do portów POP.

Aby zablokować uruchamianie serwera POP oraz uniemożliwić innym użytkownikom przypisanie aplikacji użytkownika, na przykład aplikacji gniazd, do portu używanego zwykle przez system na potrzeby protokołu POP, wykonaj następujące czynności:

1. Uruchom program System i Navigator, połącz się ze swoim systemem i rozwiń pozycję **Sieć → Serwery → TCP/IP** (Network > Servers > TCP/IP).
2. Prawym przyciskiem myszy kliknij pozycję **Konfiguracja TCP/IP** i wybierz opcję **Właściwości**.
3. W oknie Konfiguracja TCP/IP kliknij zakładkę **Ograniczenia dla portów**.
4. Na stronie Ograniczenia dla portów kliknij **Dodaj**.
5. Na stronie Dodaj ograniczenie portu podaj następujące dane:
   - **Nazwa użytkownika**: podaj nazwę profilu użytkownika, który jest chroniony w systemie (Chroniony profil użytkownika to taki profil, który nie ma praw właściciela do programów adoptujących uprawnienia, a jego hasło nie jest znane innym użytkownikom). Jeśli port jest ograniczony dla określonego użytkownika, wszyscy pozostali są automatycznie wykluczani.
   - **Port początkowy**: 110 995
   - **Port końcowy**: 110 995
   - **Protokół**: TCP
6. Kliknij przycisk **OK**, aby dodać ograniczenie.
7. Na stronie Ograniczenia dla portów kliknij **Dodaj** i powtórz czynności dla protokołu UDP.
8. Kliknij przycisk **OK**, aby zapisać ograniczenia dla portów i zamknąć okno Właściwości TCP/IP.

Ograniczenia dla portów zadziałają przy następnym uruchomieniu protokołu TCP/IP. Jeśli podczas ustawiania ograniczeń dla portów protokół TCP/IP był aktywny, należy zakończyć jego działanie, a następnie uruchomić go ponownie.

Konfigurowanie poczty elektronicznej

Aby skonfigurować pocztę elektroniczną w systemie, należy skonfigurować protokół TCP/IP, serwery SMTP i POP oraz uruchomić serwery poczty elektronicznej.

Pojęcia pokrewne

“Protokół SMTP w systemie i5/OS” na stronie 3
Protokół SMTP umożliwia systemowi operacyjnemu wysyłanie i pobieranie poczty elektronicznej.

“Planowanie korzystania z poczty elektronicznej” na stronie 10
Przed skonfigurowaniem poczty elektronicznej należy przygotować podstawowy plan korzystania z niej w systemie.

Dostęp do serwerów poczty elektronicznej za pomocą programu System i Navigator

Można wykorzystać program System i Navigator do konfigurowania serwerów poczty elektronicznej SMTP i POP i zarządzania nimi.

Aby uzyskać dostęp do serwerów POP lub SMTP w programie System i Navigator, wykonaj następujące czynności:

1. Kliknij dwukrotnie folder **Client Access Express**.
2. Kliknij dwukrotnie **System i Navigator**. Jeśli uruchamiasz System i Navigator po raz pierwszy, kliknij ikonę **Nowe połączenie** (New Connection), aby ustanowić połączenie ze swoim systemem.
3. Uruchom program System i Navigator i rozwiń pozycję ***system* → Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
4. Dwukrotnie kliknij **SMTP**, aby otworzyć okno dialogowe Właściwości SMTP lub kliknij dwukrotnie **POP**, aby otworzyć okno dialogowe Właściwości POP.

Pojęcia pokrewne

“Serwer POP w systemie i5/OS” na stronie 4
Serwer POP jest implementacją interfejsu pocztowego POP3 w systemie i5/OS.

Konfigurowanie protokołu TCP/IP na potrzeby poczty elektronicznej

Przed skonfigurowaniem w systemie poczty elektronicznej należy skonfigurować protokół TCP/IP.

Jeśli poczta elektroniczna jest konfigurowana w systemie po raz pierwszy, należy wykonać następujące czynności. Jeśli protokół TCP/IP jest już skonfigurowany w systemie, można przejść bezpośrednio do konfigurowania serwerów SMTP i POP na potrzeby poczty elektronicznej.

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** **→ Sieć → Konfigurowanie TCP/IP** (*system* > Network > TCP/IP Configuration).
2. Prawym przyciskiem myszy kliknij pozycję **Interfejsy** i wybierz opcję **Nowy interfejs TCP/IP** oraz typ sieci, którą nowy interfejs będzie reprezentował. Aby utworzyć nowy interfejs TCP/IP, postępuj zgodnie z instrukcjami kreatora. Kreator poprosi o podanie następujących informacji:
   - Typ połączenia
   - Zasób sprzętowy
   - Opis linii
   - Adres IP
   - Nazwa hosta
   - Nazwa domeny

     Podane kreatorowi nazwa hosta wraz z nazwą domeny składają się na pełną nazwę domeny. SMTP wymaga pełnej nazwy domeny, aby móc się komunikować z innymi hostami SMTP.

     Na przykład, jeśli nazwą lokalnego hosta jest ASHOST, a nazwą lokalnej domeny jest DOMAIN.COMPANY.COM, pełną nazwą domeny jest ASHOST.DOMAIN.COMPANY.COM.
   - Uruchamiane serwery
3. Po zakończeniu pracy kreatora kliknij prawym przyciskiem myszy pozycję **TCP/IP** i wybierz opcję **Właściwości**. Pojawi się okno dialogowe Właściwości TCP/IP.
4. Kliknij zakładkę **Tabela hostów**.
5. Kliknij **Dodaj**. Pojawi się okno dialogowe Pozycja tabeli hosta TCP/IP.
6. Wpisz adres IP i nazwę hosta podaną kreatorowi nowego interfejsu TCP/IP.
7. Kliknij przycisk **OK**, aby zamknąć okno dialogowe Pozycja tabeli hosta TCP/IP.
8. Kliknij przycisk **OK**, aby zamknąć okno dialogowe Właściwości TCP/IP.

Pojęcia pokrewne

"Wykrywanie problemów z pocztą elektroniczną" na stronie 49
Wykonanie prostych czynności może być pomocne w określeniu przyczyny problemu z pocztą elektroniczną.

Zadania pokrewne

"Konfigurowanie serwerów SMTP i POP na potrzeby poczty elektronicznej"
Aby móc używać poczty elektronicznej, należy skonfigurować w systemie serwery SMTP i POP.

Konfigurowanie serwerów SMTP i POP na potrzeby poczty elektronicznej

Aby móc używać poczty elektronicznej, należy skonfigurować w systemie serwery SMTP i POP.

Uwaga: Obydwa serwery, SMTP i POP, muszą zostać poprawnie skonfigurowane.

Pojęcia pokrewne

"Serwer POP w systemie i5/OS" na stronie 4
Serwer POP jest implementacją interfejsu pocztowego POP3 w systemie i5/OS.

Zadania pokrewne

"Konfigurowanie protokołu TCP/IP na potrzeby poczty elektronicznej"
Przed skonfigurowaniem w systemie poczty elektronicznej należy skonfigurować protokół TCP/IP.

Konfigurowanie serwera SMTP

W rezultacie skonfigurowania TCP/IP system automatycznie skonfigurował serwer SMTP. Jednakże należy zmienić szereg właściwości SMTP, aby serwer SMTP prawidłowo obsługiwał pocztę elektroniczną.

Aby zmienić właściwości SMTP, wykonaj następujące czynności:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** **→ Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Kliknij dwukrotnie **SMTP**.
3. Kliknij zakładki wymienione w poniższej tabeli i ustaw w nich wartości pól wskazane w kolumnie ″Wykonaj następującą czynność″.

Kliknij zakładkę	Wykonaj następującą czynność
Ogólne	Zaznacz pole **Uruchom wraz z TCP/IP**[1] (Start when TCP/IP is started).
Ogólne	Dla pola **Wielkość podziału wiadomości (32-2048)** wybierz **Bez maksimum**.
Ogólne	Jeśli istnieje router poczty, wpisz jego nazwę, na przykład mailrouter.company.com. Nazwa routera poczty jest nazwą systemu, do którego serwer SMTP kieruje nielokalną pocztę elektroniczną. Więcej informacji zawiera temat System i Navigator.
Ogólne	Jeśli w systemie skonfigurowana jest zapora firewall, wybierz **Przekazuj pocztę wysłaną do routera poprzez firewall** (Forward outgoing mail to router through firewall).
Ogólne	Jeśli wymiana poczty elektronicznej następuje przez serwery Domino, usuń zawartość pola **Interpretacja znaku procentu jako znaku routingu**.
Ogólne	Jeśli chcesz przekazać całą nielokalną pocztę elektroniczną na inny serwer SMTP, wpisz pełna nazwę domeny wymiennika poczty w polu **Domena przekaz. konc. poczty** (Forwarding mailhub domain).
Ogólne	Jeśli chcesz, aby serwer SMTP obsługiwał znaki nowego wiersza (LF) lub znaki powrotu karetki (CRLF), zaznacz **Zezwalaj na sam znak nowego wiersza** (Allow bare line feed). Jeśli chcesz, aby serwer SMTP obsługiwał wyłącznie znaki CRLF, odznacz pole wyboru **Zezwalaj na sam znak nowego wiersza**.
Rejestracja automatyczna	Jeśli do wysyłania poczty używasz komendy SNDDST, a do pobierania poczty komendy RCVDST, i korzystasz z adresów SNADS zamiast z adresów internetowych, zaznacz pole wyboru **Automatyczne dodawanie zdalnych użytkowników do katalogu systemowego**.
Rejestracja automatyczna	Jeśli do wysyłania poczty używasz komendy SNDDST, a do pobierania poczty komendy RCVDST, zaznacz **Tabela aliasów systemu** (System alias table) w polu **Dodaj użytkowników do** (Add users to).
[1] Zmiana jest uwzględniana przy następnym uruchomieniu serwera SMTP.	

4. Aby zaakceptować zmiany, kliknij przycisk **OK**.

Zadania pokrewne

“Uwierzytelnianie lokalnej i przekazywanej poczty elektronicznej” na stronie 25
Można ochronić serwer przed spamem, żądając uwierzytelnienia przy wysyłaniu poczty elektronicznej. Żądanie uwierzytelnienia nie może być wykorzystywane do ograniczenia przekazywania wiadomości. Zalecane jest skonfigurowanie uwierzytelnienia dla serwera.

Włączanie warstwy SSL pomiędzy serwerem SMTP a klientem w systemie docelowym:

Aby włączyć warstwę SSL pomiędzy serwerem SMTP a klientem w systemie docelowym, wykonaj następujące czynności. Zakłada się, że na serwerze SMTP został utworzony certyfikat serwera.

Aby wykonać to zadanie, sprawdź, czy jesteś podłączony do systemu docelowego.

Uruchamianie i konfigurowanie programu DCM

1. W przeglądarce WWW połącz się z serwerem http://*nazwa_systemu*: 2001/

2. Na stronie Zadania i5/OS (i5/OS Tasks), wybierz **Menedżer certyfikatów cyfrowych** (Digital Certificate Manager) a następnie kliknij **Wybierz bazę certyfikatów** (Select a Certificate Store).
3. Na stronie Wybierz bazę certyfikatów (Select a Certificate Store) wybierz ***SYSTEM** i kliknij **Kontynuuj** (Continue).
4. Na stronie Baza certyfikatów i hasło (Certificate Store and Password) wpisz hasło do swojej bazy certyfikatów.
5. Rozwiń pozycję **Zarządzanie aplikacjami → Aktualizacja przypisania certyfikatu** (Manage Applications > Update certificate assignment) i wybierz **Serwer** (Server).
6. Wybierz **Serwer SMTP TCP/IP i5/OS** (i5/OS TCP/IP SMTP server) i w razie potrzeby kliknij **Aktualizacja przypisania certyfikatu** (Update Certificate Assignment).

Konfigurowanie serwera SMTP

Aby włączyć obsługę SSL, ustaw parametr ALWAUTH na *LCLRLY lub *RELAY za pomocą komendy Zmiana atrybutów SMTP (Change SMTP Attributes - CHGSMTPA).

- Jeśli parametr został ustawiony na *RELAY, tylko wiadomości e-mail wysyłane z drugiego serwera SMTP będą obsługiwać SSL.
- Jeśli parametr został ustawiony na *LCLRLY, włączone zostaną także parametry Zweryfikuj komunikaty struktury MSF (Verify MSF messages - VFYMSFMSG) oraz Zweryfikuj od użytkownika (Verify from user - VFYFROMUSR). Zastosowanie wartości domyślnej może również skutkować odrzuceniem pewnych wiadomości e-mail. Należy określić, czy obsługa odrzucania wiadomości ma zostać włączona.

Konfigurowanie klienta SMTP

Należy skonfigurować klienta SMTP platformy System i w taki sposób, aby mógł on wpisywać się do docelowego serwera SMTP platformy System i. Zastosuj komendę CL Dodanie pozycji listy protokołu SMTP (Add SMTP List Entry - ADDSMTPLE), aby dodać pozycję do listy uwierzytelniania hosta:

```
ADDSMTPLE TYPE(*HOSTAUTH) HOSTNAME(twoj_system.domena.com) USERNAME(odbiorca) PASSWORD(xxxx)
```

Nazwa hosta, która zostaje zapisana wielkimi literami, musi być zgodna z adresem poczty elektronicznej. Jeśli adresem poczty elektronicznej jest mojadres@twoj_system, należy dodać następującą pozycję:

```
ADDSMTPLE TYPE(*HOSTAUTH) HOSTNAME(TWOJ_SYSTEM) USERNAME(odbiorca) PASSWORD(xxxx)
```

Włączanie warstwy SSL pomiędzy serwerem SMTP a klientem w systemie nadawcy:

Aby wykonać to zadanie, należy być podłączonym do systemu nadawcy.

1. W przeglądarce WWW połącz się z serwerem http://*nazwa_systemu*: 2001/
2. Na stronie Zadania i5/OS (i5/OS Tasks), wybierz **Menedżer certyfikatów cyfrowych** (Digital Certificate Manager) a następnie kliknij **Wybierz bazę certyfikatów** (Select a Certificate Store).
3. Na stronie Wybierz bazę certyfikatów (Select a Certificate Store) wybierz ***SYSTEM** i kliknij **Kontynuuj** (Continue).
4. Na stronie Baza certyfikatów i hasło (Certificate Store and Password) wpisz hasło dla Twojej bazy certyfikatów i kliknij **Kontynuuj** (Continue). Jeśli nie posiadasz certyfikatu użytkownika lub chcesz utworzyć certyfikat użytkownika, wykonaj czynności od 5 do 8. W przeciwnym przypadku przejdź do czynności 9.
5. Na stronie Tworzenie certyfikatu (Create Certificate) wybierz **Certyfikat użytkownika** (User certificate) i kliknij **Kontynuuj** (Continue).
6. Na stronie Tworzenie certyfikatu użytkownika (Create User Certificate) wypełnij wymagane pola informacjami o certyfikacie i kliknij **Kontynuuj** (Continue).
7. W oknie Potencjalne naruszenie skryptu (Potential Scripting Violation) kliknij **Tak**.
8. Na stronie Tworzenie certyfikatu użytkownika (Create User Certificate) kliknij **OK**. System zastosuje certyfikat użytkownika klienta.
9. Rozwiń pozycję **Zarządzanie aplikacjami → Aktualizacja przypisania certyfikatu** (Manage Applications > Update certificate assignment) i wybierz **Certyfikat serwera lub klienta** (Server or client certificate).

10. Na stronie Aktualizacja przypisania certyfikatu (Update Certificate Assignment) wybierz **Klient** (Client) i kliknij **Kontynuuj** (Continue).
11. Wybierz **Klient TCP/IP i5/OS** (i5/OS TCP/IP Client) i kliknij przycisk **Aktualizacja przypisania certyfikatu** (Update Certificate Assignment).

Instalowanie ośrodka certyfikacji dziennika w systemie nadawczym:

Jeśli certyfikat cyfrowy dziennika został wydany przez ośrodek certyfikacji (CA), który nie jest znany systemowi nadawczemu, należy zainstalować certyfikat cyfrowy dla ośrodka certyfikacji w systemie nadawczym.

Eksportowanie lokalnego certyfikatu CA i wysyłanie go do systemu nadawczego

Zakłada się, że ośrodek certyfikacji jest lokalny. Jednakże można wykorzystać tę procedurę do wyeksportowania certyfikatu, który nie jest znany systemowi nadawczemu.

Aby wyeksportować lokalny certyfikat CA, wykonaj następujące czynności:

1. Kliknij **Wybierz bazę certyfikatów** (Select a Certificate Store) i wybierz **Lokalny ośrodek certyfikacji (CA)** (Local Certificate Authority (CA)). Kliknij przycisk **Kontynuuj** (Continue).
2. Na stronie Baza certyfikatów i hasło (Certificate Store and Password) wpisz hasło.
3. Rozwiń pozycję **Zarządzanie lokalnymi ośrodkami certyfikacji (CA) → Eksport** (Manage Local CA > Export) i wybierz **Plik - Eksport do pliku** (File - Export to a file). Kliknij przycisk **Kontynuuj** (Continue).
4. Na stronie Eksportowanie certyfikatu (Export Certificate) wpisz katalog i nazwę pliku, w którym certyfikat CA ma być przechowywany. Jeśli katalog jeszcze nie istnieje, użyj komendy mkdir, aby go utworzyć.
5. Na stronie Certyfikat został pomyślnie wyeksportowany (Export Certificate Successful) kliknij **OK**.
6. Użyj protokołu FTP w trybie ASCII do wysłania certyfikatu CA z systemu odbiorczego do systemu nadawczego.

Instalowanie certyfikatu CA w systemie nadawczym

1. Na stronie Wybierz bazę certyfikatów (Select a Certificate Store) wybierz ***SYSTEM** i kliknij **Kontynuuj** (Continue).
2. Na stronie Baza certyfikatów i hasło (Certificate Store and Password) wpisz hasło i kliknij **Kontynuuj** (Continue).
3. Rozwiń pozycję **Zarządzanie certyfikatami → Importowanie certyfikatów** (Manage Certificates > Import certificates), wybierz **Ośrodek certyfikacji (CA)** (Certificate Authority (CA)) i kliknij **Kontynuuj** (Continue).
4. Na stronie Importowanie certyfikatu ośrodka certyfikacji (Import Certificate Authority (CA) Certificate) wpisz katalog, w którym przechowywany jest certyfikat systemu odbiorczego. Kliknij przycisk **Kontynuuj** (Continue).
5. Przypisz etykietę certyfikatu do swojego certyfikatu i kliknij **Kontynuuj** (Continue). Wyświetlony zostanie następujący komunikat: Certyfikat został zaimportowany (The certificate has been imported).
6. Kliknij przycisk **OK**.

Konfigurowanie serwera POP

Aby używać serwera POP do dostarczania poczty klientom POP, należy go wcześniej skonfigurować.

Po przesłaniu żądania przez klienta POP, serwer POP dostarcza do klienta POP pocztę ze skrzynki pocztowej użytkownika. Odpowiednie przygotowanie systemu do obsługi poczty elektronicznej wymaga skonfigurowania serwera POP.

Aby skonfigurować serwer POP do współpracy z programem pocztowym, takim jak Netscape Mail lub Eudora Pro, wykonaj następujące działania:

1. Uruchom program System i Navigator i rozwiń pozycję ***system* → Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Kliknij dwukrotnie **POP**.

3. Skorzystaj z poniższej tabeli, aby ustawić wartości pól.

Kliknij zakładkę	Wykonaj następującą czynność
Ogólne	Zaznacz pole **Uruchom wraz z TCP/IP**.
Ogólne	Jeśli chcesz umożliwić obsługę zarówno sesji TLS/SSL, jak i niechronionych sesji POP, wybierz **Połączenia chronione i niechronione** (Both secure and nonsecure) w polu **Obsługa warstw SSL uruchamiana z serwerem** (Socket layer support to be started with server).
Konfiguracja	Dla pola **Wielkość podziału wiadomości (32-2048)** wybierz **Bez maksimum**.
Konfiguracja	Jeśli klienci POP dostają się do systemu przez połączenie modemowe i pobierają dużo poczty, należy zwiększyć **Limit czasu nieaktywności**.
Odwzorowania	Wybierz **Używaj tylko w przypadku nieobsługiwanego CCSID**.

4. Aby zaakceptować zmiany, kliknij przycisk **OK**.

Przydzielanie certyfikatu serwerowi POP:

Jeśli certyfikat nie został przydzielony do aplikacji serwera POP podczas tworzenia lokalnego ośrodka CA (Certificate Authority) lub jeśli skonfigurowano system w taki sposób, aby żądał certyfikatu z publicznego ośrodka CA, wykonaj następujące czynności.

1. Uruchom program IBM Digital Certificate Manager (DCM). Jeśli konieczne jest uzyskanie lub utworzenie certyfikatów albo skonfigurowanie lub zmiana systemu certyfikatów, należy zrobić to w tym momencie. Więcej informacji na temat konfigurowania systemu certyfikatów można znaleźć w temacie Konfigurowanie DCM.
2. Kliknij **Wybierz bazę certyfikatów** (Select a Certificate Store).
3. Wybierz ***SYSTEM**. Kliknij przycisk **Kontynuuj** (Continue).
4. Wpisz hasło bazy certyfikatów *SYSTEM. Kliknij przycisk **Kontynuuj** (Continue).
5. Po odświeżeniu menu nawigacji po lewej stronie, rozwiń pozycję **Zarządzanie aplikacjami** (Manage Applications).
6. Kliknij **Aktualizacja przypisania certyfikatu** (Update certificate assignment).
7. Wybierz **Aplikacja serwera** (Server application). Kliknij przycisk **Kontynuuj** (Continue).
8. Wybierz opcję **Serwer TCP/IP POP systemu i5/OS** (i5/OS TCP/IP POP Server).
9. Kliknij **Aktualizacja przypisania certyfikatu** (Update Certificate Assignment), aby przypisać certyfikat do serwera POP.
10. Wybierz z listy certyfikat, który ma zostać przypisany do serwera.
11. Kliknij **Przypisz nowy certyfikat** (Assign New Certificate).
12. Po zakończeniu konfigurowania certyfikatów dla serwera POP, kliknij **Gotowe** (Done).

Rejestrowanie użytkowników poczty elektronicznej

Aby móc rejestrować użytkowników poczty elektronicznej, należy utworzyć profile użytkowników.

Profile użytkowników umożliwiają systemowi operacyjnemu i5/OS identyfikowanie nadawcy i odbiorcy wiadomości e-mail. Każdy użytkownik, który ma mieć dostęp do systemu poczty elektronicznej, musi posiadać w systemie profil użytkownika.

Podczas tworzenia profili użytkowników automatycznie rejestruje się ich w katalogu dystrybucyjnym systemu. Dzięki katalogowi dystrybucyjnemu systemu protokół SMTP może określić, gdzie dostarczyć lokalną pocztę.

W celu utworzenia profilu użytkownika dla wszystkich korzystających z poczty za pomocą protokołu POP i usług dystrybucyjnych SNADS (System Network Architecture Distribution Services), wykonaj następujące czynności:

1. W programie System i Navigator rozwiń węzły ***nazwa systemu* → Użytkownicy i grupy** (*nazwa systemu* > Users and Groups).
2. Prawym przyciskiem myszy kliknij pozycję **Wszyscy użytkownicy** i wybierz opcję **Nowy użytkownik**.
3. Wpisz nazwę i hasło dla tego użytkownika.

   Uwaga: Hasło będzie umożliwiało użytkownikom POP dostęp do skrzynek pocztowych protokołu POP.
4. Kliknij przycisk **Możliwości**.
5. Kliknij zakładkę **Uprawnienia**. Upewnij się, że pole Klasa uprawnień ma wartość **Użytkownik**.
6. Kliknij przycisk **OK**.
7. Kliknij przycisk **Dane osobowe**.
8. Kliknij zakładkę **Poczta**.
9. Wybierz **Poziom usług poczty**.
   - Jeśli użytkownik jest użytkownikiem usług SNADS, wybierz **Indeks użytkownika** (User index).
   - Jeśli użytkownik jest użytkownikiem protokołu pocztowego POP3, wybierz **Systemowa skrzynka pocztowa** (System mailbox).
10. Wybierz **Typ preferowanego adresu**.
    - Dla użytkownika usług dystrybucyjnych SNADS wybierz **ID użytkownika i adres**.
    - Jeśli użytkownik jest użytkownikiem protokołu pocztowego POP3, wybierz **Nazwa SMTP** (SMTP name).
11. Sprawdź, czy w polu Domena dla protokołu SMTP podana jest właściwa nazwa domeny. Zwykle nazwa domyślna jest poprawna. Potrzeba zmiany może zajść w przypadku, gdy w systemie jest kilka domen lokalnych.
12. Kliknij przycisk **OK**. Jeśli rejestrowany jest użytkownik usług SNADS, proces rejestracji zostaje zakończony. Jeśli rejestrowany jest użytkownik POP, który będzie używać serwera POP systemu i5/OS tylko do odbierania poczty elektronicznej, przejdź do następnego kroku.
13. Kliknij przycisk **Zadania**.
14. Kliknij zakładkę **Uruchamianie sesji**.
15. W polu **Menu początkowe** wybierz **Wypisanie się z systemu**. Przy tym ustawieniu każda próba wpisania się do systemu inna niż odbieranie poczty elektronicznej lub zmiana hasła, powoduje automatyczne wypisanie użytkownika.
16. Kliknij przycisk **OK**.
17. Kliknij przycisk **OK**.
18. Powtarzaj powyższe instrukcje, dopóki wszyscy użytkownicy nie będą mieli profili użytkownika.

Pojęcia pokrewne

“Wysyłanie i pobieranie poczty elektronicznej” na stronie 30
System jest serwerem poczty elektronicznej i ma zarejestrowanych użytkowników poczty elektronicznej (SNADS, POP lub Lotus). Użytkownicy poczty elektronicznej mogą wysyłać, pobierać i odczytywać wiadomości e-mail za pomocą klienta POP lub SNADS.

Zadania pokrewne

“Wysyłanie poczty elektronicznej za pomocą usług dystrybucyjnych Systems Network Architecture Systems (SNADS)” na stronie 33
Pocztę elektroniczną można wysyłać z systemu, korzystając z programu klienckiego usług SNADS. Nadawca poczty musi być lokalnym użytkownikiem usług dystrybucyjnych SNA.

Uruchamianie i zatrzymywanie serwerów poczty elektronicznej

Uruchom wymagane serwery, aby sprawdzić, czy wszystko działa poprawnie i czy wszystkie dokonane przez ciebie zmiany konfiguracji zostały zastosowane. Czasami może być konieczne wykonanie restartu serwerów. Wykonuje się to zatrzymując serwery, a następnie wykonując kolejno czynności ponownego uruchamiania serwerów.

Zadania pokrewne

“Sprawdzanie serwerów poczty elektronicznej” na stronie 37
Jednym z powszechnych problemów z pocztą jest to, że odpowiednie serwery nie zostały uruchomione. Przed przystąpieniem do używania serwerów poczty elektronicznej należy sprawdzić status serwerów i sprawdzić, czy wszystkie są uruchomione.

Uruchamianie serwerów poczty elektronicznej

Możesz uruchomić serwery i skonfigurować swój system jako serwer poczty elektronicznej z zarejestrowanymi użytkownikami poczty.

W celu uruchomienia serwerów, wykonaj opisane poniżej czynności:

1. W programie System i Navigator rozwiń węzły ***twój system*** → **Sieć**.
2. Prawym przyciskiem myszy kliknij pozycję **Konfiguracja TCP/IP** i wybierz opcję **Właściwości**. Wyświetlone zostanie okno dialogowe Właściwości konfiguracji TCP/IP (TCP/IP Configuration Properties).
   - Jeśli status TCP/IP ma wartość Uruchomiono, kliknij **OK** i przejdź do następnego punktu.
   - Jeśli nie, kliknij **Anuluj**, aby zamknąć okno dialogowe Właściwości konfiguracji TCP/IP, a następnie Prawym przyciskiem myszy kliknij pozycję **Konfiguracja TCP/IP** i wybierz opcję **Uruchom**. Po zakończeniu kliknij **OK**.
3. Rozwiń **Serwery** → **TCP/IP**. Jeśli serwery SMTP i POP nie zostały uruchomione, wykonaj następujące czynności, aby je uruchomić:
   a. Prawym przyciskiem myszy kliknij pozycję **SMTP** i wybierz opcję **Uruchom**.
   b. Prawym przyciskiem myszy kliknij pozycję **POP** i wybierz opcję **Uruchom**.
4. Aby uruchomić strukturę serwera poczty (MSF), w wierszu komend wpisz STRMSF.
5. Jeśli uruchomione są usługi SNADS, wpisz komendę STRSBS QSNADS, aby uruchomić podsystem QSNADS.

Serwery zostały uruchomione, a w systemie działa serwer poczty elektronicznej z zarejestrowanymi użytkownikami.

Zatrzymywanie serwerów poczty elektronicznej

Do zatrzymania serwerów poczty elektronicznej można użyć programu System i Navigator.

W celu zatrzymania serwerów, wykonaj następujące czynności:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** → **Sieć** → **Serwery** → **TCP/IP** (*system* > Network > Servers > TCP/IP).Aby zatrzymać wcześniej uruchomione serwery SMTP i POP, wykonaj następujące czynności:
   a. Prawym przyciskiem myszy kliknij pozycję **SMTP** i wybierz opcję **Zatrzymaj**.
   b. Prawym przyciskiem myszy kliknij pozycję **POP** i wybierz opcję **Uruchom**.
2. Aby zakończyć działanie struktury serwera poczty (MSF), w wierszu komend wpisz ENDMSF.
3. Jeśli uruchomione są usługi SNADS, wpisz komendę ENDSBS QSNADS, aby zatrzymać podsystem QSNADS.

Konfigurowanie profilu modemowego połączenia dla poczty elektronicznej

Jeśli obsługa AT&T Global Network nie jest dostępna, należy skonfigurować profil połączenia dla poczty elektronicznej.

Aby ręcznie utworzyć profil połączenia modemowego, wykonaj następujące czynności:

Uwaga: Jeśli obsługa AT&T Global Network jest dostępna, możesz przejść do kreatora Konfigurowanie połączenia modemowego do dostawcy ISP (Configuring the ISP Dial-up Connection).

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** → **Sieć** → **Usługi zdalnego dostępu** (*system* > Network > Remote Access Services).
2. Prawym przyciskiem myszy kliknij pozycję **Profile połączenia odbiorcy** i wybierz opcję **Nowy profil**.
3. Wybierz **PPP** jako **Rodzaj protokołu**.

4. Wybierz **Linia komutowana** jako **Typ połączenia**.
5. Rozwiń **TCP/IP** i wybierz **Konfiguracja łącza**.
6. Rozwiń **Serwery → TCP/IP**.
7. Prawym przyciskiem myszy kliknij pozycję **SMTP** i wybierz opcję **Właściwości**.
8. Kliknij zakładkę **Program planujący**. Zaznacz pole wyboru **Uruchom program planujący podczas uruchamiania SMTP** i podaj utworzony profil połączenia.
9. Kliknij stronę ETRN i zaznacz pole wyboru **Obsługa ETRN (Pobieranie poczty przez połączenie modemowe)**. Kliknij **Dodaj**, aby określić nazwę domeny dla adresu zewnętrznego serwera dostawcy ISP.
10. Uaktywnij firewall i wskaż zewnętrzny serwer poczty dostawcy usług internetowych (ISP).
11. Wykonaj polecenia kreatora, aby skonfigurować nowe połączenie modemowe do dostawcy usług internetowych.

Zadania pokrewne

"Konfigurowanie kreatora połączeń modemowych ISP"
Przed przystąpieniem do używania funkcji SMTP programu planującego, służącej do przesyłania dużej liczby wiadomości e-mail przez sieć ISP (Internet Service Provider), należy skonfigurować profil połączenia modemowego.

Konfigurowanie kreatora połączeń modemowych ISP

Przed przystąpieniem do używania funkcji SMTP programu planującego, służącej do przesyłania dużej liczby wiadomości e-mail przez sieć ISP (Internet Service Provider), należy skonfigurować profil połączenia modemowego.

Do skonfigurowania profilu połączenia modemowego ISP można użyć kreatora połączeń modemowych ISP.

Wymagania wstępne:

Jeśli obsługa AT&T Global Network nie jest dostępna, należy najpierw skonfigurować profil połączenia modemowego dla poczty elektronicznej. Kreator połączeń dostarcza adresy IP serwerów poczty (SMTP i POP), przypisane im nazwy domen, nazwy kont i hasła.

Aby uruchomić kreatora i skonfigurować program planujący SMTP, wykonaj następujące czynności:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** **→ Sieć → Usługi zdalnego dostępu** (*system* > Network > Remote Access Services).
2. Prawym przyciskiem myszy kliknij pozycję **Profile połączenia nadawcy** i wybierz opcję **Nowe połączenie telefoniczne z siecią AT&T Global Network**.
3. Na panelu powitalnym kliknij **Dalej**, aby wystartować.
4. Na panelu **Typ aplikacji** wybierz **Aplikacja wymiany poczty** i kliknij **Dalej**.
5. Wykonaj polecenia kreatora, aby skonfigurować nowe połączenie telefoniczne AT&T Global Network.

Po skonfigurowaniu połączenia modemowego można ustalić harmonogram zadań wsadowych ISP.

Zadania pokrewne

"Konfigurowanie profilu modemowego połączenia dla poczty elektronicznej" na stronie 21
Jeśli obsługa AT&T Global Network nie jest dostępna, należy skonfigurować profil połączenia dla poczty elektronicznej.

"Harmonogramu zadań wsadowych poczty elektronicznej ISP" na stronie 23
Aby ograniczyć czas nawiązywania połączenia modemowego, można ustalić harmonogram uruchamiania połączeń z dostawcą ISP (Internet Service Provider - dostawca usług internetowych) w regularnych odstępach czasu. Do określenia częstotliwości łączenia systemu z dostawcą ISP i wysyłania poczty firmowej należy użyć programu planującego SMTP.

Harmonogramu zadań wsadowych poczty elektronicznej ISP

Aby ograniczyć czas nawiązywania połączenia modemowego, można ustalić harmonogram uruchamiania połączeń z dostawcą ISP (Internet Service Provider - dostawca usług internetowych) w regularnych odstępach czasu. Do określenia częstotliwości łączenia systemu z dostawcą ISP i wysyłania poczty firmowej należy użyć programu planującego SMTP.

Wymagania wstępne:

Aby skonfigurować połączenie, można skorzystać z kreatora połączeń modemowych.

Aby program planujący wysyłał pocztę do dostawcy ISP, wykonaj następujące czynności:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** **→ Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Kliknij dwukrotnie **SMTP**.
3. Kliknij zakładkę **Program planujący**.
4. Zaznacz pole wyboru **Uruchom program planujący podczas uruchamiania SMTP**.
5. Wybierz **Profil połączenia PPP**, skonfigurowany za pomocą kreatora połączeń modemowych AT&T Global Network, lub wybierz ręcznie skonfigurowany **Profil połączenia PPP**.
6. Ustaw w minutach **Częstotliwość transferu poczty**, z jaką SMTP będzie dostarczał pocztę z kolejki.
7. Jeśli ISP nie należy do AT&T Global Network, zaznacz pole wyboru **Wyślij ETRN podczas łączenia z serwerem zdalnym**.
8. Wprowadź Adres IP serwera dla serwera poczty przychodzącej w sieci dostawcy ISP i wprowadź Zarejestrowana domena.host dostawcy ISP, dla którego serwer SMTP wyśle ETRN.
9. Kliknij przycisk **OK**.

Zadania pokrewne

"Konfigurowanie kreatora połączeń modemowych ISP" na stronie 22
Przed przystąpieniem do używania funkcji SMTP programu planującego, służącej do przesyłania dużej liczby wiadomości e-mail przez sieć ISP (Internet Service Provider), należy skonfigurować profil połączenia modemowego.

"Konfigurowanie serwera SMTP do pobierania poczty przez połączenie modemowe"
Można zastosować serwer SMTP do pobierania poczty dla zdalnych lokalizacji za pomocą połączenia modemowego.

Konfigurowanie serwera SMTP do pobierania poczty przez połączenie modemowe

Można zastosować serwer SMTP do pobierania poczty dla zdalnych lokalizacji za pomocą połączenia modemowego.

System musi mieć stały adres IP i musi być zarejestrowany w DNS. Każda domena hosta, dla której zdalne serwery połączone przez modem będą pobierać pocztę, musi również we wpisie DNS wskazującym na ten system mieć pozycje MX. System musi również zawierać aliasy dla domen hosta w tabeli hosta lokalnego. Jeśli zdalne serwery połączone przez modem działają pod kontrolą systemu operacyjnego i5/OS, muszą zostać skonfigurowane dla planowanych zadań wsadowych poczty elektronicznej ISP.

Aby odbierać żądania poczty elektronicznej od zdalnych serwerów poczty elektronicznej połączonych za pomocą modemu, wykonaj następujące czynności:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** **→ Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Kliknij dwukrotnie **SMTP**.
3. Kliknij zakładkę **ETRN**.
4. Zaznacz pole wyboru **Obsługa ETRN (Pobieranie poczty przez połączenie modemowe)**.

5. Kliknij **Dodaj**, aby podać nazwę hosta i domeny dostawcy ISP. Jeśli wiele serwerów przechowuje pocztę, można tę czynność powtórzyć wielokrotnie.
6. Kliknij przycisk **OK**.

Zadania pokrewne

"Harmonogramu zadań wsadowych poczty elektronicznej ISP" na stronie 23
Aby ograniczyć czas nawiązywania połączenia modemowego, można ustalić harmonogram uruchamiania połączeń z dostawcą ISP (Internet Service Provider - dostawca usług internetowych) w regularnych odstępach czasu. Do określenia częstotliwości łączenia systemu z dostawcą ISP i wysyłania poczty firmowej należy użyć programu planującego SMTP.

Obsługa wielu domen

Można skonfigurować serwer SMTP do obsługi wielu domen w celu udostępnienia funkcji ISP (Internet Service Provider).

Aby serwer SMTP mógł udostępniać funkcje ISP, musi zostać wyświetlony jako funkcjonujący w wielu domenach. Klient SMTP wykorzystuje te informacje konfiguracyjne do rozpoznania, z którym interfejsem ma się połączyć, kiedy wysyła wiadomość e-mail, i którą wiadomość traktować jako lokalną (to znaczy dokonać translacji i wysłać samodzielnie), a którą przekazać do skonfigurowanego demona poczty zapory firewall.

1. Uruchom program System i Navigator i rozwiń pozycję ***system* → TCP/IP → Sieć** (*system* > TCP/IP > Network).
2. Prawym przyciskiem myszy kliknij pozycję **SMTP** i wybierz opcję **Właściwości**.
3. Kliknij zakładkę **Wiele domen**.
4. Kliknij **Dodaj**, aby określić, które domeny i interfejsy mają być obsługiwane.
5. Kliknij przycisk **OK**.

Pojęcia pokrewne

"Wymagania wstępne dla routera poczty elektronicznej" na stronie 25
Informacje na temat czynności, które należy wykonać przed konfiguracją routera poczty elektronicznej.

Zabezpieczanie poczty elektronicznej

W celu lepszego zabezpieczenia poczty elektronicznej można używać zapór firewall, ograniczać przekazywanie i możliwości nawiązywania połączeń oraz filtrować wiadomości e-mail zainfekowane wirusami.

Zagwarantowanie bezpiecznego środowiska serwera SMTP jest bardzo istotne. Koniecznie trzeba chronić serwer SMTP i użytkowników przed wewnętrznymi i zewnętrznymi atakami.

Pojęcia pokrewne

| "Koncepcje poczty elektronicznej" na stronie 2
| Poczta elektroniczna (wiadomości e-mail) stała się bardzo ważnym narzędziem w wielu firmach. System
| operacyjny i5/OS używa protokołów SMTP i POP, aby zapewnić płynną i efektywną obsługę poczty w sieci.

Odsyłacze pokrewne

| tworzenie i wysyłanie poczty w standardzie MIME (Create and Send MIME E-mail - QtmsCreateSendEmail),
| funkcja API

Informacje pokrewne

| bezpieczeństwo poczty elektronicznej

Wysyłanie poczty elektronicznej przez router lub zaporę firewall

Router poczty elektronicznej jest systemem pośrednim, do którego serwer SMTP (Simple Mail Transfer Protocol) dostarcza pocztę, gdy nie może znaleźć położenia dokładnego adresu IP odbiorcy.

Router poczty wyznacza trasę poczty do adresu IP lub do kolejnego routera. Kiedy lokalny serwer nie może dostarczyć poczty do właściwego systemu, należy skierować pocztę do innego systemu. Jeśli system wyposażony jest w firewall, może on być używany jako router.

Przed skonfigurowaniem routera należy zapoznać się z tematem “Wymagania wstępne dla routera poczty elektronicznej”.

W celu skonfigurowania routera:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** **→ Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Kliknij dwukrotnie **SMTP**.
3. Kliknij zakładkę **Ogólne**.
4. Wpisz nazwę routera poczty.

W celu kierowania poczty przez firewall:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** **→ Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Kliknij dwukrotnie **SMTP**.
3. Kliknij zakładkę **Ogólne**.
4. Wpisz nazwę zapory firewall - na przykład, FWAS400.company.com - w polu **Router poczty** (Mail Router).
5. Wybierz **Przekazuj pocztę wysyłaną do routera przez firewall**.

Wymagania wstępne dla routera poczty elektronicznej

Informacje na temat czynności, które należy wykonać przed konfiguracją routera poczty elektronicznej.

Przed konfiguracją routera poczty należy uwzględnić następujące informacje:

- Serwer pośredni nie musi działać pod kontrolą systemu operacyjnego i5/OS. Router poczty wymaga jedynie tabeli hostów zawierającej wszystkie serwery hostów, do których będzie kierowana poczta elektroniczna. Jeśli router poczty działa pod kontrolą systemu operacyjnego i5/OS, nie wymaga on żadnej konkretnej wersji tego systemu.
- Można skonfigurować tylko jeden serwer pośredni do kierowania poczty między systemem źródłowym a docelowym. W takiej sytuacji nie można zagnieżdżać routerów.
- Serwer SMTP (Simple Mail Transfer Protocol) musi mieć możliwość uzyskania adresu IP routera poczty w momencie, gdy jest on uruchamiany. Adres ten pobierany jest z lokalnej tabeli hostów lub z serwera nazw domen (DNS). Jeśli serwer SMTP nie może uzyskać adresu IP routera poczty, wówczas pracuje bez używania routera.
- Obsługa firewalla klienta SMTP wykorzystuje router do przekazywania poczty, która jest przeznaczona dla hostów poza domeną lokalną (chronioną). Aby dostarczyć pocztę elektroniczną, router poczty musi być serwerem uprawnionym do przesyłania poczty elektronicznej przez firewall. Gdy włączona jest obsługa zapory firewall SMTP, z routera muszą też korzystać odbiorcy poczty, których domeny znajdują się poza systemem i5/OS. Wersja systemu i5/OS V5R1 oraz późniejsze obsługują wiele domen lokalnych. Można skonfigurować wiele domen, z których poczta nie jest wysyłana przez firewall.

  Zadania pokrewne

  “Obsługa wielu domen” na stronie 24
  Można skonfigurować serwer SMTP do obsługi wielu domen w celu udostępnienia funkcji ISP (Internet Service Provider).

Uwierzytelnianie lokalnej i przekazywanej poczty elektronicznej

Można ochronić serwer przed spamem, żądając uwierzytelnienia przy wysyłaniu poczty elektronicznej. Żądanie uwierzytelnienia nie może być wykorzystywane do ograniczenia przekazywania wiadomości. Zalecane jest skonfigurowanie uwierzytelnienia dla serwera.

Aby włączyć uwierzytelnianie na serwerze, należy wykonać następujące czynności:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** **→ Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Kliknij dwukrotnie **SMTP**.

3. Kliknij zakładkę **Uwierzytelnianie** (Authentication) i ustaw wartości pól wskazane w kolumnie ″Wykonaj następującą czynność″.

Kliknij zakładkę	Wykonaj następującą czynność
Uwierzytelnianie	Jeśli serwer ma wykorzystywać protokół TLS/SSL do uwierzytelniania przeprowadzanego lokalnie i podczas przekazywania wiadomości, wybierz **Żądaj użycia protokołu TLS/SSL do uwierzytelniania przeprowadzanego lokalnie oraz podczas przekazywania** (Require TLS/SSL and authenticate it locally and when using the relay).
Uwierzytelnianie	Jeśli serwer ma wykorzystywać protokół TLS/SSL wyłącznie do uwierzytelniania podczas przekazywania wiadomości, wybierz **Żądaj użycia protokołu TLS/SSL i przeprowadzaj uwierzytelnianie wyłącznie podczas przekazywania** (Require TLS/SSL and authenticate only the relay).
Uwierzytelnianie	Jeśli wyłącznie użytkownicy z listy autoryzowanej mają mieć prawo do wpisania się do serwera SMTP, wybierz **Weryfikuj identyfikatory podczas dostarczania lokalnego** (Verify IDs on local delivery).
Uwierzytelnianie	Jeśli serwer SMTP ma pozwalać funkcjom programu snap-in struktury serwera poczty (MSF) na odrzucanie niezweryfikowanych wiadomości e-mail, wybierz opcję **Weryfikuj nadawcę wiadomości** (Verify message originator).
Uwierzytelnianie	Jeśli serwer SMTP ma weryfikować, czy adres e-mail nadawcy znajduje się w katalogu dystrybucyjnym systemu i czy adresy te są zgodne, wybierz opcję **Użytkownicy** (Users) lub **Użytkownicy nie wymienieni na liście akceptowanych użytkowników** (Users not on the accept list). Użytkownicy, których adresy e-mail nie będą zgodne z przechowywanymi w katalogu dystrybucyjnym systemu, zostaną odrzuceni.

4. Aby zaakceptować zmiany, kliknij przycisk **OK**.

Zadania pokrewne

“Ograniczanie przekazywania wiadomości” na stronie 27
Aby zapobiec wykorzystywaniu danego serwera pocztowego do rozsyłania spamu lub masowego rozsyłania poczty elektronicznej, można zastosować funkcję ograniczania przekazywania i określić, kto może używać danego systemu do przekazywania wiadomości. Jednakże nie można uwierzytelniać poczty elektronicznej po ograniczeniu przekazywania wiadomości.

“Konfigurowanie serwera SMTP” na stronie 16
W rezultacie skonfigurowania TCP/IP system automatycznie skonfigurował serwer SMTP. Jednakże należy zmienić szereg właściwości SMTP, aby serwer SMTP prawidłowo obsługiwał pocztę elektroniczną.

Śledzenie nadawcy poczty elektronicznej

Można teraz skonfigurować serwer SMTP w taki sposób, aby odrzucał nadawcę poczty elektronicznej, który nie jest uwierzytelniony. Dodatkowo można skonfigurować funkcje programu snap-in struktury MSF serwera SMTP w taki sposób, aby odrzucały niezweryfikowaną pocztę elektroniczną.

Należy włączyć szyfrowanie transakcji, czyli protokoły TLS/SSL, aby odrzucać niezweryfikowanych nadawców lub niezweryfikowane wiadomości e-mail.

Odrzucanie niezweryfikowanego nadawcy wiadomości e-mail

Aby odrzucać niezweryfikowanych nadawców wiadomości e-mail, wykonaj następujące czynności:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** **→ Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Prawym przyciskiem myszy kliknij pozycję **SMTP** i wybierz opcję **Właściwości**.
3. Kliknij zakładkę **Uwierzytelnianie** (Authentication).
4. Jeśli chcesz, aby wszyscy nadawcy poczty elektronicznej byli weryfikowani, w polu **Weryfikuj pocztę od użytkownika** (Verify mail from user), wybierz **Wszyscy** (All). Wybierz **Użytkownicy nie wymienieni na liście akceptowanych użytkowników** (Users not on the accept list), jeśli mają być weryfikowani wyłącznie użytkownicy nie wymienieni na liście akceptowanych użytkowników.

5. Kliknij przycisk **OK**.

Serwer SMTP sprawdzi, czy nadawca znajduje się w katalogu dystrybucyjnym systemu i czy adres poczty elektronicznej jest zgodny z adresem w katalogu. Jeśli zgodność nie zostanie stwierdzona, użytkownik zostanie odrzucony.

Odrzucanie niezweryfikowanej wiadomości e-mail

Aby odrzucić niezweryfikowaną wiadomość e-mail, wykonaj następujące czynności:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** **→ Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Prawym przyciskiem myszy kliknij pozycję **SMTP** i wybierz opcję **Właściwości** (Properties).
3. Kliknij zakładkę **Uwierzytelnianie** (Authentication).
4. Wybierz opcję **Żądaj użycia protokołu TLS/SSL do uwierzytelniania przeprowadzanego lokalnie oraz podczas przekazywania** (Require TLS/SSL and authenticate it locally and when using the relay) dla pola **Zezwalaj na uwierzytelnianie** (Allow authentication).
5. Wybierz **Weryfikuj nadawcę wiadomości MSF** (Verify MSF message originator).
6. Kliknij przycisk **OK**.

Jeśli wiadomość e-mail nie pochodzi ze źródła uwierzytelnionego, wtedy użytkownikiem, który wydał komendę API QzmfCrtMailMsg(), powinien być nadawca wiadomości MSF. W przeciwnym razie funkcje programu snap-in serwera SMTP odrzucą tę wiadomość.

Ograniczanie przekazywania wiadomości

Aby zapobiec wykorzystywaniu danego serwera pocztowego do rozsyłania spamu lub masowego rozsyłania poczty elektronicznej, można zastosować funkcję ograniczania przekazywania i określić, kto może używać danego systemu do przekazywania wiadomości. Jednakże nie można uwierzytelniać poczty elektronicznej po ograniczeniu przekazywania wiadomości.

Istnieje sześć możliwości umożliwienia przekazywania:

- umożliwienie wszystkim przekazywania poczty,
- zabronienie wszystkim przekazywania poczty,
- akceptowanie poczty tylko dla odbiorców z listy najbliższych domen,
- akceptowanie poczty tylko z określonych adresów znajdujących się na liście,
- akceptowanie poczty dla odbiorców z listy najbliższych domen i z określonych adresów,
- akceptowanie poczty od klientów POP przez określony czas.

Ograniczanie przekazywania możliwe jest tylko po wybraniu opcji **Bez protokołu TLS/SSL i bez uwierzytelnienia** (No TLS/SSL and no authentication will be done). W programie System i Navigator opcja ta jest dostępna na stronie Uwierzytelnianie (Authentication) po określeniu właściwości SMTP.

Aby podać użytkowników, którzy mogą wysyłać pocztę elektroniczną do Internetu, wykonaj następujące czynności:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** **→ Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Prawym przyciskiem myszy kliknij pozycję **SMTP** i wybierz opcję **Właściwości**.
3. Kliknij zakładkę **Ograniczenia przekazywania**.
4. Wybierz właściwe ograniczenia przekazywania spośród dostępnych opcji.

   Uwaga: Jeśli wybrana zostanie opcja **Akceptuj wiadomości przekazywane tylko dla odbiorców z listy bliskich domen** (Accept relay messages for only recipients in the near domains list) lub **Akceptuj wiadomości przekazywane na podstawie listy bliskich domen i adresów** (Accept relay messages using both the near

domains and address relay lists), należy kliknąć zakładkę **Ogólne** (General), aby wyświetlić listę bliskich domen, z których akceptowane są wiadomości przekazywane.

5. Kliknij przycisk **OK**.

Pojęcia pokrewne

"Kontrolowanie dostępu do poczty elektronicznej" na stronie 10
Aby ochronić dane przed groźnymi atakami, należy kontrolować, kto uzyskuje dostęp do systemu za pośrednictwem poczty elektronicznej.

Zadania pokrewne

"Uwierzytelnianie lokalnej i przekazywanej poczty elektronicznej" na stronie 25
Można ochronić serwer przed spamem, żądając uwierzytelnienia przy wysyłaniu poczty elektronicznej. Żądanie uwierzytelnienia nie może być wykorzystywane do ograniczenia przekazywania wiadomości. Zalecane jest skonfigurowanie uwierzytelnienia dla serwera.

Odsyłacze pokrewne

| zmiana atrybutów SMTP (Change SMTP Attributes - CHGSMTPA), komenda

Akceptowanie wiadomości przekazywanych od klientów POP

Jedna z opcji dla ograniczenia przekazywania umożliwia klientom POP (Post Office Protocol) przekazywanie informacji przez protokół SMTP (Simple Mail Transfer Protocol) przez określony czas po zalogowaniu się do serwera POP.

Funkcja ta nazywana jest zwykle POP przed SMTP. Jest to szczególnie użyteczne dla niestałych pracowników, którzy używają dynamicznych adresów IP, ponieważ funkcje kontroli bezpieczeństwa korzystające ze stałych adresów IP nie są efektywne dla kontroli adresów dynamicznych IP. Umożliwia to niestałemu pracownikowi dokonywanie uwierzytelniania do serwera POP i jednocześnie wysyłanie poczty przez określony czas (15 - 65535 minut) bez konieczności ponownego uwierzytelniania.

Na przykład możliwe jest skonfigurowanie systemu tak, aby użytkownicy zdalni mogli przekazywać wiadomości za pośrednictwem serwera SMTP przez okres czterech godzin (240 minut) po zalogowaniu się na serwerze POP. W tym przykładzie niestały pracownik loguje się do serwera POP, aby pobrać swoją pocztę elektroniczną. Serwer POP zapisuje adres IP użytkownika i datownik w kolejce. Godzinę później użytkownik wysyła wiadomość pocztową. Kiedy użytkownik wysyła wiadomość e-mail za pośrednictwem serwera SMTP, serwer ten sprawdza kolejkę w celu zweryfikowania, czy użytkownik uzyskał dostęp do serwera POP, aby odebrać pocztę w skonfigurowanym okresie. Po zweryfikowaniu użytkownika serwer SMTP przekazuje wiadomość pocztową do klienta SMTP dla odbiorcy poczty elektronicznej.

Uwaga: Dla pełniejszej kontroli użytkowników, którzy mogą mieć dostęp do serwera pocztowego, można równocześnie korzystać z funkcji ograniczenia przekazywania i z funkcji ograniczenia połączenia. Na przykład można dla określonej grupy użytkowników wprowadzić ograniczenie połączenia do serwera pocztowego, a jednocześnie pozwolić wybranym klientom POP z tej grupy korzystać z serwera SMTP do wysyłania wiadomości pocztowych.

Aby umożliwić klientom POP przekazywanie wiadomości przez określony czas, należy postępować zgodnie z poniższymi zasadami:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** → **Sieć** → **Serwery** → **TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Prawym przyciskiem myszy kliknij pozycję **SMTP** i wybierz opcję **Właściwości**.
3. Kliknij zakładkę **Ograniczenia przekazywania**.
4. Dla polecenia **Zezwól na przekazywanie poczty** wybierz opcję **Określone**.
5. Wybierz **Od klienta POP dla następującego przedziału czasu (15-65535)** (From the POP client for the following duration (15 - 65535)) i wpisz czas (w minutach), przez który klient będzie mógł wysyłać pocztę za pośrednictwem serwera SMTP.
6. Kliknij przycisk **OK**.

Równoczesne korzystanie z funkcji ograniczenia przekazywania i ograniczenia połączeń

System operacyjny i5/OS umożliwia równoczesne korzystanie z funkcji ograniczenia przekazywania i funkcji ograniczenia połączeń, aby dokładnie sterować dostępem do danego serwera pocztowego.

Dla określonej grupy użytkowników można wprowadzić ograniczenie połączenia do serwera pocztowego, a jednocześnie pozwolić wybranym klientom POP (Post Office Protocol) z tej grupy na korzystanie z serwera SMTP w celu wysyłania wiadomości pocztowych.

Na przykład wiadomo, że użytkownicy z określonego zakresu adresów IP rutynowo wysyłają wiadomości spam. Chcesz zatem ograniczyć adresom z tego zakresu połączenie do serwera poczty elektronicznej. Jednak klika adresów IP z tego zakresu reprezentuje zaufanych użytkowników systemu i5/OS i istnieje potrzeba umożliwienia użytkownikom z profilami użytkownika w systemie i5/OS przekazywanie wiadomości przez określony czas po zalogowaniu się do serwera POP.

Można więc skorzystać z funkcji ograniczenia połączeń, aby ograniczyć połączenia określonego zakresu adresów IP oraz zastosować funkcję ograniczenia przekazywania w celu umożliwienia zaufanym użytkownikom (klientom POP) z ograniczonego zakresu wysyłania poczty elektronicznej za pomocą serwera SMTP. System operacyjny i5/OS najpierw sprawdzi, czy system został skonfigurowany tak, aby umożliwić klientom POP przekazywanie wiadomości przez określony czas. Następnie sprawdza ograniczone połączenia. Ta możliwość systemu i5/OS pozwala na dokładne kontrolowanie wykorzystania serwera SMTP do przekazywania wiadomości oraz sprawdzanie, kto podłącza się do serwera poczty elektronicznej.

| Jeśli funkcja ograniczenia połączeń i funkcja ograniczenia przekazywania będą wykorzystywane równocześnie, dla
| komendy CL Zmiana atrybutów SMTP (Change SMTP Attributes - CHGSMTPA) należy wybrać
| OVRRJTNNL(*YES) (Override reject connect list - Pomiń listę odrzucanych połączeń). Parametr ten umożliwia
| funkcji uwierzytelniania serwera POP przesłonięcie konfiguracji ograniczenia połączeń. Później może zaistnieć
| potrzeba usunięcia ograniczenia przekazywania, co pozwoli klientom POP z ograniczonej grupy na korzystanie z
| serwera poczty elektronicznej. W takim przypadku należy dla komendy CHGSMTPA wybrać OVRRJTNNL(*NO).

Zadania pokrewne

"Ograniczanie połączeń"
W celu zabezpieczenia systemu należy zablokować połączenia użytkowników, którzy mogliby nieprawidłowo korzystać z serwera poczty.

Odsyłacze pokrewne

| zmiana atrybutów SMTP (Change SMTP Attributes - CHGSMTPA), komenda

Ograniczanie połączeń

W celu zabezpieczenia systemu należy zablokować połączenia użytkowników, którzy mogliby nieprawidłowo korzystać z serwera poczty.

Niepożądani użytkownicy mogliby połączyć się z systemem i rozsyłać niepożądaną pocztę. Niepożądana poczta zajmuje wiele cykli jednostki przetwarzania i znaczną ilość przestrzeni. Ponadto jeśli dany system umożliwia przekazywanie niepożądanej poczty, inne systemy mogą zablokować pocztę wychodzącą z danego systemu.

Można określić adresy IP znanych i niepożądanych użytkowników lub połączyć się z hostem zawierającym serwer list RBL (Realtime Blackhole List). Takie listy zawierają spis znanych adresów IP, z których wysyłana jest niepożądana poczta.

Aby podać znane adresy IP lub adres hosta z listą RBL, wykonaj następujące czynności:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** **→ Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Prawym przyciskiem myszy kliknij pozycję **SMTP** i wybierz opcję **Właściwości**.
3. Kliknij stronę Ograniczenia połączenia.

4. Kliknij **Dodaj**, aby dodać nazwy hostów zawierających listy RBL, z których chcesz korzystać.
5. Kliknij **Dodaj**, aby dodać określone adresy IP wykorzystywane podczas ograniczenia prób połączeń.
6. Kliknij przycisk **OK**.

Pojęcia pokrewne

"Kontrolowanie dostępu do poczty elektronicznej" na stronie 10
Aby ochronić dane przed groźnymi atakami, należy kontrolować, kto uzyskuje dostęp do systemu za pośrednictwem poczty elektronicznej.

Zadania pokrewne

"Równoczesne korzystanie z funkcji ograniczenia przekazywania i ograniczenia połączeń" na stronie 29
System operacyjny i5/OS umożliwia równoczesne korzystanie z funkcji ograniczenia przekazywania i funkcji ograniczenia połączeń, aby dokładnie sterować dostępem do danego serwera pocztowego.

Filtrowanie poczty elektronicznej w celu zapobiegania rozprzestrzenianiu się wirusów

Aby zapobiec rozprzestrzenianiu się wirusów, które mogą przeniknąć do serwerów poczty elektronicznej, można utworzyć filtry szukające w poczcie przychodzącej konkretnych tematów, typów MIME, nazw plików oraz adresów nadawców. Znalezione wiadomości e-mail mogą następnie zostać poddane kwarantannie lub usunięte.

Przy aktywnym filtrowaniu wirusów podejrzane wiadomości e-mail automatycznie poddawane są kwarantannie lub usuwane, zgodnie z parametrami ustawionymi przez administratora. Wiadomości mogą być filtrowane według dowolnego podzbioru poniższych kryteriów:

1. **Adres** - osoby lub domeny,
2. **Temat** - na przykład ILOVEYOU,
3. **Nazwa załącznika** - na przykład lovebug.vbs lub *.vbs,
4. **Typ MIME** - na przykład image/* lub image/jpg.

Podane wartości mogą zawierać znaki zastępcze. Jednym ze znaków zastępczych jest gwiazdka (*), oznaczająca wystąpienie jednego lub kilku dowolnych znaków. Na przykład, aby sprawdzać pliki z rozszerzeniem .vbs, należy wpisać *.vbs. Filtr nadawcy *@us.ibm.com filtruje całą pocztę od IBM w Stanach Zjednoczonych, a filtr image/* filtruje wszystkie podtypy obrazów.

W celu utworzenia filtra:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** → **Sieć** → **Serwery** → **TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Prawym przyciskiem myszy kliknij pozycję **SMTP** i wybierz opcję **Właściwości**.
3. Wybierz stronę Filtry.
4. Wybierz **Zachowaj wiadomość** lub **Usuń wiadomość**. Wybranie **Zachowaj wiadomość** spowoduje zapisanie kopii wiadomości nie dostarczonej do odbiorcy.
5. Kliknij **Dodaj**, aby określić kryterium rozpoznawania potencjalnego wirusa. Wiadomości spełniające to kryterium nie zostaną dostarczone do odbiorcy.
6. Kliknij **OK**, aby zapisać zmiany.

Oprócz narzędzi omówionych powyżej należy zastosować dodatkowe rozwiązania antywirusowe.

Wysyłanie i pobieranie poczty elektronicznej

System jest serwerem poczty elektronicznej i ma zarejestrowanych użytkowników poczty elektronicznej (SNADS, POP lub Lotus). Użytkownicy poczty elektronicznej mogą wysyłać, pobierać i odczytywać wiadomości e-mail za pomocą klienta POP lub SNADS.

Użytkownicy systemu mogą wykorzystywać funkcję API Wysyłanie poczty MIME (Send MIME Mail - QtmmSendMail) lub Tworzenie i wysyłanie poczty MIME (Create and Send MIME Email - QtmsCreateSendEmail) do wysyłania poczty elektronicznej z programu i5/OS. Za pomocą funkcji API QtmsCreateSendEmail użytkownicy mogą podpisywać i szyfrować dokument MIME w standardzie secure/MIME, który jest bezpieczną wersją protokołu MIME. Funkcja API QtmsCreateSendEmail jest preferowanym sposobem programowego wysyłania poczty elektronicznej.

Użytkownicy mogą ponadto wysyłać i pobierać pocztę elektroniczną na kilka różnych sposobów.

Pojęcia pokrewne

"Koncepcje poczty elektronicznej" na stronie 2
Poczta elektroniczna (wiadomości e-mail) stała się bardzo ważnym narzędziem w wielu firmach. System operacyjny i5/OS używa protokołów SMTP i POP, aby zapewnić płynną i efektywną obsługę poczty w sieci.

Zadania pokrewne

"Rejestrowanie użytkowników poczty elektronicznej" na stronie 19
Aby móc rejestrować użytkowników poczty elektronicznej, należy utworzyć profile użytkowników.

Odsyłacze pokrewne

tworzenie i wysyłanie poczty w standardzie MIME (Create and Send MIME E-mail - QtmsCreateSendEmail), funkcja API

wysyłanie poczty w standardzie MIME (Send MIME Mail - QtmmSendMail), funkcja API

Konfigurowanie klientów poczty POP

Jeśli poczta ma być pobierana i przechowywana za pomocą serwera POP, należy najpierw skonfigurować klienta poczty elektronicznej.

System wykorzystuje serwer POP do przechowywania i przesyłania poczty elektronicznej. Klient poczty elektronicznej współdziała z serwerem POP, odbierając pocztę użytkowników i przechowując ją po stronie klienta. Istnieje wiele klientów poczty współpracujących z serwerem POP, między innymi Eudora, Outlook Express i Lotus Notes. Czynności, jakie trzeba wykonać podczas konfigurowania programu typu klient, różnią się w zależności od jego interfejsu. Jednak informacje, jakich trzeba dostarczyć, są takie same. W przypadku programu Outlook Express, czynności te są następujące:

1. Zebranie informacji wymaganych przez program typu klient poczty elektronicznej POP.
   - ID użytkownika i pełna nazwa domeny (nazwa hosta plus nazwa domeny). Jest to adres poczty elektronicznej użytkownika służący do odbierania poczty, jego typowa postać to ID_użytkownika@nazwa_hosta.nazwa_domeny.

     Uwaga: W przypadku niektórych programów konieczne może być kilkakrotne podanie nazwy hosta, na przykład, aby określić hosta serwera POP do odbierania poczty, hosta serwera SMTP do wysyłania poczty oraz w celu umożliwienia odbiorcom identyfikacji nadawcy.
   - Nazwa użytkownika POP lub nazwa konta. Jest to ta sama nazwa co nazwa profilu użytkownika systemu i5/OS.
   - Hasło użytkownika. Hasło to musi być takie samo jak hasło profilu użytkownika systemu i5/OS.
2. Identyfikacja użytkownika i jego preferencji. Na przykład w programie Outlook Express należy kliknąć **Narzędzia → Konta** (Tools > Accounts), a następnie przejść na kartę **Poczta** (Mail) i podać informacje o użytkowniku i preferencje użytkownika.
   - Nazwa użytkownika. Jest to nazwa profilu użytkownika systemu i5/OS.
   - Adres poczty elektronicznej użytkownika. Składa się on z ID użytkownika i pełnej nazwy domeny.
   - Adres zwrotny. Może być to taki sam adres jak przydzielony przez administratora sieci adres poczty elektronicznej użytkownika, ale w systemie musi być zdefiniowany profil użytkownika systemu i5/OS.
3. Identyfikacja serwera poczty wychodzącej (SMTP). Identyfikacja serwera SMTP jest konieczna, gdyż jest on serwerem umożliwiającym użytkownikom programów typu klient wysyłanie poczty na zewnątrz. Na przykład w programie Outlook Express należy kliknąć **Narzędzia → Konta** (Tools > Accounts), wybrać konto pocztowe i kliknąć **Właściwości** (Properties). Następnie należy kliknąć zakładkę **Serwery** (Servers) i podać dane serwera SMTP.

- Nazwa użytkownika POP lub nazwa konta. Jest to identyfikator użytkownika związany z adresem poczty użytkownika; jest to również nazwa profilu użytkownika systemu i5/OS.
- Serwer poczty wychodzącej (SMTP). Jest to nazwa hosta systemu.

4. Identyfikacja serwera poczty przychodzącej (POP). Na przykład w programie Outlook Express należy kliknąć **Narzędzia → Konta** (Tools > Accounts), wybrać konto pocztowe i kliknąć **Właściwości** (Properties). Następnie należy kliknąć zakładkę **Serwery** (Servers) i podać dane serwera POP.
   - Serwer poczty przychodzącej. Jest to nazwa hosta systemu.
5. Skonfiguruj program kliencki do obsługi TLS/SSL. Na przykład w programie Outlook Express należy wykonać następujące czynności konfiguracyjne:
   a. Kliknij **Narzędzia → Konta** (Tools > Accounts) i wybierz konto pocztowe.
   b. Kliknij **Właściwości** (Properties), a następnie kliknij zakładkę **Serwery** (Servers).
   c. Wybierz **Serwer wymaga uwierzytelniania** (My server requires authentication) i kliknij **Ustawienia** (Settings).
   d. Wybierz **Użyj tych samych ustawień co mój serwer poczty przychodzącej** (User name settings as my incoming mail server) i kliknij **OK**.
   e. Kliknij zakładkę **Zaawansowane** (Advanced) i wybierz **Ten serwer wymaga bezpiecznego połączenia (SSL)** (This server requires a secure connection (SSL)) zarówno dla serwera poczty przychodzącej (POP), jak i dla serwera poczty wychodzącej (SMTP). Kliknij przycisk **OK**.
   f. Kliknij **Zastosuj** (Apply) a następnie **OK**, aby zamknąć okno Właściwości.

JavaMail

Aplikacje klienckie poczty elektronicznej można tworzyć za pomocą JavaMail.

Interfejs API JavaMail dostarcza strukturę, niezależną od platformy i protokołu, której użytkownik może użyć do tworzenia własnych aplikacji klienta poczty elektronicznej w oparciu o technologię Java. Interfejsu API JavaMail można użyć do stworzenia klienta poczty, który będzie obsługiwać wysyłanie multimedialnych wiadomości e-mail i umożliwi implementację protokołu IMAP (Internet Mail Access Protocol), w którym możliwa jest obsługa folderów, uwierzytelnianie i obsługa załączników.

Protokół SMTP obsługuje wyłącznie dane znakowe, dlatego używa standardu MIME do reprezentowania danych złożonych, takich jak tekst sformatowany, pliki załączników (tekstowe i binarne) oraz treści multimedialnych. Jeśli wykorzystywana jest funkcja API Send MIME Mail (QtmmSendMail), aplikacja musi dokonać konwersji danych na odpowiednią treść. Implementacja JavaMail udostępnia zintegrowane możliwości obsługi standardu MIME.

Komponenty JavaMail stanowią część pakietu IBM Developer Kit for Java.

Pojęcia pokrewne

JavaMail

Przesyłanie zbiorów buforowych jako plików PDF

Można przesyłać zbiory buforowe w formacie Adobe Portable Document Format (PDF) za pomocą poczty elektronicznej.

Za pomocą programu licencjonowanego IBM Infoprint Server for iSeries (5722-IP1) można generować pliki Adobe PDF z dowolnych danych wyjściowych systemu i5/OS. Pliki te można wysyłać jako załączniki wiadomości poczty elektronicznej. Można wysłać cały zbiór buforowy pod wskazany adres. Można także podzielić zbiór buforowy na kilka części, zapisanych w osobnych plikach PDF, i wysłać każdy z nich pod inny adres. Dzięki temu można na przykład zapisać faktury klientów w osobnych plikach PDF i wysłać je każdemu klientowi pocztą elektroniczną. Do zastosowania tej metody wymagany jest program licencjonowany IBM Infoprint Server for iSeries.

Informacje pokrewne


podręcznik użytkownika InfoPrint Server, plik PDF

IBM eServer iSeries Printing Redbooks VI -- The Output of e-business

Wykorzystanie Lightweight Directory Access Protocol (LDAP) w odniesieniu do adresów

Można wykorzystać protokół LDAP do udostępnienia publicznej książki adresowej opartej na katalogu dystrybucyjnym systemu.

Można zastosować rozwiązanie IBM Tivoli Directory Server for i5/OS (które jest implementacją LDAP firmy IBM) do zastąpienia funkcji poprzednio obsługiwanej przez MAPI. Za pomocą protokołu LDAP można utworzyć jedną książkę adresową, dostępną dla wszystkich użytkowników korzystających z aplikacji klienta poczty.

Aby zastosować protokół LDAP, wykonaj następujące czynności:

1. Uruchom serwer katalogów (Directory Server).
2. Przekaż informacje do serwera katalogów.
3. Skonfigurowanie klienta poczty, tak aby mógł korzystać z serwera LDAP. W tym przypadku czynności, które trzeba wykonać, zależą od klienta poczty (na przykład Netscape lub Eudora). Jako serwer katalogu adresów należy ustawić serwer LDAP.

Zadania pokrewne

pierwsze kroki z serwerem katalogów (Directory Server)

publikowanie informacji na serwer katalogów

Odsyłacze pokrewne

IBM Tivoli Directory Server for i5/OS (LDAP)

Wysyłanie poczty elektronicznej za pomocą usług dystrybucyjnych Systems Network Architecture Systems (SNADS)

Pocztę elektroniczną można wysyłać z systemu, korzystając z programu klienckiego usług SNADS. Nadawca poczty musi być lokalnym użytkownikiem usług dystrybucyjnych SNA.

Wymagania wstępne

Lokalny użytkownik SNADS musi dysponować profilem użytkownika, aby zarejestrować się w pozycji katalogu dystrybucyjnego systemu lokalnego. Informacje na temat rejestrowania lokalnych użytkowników poczty SNADS znajdują się w rozdziale Rejestrowanie użytkowników poczty elektronicznej.

Aby wysłać pocztę elektroniczną, wykonaj następujące czynności:

1. W interfejsie znakowym systemu i5/OS wpisz SNDDST (komenda Wysłanie dystrybucji - Send Distribution) i naciśnij Enter.
2. Naciśnij klawisz F10, aby zobaczyć wszystkie parametry.
3. Po pierwszej podpowiedzi *Informacja do wysłania* wpisz *LMSG i naciśnij klawisz Enter.
4. Wpisz ID użytkownika odbiorcy, adres serwera lub adres internetowy.
5. Wpisz opis wiadomości po znaku zachęty *Opis*.
6. Naciśnij klawisz Page Down i wpisz treść wiadomości po znaku zachęty *Długi komunikat*.
7. Naciśnij klawisz Enter, aby wysłać pocztę.

Uwaga: Wysyłając pocztę za pomocą komendy Wysłanie dystrybucji (Send Distribution - SNDDST) można użyć adresowania internetowego.

Zadania pokrewne

“Rejestrowanie użytkowników poczty elektronicznej” na stronie 19
Aby móc rejestrować użytkowników poczty elektronicznej, należy utworzyć profile użytkowników.

“Pobieranie poczty elektronicznej za pomocą usług dystrybucyjnych Systems Network Architecture (SNADS)” na stronie 36
Pocztę elektroniczną można odbierać na system, korzystając z programu klienckiego usług SNADS. Odbiorca poczty musi być lokalnym użytkownikiem usług dystrybucyjnych SNA.

Konfigurowanie nagłówków w celu rozróżniania odbiorców

Komenda Zmiana atrybutów dystrybucji (CHGDSTA - The Change Distribution Attributes) zmienia treść atrybutów usług dystrybucji (X.400 obsługa) dla dystrybucji poczty.

Parametr Zachowanie odbiorców (Keep Recipient - KEEPRCP) określa, które informacje o odbiorcy są przechowywane i wysyłane podczas dystrybucji poczty. Ustawienie tego parametru ma wpływ na to, jak tworzone są nagłówki MIME w treści wiadomości otrzymanej z komendy SNDDST.

Aby znaczniki CC i BCC znalazły się w nagłówku MIME (i na ekranie klienta), należy parametr KEEPRCP ustawić na *ALL. Odbiorcy umieszczeni w znaczniku BCC nie zostaną pokazani, niezależnie od ustawienia tego parametru, ponieważ nie mają być widoczni. Odbiorcy umieszczeni w znacznikach TO i CC są pokazywani w treści wiadomości SNDDST.

Typy zawartości Multipurpose Internet Mail Extension

Standardowe wiadomości internetowe składają się z ogólnego nagłówka i treści w postaci tekstu. Wiadomości w formacie MIME (Multipurpose Internet Mail Extension) mogą zawierać wiele części, co umożliwia włączanie załączników multimedialnych do tekstu.

Jeśli ogólny nagłówek zawiera typ zawartości Multipart/Mixed, wystąpi po nim jeden lub więcej załączników. Każdy załącznik ma granice początku i końca. Identyfikator granicy to parametr *boundary*=, po którym następuje znacznik nagłówka ″Content-Type″. Rysunek 1 przedstawia przykład wieloczęściowej wiadomości w formacie MIME. W przykładzie każda część ma zdefiniowany typ zawartości i każdy tekst może mieć zdefiniowany zestaw znaków.

```
    Od
@SYSNAM6.CITY.COMPANY.COM:popct08@SYSNAM6.city.company.com Wed
Jan 10
11:33:18 1996 Return-Path: <@SYSNAM6.CITY.COMPANY.COM:popct08@SYSNAM6.city.company.com> Received: from SYSNAM6.city.company.com by
fakeps2.city.company.com (COMPANY
         OS/2 SENDMAIL VERSION 1.3.2)/1.0) id AA0329; Wed, 10
Jan 96 11:33:18 -0500 Date: Wed, 10
Jan 96
11:33:18 -0500 Message-Id: <9601101633.AA0329@fakeps2.city.company.com> Received:
  from endmail9 by SYSNAM6.CITY.COMPANY. (IBM i5/OS SMTP V03R02M00) with TCP;
Wed, 10
Jan 1996 10:23:42
+0000. X-Sender: popct08@SYSNAM6.city.ibm.com (Unverified) X-Mailer: Windows
Eudora Pro
Version 2.1.2
Mime-Version:1.0Content-Type:multipart/mixed;boundary="====================_821301929==
_"
To: fake@fakeps2.city.company.com From:
endmail9 <popct08@SYSNAM6.city.company.com> Subject:
eudora attachments
X-Attachments:C:\EUDORA\ARGYLE.BMP;--====================_821301929==_
Content-Type: text/plain; charset=

 "us-ascii" Przykład wykorzystania klienta poczty Eudora do wysyłania tekstu
i obrazu.--====================_821301929==_
Content-Type: application/octet-stream; name="ARGYLE.BMP";
x-mac-type="424D5070"; x-mac-creator="4A565752"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=


"ARGYLE.BMP"
Qk12AgAAAAAAHYAAAAoAAAAIAAAACAAAAABAAQAAAAAAAACAAAAAAAAAAAAAAAAAAAQAAAAAAAA
AAAAgAAAgAAAAICAAIAAAACAAIAAgIAAAICAgADAwMAAAAD/AAD/AAAA//8A/wAAAP8A/wD//wAA
////AE1EREREREZEREREREE1E1EREREERERsZEREREETURE1EREREGxsZEREREERNRERE1ERE
REbGxsZEREREE1EREE1ERERsbGxsZERETUREREE1ERGxsbGxsZERNREREREE1EbGxsbGxsZE1E
RERERERE1sbGxsbGxsbUREREREREERG1sbGxsbGxtZEREREREREbG1sbGxsbG1sZEREREERERsbG1s
bGxsbWxsZEREREERGxsbG1sbGxtbGxsZEREREbGxsbG1sbG1sbGxsZEREREbGxsbG1sbWxsbGxsZE
RGxsbGxsbG1tbGxsbGxsZEbGxsbGxsbG1sbGxsbGxsZEbGxsbGxsbW1sbGxsbGxkREbGxsbGxtbG
1sbGxsbGREREbGxsbG1sbG1sbGxsZEREREbGxsbWxsbG1sbGxkREREREbGxtbGxsbG1sbGREREREE
REbG1sbGxsbG1sZEREREREREbWxsbGxsbG1kREREREERERNbGxsbGxsbG1EREREREE1EbGxsbGxs
ZE1EREREETUREbGxsbGxkRE1EREREERNREREbGxsbGREREE1EREREbGxsZEREREE1ERETURE
REREbGxkRERERE1ERNREREREREbGREREREE1E1EREREREREZEREREREE3UREREREREREREREREERE--====================_821301929==_--
```

Rysunek 2. Przykład wieloczęściowej wiadomości w formacie MIME

Obsługa adresowania internetowego dla komendy SNDDST

Można wysyłać pocztę elektroniczną do odbiorców internetowych za pomocą komendy SNDDST poprzez wpisanie adresu internetowego poczty elektronicznej w podpowiedzi *Adresat w Internecie* (Internet Recipient).

Jeśli sieć wykorzystuje usługi SNADS (SNA distribution services) i aplikację biurową do wysyłania i odbierania poczty elektronicznej, należy skonfigurować system pocztowy tak, aby użytkownicy mogli stosować adresy internetowe dla komendy Wysyłanie dystrybucji (Send Distribution - SNDDST).

W celu skonfigurowania systemu poczty wykonaj opisane poniżej czynności:

1. W interfejsie znakowym systemu i5/OS wpisz: ADDDIRE USRID(INTERNET GATEWAY) USRD('Allow SNDDST to send INTERNET Mail') SYSNAME(INTERNET) MSFSRVLVL(*USRIDX) PREFADR(NETUSRID *IBM ATCONTXT)
2. Wpisz CHGDSTA SMTPRTE(INTERNET GATEWAY) i naciśnij Enter.

Teraz użytkownicy usług SNADS będą mogli wysyłać pocztę elektroniczną do odbiorców internetowych za pomocą komendy SNDDST poprzez wpisanie adresu internetowego poczty elektronicznej w podpowiedzi *Adresat w Internecie* (Internet Recipient).

Informacje pokrewne

AS/400 Electronic-Mail Capabilities Redbook

Dołączanie plików

Podczas wysyłania poczty za pomocą komendy SNDDST można dołączyć do wiadomości e-mail zbiór lub dokument.

Można wysłać wiadomość e-mail z dołączonym zbiorem lub dokumentem za pomocą komendy Wysłanie dystrybucji (Send Distribution - SNDDST). Za pomocą tej komendy możliwe jest wysłanie tylko jednego zbioru lub dokumentu. Aby wysłać więcej załączników, należy użyć funkcji API Wysyłanie poczty MIME (Send MIME Mail - QtmmSendMail).

Aby do poczty elektronicznej dołączyć *dokument*, w znakowym wierszu komend należy wpisać:

```
SNDDST TYPE(*DOC) DSTD(opis) TOUSRID(dowolny_użytkownik) DOC(dokument) FLR(folder)
```

Aby do poczty elektronicznej dołączyć *zbiór*, w znakowym wierszu komend należy wpisać:

```
SNDDST TYPE(*FILE) DSTD(opis) TOUSRID(dowolny_użytkownik)
MSG(wiadomość) DOCFILE(biblioteka/zbiór) DOCMBR(podzbiór)
```

Otrzymanie komunikatu o błędzie może oznaczać próbę wysłania zbioru lub dokumentu niezgodnego z komendą Wysłanie dystrybucji (Send Distribution - SNDDST). Można użyć komend CL CPY systemu i5/OS w celu przekształcenia zbioru w zbiór zgodny z komendą SNDDST.

Przekształcanie typów zbiorów do wysłania za pomocą komendy SNDDST

Jeżeli zbiór buforowy został już utworzony i istnieją już zbiór fizyczny oraz folder, należy przekształcić zbiór do formatu właściwego do wysłania.

1. Przeniesienie zbioru buforowego do zbioru fizycznego bazy danych:

   ```
   CPYSPLF   FILE(zbiór_buforowy)  TOFILE(zbiór_bazy_danych)  JOB(zadanie3/zadanie2/zadanie1)
   SPLNBR(numer_zbioru_buforowego) TOMBR(podzbiór)
   ```

2. Przeniesienie fizycznego zbioru bazy danych do folderu:

   ```
   CPYTOPCD   FROMFILE(biblioteka/zbiór_bazy_danych)  TOFLR(folder) FROMMBR(podzbiór)  REPLACE(*YES)
   ```

3. Wysłanie dokumentu:

   ```
   SNDDST   TYPE(*DOC)  TOUSRID(adres_użytkownika) DSTD(MAIL) DOC(podzbiór)  FLR(folder)
   ```

   Odsyłacze pokrewne

   wysyłanie poczty w standardzie MIME (Send MIME Mail - QtmmSendMail), funkcja API

Pobieranie poczty elektronicznej za pomocą usług dystrybucyjnych Systems Network Architecture (SNADS)

Pocztę elektroniczną można odbierać na system, korzystając z programu klienckiego usług SNADS. Odbiorca poczty musi być lokalnym użytkownikiem usług dystrybucyjnych SNA.

Acby pobrać pocztę, wykonaj następujące czynności.

1. W wierszu komend wpisz komendę QRYDST (Query Distribution - Zapytanie o dystrybucję) i naciśnij klawisz F4. Pojawi się lista dystrybucji.
2. Naciśnij F10, aby zobaczyć dodatkowe parametry.
3. W polu **Zbiór wyjściowy do zapisania** wpisz łatwe do zapamiętania nazwy zbioru i biblioteki i naciśnij klawisz Enter. System utworzy zbiory fizyczne.
4. Wpisz komendę WRKF (Work with Files - Praca ze zbiorami) i naciśnij klawisz Enter. Pojawi się ekran Praca ze zbiorami (Work with Files - WRKF).
5. Wpisz nazwę zbioru i biblioteki podaną w punkcie 3 i naciśnij klawisz F4.
6. Na ekranie zostaną wyświetlone wszystkie dystrybucje (poczta elektroniczna). Wpisz 5 obok dystrybucji, która ma być wyświetlona i naciśnij klawisz Enter.
7. Gdy pojawi się ekran Wyświetlenie zbioru fizycznego (Display Physical File Member - DSPPFM), naciśnij klawisz Enter.

8. Na następnym ekranie pojawi się długi ciąg liczb dla każdej wiadomości. Skopiuj znaki od siódmego do dwudziestego szóstego.
9. Aby wyjść, naciśnij dwukrotnie klawisz F3.
10. Wpisz komendę RCVDST (Receive Distribution - Pobranie dystrybucji) i naciśnij klawisz Enter.
11. W polu **Identyfikator dystrybucji** wklej skopiowane znaki od siódmego do dwudziestego szóstego.
12. W polu **Zbiór wyjściowy do zapisania** wpisz nazwę zbioru i nazwę biblioteki podaną uprzednio i naciśnij klawisz Enter.
13. Wpisz komendę DSPPFM (Wyświetlenie zbioru fizycznego - Display Physical File Member), aby wyświetlić utworzony zbiór.
14. Naciśnij klawisz F20 (Shift + F8), aby przewinąć ekran w lewo i przeczytać wiadomość lub wiadomości.

Zadania pokrewne

"Wysyłanie poczty elektronicznej za pomocą usług dystrybucyjnych Systems Network Architecture Systems (SNADS)" na stronie 33
Pocztę elektroniczną można wysyłać z systemu, korzystając z programu klienckiego usług SNADS. Nadawca poczty musi być lokalnym użytkownikiem usług dystrybucyjnych SNA.

Zarządzanie pocztą elektroniczną

Doświadczony użytkownik lub administrator może zarządzać serwerami poczty elektronicznej, użytkownikami oraz komunikatami w celu zapewnienia odpowiedniej dystrybucji poczty w sieci.

Sprawdzanie serwerów poczty elektronicznej

Jednym z powszechnych problemów z pocztą jest to, że odpowiednie serwery nie zostały uruchomione. Przed przystąpieniem do używania serwerów poczty elektronicznej należy sprawdzić status serwerów i sprawdzić, czy wszystkie są uruchomione.

Aby sprawdzić status serwerów, wykonaj następujące czynności:

1. Uruchom program System i Navigator i rozwiń pozycję ***system* → Zarządzanie pracą → Zadania serwera** (*system* > Work Management > Server Jobs).
2. Upewnij się, że serwer SMTP jest aktywny. Na liście Aktywne zadania serwera w kolumnie Nazwa zadania znajdź wartości **Qtsmtp**.
3. Jeśli na liście nie ma zadań **Qtsmtp**, uruchom serwery SMTP.
4. Upewnij się, że serwer Mail Server Framework jest aktywny. Znajdź zadania **Qmsf** w kolumnie Nazwa zadania na liście Aktywne zadania serwera.
5. Jeśli na liście nie ma zadań Qmsf, w wierszu komend wpisz komendę STRMSF (Start the Mail Server Framework - Uruchomienie struktury serwera poczty).
6. Upewnij się, że serwer POP jest aktywny. Znajdź zadania **Qtpop** w kolumnie Nazwa zadania na liście Aktywne zadania serwera.
7. Jeśli na liście nie ma zadań **Qtpop**, uruchom serwery POP.
8. Upewnij się, że serwer SNADS jest aktywny. Znajdź zadania **Qsnads** w kolumnie Nazwa zadania na liście Aktywne zadania serwera.
9. Jeśli nie zostaną wyświetlone żadne zadania QSNADS, uruchom usługi dystrybucyjne SNA. W wierszu komend wpisz komendę STRSBS QSNADS.

Aby poczta elektroniczna działała, muszą być włączone wszystkie serwery pocztowe.

Pojęcia pokrewne

"Uruchamianie i zatrzymywanie serwerów poczty elektronicznej" na stronie 20
Uruchom wymagane serwery, aby sprawdzić, czy wszystko działa poprawnie i czy wszystkie dokonane przez ciebie zmiany konfiguracji zostały zastosowane. Czasami może być konieczne wykonanie restartu serwerów. Wykonuje się to zatrzymując serwery, a następnie wykonując kolejno czynności ponownego uruchamiania serwerów.

“Wykrywanie problemów z pocztą elektroniczną” na stronie 49
Wykonanie prostych czynności może być pomocne w określeniu przyczyny problemu z pocztą elektroniczną.

Usuwanie użytkowników poczty POP

Możliwe jest usuwanie użytkowników poczty POP za pomocą programu System i Navigator.

Aby usunąć użytkownika poczty z systemu operacyjnego, należy usunąć pozycję katalogu dystrybucyjnego systemu, wykonując następujące czynności:

1. W wierszu komend wpisz komendę WRKDIRE (Work with Directory Entries - Praca z pozycjami katalogów).
2. Przewiń ekran klawiszem Tab w dół, aż do pola *Opc* obok użytkownika, który ma zostać usunięty.
3. Wpisz 4 (Usuń) i naciśnij klawisz Enter. Naciśnij ponownie klawisz Enter, aby potwierdzić usunięcie. Odtąd poczta nie będzie już dostarczana do skrzynki pocztowej POP użytkownika.
4. Wpisz się do programu pocztowego POP jako ten użytkownik. Odbierz i usuń wszelką pocztę.

Zapobieganie dzieleniu dużych wiadomości e-mail

Może wystąpić potrzeba uniemożliwienia podziału dużych wiadomości oraz dostarczania ich w małych, niewygodnych plikach.

Serwer SMTP (Simple Mail Transfer Protocol) może zostać tak skonfigurowany, aby duże wiadomości były dzielone na części. Jednak wielu klientów poczty nie radzi sobie ze składaniem podzielonych wiadomości, przez co stają się one nieczytelne. Jeśli odbiorca poczty ma problem ze składaniem wiadomości, można wyłączyć funkcję dzielenia wiadomości przez serwer SMTP.

W celu wyłączenia podziału poczty przez serwer SMTP:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** → **Sieć** → **Serwery** → **TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Kliknij dwukrotnie **POP**. Pojawi się okno dialogowe Właściwości POP.
3. Kliknij zakładkę **Konfiguracja**.
4. W polu **Wielkość podziału wiadomości** wybierz **Bez maksimum**.

Uwaga: Wyłączenie dzielenia wiadomości pocztowych może spowodować problemy w przypadku wysyłania dużych wiadomości do sieci, które nie potrafią obsługiwać dużych wiadomości.

Pojęcia pokrewne

“Rozwiązywanie problemów dotyczących poczty elektronicznej” na stronie 49
Poniższe informacje są pomocne w rozwiązywaniu problemów dotyczących poczty elektronicznej, z którymi użytkownik może mieć do czynienia.

Pobieranie statusu dostarczenia poczty elektronicznej

Jeśli użytkownicy chcieliby otrzymywać komunikaty o statusie dostarczenia swojej poczty wychodzącej, należy włączyć funkcję powiadomienia o statusie dostarczenia.

Powiadomienie o statusie dostarczenia umożliwia klientom poczty elektronicznej otrzymywanie komunikatów o statusie w przypadku dostarczenia, przekazania lub nieudanego przesłania wiadomości e-mail. Jeśli klienci poczty elektronicznej mają mieć prawo do zgłaszania tego żądania, należy włączyć powiadomienia o statusie dostarczenia.

Funkcja powiadamiania o statusie dostarczenia zostanie włączona tylko dla użytkowników systemu. Jeśli użytkownicy chcą używać funkcji powiadamiania o statusie dostarczenia poczty, muszą ustawić odpowiednie parametry w swoich lokalnych klientach pocztowych. Parametry takie są różne dla różnych klientów pocztowych.

Aby włączyć powiadomienia o statusie dostarczenia poczty, wykonaj następujące czynności:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** → **Sieć** → **Serwery** → **TCP/IP** (*system* > Network > Servers > TCP/IP).

2. Prawym przyciskiem myszy kliknij pozycję **SMTP** i wybierz opcję **Właściwości**.
3. Kliknij stronę Parametry dodatkowe.
4. Zaznacz pole wyboru **Obsługa powiadamiania o statusie dostarczenia (DSN)** i wprowadź Powiadomienie DSN o adresie osoby odpowiedzialnej (Responsible person).
5. Kliknij przycisk **OK**.

Korzystanie z funkcji powiadamiania o statusie dostarczenia poczty wymaga pewnych zasobów, co może mieć wpływ na maksymalną liczbę odbiorców wiadomości e-mail.

Udostępnianie serwera Domino i serwera SMTP w tym samym systemie

Jeśli w tym samym systemie używane są jednocześnie serwer Domino i serwer SMTP, zaleca się skonfigurowanie każdego z nich w taki sposób, aby przypisane im były konkretne określone adresy IP.

Jeśli jednocześnie używane są w tym samym systemie serwery Domino i SMTP, należy powiązać każdy serwer z adresem IP. Poczta elektroniczna będzie wtedy wysyłana do użytkowników serwera Domino lub SMTP za pomocą odpowiedniego adresu IP i, pomimo że używany jest wspólny port, poczta elektroniczna będzie obsługiwana tylko przez ten system, dla którego jest przeznaczona.

Aby zmusić serwer SMTP do używania konkretnego adresu internetowego, wykonaj następujące czynności:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** → **Sieć** → **Serwery** → **TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Prawym przyciskiem myszy kliknij pozycję **SMTP** i wybierz opcję **Właściwości**.
3. Kliknij zakładkę **Powiązania**.
4. Kliknij przełącznik **Używaj wszystkich interfejsów** (Use all interfaces), aby przypisać wszystkie interfejsy do portu 25.
5. Kliknij przełącznik **Wybierz interfejs** (Select an interface), aby przypisać klientowi i serwerowi wybrane interfejsy.

   Uwaga: Jeśli w systemie lub zaporze firewall ma być używana translacja NAT, należy wymusić na kliencie SMTP systemu i5/OS stosowanie określonego adresu internetowego.
6. Kliknij przycisk **OK**.

Teraz serwer SMTP będzie pobierać jedynie pocztę skierowaną na określony adres internetowy. Należy upewnić się, czy wybrany adres internetowy występuje w serwerze nazw domen (DNS), lokalnej tabeli hostów oraz katalogu dystrybucyjnym systemu.

Biblioteka odniesienia Lotus Domino zawiera instrukcje na temat przypisania serwerowi SMTP Domino określonego adresu TCP/IP.

Pojęcia pokrewne

“Planowanie korzystania z poczty elektronicznej” na stronie 10
Przed skonfigurowaniem poczty elektronicznej należy przygotować podstawowy plan korzystania z niej w systemie.

filtrowanie IP i translacja adresów sieciowych (NAT - Network Address Translation)

Wykorzystanie Domino LDAP oraz Directory Server w tym samym systemie

Jeśli używasz Domino LDAP oraz IBM Tivoli Directory Server for i5/OS (serwer katalogów) w tym samym systemie, sugerowane jest skonfigurowanie każdego z nich tak, by miał przypisany konkretny adres IP.

Jeśli Domino LDAP oraz Directory Server wykorzystywane są w tym samym systemie, można ustawić różne numery portów dla każdego serwera lub przypisać każdemu serwerowi adres IP. Zmiana numeru portu może być niewygodna

dla klientów, lepszym rozwiązaniem może się okazać przypisanie adresów IP. Domino i protokół SMTP używają odpowiednich serwerów LDAP do adresowania poczty elektronicznej.

Aby wymusić na serwerze katalogów wykorzystywanie konkretnych adresów internetowych, wykonaj następujące czynności:

1. W programie System i Navigator wybierz pozycję ***system*** → **Sieć** → **Serwery** → **TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Prawym przyciskiem myszy kliknij pozycję **Katalog** i wybierz opcję **Właściwości**.
3. Kliknij zakładkę **Sieć**.
4. Kliknij **Adresy IP**.
5. Zaznacz pole **Użyj wybranych adresów IP** i wybierz z listy interfejsy, którym mają być przypisane adresy.
6. Kliknij **OK**, aby zamknąć stronę Katalog - adresy IP.
7. Kliknij **OK**, aby zamknąć stronę Właściwości katalogu.
8. Opcjonalne: Jeśli używasz Domino LDAP, w bibliotece odniesienia Lotus Domino znajdziesz instrukcje na temat przypisywania Domino LDAP do konkretnego adresu TCP/IP.
9. Uruchom serwery poczty elektronicznej.

Informacje pokrewne

Lotus Domino Reference Library

Zarządzanie wydajnością serwera SMTP

Wskazówki do zarządzania serwerem SMTP (Simple Mail Transfer Protocol) używającym wielowątkowości.

Serwer SMTP może być zajęty, ponieważ zużywa całą swoją moc na dodawanie i kończenie zadań prestartu dla każdego żądania poczty elektronicznej.

Jeśli liczba zadań prestartu wpływa na wydajność systemu, możliwe jest ustawienie progu na niższym poziomie. Kiedy natomiast zaistnieje potrzeba wykonywania większej liczby zadań, można zwiększyć liczbę zadań prestartu.

Dzięki zadaniom prestartu, każde żądanie poczty elektronicznej jest uruchamiane jako odrębne zadanie. Metoda ta umożliwia każdemu zadaniu skupienie się wyłącznie na potrzebach i żądaniach swojego programu typu klient lub serwer. Aby zapobiec zalewowi niepożądanej poczty elektronicznej, każde zadanie może mieć dłuższy limit czasu oczekiwania na wywołanie.

Aby odciążyć serwer SMTP, można zmienić następujące wartości:

- Liczba zadań uruchamianych podczas inicjowania
- Wartość progowa dla zadań
- Liczba zadań dodawanych po osiągnięciu przez system wartości progowej
- Dozwolone maksimum uruchomionych zadań
- Wybór podsystemu dla zadań

Aby zarządzać systemem obciążonym zadaniami, należy zmienić wartości parametrów dla serwera i klienta SMTP.

Serwer SMTP działa z zadaniem typu demon i zadaniem prestartu: QTSMTPSRVD i QTMSMTPSRVP. Klient SMTP działa z zadaniem typu demon i zadaniem prestartu: QTSMTPCLTD i QTSMTPCLTP.

Aby zmienić wartości dla serwera SMTP, wykonaj następujące czynności:

1. W interfejsie znakowym wpisz komendę Zmiana pozycji zadania (Change Job Entries - CHGPJE).
2. Wpisz następujące wartości przy stosownych podpowiedziach i naciśnij Enter.

Podpowiedź	Wartość
Podsystem	QSYSWRK
Biblioteka	QSYS
Program	QTMSSRCP
Biblioteka	QTCP
Uruchamianie zadań	*SAME
Początkowa liczba zadań	4
Próg	2
Dodatkowa liczba zadań	2
Maksymalna liczba zadań	20

Wartości te gwarantują uruchomienie przez system czterech zadań prestartu, uruchomienie dwóch dodatkowych zadań kiedy ilość dostępnych zadań spadnie poniżej dwóch, oraz umożliwienie wykonywania maksymalnie 20 zadań prestartu.

Zmiana wartości dla serwera SMTP

Wykonaj tę procedurę, aby zmienić wartości dla serwera SMTP.

1. W interfejsie znakowym wpisz komendę Zmiana pozycji zadania (Change Job Entries - CHGPJE).
2. Wpisz następujące wartości przy stosownych podpowiedziach i naciśnij Enter.

Podpowiedź	Wartość
Podsystem	QSYSWRK
Biblioteka	QSYS
Program	QTMSSRCP
Biblioteka	QTCP
Uruchamianie zadań	*SAME
Początkowa liczba zadań	4
Próg	2
Dodatkowa liczba zadań	2
Maksymalna liczba zadań	20

Wartości te gwarantują uruchomienie przez system czterech zadań prestartu, uruchomienie dwóch dodatkowych zadań kiedy ilość dostępnych zadań spadnie poniżej dwóch, oraz umożliwienie wykonywania maksymalnie 20 zadań prestartu.

Zmiana wartości dla klienta SMTP

Wykonaj tę procedurę, aby zmienić wartości dla klienta SMTP.

1. W interfejsie znakowym wpisz komendę CHGPIE (Change Job Entries - Zmiana zapisu zadania).
2. Wpisz poniższe wartości i naciśnij klawisz Enter.

Podpowiedź	Wartość
Podsystem	QSYSWRK
Biblioteka	QSYS
Program	QTMSCLCP
Biblioteka	QTCP
Uruchamianie zadań	*SAME

Podpowiedź	Wartość
Początkowa liczba zadań	4
Próg	2
Dodatkowa liczba zadań	2
Maksymalna liczba zadań	20

Wartości te gwarantują uruchomienie przez klienta SMTP czterech zadań prestartu, uruchomienie dwóch dodatkowych zadań kiedy ilość dostępnych zadań spadnie poniżej dwóch, oraz umożliwienie wykonywania maksymalnie 20 zadań prestartu.

Wybór nowego podsystemu dla zadań serwera SMTP

Aby wybrać nowy podsystem dla zadań serwera SMTP, zastosuj następującą procedurę.

1. Można określić odrębny podsystem dla serwera SMTP. Powinno to zwiększyć wydajność przez wyeliminowanie współużytkowania zasobów.
2. Aby określić osobny podsystem, wykonaj następujące czynności:
   a. Uruchom program System i Navigator i rozwiń pozycję ***system*** → **Sieć** → **Serwery** → **TCP/IP** (*system* > Network > Servers > TCP/IP).
   b. Prawym przyciskiem myszy kliknij pozycję **SMTP** i wybierz opcję **Właściwości**.
   c. Kliknij zakładkę **Parametry dodatkowe**.
   d. Wybierz przełącznik **Opis podsystemu**.
   e. Wprowadź nazwę nowego podsystemu i bibliotekę, w której zostanie utworzony opis podsystemu i kolejka zadań.

Program sprawdzi istnienie określonego podsystemu. Jeśli stwierdzi, że podsystem nie istnieje, utworzy go wraz z pozycjami tablicy routingu, pozycjami zadań autostartu, pozycjami zadań prestartu i opisami zadań. Nawet jeśli podsystem jeszcze nie istnieje, muszą istnieć: biblioteka dla opisu podsystemu i kolejka zadań. Podczas wykonywania zadań startowych serwera zostaną określone parametry dla nowo utworzonego podsystemu, a następnie wysłane zostaną zadania serwera dla startowych zadań wsadowych w podsystemie.

Informacje dotyczące poczty elektronicznej

Dostępne są informacje uzupełniające na temat pozycji kroniki serwera poczty, komend SMTP oraz rozkazów i parametrów protokołu POP.

Pozycje kroniki serwera poczty

Poniższe informacje ułatwiają zrozumienie kodów i komunikatów używanych w pozycjach kroniki.

Poniższe tabele zawierają bardziej szczegółowe informacje na temat odczytywania pozycji kroniki.

- “Skróty zapisów kroniki”
- “Pozycje protokołu dla klienta protokołu SMTP” na stronie 43
- “Pozycje protokołu dla serwera protokołu SMTP” na stronie 44
- “Pozycje kroniki dla serwera mostu” na stronie 45
- “Wyjścia i tworzenie funkcji struktury MSF” na stronie 46

Skróty zapisów kroniki

Skrót	Definicja
LIN	Local in, otrzymano informację dla poczty lokalnej. Adresem IP jest host, który wysłał uwagę.

Skrót	Definicja
RIN	Relay in, otrzymano informację dotyczącą przekazu do innego demona SMTP. Adres IP, z którego wysłano uwagę.
R	Odbiorca
O	Nadawca
U	Odbiorca, któremu nie dostarczono poczty elektronicznej
QTMSINQ	Kolejka wejściowa protokołu SMTP
QTMSOUTQ	Kolejka wyjściowa protokołu SMTP
QTMSBSSQ	Kolejka wstrzymań, w której umieszczone zostają wiadomości, kiedy przekroczony zostaje próg pamięci systemu.
QTMSRTQ1	Kolejka ponownych przetworzeń pierwszego poziomu
QTMSRTQ2	Kolejka ponownych przetworzeń drugiego poziomu
RRSL	Odbiorca znaleziony

Każda pozycja kroniki poprzedzona jest dwuznakowym oznaczeniem podtypu lub kodu. Pierwszy znak podtypu lub kodu zawiera identyfikator funkcji dla danej pozycji. Drugi znak podtypu lub kodu określa działanie, które dokumentuje dana pozycja kroniki. Identyfikatory funkcji opisuje poniższa tabela:

Identyfikator funkcji	Opis
7	Pozycja serwer Bridge
8	Klient SMTP
9	Serwer SMTP
A	MSF - nie dostarczono poczty
B	MSF - poczta lokalna
C	MSF - przekazanie poczty
D	Utworzenie wiadomości POP
E	Funkcje API Send Mail
F	Domino MTA
G	Tunelowany program snap-in
H	Usługi SNADS (program przełączający)
I	Analizator składni MIME (program snap-in dla poczty lokalnej)
L	FAX (Poczta lokalna)
M	Usługi SNADS
O	Filtrowanie
P	Program translacji adresów SMTP w strukturze MSF

Wszystkie udokumentowane tu pozycje kroniki są typu LG (log entry - pozycja protokołu).

Pozycje protokołu dla klienta protokołu SMTP

Typ	Działanie	Podtypy lub kody	Komentarze
LG	Usuwanie z kolejki pojemnika w celu przetwarzania	8B	Zapisywanie usunięcia poczty z kolejki po ustawieniu znacznika.

Typ	Działanie	Podtypy lub kody	Komentarze
LG	Dostarczenie poczty powiodło się	88 82	Wysłanie protokołu poczty powiodło się. Protokołowanie każdego odbiorcy.
LG	Poczta niedoręczona	83	Protokołowanie niedoręczonej poczty.
LG	Przekroczenie limitu czasu pierwszego poziomu	8C	Protokołowanie faktu dodania do kolejki powtórzenia pierwszego poziomu.
LG	Przekroczenie limitu czasu drugiego poziomu	8D	Protokołowanie faktu dodania do kolejki powtórzenia drugiego poziomu.
LG	Poczta jest gotowa do ponownego przesłania	8E 8F	Protokołowanie powrotu ponownie wysłanej poczty do QTMSOUTQ.
LG	COD wysyłany zwrotnie do nadawcy	87	Protokołowanie umieszczenia potwierdzenia dostarczenia (cofirm on delivery - COD) w kolejce BRSR.
LG	Nie można wykonać przetwarzania, zasoby są zajęte	86	Protokołowanie zwrócenia poczty do kolejki QTMSOUTQ ze względu na przepełnienie macierzy połączeń.
LG	Sprawdzanie rekordów odbiorców	86	Protokołowanie zwrócenia poczty do kolejki QTMSOUTQ ze względu na zmianę statusu odbiorcy, tj. w sytuacji, kiedy rekord MS wskazuje gotowość do dostarczenia wiadomości.
LG	Niedoręczono	87	Protokołowanie przekazania poczty do kolejki QTMSINQ dla niedoręczonej noty na dwóch pozycjach.
LG	Zapytanie MX	8K	Protokołowanie pozycji res_send failure (nieudane wysłanie zasobu) oraz errno (numer błędu) przyczyny niepowodzenia, razem z buforem zapytań.

Pozycje protokołu dla serwera protokołu SMTP

Typ	Działanie	Podtypy lub kody	Komentarze
LG	Odebrano pocztę	94 91 92 9T 99	Protokołowanie odbioru poczty bezpośrednio po otrzymaniu sekwencji zakończenia CRLF <.> CRLF (lokalne). Nadawca i odbiorca są protokołowani. Wielkość wiadomości *nnnnn*, gdzie *nnnnn* oznacza liczbę bajtów. MSGID

Typ	Działanie	Podtypy lub kody	Komentarze
LG	Pobieranie przekazanej poczty	95 91 92	Protokołowanie pozycji MAIL (poczta) bezpośrednio po otrzymaniu sekwencji zakończenia CRLF <.> CRLF (przekazana). Nadawca i odbiorca są protokołowani.
LG	Przekazanie poczty do serwera Bridge	97	Protokołowanie wstawienia poczty do kolejki QTMSINQ (poczta przychodząca).
LG	Przekazanie poczty do klienta do zdalnego dostarczenia	96	Protokołowanie wstawienia poczty do kolejki QTMSOUTQ (poczta przekazana).
LG	ODRZUCONE POŁĄCZENIE 1.2.3.4....	9S	Połączenia odrzucone na podstawie ustawień ograniczenia połączeń. 1.2.3.4 to odrzucony adres IP.
LG	ODRZUCONE PRZEKAZANIE 1.2.3.4....	9V	Przekazanie wiadomości odrzucone na podstawie ustawień ograniczenia przekazywania. 1.2.3.4 to odrzucony adres IP.
LG	Odrzucone przez serwer SMTP	9W	Wiadomość została odrzucona przez serwer SMTP.

Pozycje kroniki dla serwera mostu

Typ	Działanie	Podtypy lub kody	Komentarze
LG	Pobieranie poczty z kolejki IN	7A	Protokołowanie usunięcia poczty z kolejki QTMSINQ.
LG	Przekazanie poczty do usług SNADS	7O	Zapisanie udanego przekazania do QSNADS.
LG	Wstawienie kontenera do kolejki BUSY ze względu na wykorzystanie przestrzeni	7L	Zapisanie wstawienia poczty do kolejki QTMSBSSQ z powodu przekroczenia progu.
LG	Pobranie poczty z kolejki BUSY	7M	Zapisanie usunięcia poczty z kolejki QTMSBSSQ. Przestrzeń została odzyskana i poczta może zostać przetworzona.
LG	Przekazywanie wiadomości do MSF	7H 71 72	Zapisanie wstawienia wiadomości do struktury MSF.
LG	Utworzenie wiadomości COD	7R 7G	Zapisanie wstawienia wiadomości COD do struktury MSF. Zapisanie identyfikatora wiadomości MSF (MSF MSGID) ze względu na utworzenie nowej wiadomości COD.

Typ	Działanie	Podtypy lub kody	Komentarze
LG	Nie można dostarczyć danej części wiadomości e-mail do odbiorcy	7P 7G	Zapisanie faktu tworzenia noty, która nie mogła zostać dostarczona. Zapisanie identyfikatora wiadomości (MSGID) nowej niedostarczonej noty wiadomości.

Wyjścia i tworzenie funkcji struktury MSF

Typ	Działanie	Podtypy lub kody	Komentarze
LG	Utworzenie wiadomości, której nie można dostarczyć	AP A1 A2	Zapisanie wstawienia niedostarczonej wiadomości do struktury MSF.
LG	Poczta została dostarczona do skrzynki pocztowej POP	B8 B2	Zapisanie dostarczenia wiadomości do lokalnej skrzynki pocztowej POP. Katalogiem skrzynki pocztowej POP jest ipaddress (adres IP). Wskazany jest także odbiorca.
LG	Wysłanie wiadomości COD do struktury MSF	BR B1 B2	Zapisanie wstawienia wiadomości COD do struktury MSF.
LG	Sprawdzanie dostępności	CN	Przekazanie wiadomości SMTP - program obsługi wyjścia MSF. Zapisanie identyfikatora wiadomości (MSGID), która została zwrócona do kolejki QMSF z powodu nie uruchomienia serwera SMTP.
LG	Wstawianie poczty do kolejki	C6 C1 C2	Protokołowanie wstawienia poczty do kolejki QTMSOUTQ.
LG	Użycie funkcji API Sendmail	EH E1 E2 ET	Zapisanie faktu utworzenia wiadomości przez funkcję API SendMail. Wielkość wiadomości *nnnnn*, gdzie *nnnnn* jest wielkością wiadomości (wszystkie załączniki).
LG	Poczta jest skierowana do zdalnego systemu dostępnego za pośrednictwem usług SNADS	G8 G2	Zapisywany jest fakt tunelowania wiadomości. Uwzględniony jest system przekazany do odbiorcy.
LG	Odebranie poczty tunelowanej za pośrednictwem usług SNADS	GQ G2	Zapisanie odebrania poczty tunelowanej dla odbiorcy lokalnego dostarczenia.
LG	Przełączenie translacji adresów w usługach SNADS	H1	Usługi SNADS przełączyły wiadomość do struktury MSF.

Typ	Działanie	Podtypy lub kody	Komentarze
LG	Ponowne wstawienie przeanalizowanej wiadomości MIME do struktury MSF	IH I1 I2 IG	Zapisywane jest wstawienie przeanalizowanej wiadomości MIME do struktury MSF.
LG	Odrzucenie przez filtr	OW	Wiadomość została odrzucona. Zapisuje się, czy została usunięta, czy zachowana. Jeśli została zmodyfikowana i dostarczona, zostanie to odnotowane.
LG	Wiadomość oznaczona przez program tłumaczenia adresów SMTP	P2	Wiadomość została oznaczona w następujący sposób: • **POP LclDel:** wiadomość zostanie dostarczona lokalnie przez serwer POP. • **SMTP MsgFwd:** wiadomość zostanie przekazana do serwera SMTP. • **SMTP NonDel:** w razie niedostarczenia wiadomości nastąpi powiadomienie. • **Parse:** wiadomość wysłana do analizatora składni. • **PutBk:** wiadomość wstawiona ponownie do struktury MSF, obsługiwana przez inny program obsługi wyjścia (na przykład Domino lub SNADS). • **chg to SNADS:** typ adresu zostanie zmieniony na SNADS.

Zadania pokrewne

“Sprawdzanie kronik komponentów” na stronie 51
W celu określenia sposobu rozwiązania problemu z pocztą elektroniczną, należy sprawdzić kroniki, w których zapisywane są problemy.

Protokół SMTP (Simple Mail Transfer Protocol)

Protokół SMTP (Simple Mail Transfer Protocol) jest protokołem TCP/IP używanym przy wysyłaniu i odbieraniu poczty elektronicznej. Jest on zazwyczaj używany razem z protokołem POP3 lub protokołem IMAP (Internet Message Access Protocol) w celu zapisania wiadomości w skrzynce pocztowej serwera i okresowym pobieraniu ich z serwera przez użytkownika.

Komendy SMTP

Poniższa tabela przedstawia komendy SMTP, funkcje komend oraz informacje, czy serwer SMTP systemu i5/OS obsługuje te komendy.

Komenda SMTP	Do czego służy	Czy obsługiwane przez System i
AUTH (Uwierzytelnianie)	Wskazanie mechanizmu uwierzytelnienia dla serwera SMTP. Obsługiwane zarówno PLAIN, jak i LOGIN.	Tak
DATA (Dane)	Traktuje wiersze występujące po komendzie jako pocztę elektroniczną od nadawcy.	Tak
EHLO (Rozszerzenie Witaj)	Aktywuje rozszerzenia SMTP.	Tak
EXPN (Rozwiń)	Prosi odbiorcę o potwierdzenie identyfikacji listy pocztowej.	Nie
HELO (Witaj)	Identyfikuje nadawcę SMTP odbiorcy SMTP.	Tak
HELP (Pomoc)	Prosi odbiorcę o przesłanie pomocnych informacji do nadawcy.	Tak
MAIL (Poczta)	Uruchamia transakcję przesłania poczty elektronicznej do jednego lub wielu odbiorców.	Tak
NOOP (Noop)	Prosi odbiorcę o przesłanie twierdzącej odpowiedzi (ale nie określa innego działania).	Tak
QUIT (Wyjdź)	Prosi odbiorcę o wysłanie odpowiedzi twierdzącej, a następnie zamknięcie kanału transmisji.	Tak
RCPT (Adresat)	Identyfikuje indywidualnego odbiorcę poczty elektronicznej.	Tak
RSET (Resetuj)	Kończy bieżącą transakcję poczty elektronicznej.	Tak
SAML (Wyślij i roześlij)	Dostarcza pocztę elektroniczną do jednej lub większej ilości stacji roboczych i odbiorców, jeśli użytkownik nie jest aktywny.	Nie
SEND (Wyślij)	Dostarcza pocztę elektroniczną do jednej lub większej ilości stacji roboczych.	Nie
SOML (Wyślij lub roześlij)	Dostarcza pocztę elektroniczną do jednej lub większej ilości stacji roboczych lub odbiorców, jeśli użytkownik nie jest aktywny.	Nie
STARTTLS (Start Transport Layer Security - Uruchom Zabezpieczenia Warstwy Transportowej)	Prosi serwer SMTP o uruchomienie uzgadniania SSL (Secure Sockets Layer) lub TLS z klientem SMTP w celu ustanowienia sesji SSL lub TLS.	Tak
TURN (Zwrot)	Prosi odbiorcę o wysłanie odpowiedzi twierdzącej, a następnie prosi, aby został on nadawcą SMTP, lub prosi go o wysłanie odpowiedzi odmownej i pełnienie funkcji odbiorcy SMTP.	Nie
VRFY (Zweryfikuj)	Prosi odbiorcę o potwierdzenie identyfikacji użytkownika.	Tak

Pojęcia pokrewne

“Scenariusz: wysyłanie i odbieranie poczty elektronicznej lokalnie” na stronie 4
Scenariusz ten demonstruje sposób, w jaki poczta elektroniczna jest przetwarzana pomiędzy użytkownikami lokalnymi.

Protokół POP (Post Office Protocol)

Interfejs poczty elektronicznej Post Office Protocol (POP) Version 3 zdefiniowany jest w Request for Comments (RFC) 1939 (POP3), RFC 2449 (POP3 Extension Mechanism), i RFC 2595 (Using TLS with IMAP, POP3, and ACAP). RFC jest mechanizmem służącym do definiowania ciągle rozwijających się standardów w sieci Internet.

Oprogramowanie klienta korzysta z komend nazywanych *rozkazami* w komunikacji z serwerem POP. Serwer POP systemu i5/OS obsługuje następujące rozkazy.

Rozkaz i parametry	Opis
USER <id>	Przekazanie identyfikatora użytkownika
PASS <password>	Hasło
STAT	Skrzynka pocztowa zapytań
LIST <opt msg #>	Zapytanie o statystykę wiadomości
RETR <msg #>	Odtworzenie komunikatu
DELE <msg #>	Usunięcie komunikatu
RSET	Zerowanie statusu usunięcia wiadomości
TOP <msg #> <lines>	Pobranie nagłówka wiadomości i jej danych
UIDL <opt msg #>	Listing unikalnych identyfikatorów wiadomości
NOOP	Bez działania
QUIT	Zakończenie sesji klienta
CAPA	Lista możliwości
STLS	Uruchomienie ochrony warstwy transportowej (Start Transport Layer Security)

Pojęcia pokrewne

“Scenariusz: wysyłanie i odbieranie poczty elektronicznej lokalnie” na stronie 4
Scenariusz ten demonstruje sposób, w jaki poczta elektroniczna jest przetwarzana pomiędzy użytkownikami lokalnymi.

“Serwer POP w systemie i5/OS” na stronie 4
Serwer POP jest implementacją interfejsu pocztowego POP3 w systemie i5/OS.

Rozwiązywanie problemów dotyczących poczty elektronicznej

Poniższe informacje są pomocne w rozwiązywaniu problemów dotyczących poczty elektronicznej, z którymi użytkownik może mieć do czynienia.

Zadania pokrewne

“Zapobieganie dzieleniu dużych wiadomości e-mail” na stronie 38
Może wystąpić potrzeba uniemożliwienia podziału dużych wiadomości oraz dostarczania ich w małych, niewygodnych plikach.

Wykrywanie problemów z pocztą elektroniczną

Wykonanie prostych czynności może być pomocne w określeniu przyczyny problemu z pocztą elektroniczną.

Aby zidentyfikować prawdopodobne źródła problemów z protokołem SMTP (Simple Mail Transfer Protocol), wykonaj następujące czynności:

1. Sprawdź, czy protokół TCP/IP został skonfigurowany dla potrzeb poczty elektronicznej.
   a. Sprawdź, czy zainstalowane zostały wymagane poprawki tymczasowe do programów (PTF).
   b. Sprawdź serwery poczty. Wszystkie niezbędne serwery muszą zostać uruchomione.
2. Sprawdź nazwę domeny lokalnej.
   a. W programie System i Navigator rozwiń węzły ***twój system*** → **Sieć**.
   b. Prawym przyciskiem myszy kliknij pozycję **Konfiguracja TCP/IP** i wybierz opcję **Właściwości**.
   c. Kliknij zakładkę **Informacje o domenie hosta** i sprawdź nazwę domeny lokalnej.
3. Zmniejsz wartość Ponowienia SMTP.
   a. Uruchom program System i Navigator i rozwiń pozycję ***system*** → **Sieć** → **Serwery** → **TCP/IP** (*system* > Network > Servers > TCP/IP).
   b. Kliknij dwukrotnie **SMTP**.
   c. Kliknij zakładkę **Ponowienia poczty wychodzącej**.
4. Sprawdź, czy ID użytkownika i adres odbiorcy znajdują się w katalogu dystrybucyjnym systemu.
   a. Uruchom program System i Navigator i rozwiń pozycję ***system*** → **Użytkownicy i grupy** → **Wszyscy użytkownicy** (*system* > Users and Groups > All Users).
   b. Prawym przyciskiem myszy kliknij pozycję **Profil** danego identyfikatora użytkownika i wybierz **Właściwości**..
   c. Kliknij **Dane osobowe** i przejdź do zakładki **Poczta**, aby sprawdzić adres.
5. Sprawdź, czy pozycja tabeli hostów jest niezbędna, aby poczta osiągnęła adres docelowy.
   a. W wierszu komend wpisz CHGTCPHTE (Change TCP/IP Host Table Entry - Zmiana pozycji w tabeli hostów TCP/IP) i podaj adres internetowy serwera poczty.
   b. Jeśli tabela hostów nie pojawi się, podaj nazwę hosta dla tego adresu internetowego.
6. Sprawdź, czy nie przekroczyłeś progu pamięci.
   a. Uruchom program System i Navigator i rozwiń pozycję ***system*** → **Konfiguracja i usługi** → **Sprzęt** → **Jednostki dyskowe** → **Pule dyskowe** (*system* > Configuration and Service > Hardware > Disk Units > Disk Pools).
   b. Kliknij prawym przyciskiem myszy wybraną pulę dyskową i wybierz **Właściwości**.
   c. Kliknij zakładkę **Pojemność**.

      Jeśli wykorzystanie systemu przekracza określony próg, poczta może przestać działać.
7. Upewnij się, czy wyłączone jest dzielenie wiadomości.
   a. Uruchom program System i Navigator i rozwiń pozycję ***system*** → **Sieć** → **Serwery** → **TCP/IP** (*system* > Network > Servers > TCP/IP).
   b. Kliknij dwukrotnie **POP**. Pojawi się okno dialogowe Właściwości POP.
   c. Kliknij zakładkę **Konfiguracja**.
   d. W polu **Wielkość podziału wiadomości** powinna być wybrana wartość **Bez maksimum**.
8. Uruchom komendę Śledzenie aplikacji TCP/IP (Trace TCP/IP Applications). W wierszu komend wpisz komendę TRCTCPAPP.
9. Aby zlokalizować problem, sprawdź kroniki komponentów.

Pojęcia pokrewne

“Kontrolowanie dostępu do poczty elektronicznej” na stronie 10
Aby ochronić dane przed groźnymi atakami, należy kontrolować, kto uzyskuje dostęp do systemu za pośrednictwem poczty elektronicznej.

przykłady niezależnej puli dyskowej

“Kontrola dostępu do serwera POP” na stronie 11
Aby zapewnić bezpieczeństwo systemu, należy kontrolować dostęp do serwera POP.

“Rozwiązywanie problemów związanych z funkcją API QtmmSendMail” na stronie 52
Poniższe czynności mogą pomóc w rozwiązaniu problemów związanych z funkcją API Wysyłanie poczty MIME (Send MIME Mail - QtmmSendMail).

Zadania pokrewne

“Sprawdzanie serwerów poczty elektronicznej” na stronie 37
Jednym z powszechnych problemów z pocztą jest to, że odpowiednie serwery nie zostały uruchomione. Przed przystąpieniem do używania serwerów poczty elektronicznej należy sprawdzić status serwerów i sprawdzić, czy wszystkie są uruchomione.

“Konfigurowanie protokołu TCP/IP na potrzeby poczty elektronicznej” na stronie 15
Przed skonfigurowaniem w systemie poczty elektronicznej należy skonfigurować protokół TCP/IP.

“Sprawdzanie zadań struktury serwera poczty” na stronie 53
Należy sprawdzać zadania struktury serwera poczty w systemie QSYSWRK w celu określenia potencjalnych przyczyn błędu w funkcji API QtmmSendMail.

“Sprawdzanie kronik komponentów”
W celu określenia sposobu rozwiązania problemu z pocztą elektroniczną, należy sprawdzić kroniki, w których zapisywane są problemy.

“Śledzenie niedoręczonej poczty elektronicznej” na stronie 52
Do śledzenia problemów z dostarczaniem poczty można używać ogólnego ID użytkownika. Metoda ta może być użyteczna zarówno w przypadku problemów z dostarczaniem poczty elektronicznej, jak i z jej konfigurowaniem.

Informacje pokrewne

praca z systemem IBM System i

Sprawdzanie kronik komponentów

W celu określenia sposobu rozwiązania problemu z pocztą elektroniczną, należy sprawdzić kroniki, w których zapisywane są problemy.

System operacyjny wykorzystuje różne kolejki, programy i dokumenty kronikowania, aby umożliwić określenie przyczyn nie dostarczania poczty elektronicznej przez serwer poczty elektronicznej. Kronikowanie może być pomocne, ponieważ ułatwia znalezienie możliwych przyczyn niepowodzeń w systemie poczty elektronicznej. Kronikowanie korzysta z cykli jednostki przetwarzania, a zatem wydajność systemu jest wyższa przy wyłączonym kronikowaniu.

Funkcje kronikowania dokumentują następujące elementy:

- Przejścia- z programów do kolejek, z kolejek do programów.
- Zdarzenia- przejście poczty przez serwer, dostarczenie poczty przez klienta, zachowanie poczty w kolejce do kolejnej próby dostarczenia lub w kolejce oczekującej na zwolnienie zasobów.
- Droga i niektóre dane pomiarowe- identyfikator komunikatu 822, identyfikator komunikatu MSF, wielkość wiadomości, nadawca, odbiorca.

Rekordy kronik są zapisywane w dziennikach. Dziennikami zarządza użytkownik. Gdy dziennik się zapełni, należy uruchomić komendę Zmiana kroniki (Change Journal - CHGJRN), aby ustalić nowy dziennik. Nowa funkcja kronikowania SMTP korzysta z dziennika QZMF.

Aby włączyć kronikowanie i obejrzeć zawartość kronik:

1. Uruchom program System i Navigator i rozwiń pozycję ***system*** **→ Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Kliknij dwukrotnie **SMTP**.
3. Kliknij zakładkę **Ogólne**.
4. Zaznacz pole wyboru **Uaktywnij pozycje kroniki**.
5. Otwórz sesję emulacji.
6. Aby przekształcić pozycje kroniki w czytelną postać, wpisz w wierszu komend: DSPJRN JRN(QZMF) OUTPUT(*OUTFILE) OUTFILE(*biblioteka/zbiór_fizyczny*) OUTMBR(*MAR2*) ENTDTALEN(512), gdzie *biblioteka* jest nazwą biblioteki, a *zbiór_fizyczny* jest nazwą zbioru fizycznego.
7. Aby wyświetlić pozycje kroniki SMTP, wpisz w wierszu komend: DSPPFM FILE(*biblioteka/zbiór_fizyczny*) MBR(*MAR2*).

8. Naciśnij F20 (Shift + F8), aby zobaczyć informacje z kroniki.

Pojęcia pokrewne

“Wykrywanie problemów z pocztą elektroniczną” na stronie 49
Wykonanie prostych czynności może być pomocne w określeniu przyczyny problemu z pocztą elektroniczną.

Odsyłacze pokrewne

“Pozycje kroniki serwera poczty” na stronie 42
Poniższe informacje ułatwiają zrozumienie kodów i komunikatów używanych w pozycjach kroniki.

Śledzenie niedoręczonej poczty elektronicznej

Do śledzenia problemów z dostarczaniem poczty można używać ogólnego ID użytkownika. Metoda ta może być użyteczna zarówno w przypadku problemów z dostarczaniem poczty elektronicznej, jak i z jej konfigurowaniem.

1. Aby otrzymywać powiadomienia, wybierz lub utwórz ID użytkownika. W wierszu komend wpisz komendę CRTUSRPRF (Create User Profile - Utworzenie profilu użytkownika) i naciśnij klawisz Enter.
2. Wpisz komendę WRKDIRE (Work with Directory Entries - Praca z zapisami katalogu) i naciśnij klawisz Enter.
3. Wpisz 1, aby dodać użytkownika do katalogu dystrybucyjnego systemu.
4. Upewnij się, że pole Zapisywanie wiadomości (Mail Store) ma wartość 2, a pole Preferowany adres ma wartość 3.
5. Naciśnij klawisz F19 (Dodaj adres SMTP - Add Name for SMTP).
6. Wpisz NONDELIVERY@lokalny_host.domena jako adres SMTP dla dowolnego użytkownika POP.

Użytkownik ten będzie otrzymywał kopie niedoręczonej poczty.

Uwaga: Podany ID użytkownika, żeby efektywnie monitorować przypadki niedoręczenia, musi być rzeczywistym jego identyfikatorem. Nadawca otrzymuje kopię noty o niedoręczeniu wraz z listą odbiorców, którzy nie otrzymali poczty.

Pojęcia pokrewne

“Wykrywanie problemów z pocztą elektroniczną” na stronie 49
Wykonanie prostych czynności może być pomocne w określeniu przyczyny problemu z pocztą elektroniczną.

Rozwiązywanie problemów związanych z funkcją API QtmmSendMail

Poniższe czynności mogą pomóc w rozwiązaniu problemów związanych z funkcją API Wysyłanie poczty MIME (Send MIME Mail - QtmmSendMail).

| Użytkownik może mieć do czynienia z błędami zwróconymi przez funkcję API QtmmSendMail. Opisy komunikatów o
| błędzie zwracanych przez funkcję API znajdują się w rozdziale dotyczącym funkcji API QtmmSendMail.

Pojęcia pokrewne

“Wykrywanie problemów z pocztą elektroniczną” na stronie 49
Wykonanie prostych czynności może być pomocne w określeniu przyczyny problemu z pocztą elektroniczną.

Odsyłacze pokrewne

wysyłanie poczty w standardzie MIME (Send MIME Mail - QtmmSendMail), funkcja API

Sprawdzanie wywołania funkcji API

Aby wykonać odzyskiwanie po wystąpieniu błędu w aplikacyjnym interfejsie programistycznym QtmmSendMail, należy sprawdzić, czy na stacji roboczej wyświetlane są komunikaty o błędach z funkcji API.

Jeśli zaprogramowane zostanie zwrócenie błędu, będzie on przesłany do programu. Jeśli jednak wartość ta zostanie ustawiona na zero, jak pokazano na przykładzie poniżej, błąd zostanie wyświetlony na ekranie stacji roboczej.

Przykład w języku C

```
Qus_EC_t         Snd_Error_Code;
Snd_Error_Code.Bytes_Provided=0;
```

Przykład w języku RPG

```
DAPIError     DS
D APIBytes          1     4B 0
D CPFId             9    15
C              Eval    APIBytes   = 0
```

Sprawdzanie pliku MIME (Multipurpose Internet Mail Extension)

Mogą wystąpić problemy z plikiem MIME, który powoduje zwracanie błędu przez funkcję API QtmmSendMail. Należy sprawdzić, czy w pliku MIME powyższe problemy nie występują.

1. Sprawdź położenie pliku MIME. Plik MIME musi znajdować się w systemie ROOT i zaczynać się od ″/″, na przykład /mój_plik.txt, a nazwa pliku musi zawierać ścieżkę /mój_katalog/mój_plik.mime.
2. Sprawdź poziomy uprawnień. Profile QMSF i QTCP muszą posiadać uprawnienia do odczytu i usuwania pliku MIME.
   a. W interfejsie znakowym wpisz komendę WRKLNK (Work with Object Links - Praca z dowiązaniami obiektów).
   b. Wpisz 9 (Ekran), aby pracować z uprawnieniami QMST i QTCP. Pojawi się ekran Praca z dowiązaniami obiektów (Work with Object Links).
3. Sprawdź, czy plik MIME zawiera instrukcję zakończenia nagłówka (CRLFCRLF) pomiędzy nagłówkiem i treścią.
4. Sprawdź, czy plik MIME jest zgodny ze standardem MIME Request for Comments (RFC).

Uwaga: Więcej informacji na temat instrukcji zakończenia nagłówka zawiera sekcja 2.1 w RFC2822 (http://rfc.net/rfc2822.html).

Sprawdzanie zadań struktury serwera poczty

Należy sprawdzać zadania struktury serwera poczty w systemie QSYSWRK w celu określenia potencjalnych przyczyn błędu w funkcji API QtmmSendMail.

1. Jeśli to struktura serwera poczty zatrzymała przetwarzanie wiadomości, sprawdź zadania struktury MSF pod kątem komunikatów o błędach.
2. Po zakończeniu zadania struktury, plik MIME powinien zostać usunięty. Oznacza to, że struktura przetworzyła plik MIME. A zatem problem nie tkwi w funkcji API, lecz w konfiguracji SMTP.

Pojęcia pokrewne

“Wykrywanie problemów z pocztą elektroniczną” na stronie 49
Wykonanie prostych czynności może być pomocne w określeniu przyczyny problemu z pocztą elektroniczną.

Informacje pokrewne dotyczące poczty elektronicznej

Informacje, które wiążą się z kolekcją tematów dotyczących poczty elektronicznej, można znaleźć w podręcznikach produktów, dokumentacji technicznej IBM (Redbooks), serwisach WWW i w innych kolekcjach tematów centrum informacyjnego. Wszystkie pliki PDF można wyświetlić lub wydrukować.

Podręczniki

AnyMail/400 Mail Server Framework Support  (około 622 KB)

Przeczytaj na temat struktury środowiska serwera poczty elektronicznej systemu i5/OS.

IBM Redbooks (Dokumentacja techniczna)

- AS/400 Electronic-Mail Capabilities  (około 3593 KB)

  Szczegółowe informacje na temat poczty elektronicznej i protokołu SMTP dostępne są w dokumentacji technicznej IBM Redbooks.

- AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet  (około 2160 KB)

Dokumentacja techniczna Redbooks zawiera informacje o bezpieczeństwie, w tym o czynnościach związanych z procedurami czyszczącymi systemu operacyjnego i5/OS w przypadku dotknięcia systemu atakiem blokującym.

Serwisy WWW

- Praca z systemem IBM System i

  Pobierz aktualne dokumenty PDF do systemu operacyjnego i5/OS, wykorzystując swoją stację roboczą jako bramę do strony WWW z poprawkami PTF, lub zapoznaj się z rozwiązaniami dla systemu i5/OS w kategorii informacji technicznych i informacji na temat baz danych.

- Indeks RFC

  Protokoły poczty elektronicznej zdefiniowane są w dokumentach RFC (Request for Comments). Dokumenty RFC służą do definiowania ciągle rozwijających się standardów w sieci Internet. Więcej informacji na temat protokołu SMTP znajduje się w dokumentach RFC 1939 (POP3), RFC 2449 (POP3 Extension Mechanism) oraz RFC 2595 (Using TLS with IMAP, POP3 and ACAP).

- Lotus Domino for i5/OS

  Strona zawiera informacje na temat Lotus Domino for i5/OS oraz rozwiązań zawartych w programie licencjonowanym.

- Lotus Domino Biblioteka odniesień

  Więcej informacji na temat produktu Domino znajduje się w raportach, książkach, prezentacjach itp.

- Lotus Dokumentacja techniczna

  Strony WWW z dokumentacją techniczną systemu Lotus zawierają odsyłacze do zasobów, takich jak dokumentacja techniczna produktu, raporty, dokumentacja techniczna Redbooks i inne.

Inne informacje

System i - bezpieczeństwo w Internecie.

Aby zapoznać się z informacjami na temat bezpieczeństwa sieci w systemie System i, przeczytaj tę kolekcję tematów centrum informacyjnego.

Odsyłacze pokrewne

“Plik PDF z informacjami na temat poczty elektronicznej” na stronie 2
Informacje zawarte w tym temacie są także dostępne w postaci pliku PDF, który można wyświetlić i wydrukować.

Dodatek. Uwagi

Niniejsza publikacja została przygotowana z myślą o produktach i usługach oferowanych w Stanach Zjednoczonych.

IBM może nie oferować w innych krajach produktów, usług lub opcji, omawianych w tej publikacji. Informacje o produktach i usługach dostępnych w danym kraju można uzyskać od lokalnego przedstawiciela IBM. Odwołanie do produktu, programu lub usługi IBM nie oznacza, że można użyć wyłącznie tego produktu, programu lub usługi. Zamiast nich można zastosować ich odpowiednik funkcjonalny pod warunkiem, że nie narusza to praw własności intelektualnej IBM. Jednakże cała odpowiedzialność za ocenę przydatności i sprawdzenie działania produktu, programu lub usługi pochodzących od producenta innego niż IBM spoczywa na użytkowniku.

IBM może posiadać patenty lub złożone wnioski patentowe na towary i usługi, o których mowa w niniejszej publikacji. Przedstawienie niniejszej publikacji nie daje żadnych uprawnień licencyjnych do tychże patentów. Pisemne zapytania w sprawie licencji można przesyłać na adres:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
USA

Zapytania w sprawie licencji na informacje dotyczące zestawów znaków dwubajtowych (DBCS) należy kierować do lokalnych działów własności intelektualnej IBM (IBM Intellectual Property Department) lub zgłaszać na piśmie pod adresem:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokio 106-0032, Japonia

Poniższy akapit nie obowiązuje w Wielkiej Brytanii, a także w innych krajach, w których jego treść pozostaje w sprzeczności z przepisami prawa miejscowego: INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W STANIE, W JAKIM SIĘ ZNAJDUJE “AS IS” BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŹNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ GWARANCJI, ŻE PUBLIKACJA NIE NARUSZA PRAW STRON TRZECICH. Ustawodawstwa niektórych krajów nie dopuszczają zastrzeżeń dotyczących gwarancji wyraźnych lub domniemanych w odniesieniu do pewnych transakcji; w takiej sytuacji powyższe zdanie nie ma zastosowania.

Informacje zawarte w niniejszej publikacji mogą zawierać nieścisłości techniczne lub błędy drukarskie. Informacje te są okresowo aktualizowane, a zmiany te zostaną uwzględnione w kolejnych wydaniach tej publikacji. IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

Wszelkie wzmianki w tej publikacji na temat stron internetowych innych firm zostały wprowadzone wyłącznie dla wygody użytkowników i w żadnym wypadku nie stanowią zachęty do ich odwiedzania. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych dla tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

IBM ma prawo do korzystania i rozpowszechniania informacji przysłanych przez użytkownika w dowolny sposób, jaki uzna za właściwy, bez żadnych zobowiązań wobec ich autora.

Licencjobiorcy tego programu, którzy chcieliby uzyskać informacje na temat programu w celu: (i) wdrożenia wymiany informacji między niezależnie utworzonymi programami i innymi programami (łącznie z tym opisywanym) oraz (ii) wspólnego wykorzystywania wymienianych informacji, powinni skontaktować się z:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
USA

Informacje takie mogą być udostępnione, o ile spełnione zostaną odpowiednie warunki, w tym, w niektórych przypadkach, uiszczenie odpowiedniej opłaty.

Licencjonowany program opisany w niniejszym dokumencie oraz wszystkie inne licencjonowane materiały dostępne dla tego programu są dostarczane przez IBM na warunkach określonych w Umowie IBM z Klientem, Międzynarodowej Umowie Licencyjnej IBM na Program, Umowie Licencyjnej IBM na Kod Maszynowy lub w innych podobnych umowach zawartych między IBM i użytkownikami.

Wszelkie dane dotyczące wydajności zostały zebrane w kontrolowanym środowisku. W związku z tym rezultaty uzyskane w innych środowiskach operacyjnych mogą się znacząco różnić. Niektóre pomiary mogły być dokonywane na systemach będących w fazie rozwoju i nie ma gwarancji, że pomiary te wykonane na ogólnie dostępnych systemach dadzą takie same wyniki. Niektóre z pomiarów mogły być estymowane przez ekstrapolację. Rzeczywiste wyniki mogą być inne. Użytkownicy powinni we własnym zakresie sprawdzić odpowiednie dane dla ich środowiska.

Informacje dotyczące produktów firm innych niż IBM pochodzą od dostawców tych produktów, z opublikowanych przez nich zapowiedzi lub innych powszechnie dostępnych źródeł. Firma IBM nie testowała tych produktów i nie może potwierdzić dokładności pomiarów wydajności, kompatybilności ani żadnych innych danych związanych z tymi produktami. Pytania dotyczące możliwości produktów firm innych niż IBM należy kierować do dostawców tych produktów.

Wszelkie stwierdzenia dotyczące przyszłych kierunków rozwoju i zamierzeń IBM mogą zostać zmienione lub wycofane bez powiadomienia.

Publikacja ta zawiera przykładowe dane i raporty używane w codziennych operacjach działalności gospodarczej. W celu kompleksowego ich zilustrowania, podane przykłady zawierają nazwiska osób prywatnych, nazwy przedsiębiorstw oraz nazwy produktów. Wszystkie te nazwy/nazwiska są fikcyjne i jakiekolwiek podobieństwo do istniejących nazw/nazwisk i adresów jest całkowicie przypadkowe.

LICENCJA W ZAKRESIE PRAW AUTORSKICH:

Niniejsza publikacja zawiera przykładowe aplikacje w kodzie źródłowym, ilustrujące techniki programowania w różnych systemach operacyjnych. Użytkownik może kopiować, modyfikować i dystrybuować te programy przykładowe w dowolnej formie bez uiszczania opłat na rzecz IBM, w celu projektowania, używania, sprzedaży lub dystrybucji aplikacji zgodnych z aplikacyjnym interfejsem programowym dla tego systemu operacyjnego, dla którego napisane zostały programy przykładowe. Programy przykładowe nie zostały gruntownie przetestowane. IBM nie może zatem gwarantować ani sugerować niezawodności, użyteczności i funkcjonalności tych programów.

Każda kopia programu przykładowego lub jakikolwiek jego fragment, jak też jakiekolwiek prace pochodne muszą zawierać następujące uwagi dotyczące praw autorskich:

© (nazwa przedsiębiorstwa użytkownika, rok). Fragmenty tego kodu pochodzą z programów przykładowych IBM Corp. © Copyright IBM Corp. (wpisać rok lub lata). Wszelkie prawa zastrzeżone.

W przypadku przeglądania niniejszych informacji w formie elektronicznej, zdjęcia i kolorowe ilustracje mogą nie być wyświetlane.

Informacje o interfejsie programistycznym

Niniejsza publikacja dotycząca poczty elektronicznej opisuje planowane interfejsy programistyczne, pozwalające na pisanie programów umożliwiających korzystanie z usług systemu operacyjnego IBM i5/OS.

Znaki towarowe

Następujące nazwy są znakami towarowymi International Business Machines Corporation w Stanach Zjednoczonych i/lub w innych krajach:

AIX
AS/400
Domino
eServer
i5/OS
IBM
IBM (logo)
Infoprint
iSeries
Lotus
Lotus Notes
Redbooks
System i
The Output of e-business
Tivoli

Adobe, logo Adobe logo, PostScript oraz logo PostScript są znakami towarowymi lub zastrzeżonymi znakami towarowymi Adobe Systems Incorporated w Stanach Zjednoczonych i/lub w innych krajach.

Linux jest zastrzeżonym znakiem towarowym Linusa Torvaldsa w Stanach Zjednoczonych i/lub w innych krajach.

Microsoft, Windows, Windows NT oraz logo Windows są znakami towarowymi Microsoft Corporation w Stanach Zjednoczonych i/lub w innych krajach.

Java oraz wszystkie znaki towarowe dotyczące języka Java są znakami towarowymi Sun Microsystems, Inc. w Stanach Zjednoczonych i/lub w innych krajach.

Nazwy innych przedsiębiorstw, produktów lub usług mogą być znakami towarowymi lub znakami usług innych podmiotów.

Warunki

Zezwolenie na korzystanie z tych publikacji jest przyznawane na poniższych warunkach.

Użytek osobisty: Użytkownik ma prawo kopiować te publikacje do własnego, niekomercyjnego użytku pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa dystrybuować ani wyświetlać tych publikacji czy ich części, ani też wykonywać na ich podstawie prac pochodnych bez wyraźnej zgody IBM.

Użytek służbowy: Użytkownik ma prawo kopiować te publikacje, dystrybuować je i wyświetlać wyłącznie w ramach przedsiębiorstwa Użytkownika pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa wykonywać na podstawie tych publikacji ani ich fragmentów prac pochodnych, kopiować ich, dystrybuować ani wyświetlać poza przedsiębiorstwem Użytkownika bez wyraźnej zgody IBM.

Z wyjątkiem zezwoleń wyraźnie udzielonych w niniejszym dokumencie, nie udziela się jakichkolwiek innych zezwoleń, licencji ani praw, wyraźnych czy domniemanych, odnoszących się do tych publikacji czy jakichkolwiek informacji, danych, oprogramowania lub innej własności intelektualnej, o których mowa w niniejszym dokumencie.

IBM zastrzega sobie prawo do anulowania zezwolenia przyznanego w niniejszym dokumencie w każdej sytuacji, gdy, według uznania IBM, korzystanie z tych publikacji jest szkodliwe dla IBM lub jeśli IBM uzna, że warunki niniejszego dokumentu nie są przestrzegane.

Użytkownik ma prawo pobierać, eksportować lub reeksportować niniejsze informacje pod warunkiem zachowania bezwzględnej i pełnej zgodności z obowiązującym prawem i przepisami, w tym ze wszelkimi prawami i przepisami eksportowymi Stanów Zjednoczonych.

IBM NIE UDZIELA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, DOTYCZĄCYCH TREŚCI TYCH PUBLIKACJI. PUBLIKACJE TE SĄ DOSTARCZANE W STANIE, W JAKIM SIĘ ZNAJDUJĄ (″AS IS″) BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, WYRAŹNYCH CZY DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ NIENARUSZANIA PRAW STRON TRZECICH.

Drukowane w USA